CompTIA Security+ Study Guide with over 500 Practice Test Questions

Exam SY0-701 (9th Edition)

By Mike Chapple and David Seidl

Contents

Domain Table

Domain	% of Exam
1.0 General Security Concepts	12%
2.0 Threats, Vulnerabilities, and Mitigations	22%
3.0 Security Architecture	18%
4.0 Security Operations	28%
5.0 Security Program Management and Oversight	20%

SY0-701 Certification Exam Objective Map

Objective	Chapter(s)
1.0 General Security Concepts	
1.1 Compare and contrast various types of security controls	1
1.2 Summarize fundamental security concepts	1, 8, 9, 12
1.3 Explain the importance of change management processes and the impact to security	16
1.4 Explain the importance of using appropriate cryptographic solutions	1, 7, 11
2.0 Threats, Vulnerabilities, and Mitigations	
2.1 Compare and contrast common threat actors and motivations	2
2.2 Explain common threat vectors and attack surfaces	2, 4
2.3 Explain various types of vulnerabilities	2, 6, 7, 10, 11, 13
2.4 Given a scenario, analyze indicators of malicious activity	3, 4, 6, 9, 12, 13, 14
2.5 Explain the purpose of mitigation techniques used to secure the enterprise	8, 11, 12, 14, 16
3.0 Security Architecture	
3.1 Compare and contrast security implications of different architecture models	9, 10, 11, 12
3.2 Given a scenario, apply security principles to secure enterprise infrastructure	12
3.3 Compare and contrast concepts and strategies to protect data	1, 10, 13, 17
3.4 Explain the importance of resilience and recovery in security architecture	9, 17
4.0 Security Operations	
4.1 Given a scenario, apply common security techniques to computing resources	6, 10, 11, 12, 13
4.2 Explain the security implications of proper hardware, software, and data asset management	11
4.3 Explain various activities associated with vulnerability management	2, 5, 6

Objective	Chapter(s)
4.4 Explain security alerting and monitoring concepts and tools	5, 11, 12, 14
4.5 Given a scenario, modify enterprise capabilities to enhance security	11, 12
4.6 Given a scenario, implement and maintain identity and access management	8
4.7 Explain the importance of automation and orchestration related to secure operations	6
4.8 Explain appropriate incident response activities	14, 15
4.9 Given a scenario, use data sources to support an investigation	14
5.0 Security Program Management and Oversight	
5.1 Summarize elements of effective security governance	16, 17
5.2 Explain elements of the risk management process	17
5.3 Explain the processes associated with third-party risk assessment and management	16
5.4 Summarize elements of effective security compliance	16
5.5 Explain types and purposes of audits and assessments	5
5.6 Given a scenario, implement security awareness practices	16

Assessment Test: Data Table (Question 18)

Order Number	Amount	Date	Credit Card Number
1023	$25,684	10/7/2023	c4ca4238a0b923820dcc509a6f75849b
1024	$65,561	12/6/2023	c81e728d9d4c2f636f067f89cc14862c
1025	$44,015	11/7/2023	eccbc87e4b5ce2fe28308fd9f2a7baf3
1026	$89,553	7/6/2023	a87ff679a2f3e71d9181a67b7542122c
1027	$50,316	10/16/2023	e4da3b7fbbce2345d7772b0674a318d5
1028	$39,200	5/3/2023	b53b3a3d6ab90ce0268229151c9bde11
1029	$67,897	3/1/2023	6364d3f0f495b6ab9dcf8d3b5c6e0b01
1030	$98,141	1/21/2023	5821bb96cd2066d808a7b64b5b58b394
1031	$13,851	10/29/2023	89d948e603f12c523728803d61347951
1032	$60,475	3/13/2023	b02ac13e3fadb4ecf1874b34087eb096
1033	$67,207	9/15/2023	1ed3c76c640836c99be028b261311643
1034	$2,525	10/9/2023	e53a0a2978c28872a4505bdb51db06dc
1035	$66,399	3/5/2023	4903e02b3b0ae4b6b824a0a4c187e5c5
1036	$37,676	11/4/2023	8fd7e6c0a7120aa9778b5fb08a1fa8ee

FIGURE 1.1 The three key objectives of cybersecurity programs are confidentiality, integrity, and availability.

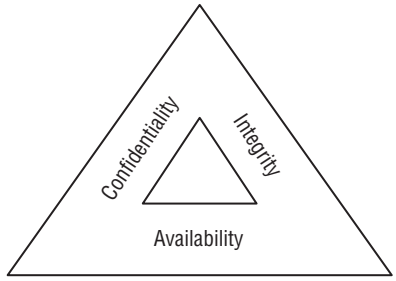
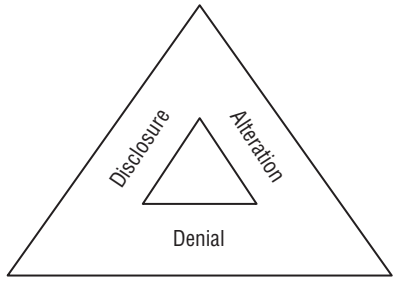


FIGURE 1.2 The three key threats to cybersecurity programs are disclosure, alteration, and denial.



Chapter 1 Review: Table (Question 4)

Order Number	Amount	Date	Credit Card Number
1023	$46,438	11/3/2020	*** *** *** 1858
1024	$83,007	9/22/2020	*** *** *** 8925
1025	$42,289	7/19/2020	*** *** *** 8184
1026	$10,119	8/4/2020	*** *** *** 5660
1027	$24,223	7/16/2020	*** *** *** 8823
1028	$57,657	7/8/2020	*** *** *** 3691
1029	$94,558	2/10/2020	*** *** *** 8371
1030	$33,570	5/17/2020	*** *** *** 8661
1031	$96,829	3/20/2020	*** *** *** 3711
1032	$32,487	12/17/2020	*** *** *** 4868
1033	$29,055	6/14/2020	*** *** *** 1698
1034	$14,932	5/4/2020	*** *** *** 8844
1035	$20,734	1/19/2020	*** *** *** 9030
1036	$90,210	6/2/2020	*** *** *** 1946
1037	$36,104	6/11/2020	*** *** *** 1595
1038	$81,171	3/13/2020	*** *** *** 9520
1039	$57,738	4/4/2020	*** *** *** 1612
1040	$60,712	5/25/2020	*** *** *** 8166
1041	$37,572	1/22/2020	*** *** *** 6566
1042	$21,496	12/17/2020	*** *** *** 4009

Chapter 1 Review: Sign (Question 13)

Source: Gabriel Cassan / Adobe Stock

FIGURE 2.1 Logo of the hacktivist group Anonymous

FIGURE 2.2 Dark web market

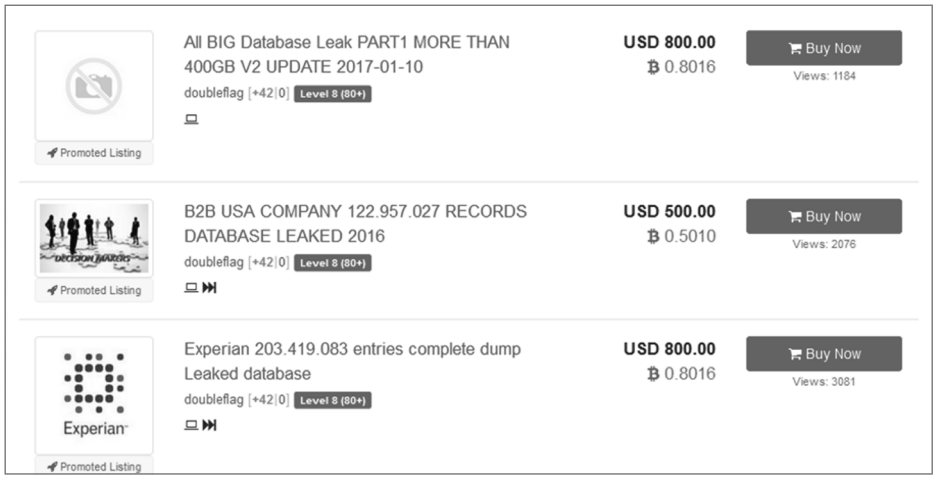


FIGURE 2.3 Alert listing from the CISA website

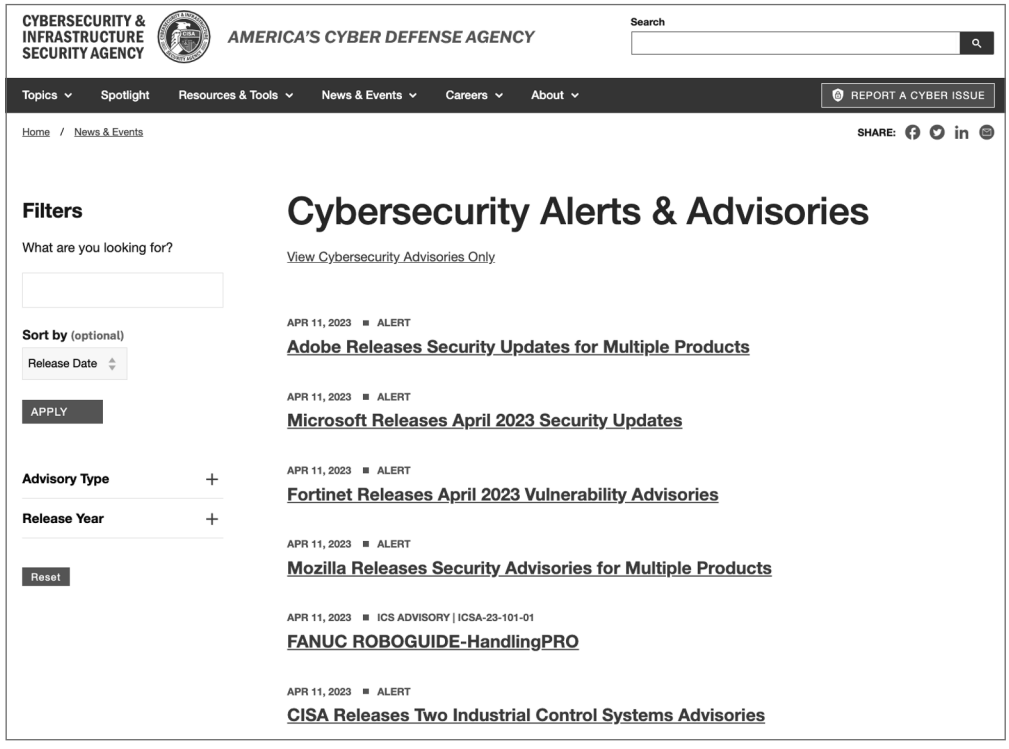
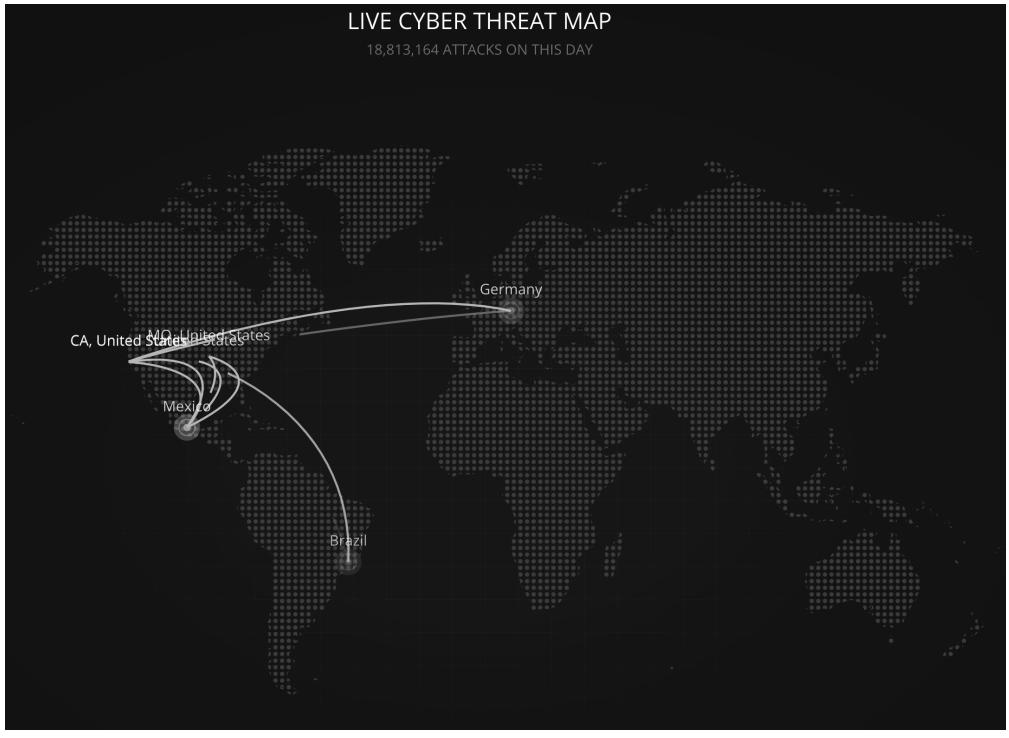


FIGURE 2.4 Check Point CyberThreat Map



STIX JSON Description of a Threat Actor

```
{
 "type": "threat-actor",
 "created": "2019-10-20T19:17:05.000Z",
 "modified": "2019-10-21T12:22:20.000Z",
 "labels": [ "crime-syndicate"],
 "name": "Evil Maid, Inc",
 "description": "Threat actors with access to hotel rooms",
 "aliases": ["Local USB threats"],
 "goals": ["Gain physical access to devices", "Acquire data"],
 "sophistication": "intermediate",
 "resource_level": "government",
 "primary_motivation": "organizational-gain"
}
```

Chapter 2 Review: URLs (Question 20)

```
www.myschool.edu/grades.php&studentID=1023423
www.myschool.edu/grades.php&studentID=1023424
www.myschool.edu/grades.php&studentID=1023426
www.myschool.edu/grades.php&studentID=1023427
```

FIGURE 3.1 Trojan application download and infection process

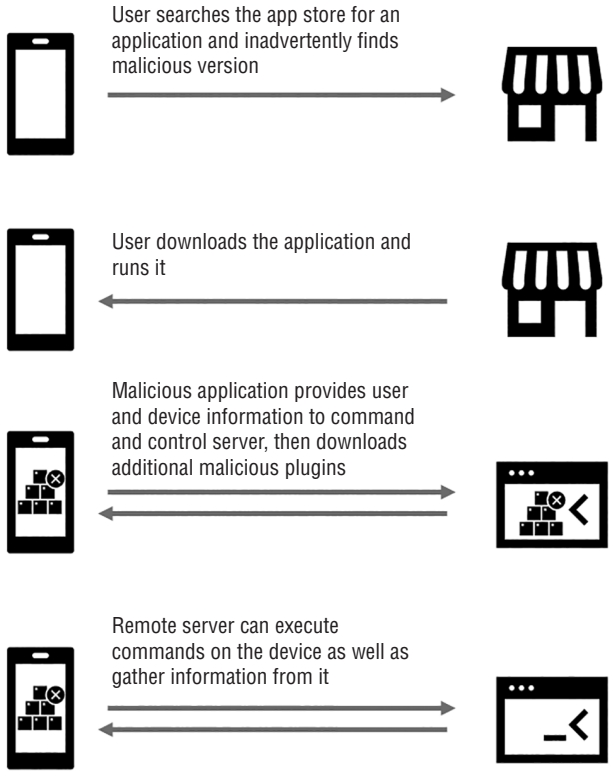


FIGURE 3.2 Fileless virus attack chain

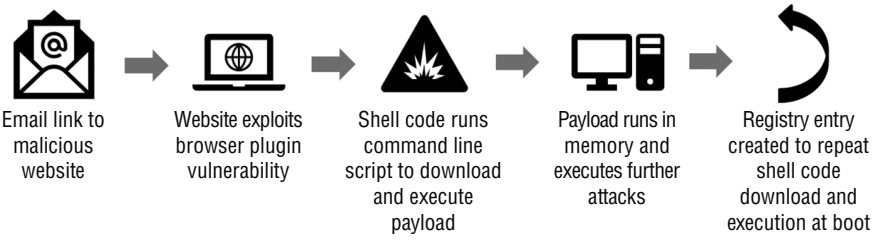


FIGURE 4.1 Brand impersonation email

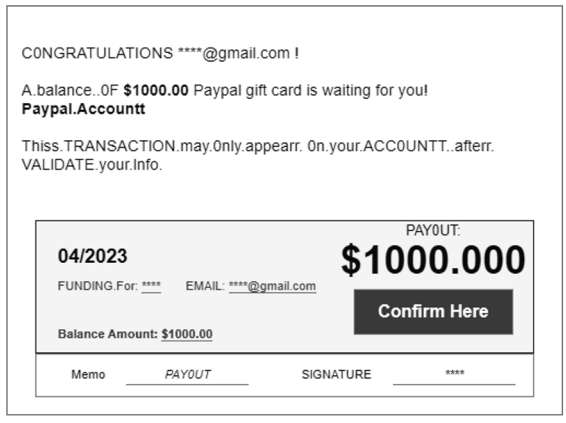


FIGURE 4.2 John the Ripper

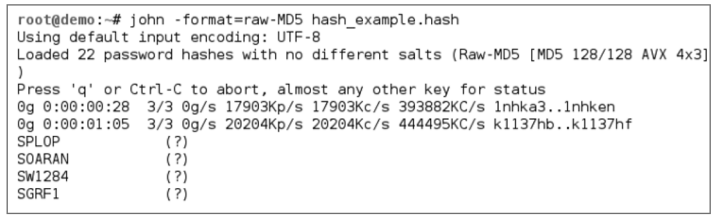


FIGURE 5.1 Qualys asset map

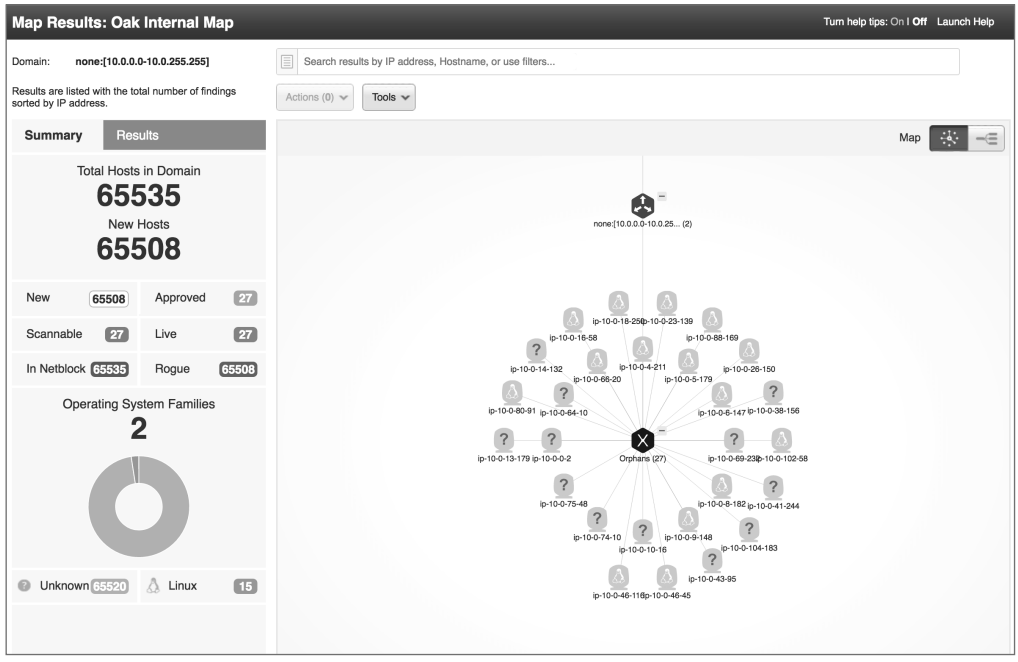


FIGURE 5.2 Configuring a Nessus scan

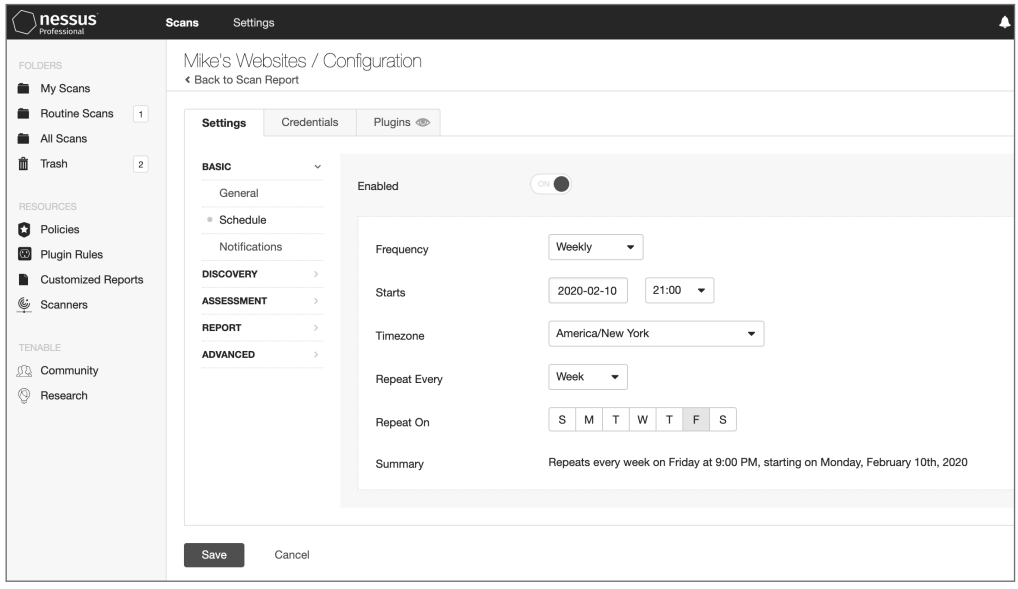
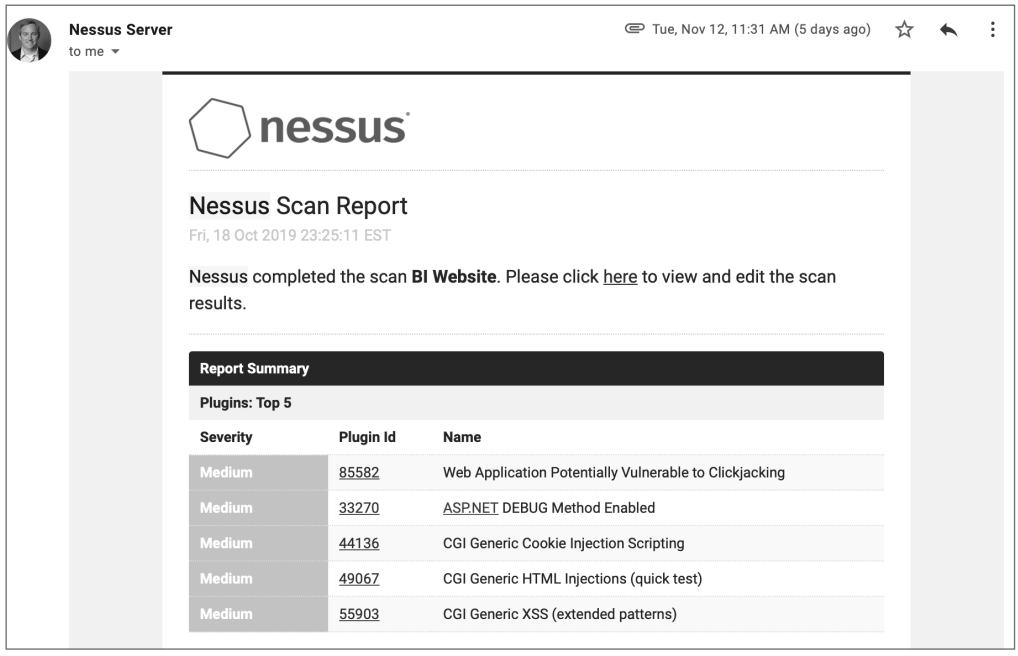


FIGURE 5.3 Sample Nessus scan report



Nessus Server
to me

Tue, Nov 12, 11:31 AM (5 days ago)

nessus

Nessus Scan Report

Fri, 18 Oct 2019 23:25:11 EST

Nessus completed the scan **BI Website**. Please click here to view and edit the scan results.

Report Summary

Plugins: Top 5

Severity	Plugin Id	Name
Medium	85582	Web Application Potentially Vulnerable to Clickjacking
Medium	33270	ASP.NET DEBUG Method Enabled
Medium	44136	CGI Generic Cookie Injection Scripting
Medium	49067	CGI Generic HTML Injections (quick test)
Medium	55903	CGI Generic XSS (extended patterns)

FIGURE 5.4 Nessus scan templates

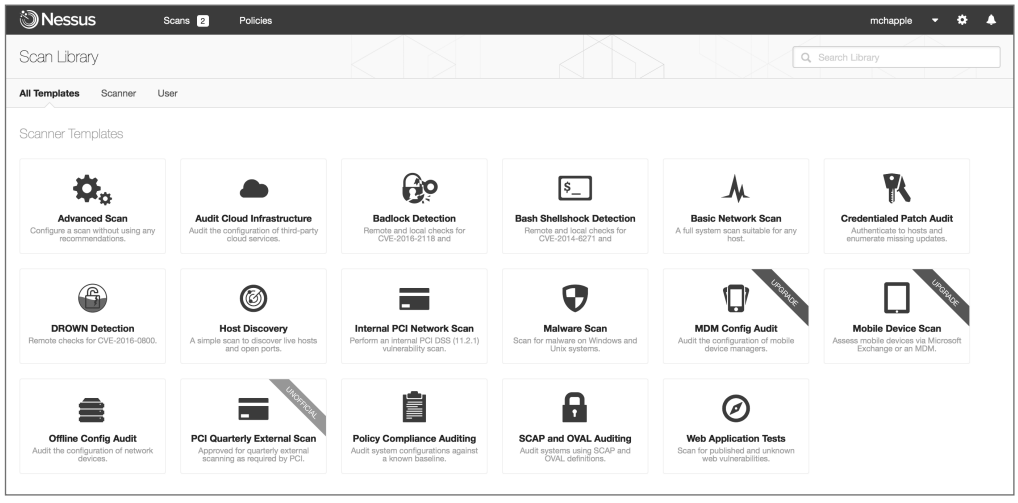


FIGURE 5.5 Disabling unused plug-ins

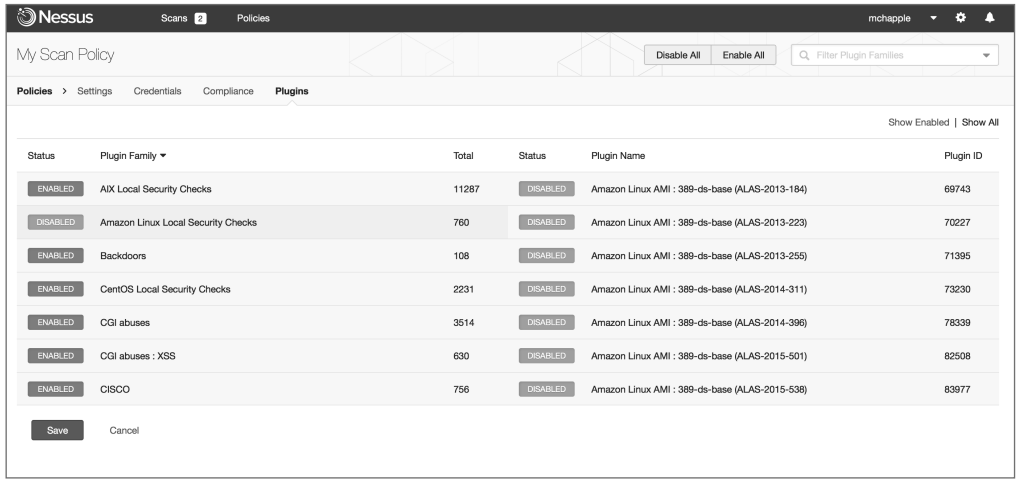


FIGURE 5.6 Configuring credentialed scanning

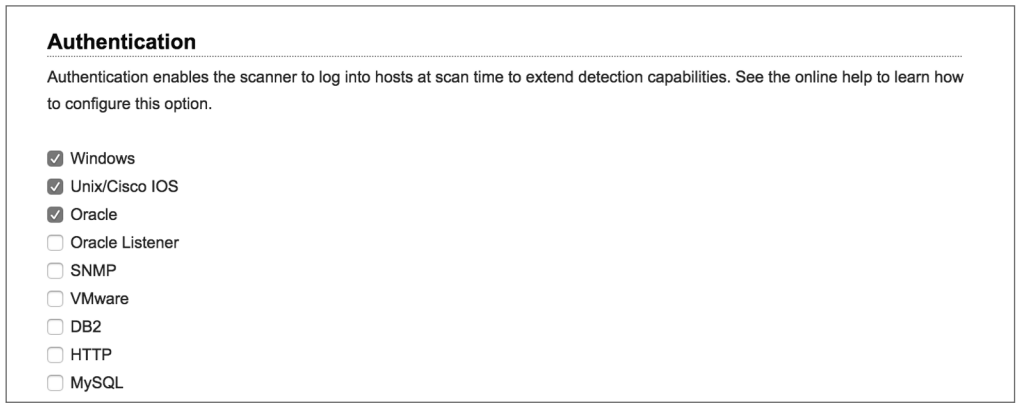


FIGURE 5.7 Choosing a scan appliance

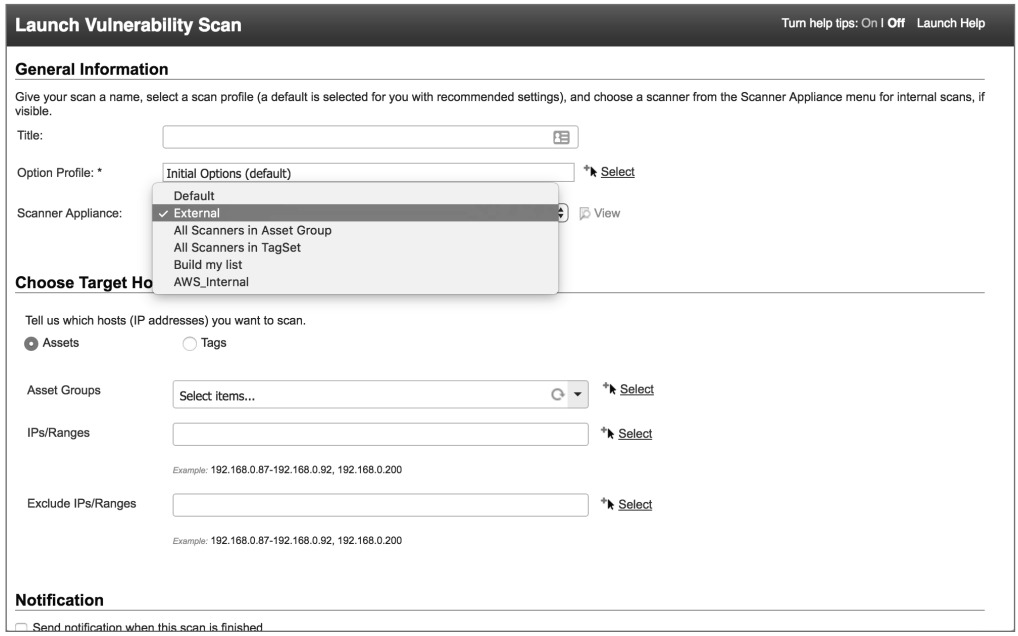
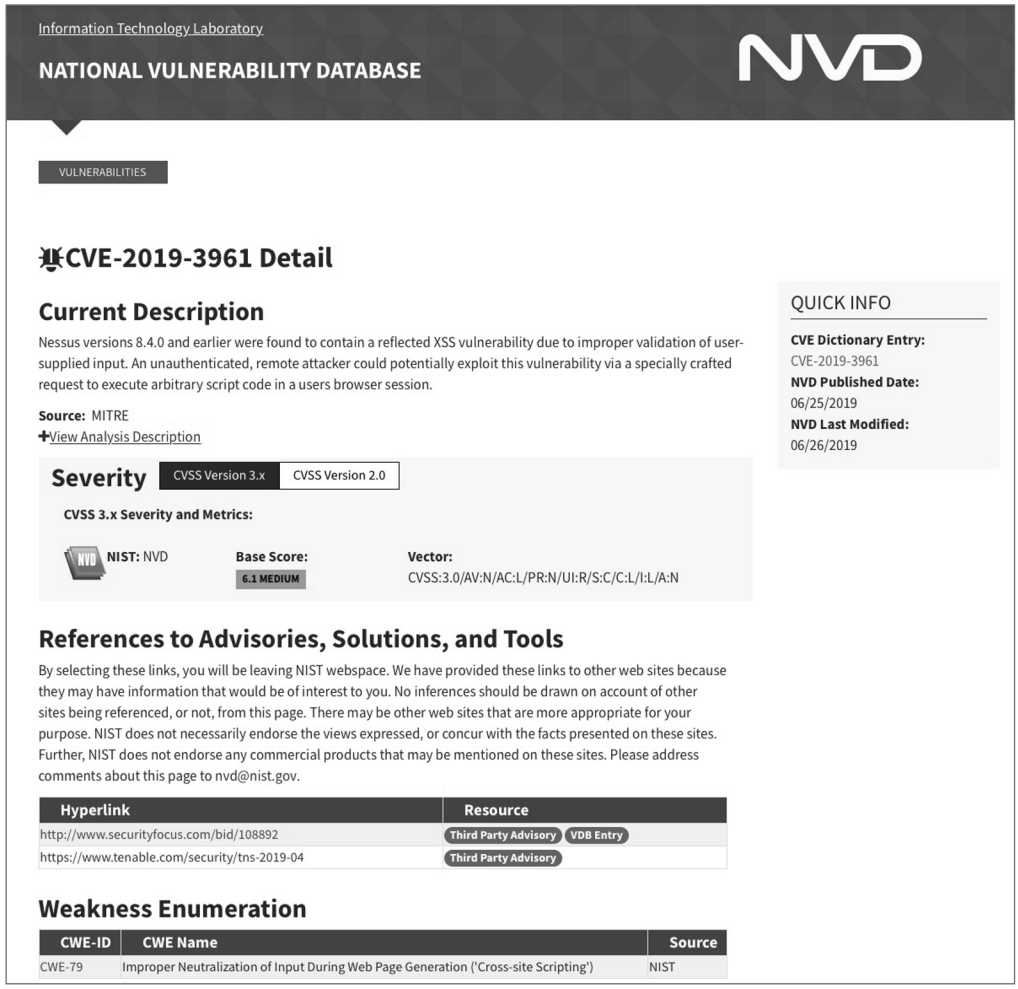


FIGURE 5.8 Nessus vulnerability in the NIST National Vulnerability Database



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2019-3961 Detail

Current Description

Nessus versions 8.4.0 and earlier were found to contain a reflected XSS vulnerability due to improper validation of user-supplied input. An unauthenticated, remote attacker could potentially exploit this vulnerability via a specially crafted request to execute arbitrary script code in a users browser session.

Source: MITRE

+View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2019-3961
NVD Published Date:
06/25/2019
NVD Last Modified:
06/26/2019

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 6.1 MEDIUM

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://www.securityfocus.com/bid/108892	Third Party Advisory, VDB Entry
https://www.tenable.com/security/tns-2019-04	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	NIST

Source: National Institute of Standards and Technology

FIGURE 5.9 Nessus Automatic Updates

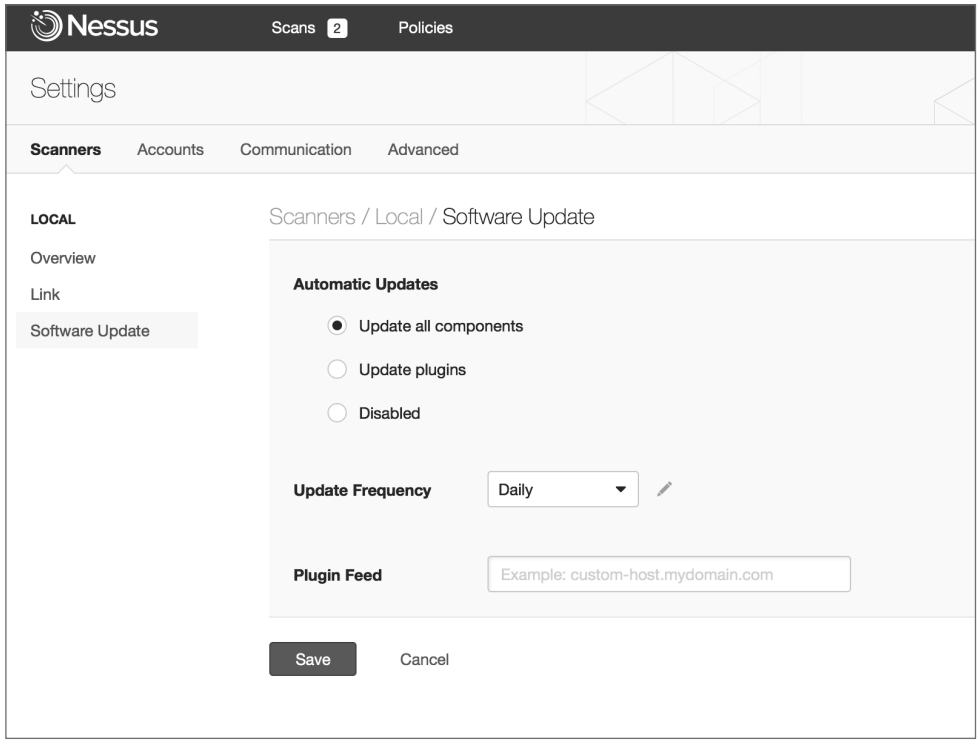


FIGURE 5.10 Nikto web application scanner

```
 Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.ContainerServlet/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerab
le to Cross Site Scripting (XSS) by invoking java classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.Context/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cro
ss Site Scripting (XSS) by invoking java classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.Globals/<script>alert('Vulnerable')</script>: Apache-Tomcat is vulnerable to Cro
ss Site Scripting (XSS) by invoking java classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /servlet/org.apache.catalina.servlets.WebdavStatus/<script>alert('Vulnerable')</script>: Apache-Tomcat is vul
nerable to Cross Site Scripting (XSS) by invoking java classes. http://www.cert.org/advisories/CA-2000-02.html.
+ /nosuchurl/><script>alert('Vulnerable')</script>: JEUS is vulnerable to Cross Site Scripting (XSS) when reque
sting non-existing JSP pages. http://securitytracker.com/alerts/2003/Jun/1007004.html
+ /~/<script>alert('Vulnerable')</script>.aspx?aspxerrorpath=null: Cross site scripting (XSS) is allowed with .
aspx file requests (may be Microsoft .net). http://www.cert.org/advisories/CA-2000-02.html
+ /~/<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is allowed with .aspx file requests
(may be Microsoft .net). http://www.cert.org/advisories/CA-2000-02.html
+ /~/<script>alert('Vulnerable')</script>.asp: Cross site scripting (XSS) is allowed with .asp file requests (m
ay be Microsoft .net). http://www.cert.org/advisories/CA-2000-02.html
+ /node/view/666\"><script>alert(document.domain)</script>: Drupal 4.2.0 RC is vulnerable to Cross Site Scripti
ng (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /mailman/listinfo/<script>alert('Vulnerable')</script>: Mailman is vulnerable to Cross Site Scripting (XSS).
Upgrade to version 2.0.8 to fix. http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-27095: /bb000001.pl<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to C
ross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-54589: /a.jsp/<script>alert('Vulnerable')</script>: JServ is vulnerable to Cross Site Scripting (XSS) w
hen a non-existent JSP file is requested. Upgrade to the latest version of JServ. http://www.cert.org/advisorie
s/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.thtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.c
ert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.shtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.c
ert.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.jsp: Server is vulnerable to Cross Site Scripting (XSS). http://www.cer
t.org/advisories/CA-2000-02.html.
+ /<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is allowed with .aspx file requests (m
ay be Microsoft .net). http://www.cert.org/advisories/CA-2000-02.html.
```

FIGURE 5.11 Arachni web application scanner

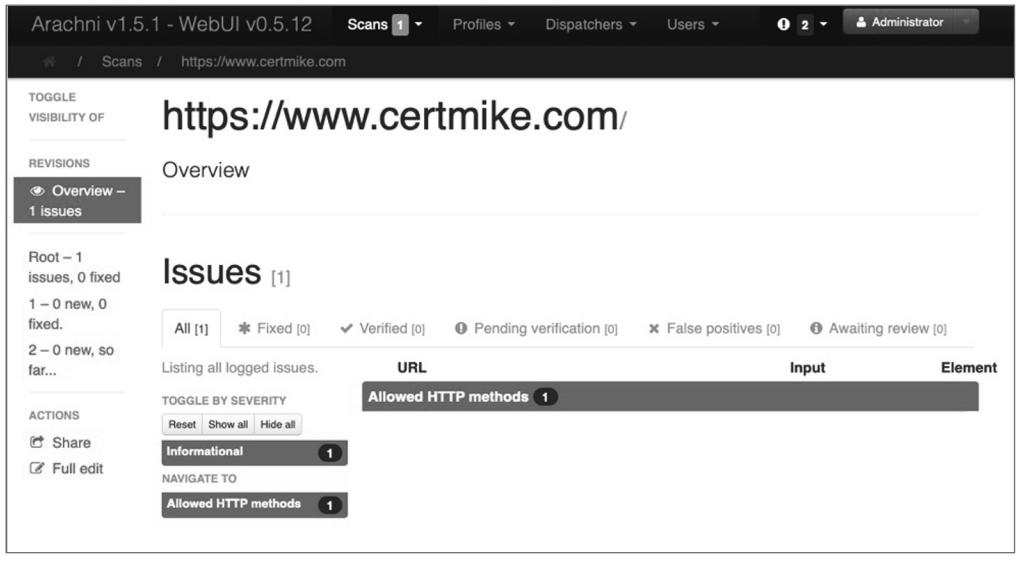
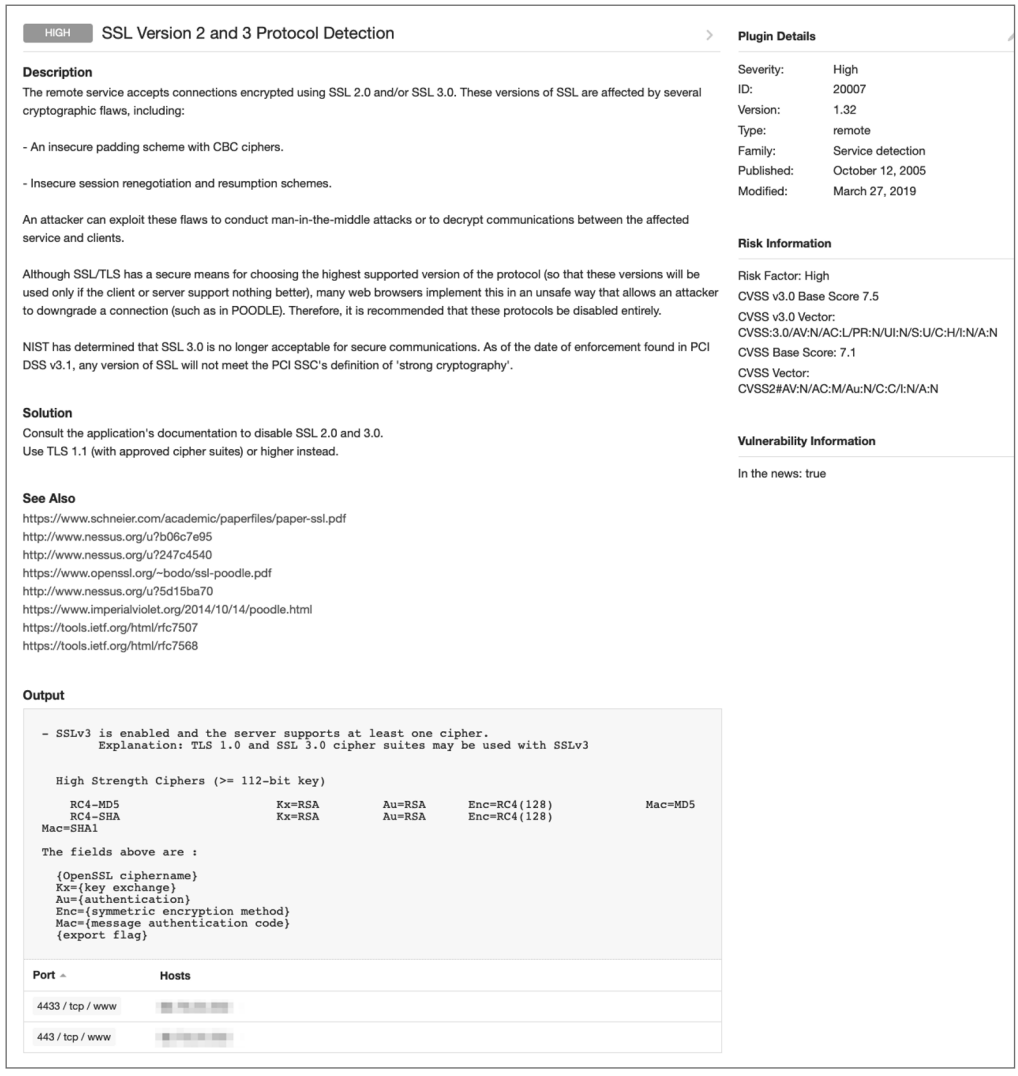


FIGURE 5.12 Nessus vulnerability scan report



HIGH SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Output

```
- SSLv3 is enabled and the server supports at least one cipher.
        Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)
Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Port	Hosts
4433 / tcp / www	[redacted]
443 / tcp / www	[redacted]

Plugin Details

Severity:	High
ID:	20007
Version:	1.32
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	March 27, 2019

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS Base Score: 7.1
CVSS Vector:
CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N

Vulnerability Information

In the news: true

TABLE 5.1 CVSS attack vector metric

Value	Description	Score
Physical (P)	The attacker must physically touch the vulnerable device.	0.20
Local (L)	The attacker must have physical or logical access to the affected system.	0.55
Adjacent (A)	The attacker must have access to the local network that the affected system is connected to.	0.62
Network (N)	The attacker can exploit the vulnerability remotely over a network.	0.85

TABLE 5.2 CVSS attack complexity metric

Value	Description	Score
High (H)	Exploiting the vulnerability requires "specialized" conditions that would be difficult to find.	0.44
Low (L)	Exploiting the vulnerability does not require any specialized conditions.	0.77

TABLE 5.3 CVSS privileges required metric

Value	Description	Score
High (H)	Attackers require administrative privileges to conduct the attack.	0.270 (or 0.50 if Scope is Changed)
Low (L)	Attackers require basic user privileges to conduct the attack.	0.62 (or 0.68 if Scope is Changed)
None (N)	Attackers do not need to authenticate to exploit the vulnerability.	0.85

TABLE 5.4 CVSS user interaction metric

Value	Description	Score
None (N)	Successful exploitation does not require action by any user other than the attacker.	0.85
Required (R)	Successful exploitation does require action by a user other than the attacker.	0.62

TABLE 5.5 CVSS confidentiality metric

Value	Description	Score
None (N)	There is no confidentiality impact.	0.00
Low (L)	Access to some information is possible, but the attacker does not have control over what information is compromised.	0.22
High (H)	All information on the system is compromised.	0.56

TABLE 5.6 CVSS integrity metric

Value	Description	Score
None (N)	There is no integrity impact.	0.00
Low (L)	Modification of some information is possible, but the attacker does not have control over what information is modified.	0.22
High (H)	The integrity of the system is totally compromised, and the attacker may change any information at will.	0.56

TABLE 5.7 CVSS availability metric

Value	Description	Score
None (N)	There is no availability impact.	0.00
Low (L)	The performance of the system is degraded.	0.22
High (H)	The system is completely shut down.	0.56

TABLE 5.8 CVSS scope metric

Value	Description
Unchanged (U)	The exploited vulnerability can only affect resources managed by the same security authority.
Changed (C)	The exploited vulnerability can affect resources beyond the scope of the security authority managing the component containing the vulnerability.

TABLE 5.9 CVSS Qualitative Severity Rating Scale

CVSS score	Rating
0.0	None
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

FIGURE 5.13 Missing patch vulnerability

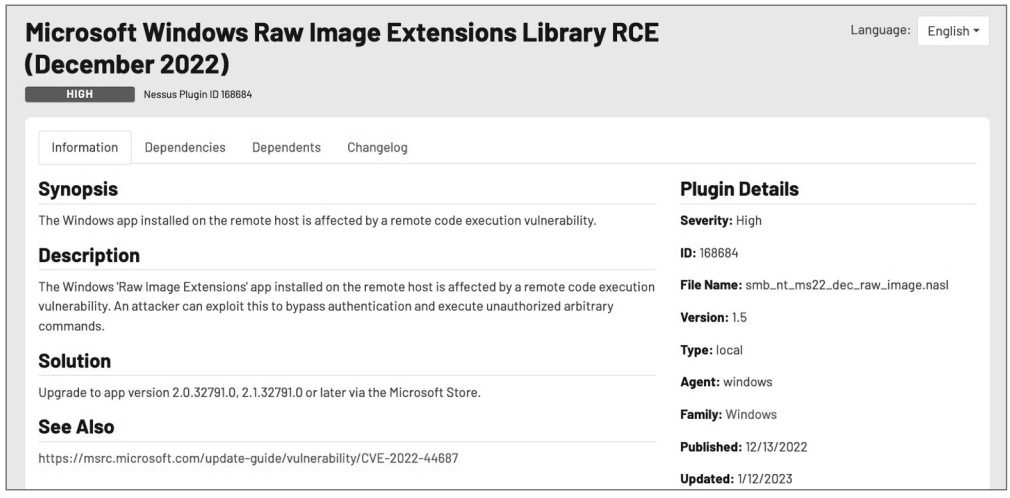


FIGURE 5.14 Unsupported operating system vulnerability

FIGURE 5.15 Debug mode vulnerability

FIGURE 5.16 FTP cleartext authentication vulnerability

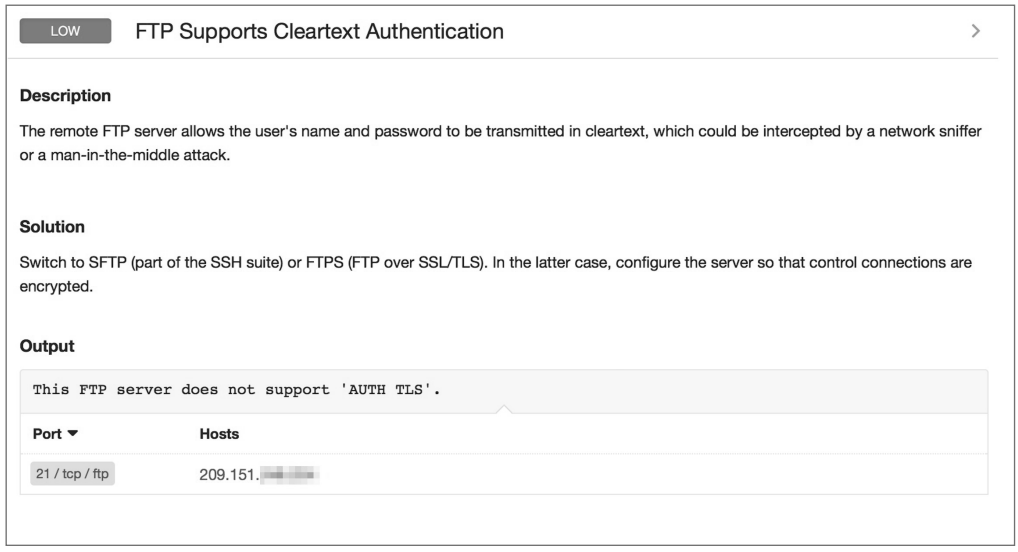
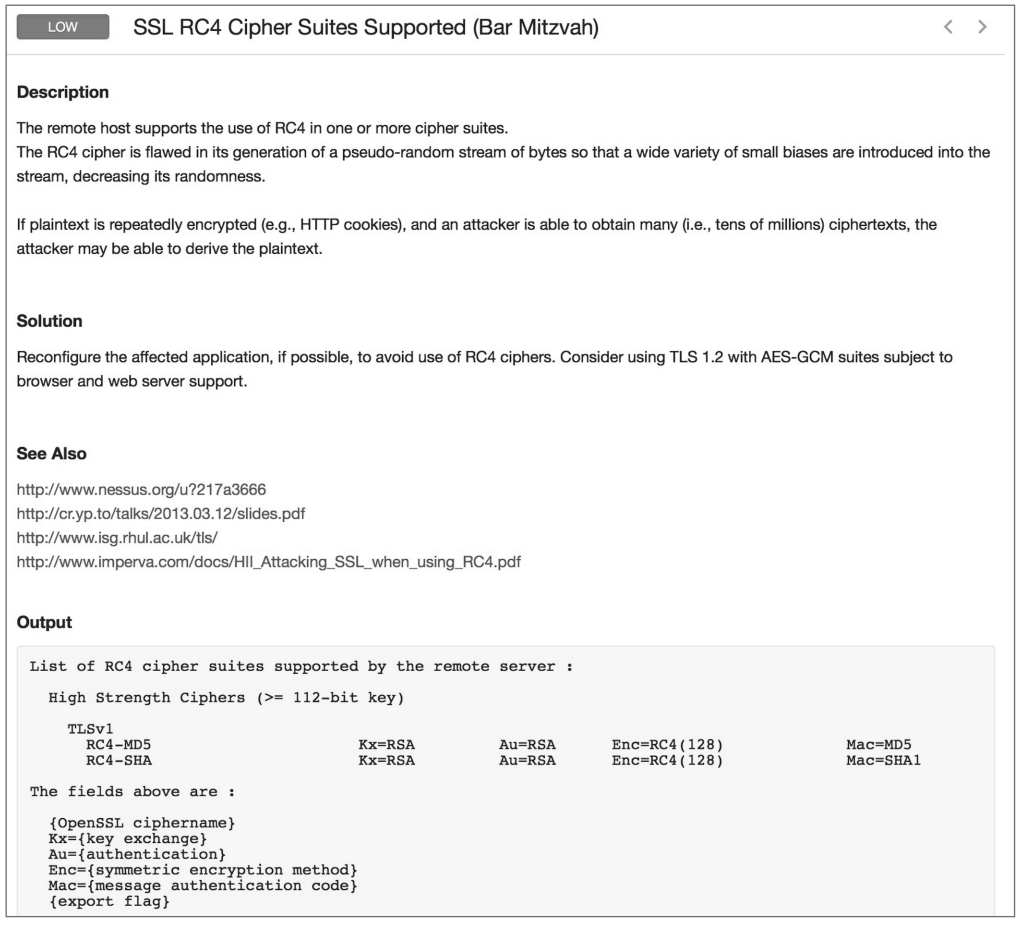


FIGURE 5.17 Insecure SSL cipher vulnerability



LOW SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

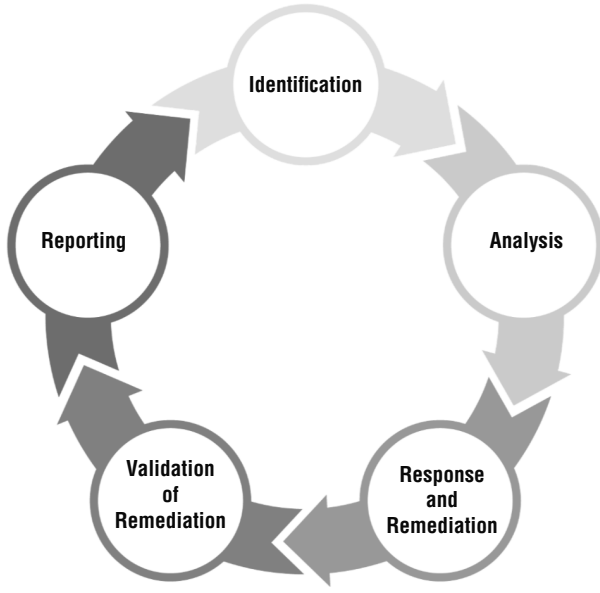
See Also

http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

FIGURE 5.18 Vulnerability life cycle



Chapter 5 Review: Vulnerability Scan Result (Question 8)

THREAT:

Microsoft Server Message Block (SMB) Protocol is a Microsoft network file sharing protocol used in Microsoft Windows.
The Microsoft SMB Server is vulnerable to multiple remote code execution vulnerabilities due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
This security update is rated Critical for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012 and 2012 R2, Windows 8.1 and RT 8.1, Windows 10 and Windows Server 2016.

IMPACT:

A remote attacker could gain the ability to execute code by sending crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

SOLUTION:

Customers are advised to refer to Microsoft Advisory MS17-010 for more details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

FIGURE 6.1 High-level SDLC view

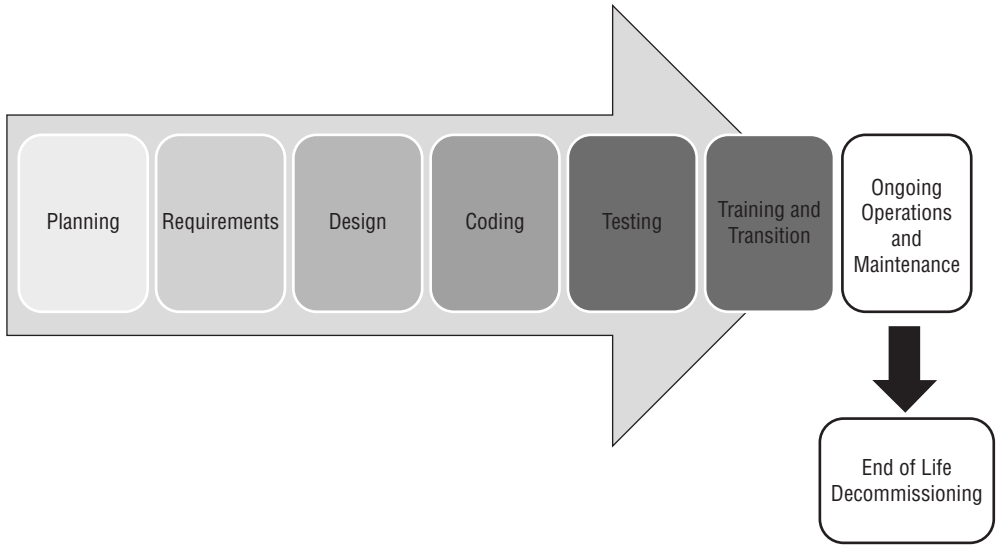
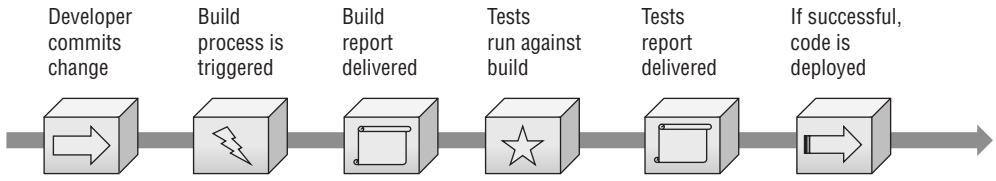


FIGURE 6.2 The CI/CD pipeline



Database Query for 'Orange,' 'Tiger,' and 'Pillow'

```
SELECT ItemName, ItemDescription, ItemPrice
FROM Products
WHERE ItemName LIKE '%orange%' AND
ItemName LIKE '%tiger%' AND
ItemName LIKE '%pillow%'
```

Attacker's Query Sent to Database Server

```
SELECT ItemName, ItemDescription, ItemPrice
FROM Products
WHERE ItemName LIKE '%orange%' AND
ItemName LIKE '%tiger%' AND
ItemName LIKE '%pillow';
SELECT CustomerName, CreditCardNumber
FROM Orders;
--%'
```

FIGURE 6.3 Account number input page

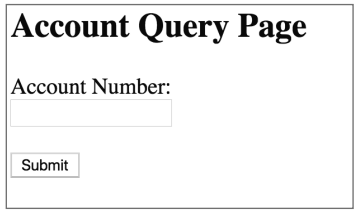
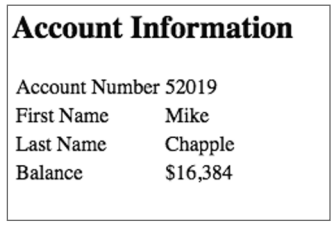


FIGURE 6.4 Account information page



SQL Query Coding

```
SELECT FirstName, LastName, Balance
FROM Accounts
WHERE AccountNumber = '$account'
```

Query to Database with "'52019' OR 1=1" Input Coding

```
SELECT FirstName, LastName, Balance
FROM Accounts
WHERE AccountNumber = '52019' OR 1=1
```

Query to Database with "'52019' AND 1=2" Input Coding

```
SELECT FirstName, LastName, Balance
FROM Accounts
WHERE AccountNumber = '52019' AND 1=2
```

FIGURE 6.5 Account information page after blind SQL injection

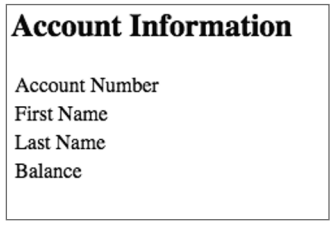


FIGURE 6.6 Account creation page

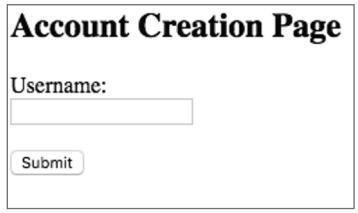
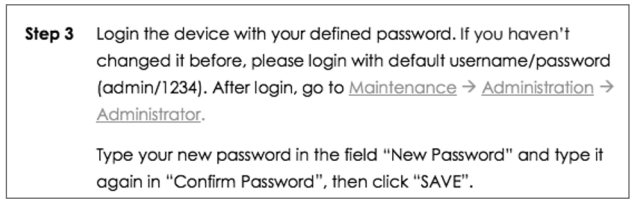


FIGURE 6.7 Zyxel router default password



Source: www.router-reset.com/default-password-ip-list/ZyXEL

FIGURE 6.8 Session authentication with cookies

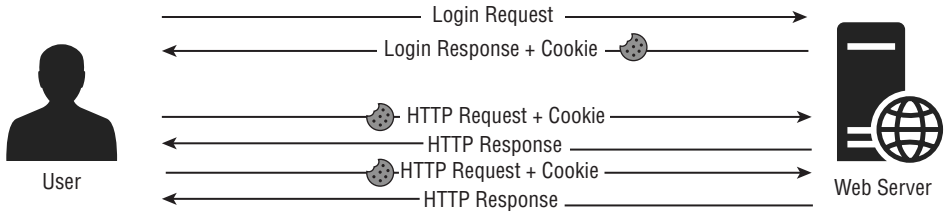


FIGURE 6.9 Session cookie from Cable News Network

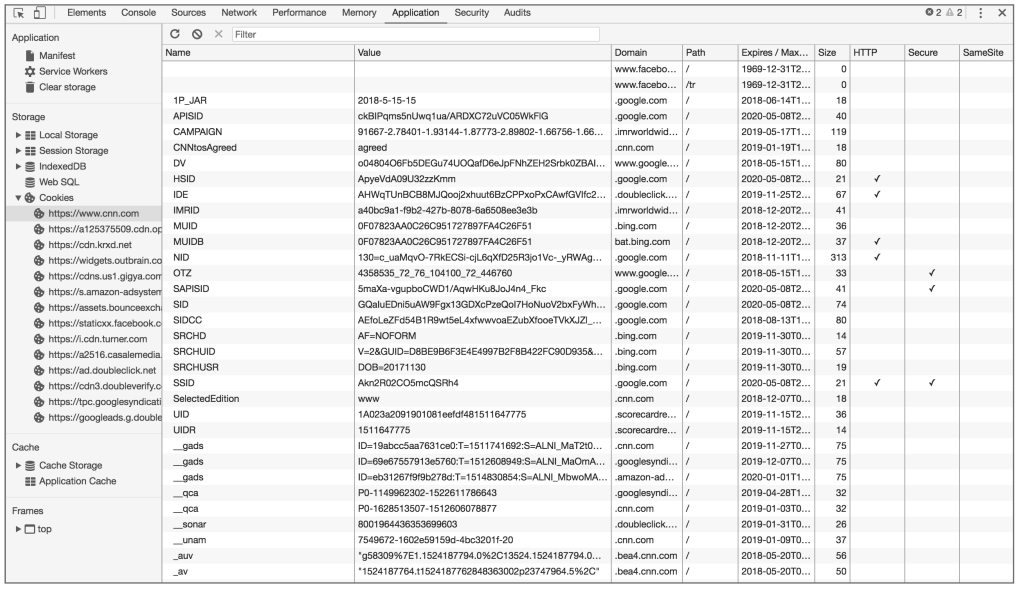
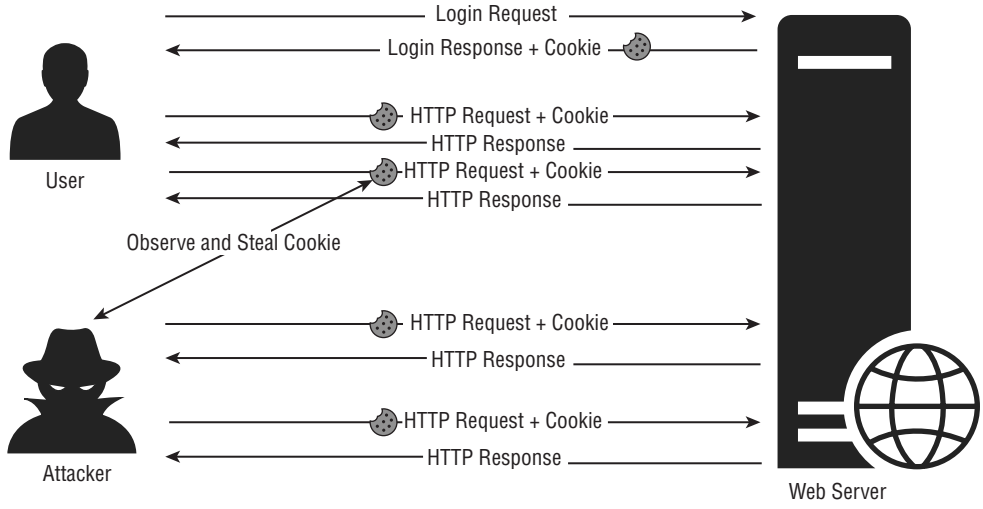


FIGURE 6.10 Session replay



Ordering Page URL

```
www.mycompany.com/ordering.php?redirect=http%3a//www.mycompany.com/
thankyou.htm
```

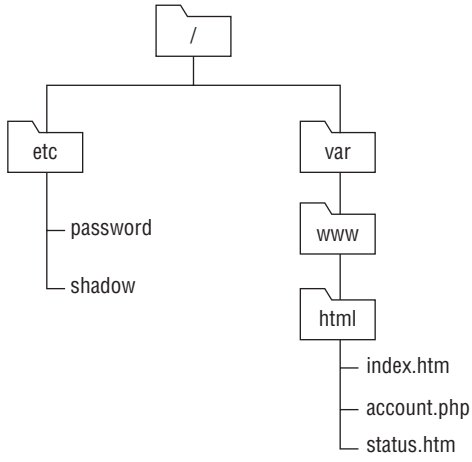
Unvalidated Redirect URL

```
www.mycompany.com/ordering.php?redirect=http%3a//www.evilhacker.com/
passwordstealer.htm
```

Modified URLs

```
www.mycompany.com/getDocument.php?documentID=1841
www.mycompany.com/getDocument.php?documentID=1843
www.mycompany.com/getDocument.php?documentID=1844
```

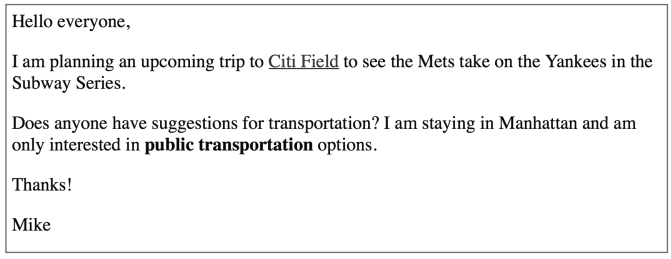
FIGURE 6.11 Example web server directory structure



Message Board Code

```
<p>Hello everyone,</p>
<p>I am planning an upcoming trip to <A HREF=
'https://www.mlb.com/mets/ballpark'>Citi Field</A> to see the Mets take on the
Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation? I am staying in Manhattan
and am only interested in <B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
```

FIGURE 6.12 Message board post rendered in a browser



Attacker Code

```
<p>Hello everyone,</p>
<p>I am planning an upcoming trip to <A HREF=
'https://www.mlb.com/mets/ballpark'>Citi Field</A> to see the Mets take on the
Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation? I am staying in Manhattan
and am only interested in <B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
<SCRIPT>alert('Cross-sitescripting!')</SCRIPT>
```

FIGURE 6.13 XSS attack rendered in a browser

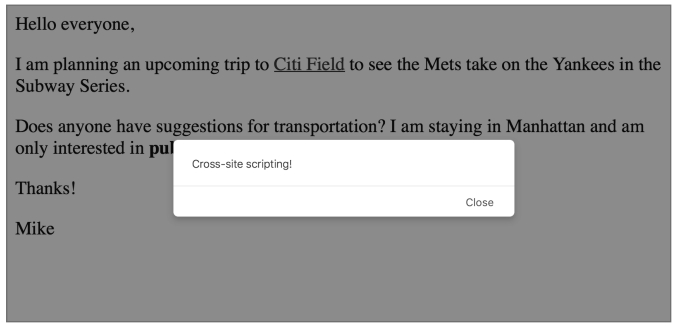


FIGURE 6.14 Web application firewall

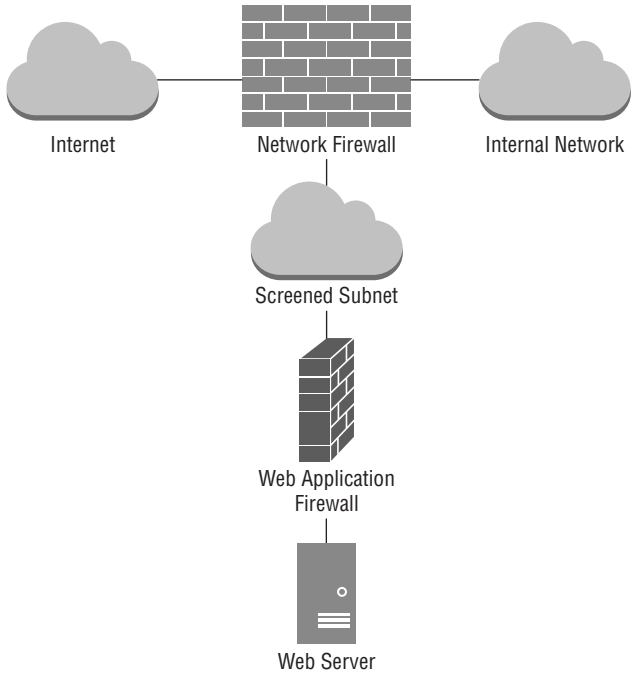
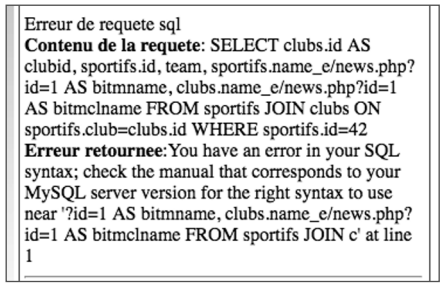


FIGURE 6.15 SQL error disclosure



Chapter 6 Review: Query String (Question 16)

```
www.mycompany.com/servicestatus.php?serviceID=892&serviceID=892'%20
;DROP%20TABLE%20Services;--
```

Chapter 6 Review: Requests to the Same URL (Question 17)

```
www.mycompany.com/servicestatus.php?serviceID=1
www.mycompany.com/servicestatus.php?serviceID=2
www.mycompany.com/servicestatus.php?serviceID=3
www.mycompany.com/servicestatus.php?serviceID=4
www.mycompany.com/servicestatus.php?serviceID=5
www.mycompany.com/servicestatus.php?serviceID=6
```

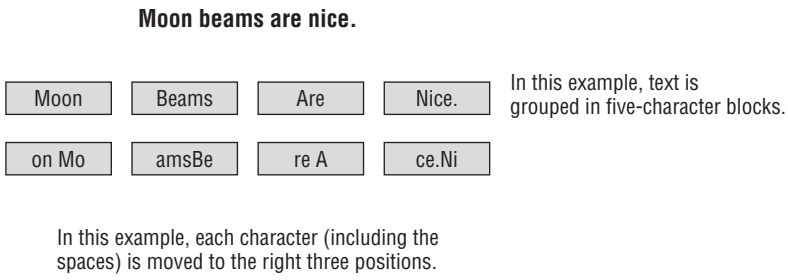
FIGURE 7.1 Vigenère cipher table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Encrypted Phrase "Secret Message" with Keyword "Apple"

```
S E C R E T M E S S A G E
A P P L E A P P L E A P P
```

FIGURE 7.2 A simple transposition cipher in action



Message in Four Rows

```
M M T T
E E H O
E I E R
T N S E
```

FIGURE 7.3 Enigma machine from the National Security Agency's National Cryptologic Museum

Source: USA.gov

FIGURE 7.4 OpenStego steganography tool

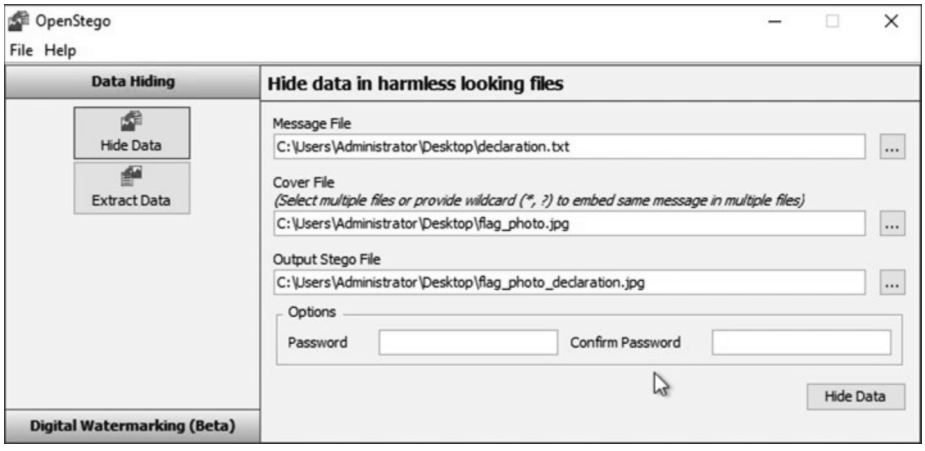


FIGURE 7.5 Image with embedded message

Source: vadiml/Adobe Stock Photos

FIGURE 7.6 Challenge-response authentication protocol

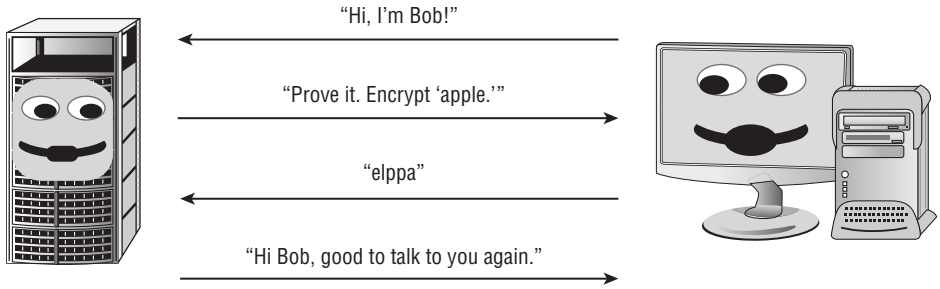


FIGURE 7.7 Symmetric key cryptography

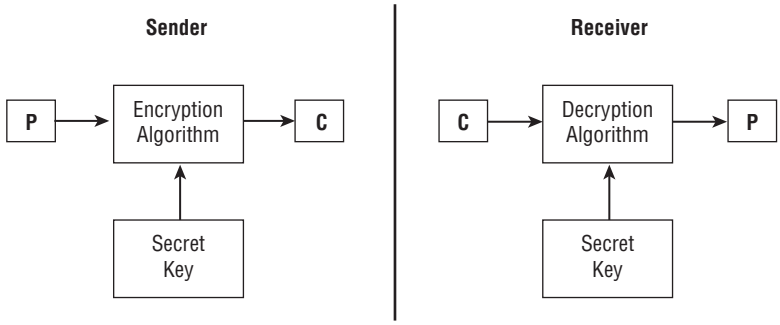
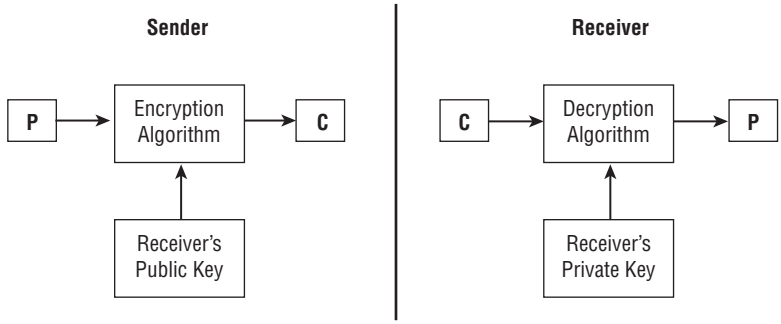


FIGURE 7.8 Asymmetric key cryptography



Key Requirements Table

Number of participants	Number of symmetric keys required	Number of asymmetric keys required
2	1	4
3	3	6
4	6	8
5	10	10
10	45	20
100	4,950	200
1,000	499,500	2,000
10,000	49,995,000	20,000

TABLE 7.1 Comparison of symmetric and asymmetric cryptography systems

Symmetric	Asymmetric
Single shared key	Key pair sets
Out-of-band exchange	In-band exchange
Not scalable	Scalable
Fast	Slow
Bulk encryption	Small blocks of data, digital signatures, digital certificates
Confidentiality, integrity	Confidentiality, integrity, authentication, non-repudiation

TABLE 7.2 Digital certificate formats

Standard	Format	File extension(s)
Distinguished Encoding Rules (DER)	Binary	`.der`, `.crt`, `.cer`
Privacy Enhanced Mail (PEM)	Text	`.pem`, `.crt`
Personal Information Exchange (PFX)	Binary	`.pfx`, `.p12`
P7B	Text	`.p7b`

FIGURE 8.1 CHAP challenge and response sequence

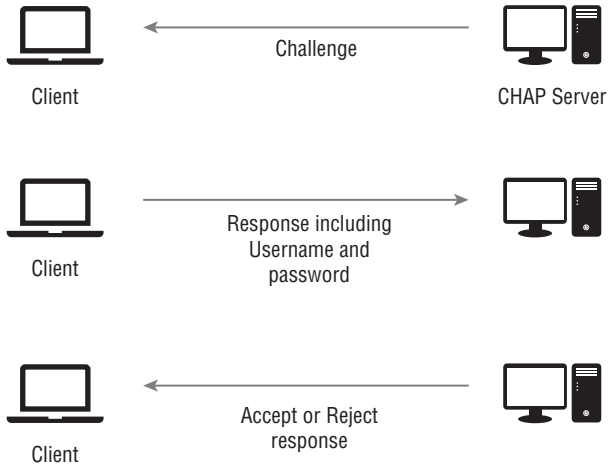


FIGURE 8.2 802.1X authentication architecture with EAP, RADIUS, and LDAP

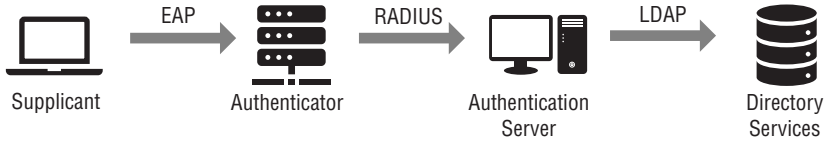


FIGURE 8.3 Kerberos authentication process

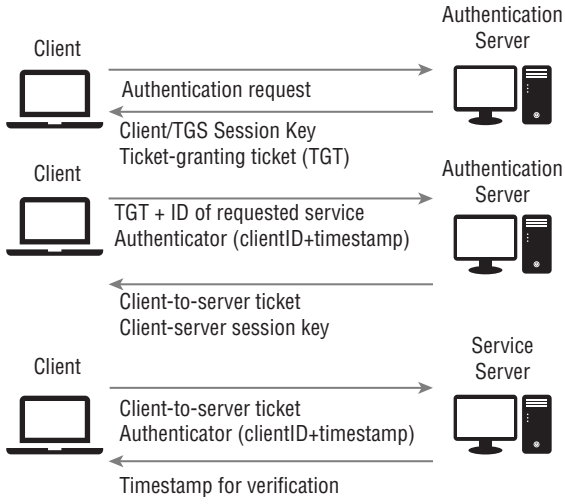


FIGURE 8.4 LDAP organizational hierarchy

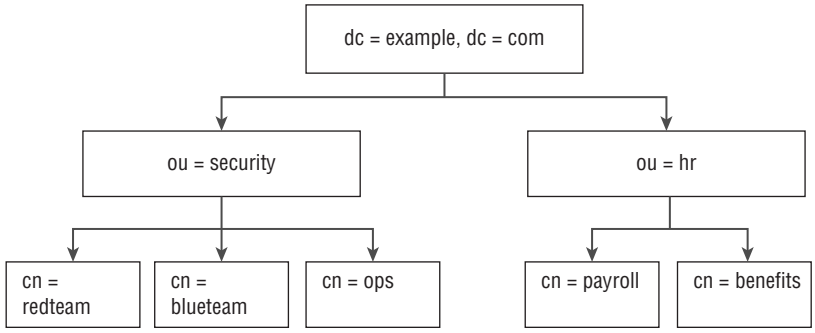


FIGURE 8.5 Windows local password policy options

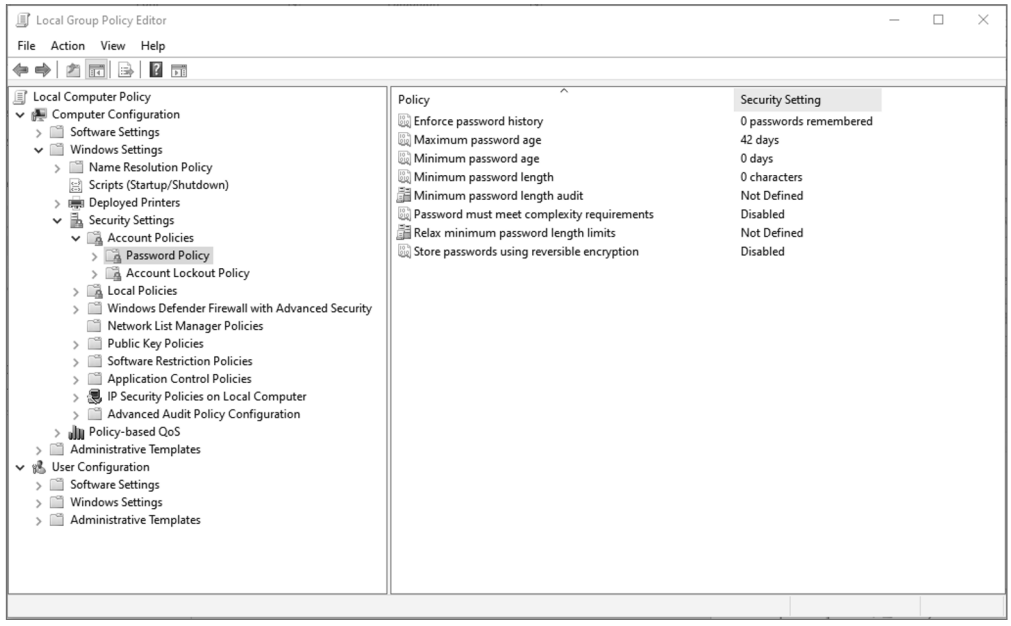


FIGURE 8.6 Windows Credential Manager

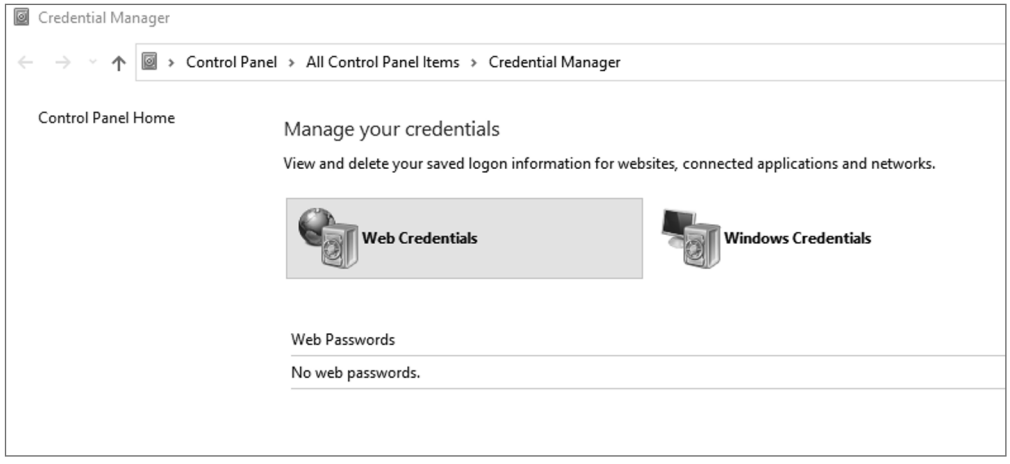


FIGURE 8.7 A Titan USB security key

FIGURE 8.8 Google authenticator showing TOTP code generation

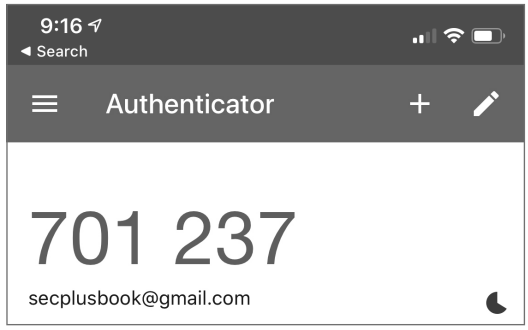
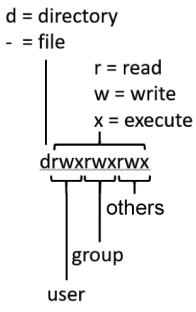


FIGURE 8.9 An HOTP PayPal token

FIGURE 8.10 Linux/Unix file permissions



Numeric representation	Permission	Letter representation
0	No permission	---
1	Execute	--x
2	Write	-w-
3	Execute + Write	-wx
4	Read	r--
5	Read + Execute	r-x
6	Read + Write	rw-
7	Read + Write + Execute	rwx

FIGURE 8.11 Windows file permissions

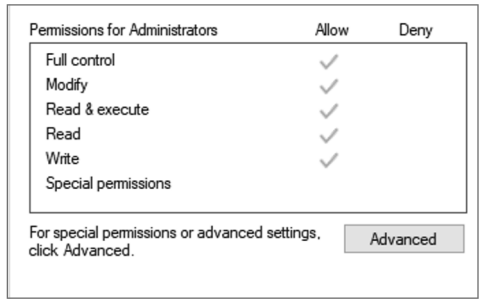
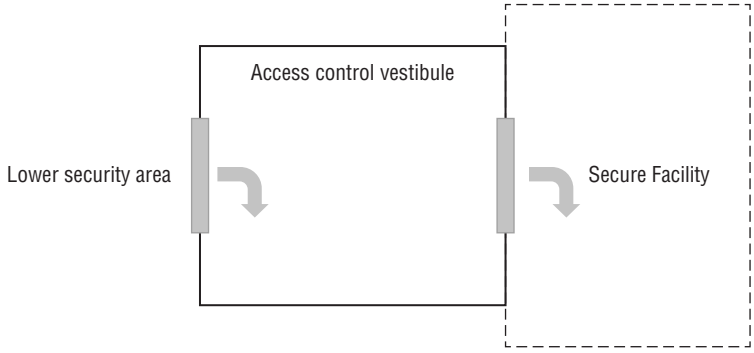


TABLE 9.1 RAID levels, advantages, and disadvantages

RAID description	Description	Advantage	Disadvantage
RAID 0 – Striping	Data is spread across all drives in the array.	Better I/O performance (speed); all capacity used.	Not fault tolerant—all data lost if a drive is lost.
RAID 1 – Mirroring	All data is duplicated to another drive or drives.	High read speeds from multiple drives; data available if a drive fails.	Uses twice the storage for the same amount of data.
RAID 5 – Striping with parity	Data is striped across drives, with one drive used for parity (checksum) of the data. Parity is spread across drives as well as data.	Data reads are fast; data writes are slightly slower. Drive failures can be rebuilt as long as only a single drive fails.	Can tolerate only a single drive failure at a time. Rebuilding arrays after a drive loss can be slow and impact performance.
RAID 10 – Mirroring and striping	Requires at least four drives, with drives added in pairs. Data is mirrored, then striped across drives.	Combines the advantages and disadvantages of both RAID 0 and RAID 1.	Combines the advantages and disadvantages of both RAID 0 and RAID 1. Sometimes written as RAID 1+0.

FIGURE 9.1 A bollard

FIGURE 9.2 An access control vestibule



Chapter 9 Review: Physical Security Control (Question 19)

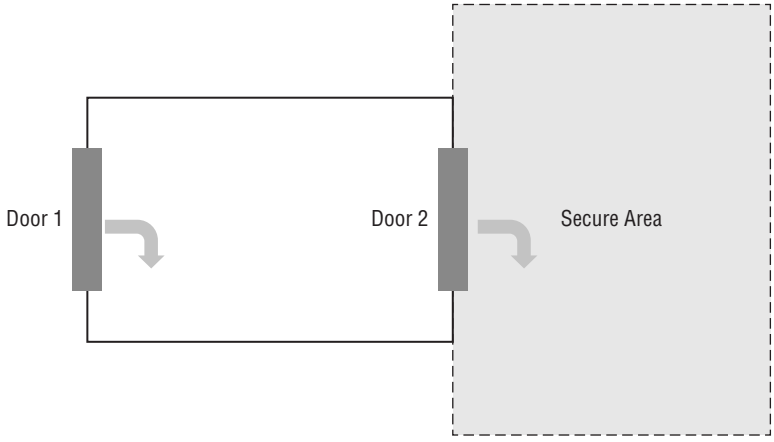


FIGURE 10.1 (a) Vertical scaling vs. (b) Horizontal scaling

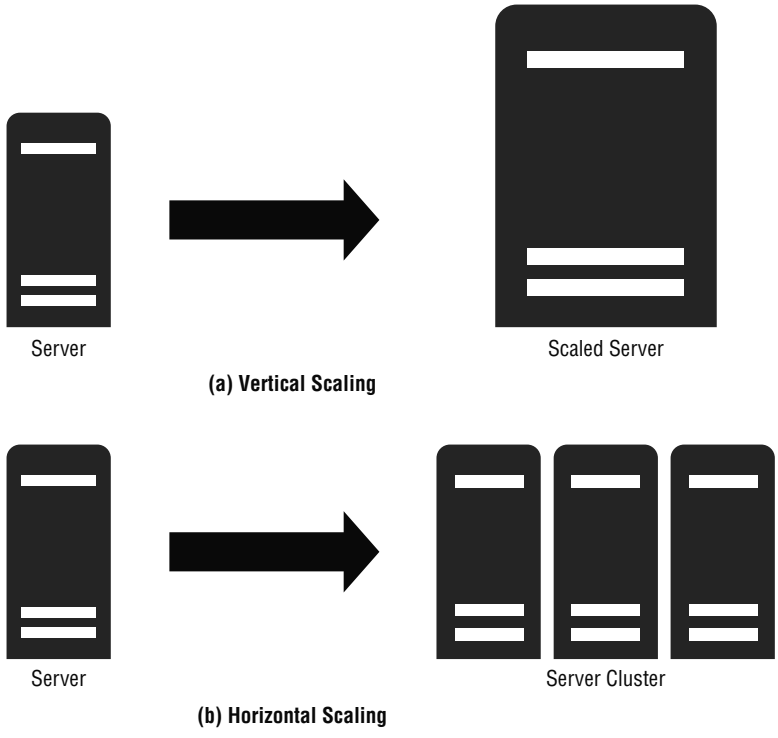


FIGURE 10.2 Thin clients, such as this Samsung Google Chromebook, are sufficient to access SaaS applications.

FIGURE 10.3 AWS Lambda function-as-a-service environment

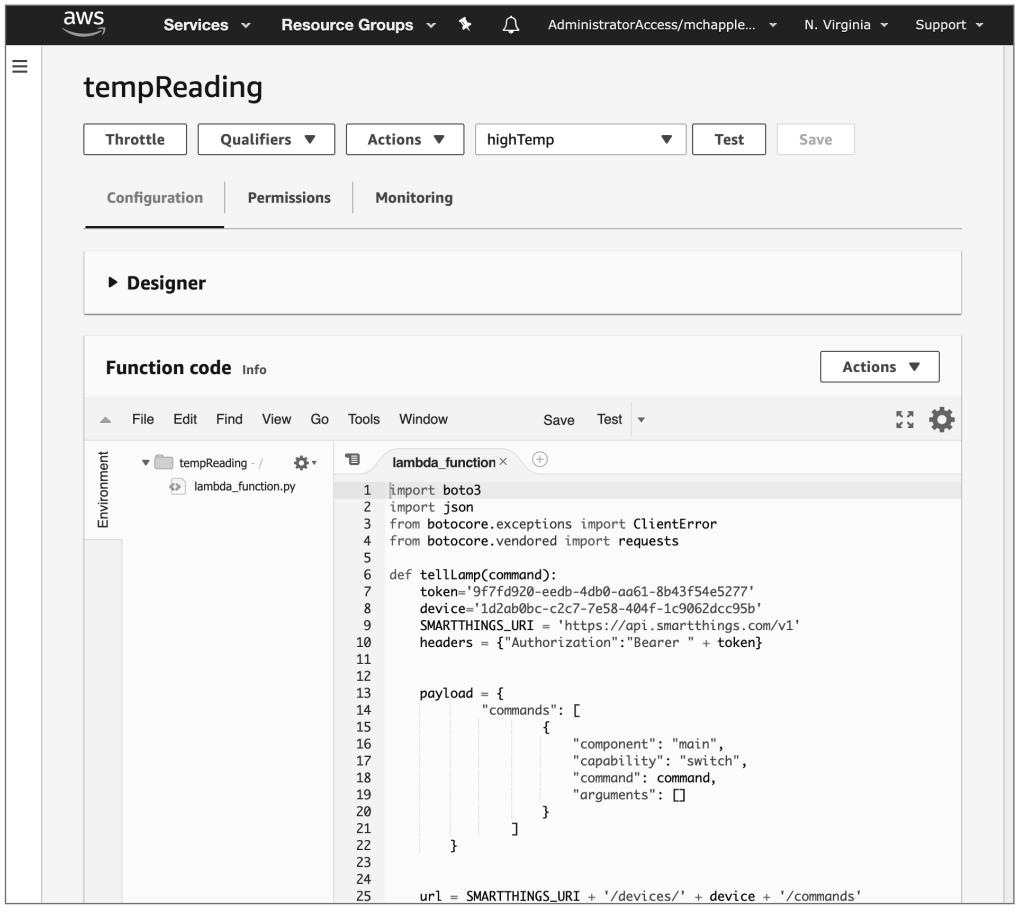


FIGURE 10.4 HathiTrust is an example of community cloud computing.

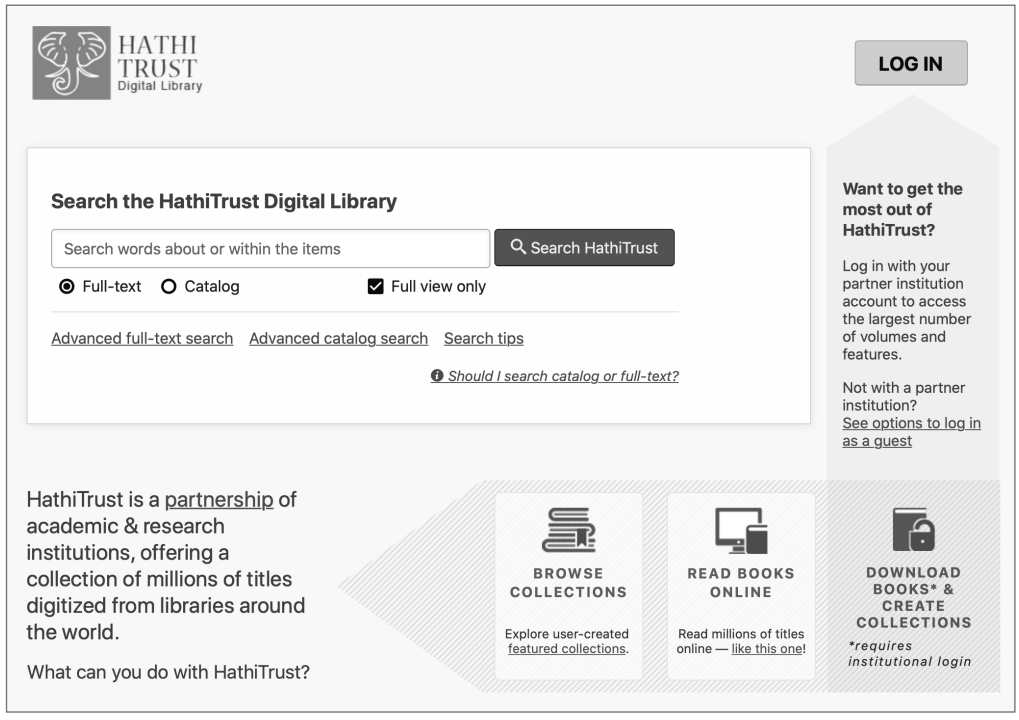


FIGURE 10.5 AWS Outposts offer hybrid cloud capability.

Image property of Amazon Web Services; used with permission

FIGURE 10.6 Shared responsibility model for cloud computing

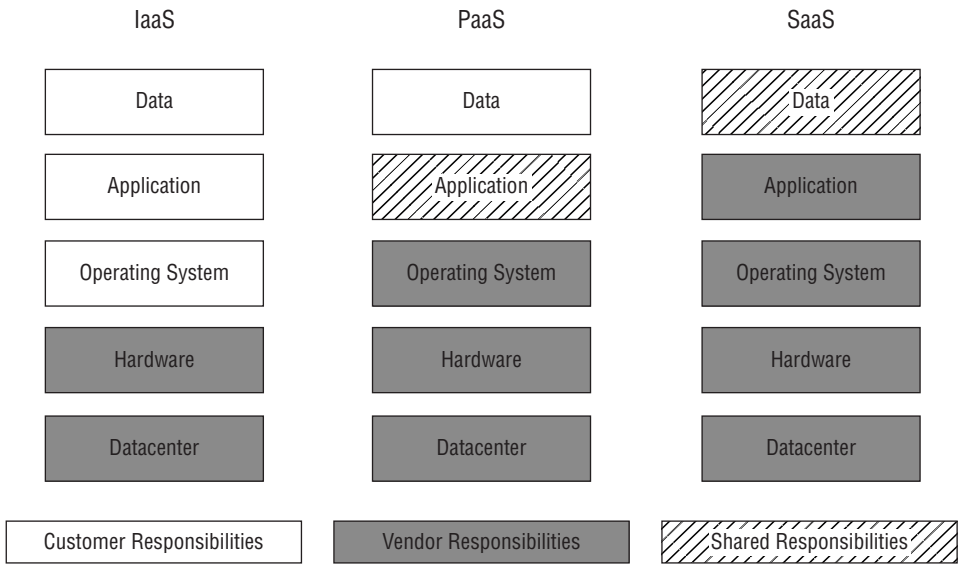
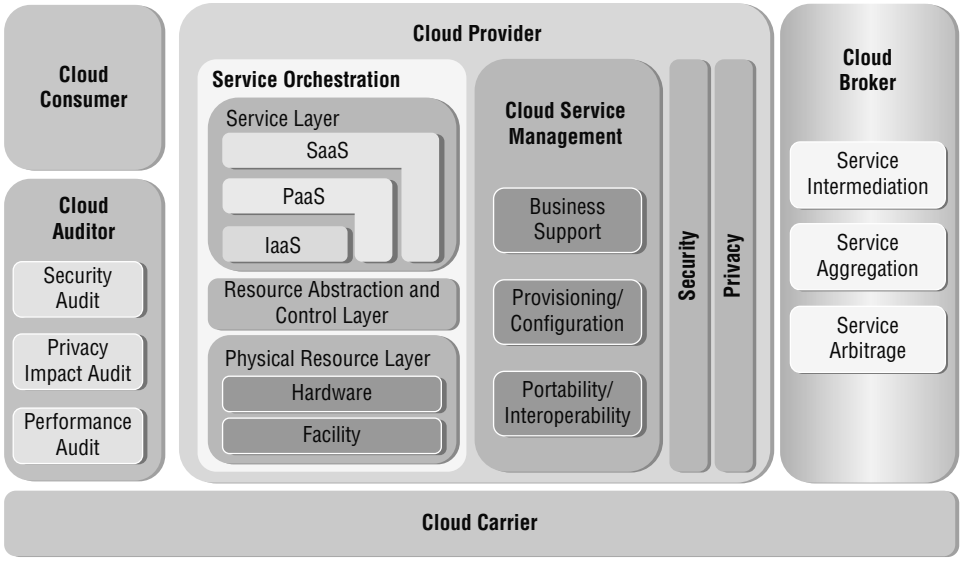


FIGURE 10.7 Cloud Reference Architecture



Source: NIST SP 500-292 / U.S. Department of Commerce / Public Domain.

FIGURE 10.8 Cloud Controls Matrix excerpt

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance
			Phys	Network	Compute	Storage	App	Data	
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X	X	X	X	
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	X	X	X	X	X	X	X
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.		X	X	X	X	X	

Source: Cloud Security Alliance

FIGURE 10.9 Type I hypervisor

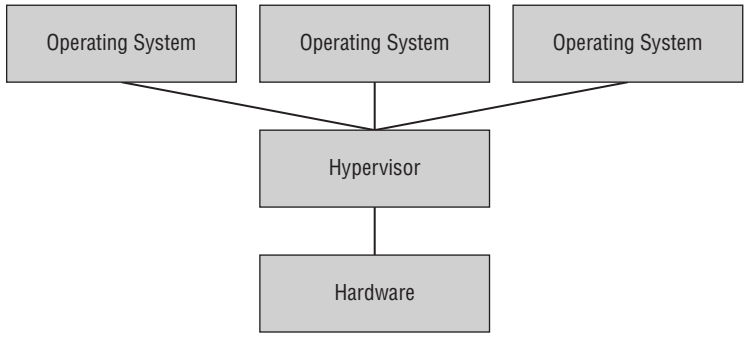


FIGURE 10.10 Type II hypervisor

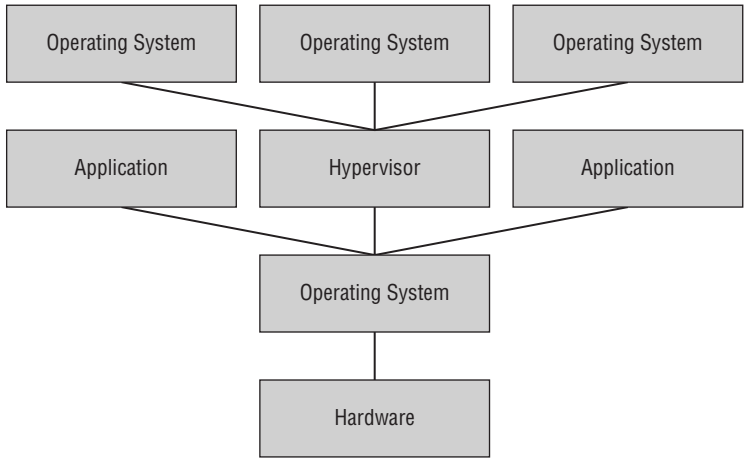


FIGURE 10.11 Provisioning a virtualized server in AWS

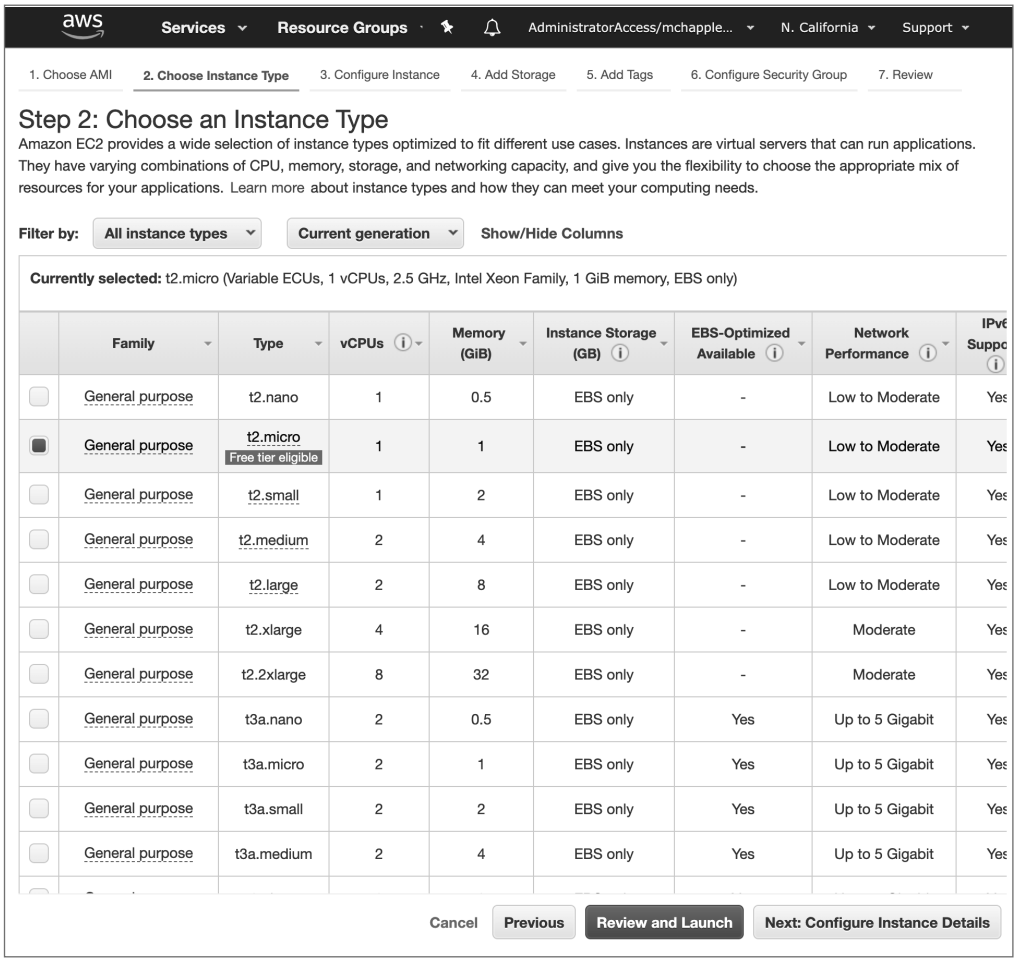


FIGURE 10.12 Connecting to an AWS virtual server instance with SSH

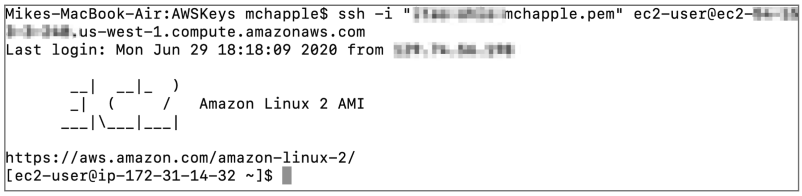


FIGURE 10.13 Connecting to an AWS virtual server instance with RDP

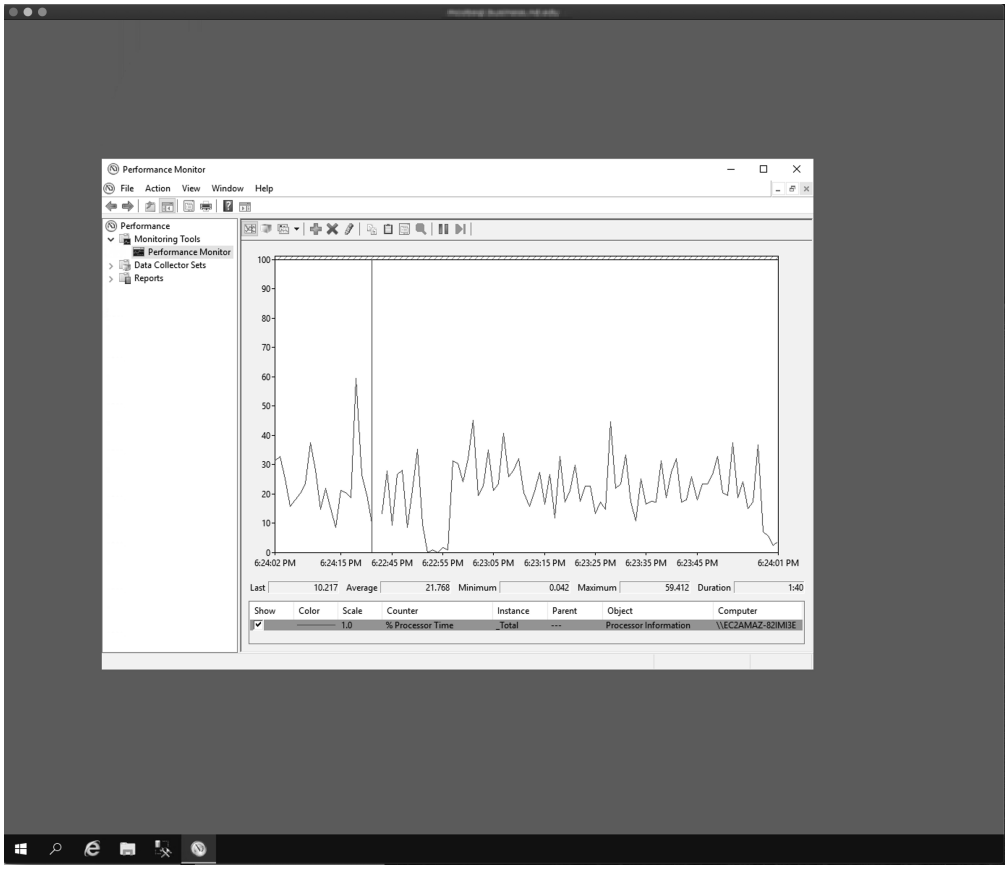


FIGURE 10.14 AWS Elastic Block Storage (EBS) volumes

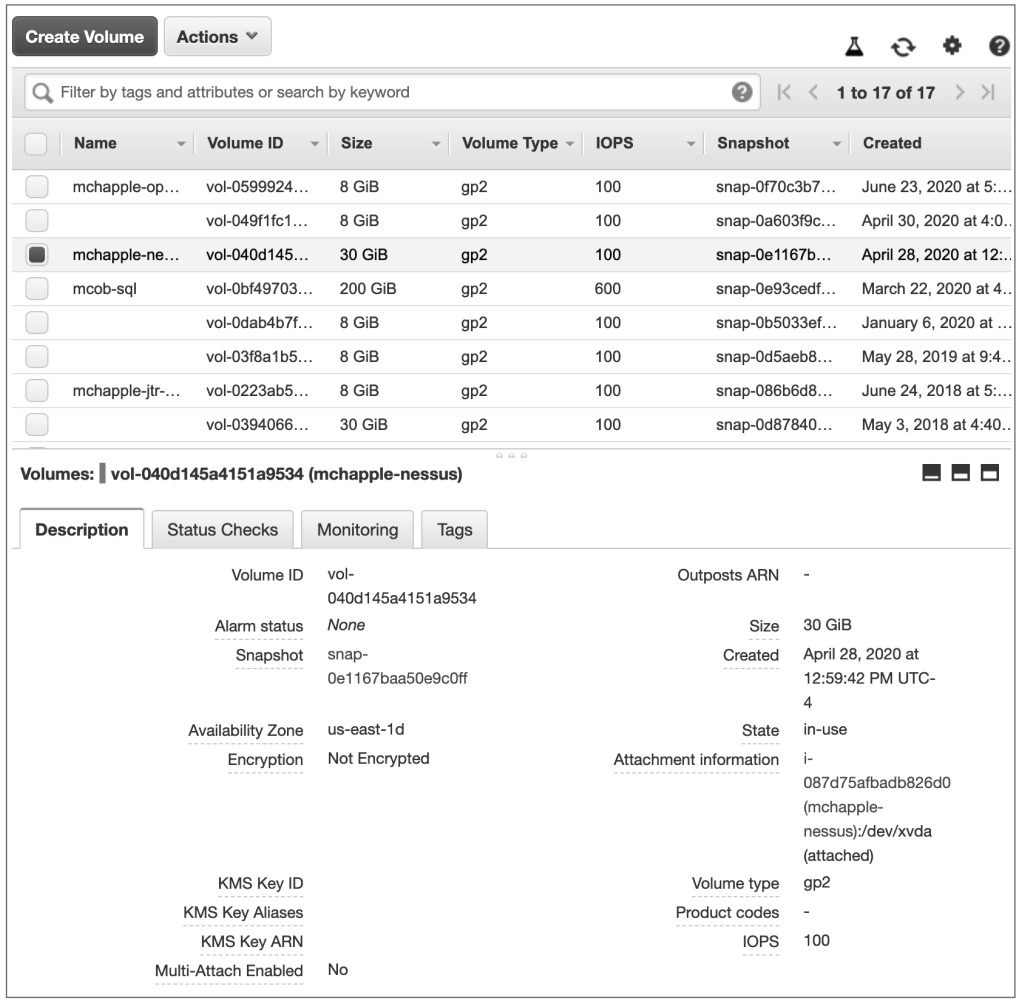


FIGURE 10.15 AWS Simple Storage Service (S3) bucket

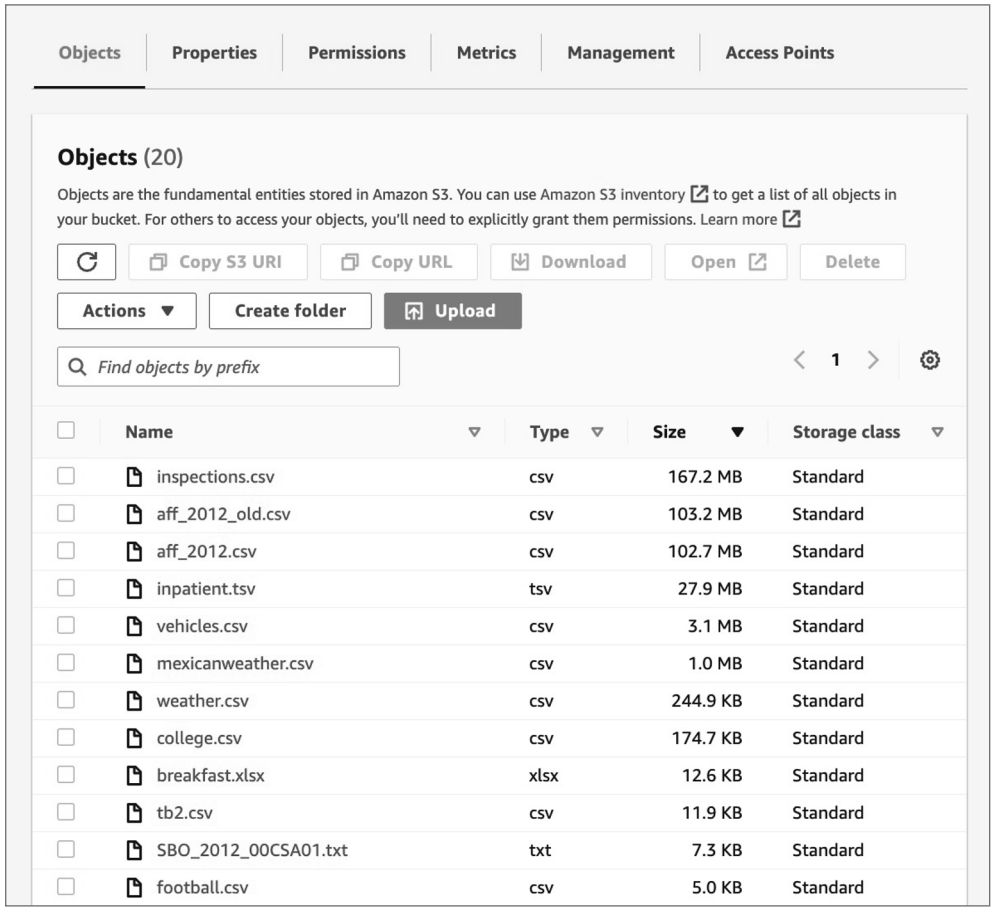


FIGURE 10.16 Enabling full-disk encryption on an EBS volume

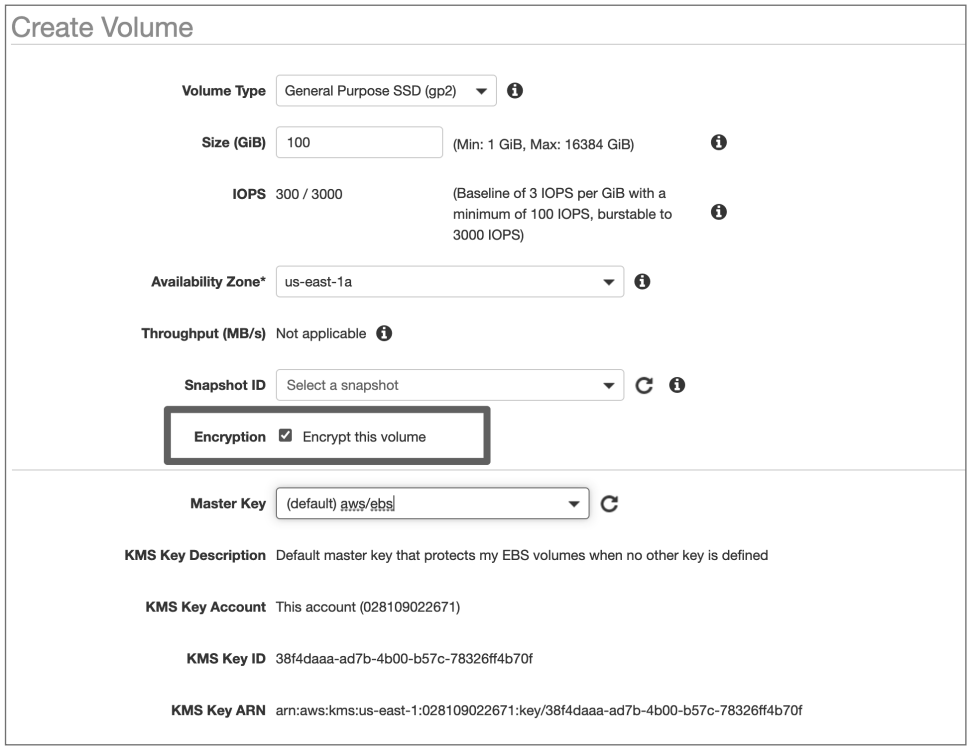
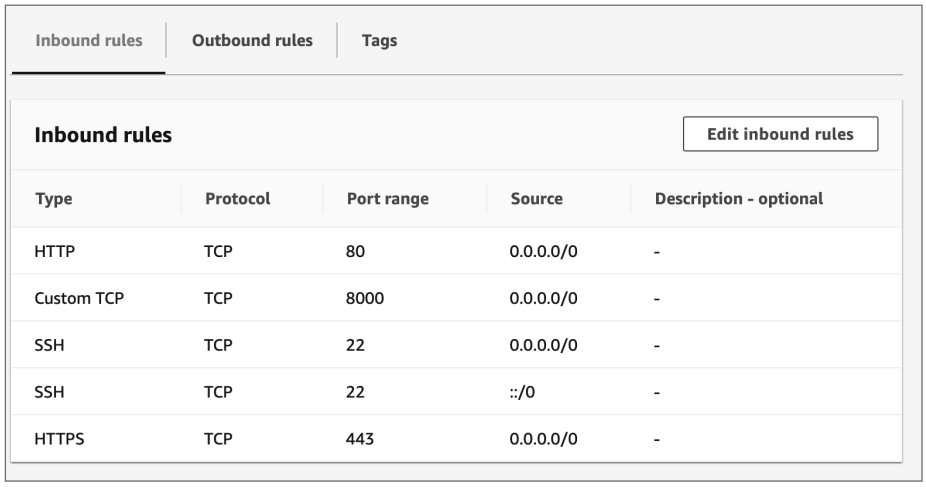


FIGURE 10.17 Security group restricting access to a cloud server



Inbound rules | Outbound rules | Tags

Inbound rules [Edit inbound rules]

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
Custom TCP	TCP	8000	0.0.0.0/0	-
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	::/0	-
HTTPS	TCP	443	0.0.0.0/0	-

FIGURE 10.18 Creating a virtual private cloud

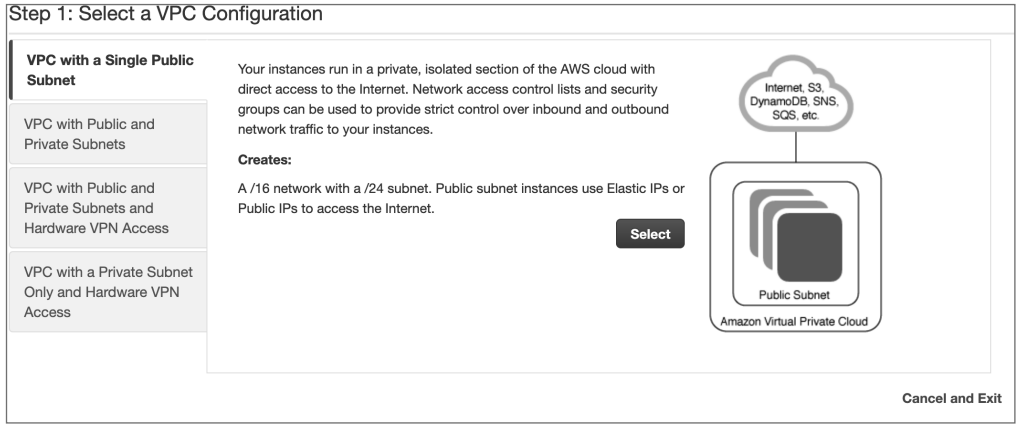
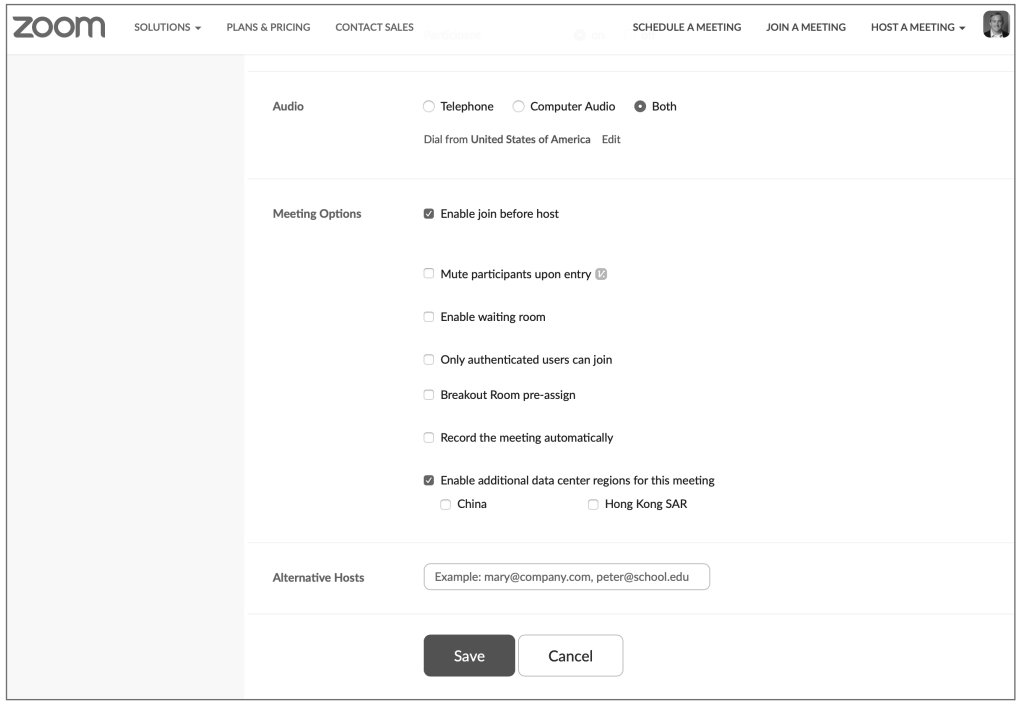


FIGURE 10.19 Creating an EC2 instance with CloudFormation JSON

```
"Ec2Instance" : {
  "Type" : "AWS::EC2::Instance",
  "Properties" : {
    "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" : "AWS::Region" },
                                      { "Fn::FindInMap" : [ "AWSInstanceType2Arch", { "Ref" : "InstanceType" }, "Arch" ] } ] },
    "KeyName" : { "Ref" : "KeyName" },
    "InstanceType" : { "Ref" : "InstanceType" },
    "SecurityGroups" : [{ "Ref" : "Ec2SecurityGroup" }],
    "BlockDeviceMappings" : [
      {
        "DeviceName" : "/dev/sda1",
        "Ebs" : { "VolumeSize" : "50" }
      },{
        "DeviceName" : "/dev/sdm",
        "Ebs" : { "VolumeSize" : "100" }
      }
    ]
  }
}
```

FIGURE 10.20 Limiting the datacenter regions used for a Zoom meeting



Service Control Policy Written in JSON Coding

```
{
    "Statement": [
        {
            "Sid": "DenyAllOutsideUSEastEUWest1",
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                       "us-east-1",
                       "us-east-2",
                       "eu-west-1"
                    ]
                }
            }
        },
        {
            "Condition": {
                "ForAnyValue:StringNotLike": {
                    "ec2:InstanceType": [
                        "*.micro",
                        "*.small",
                        "*.nano"
                    ]
                }
            },
            "Action": [
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute"
```

```
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Effect": "Deny",
            "Sid": "DenyLargeInstances"
        }
    ]
}
```

FIGURE 11.1 UEFI Secure boot high-level process

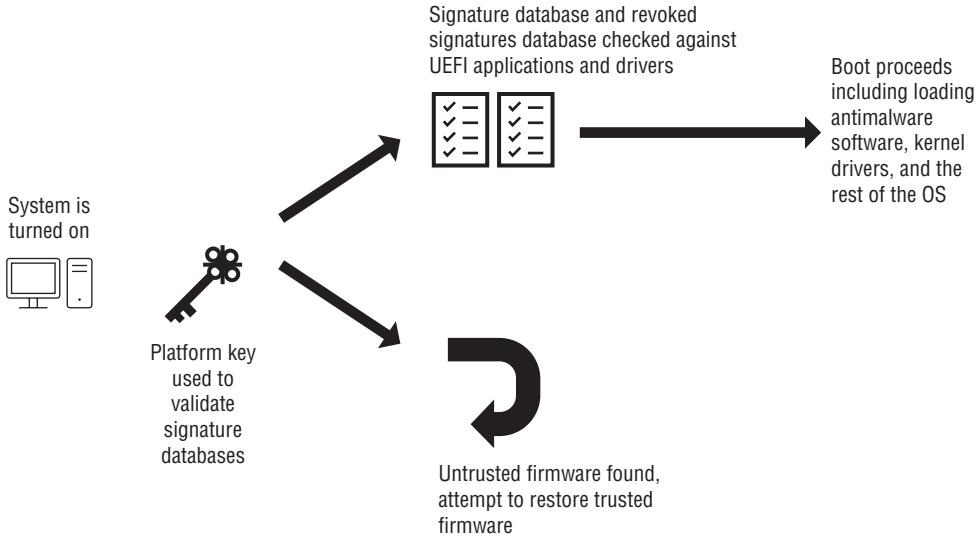


FIGURE 11.2 Host firewalls and IPS systems vs. network firewalls and IPS systems

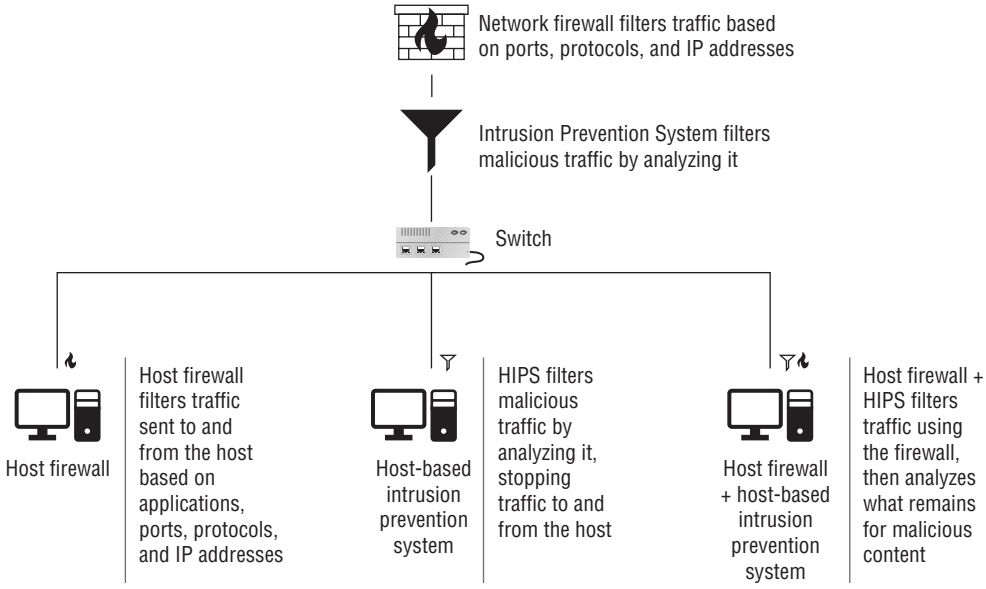


TABLE 11.1 Common ports and services

Port and protocol	Windows	Linux
22/TCP—Secure Shell (SSH)	Uncommon	Common
53/TCP and UDP—DNS	Common (servers)	Common (servers)
80/TCP—HTTP	Common (servers)	Common (servers)
125-139/TCP and UDP—NetBIOS	Common	Occasional
389/TCP and UDP—LDAP	Common (servers)	Common (servers)
443/TCP—HTTPS	Common (servers)	Common (servers)
3389/TCP and UDP—Remote Desktop Protocol	Common	Uncommon

FIGURE 11.3 `Services.msc` showing Remote Desktop Services set to manual

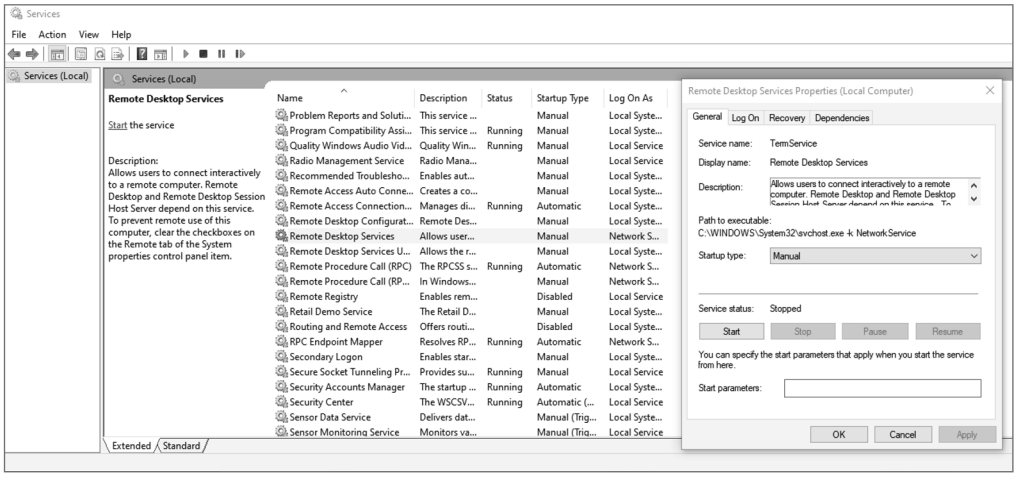


FIGURE 11.4 Windows Local Security Policy

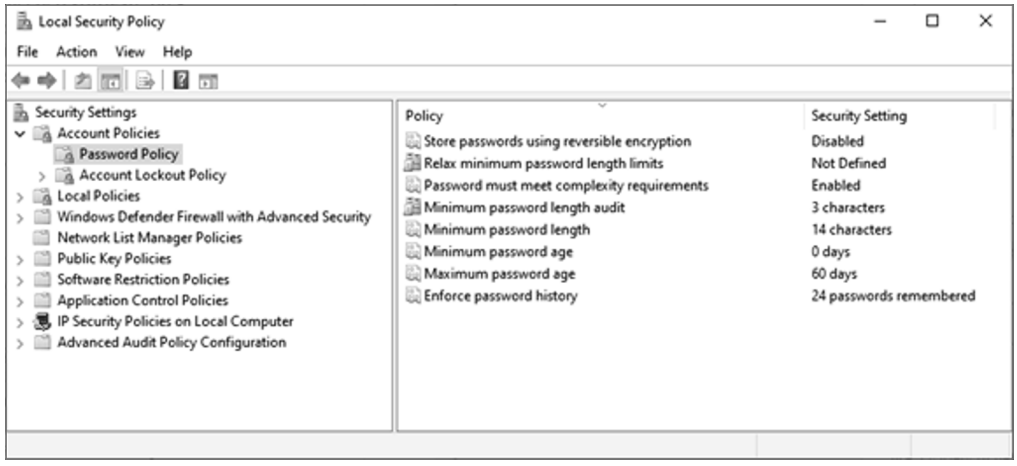


FIGURE 11.5 Policy Analyzer using Microsoft's baseline against a default Windows system

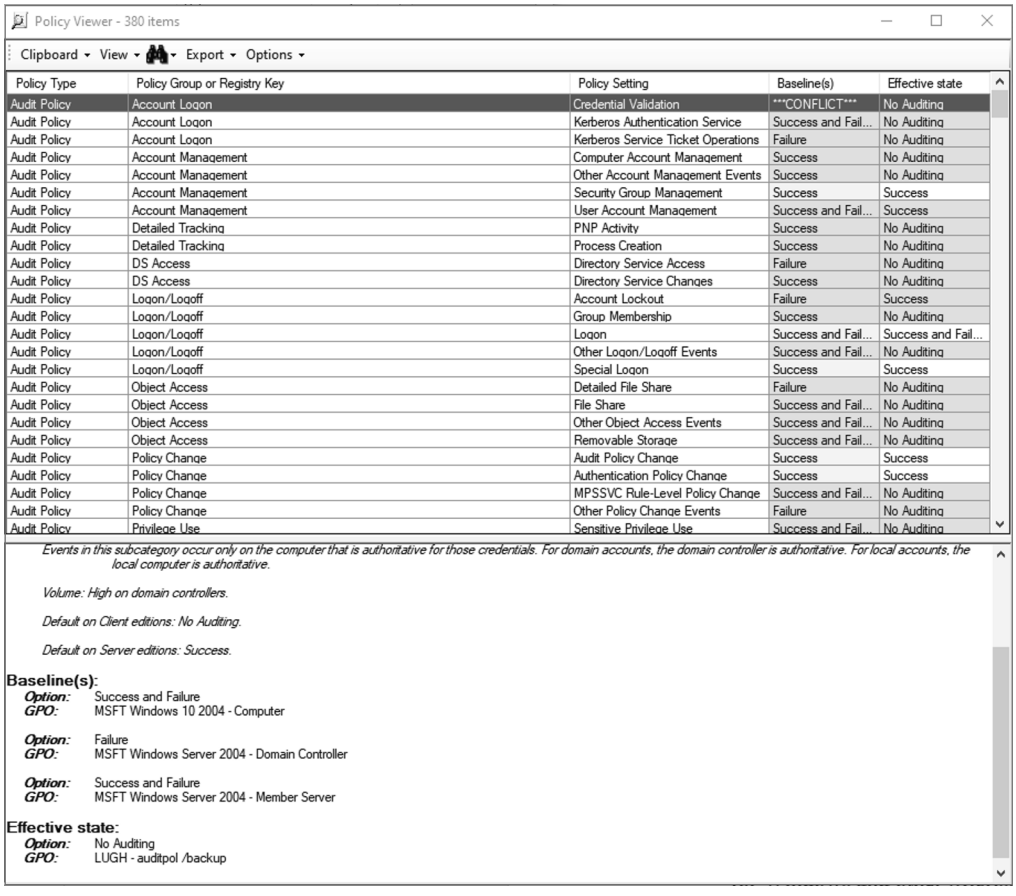
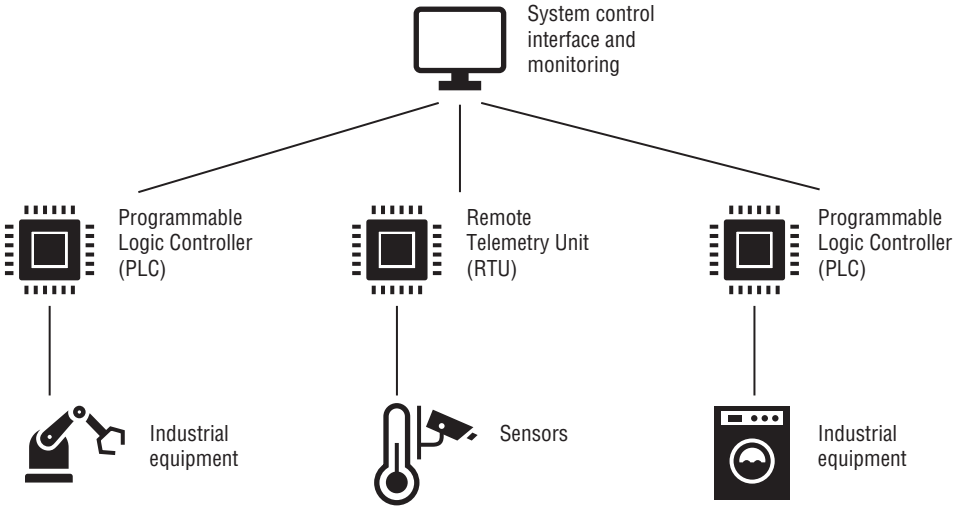


FIGURE 11.6 A SCADA system showing PLCs and RTUs with sensors and equipment



The OSI Model Graphic

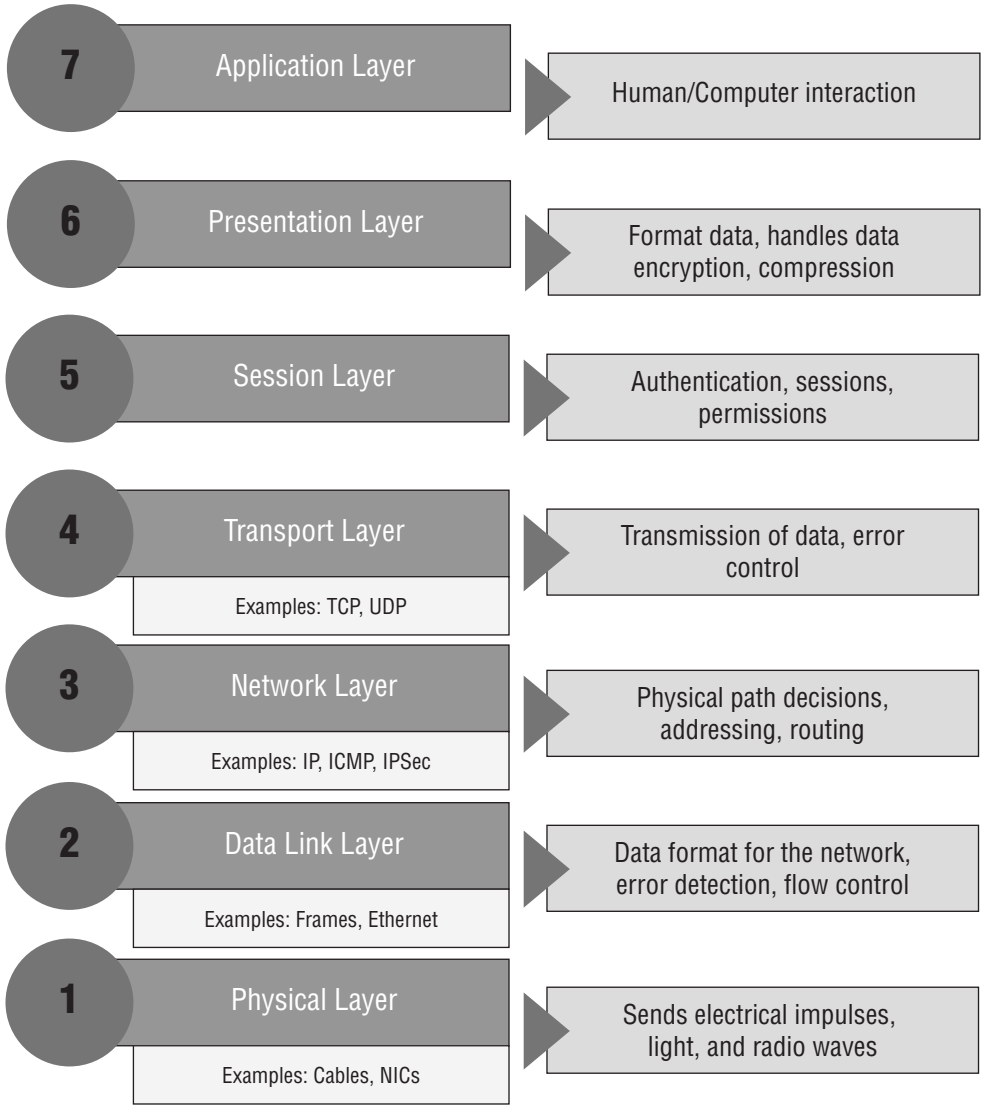
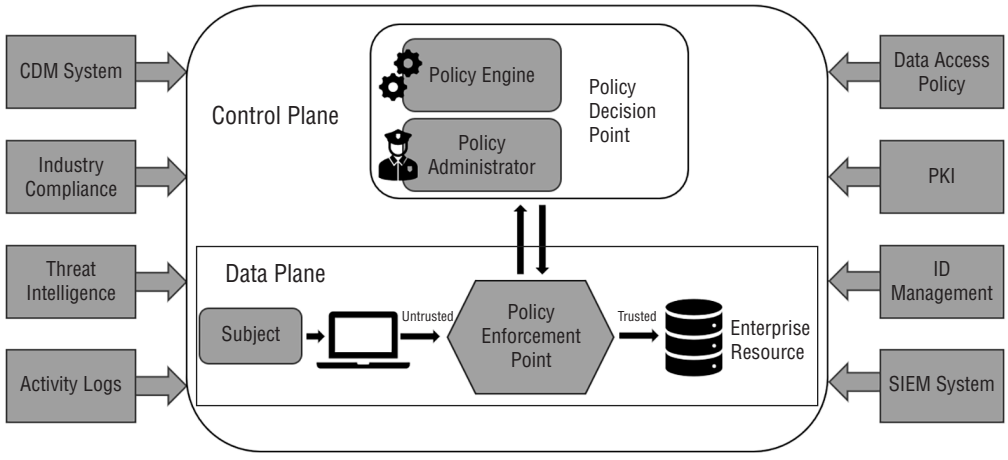


FIGURE 12.1 NIST Zero Trust core trust logical components



Broadcast Storm Graphic

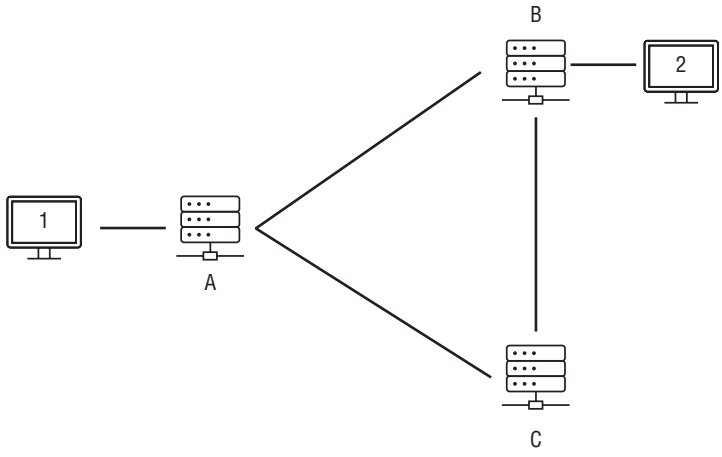


FIGURE 12.2 Inline IPS vs. passive IDS deployment using a tap or SPAN port

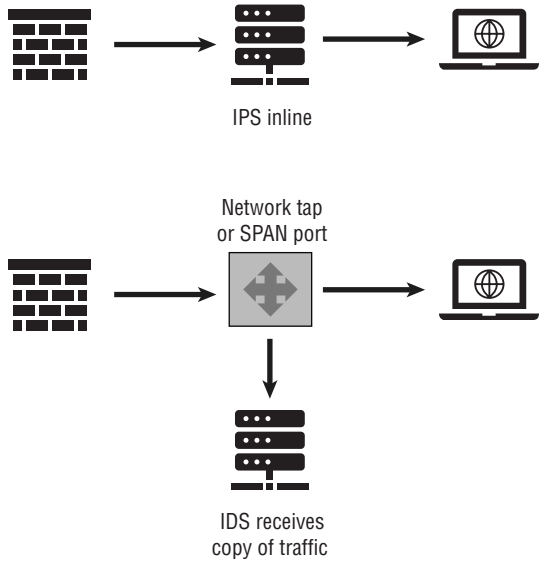
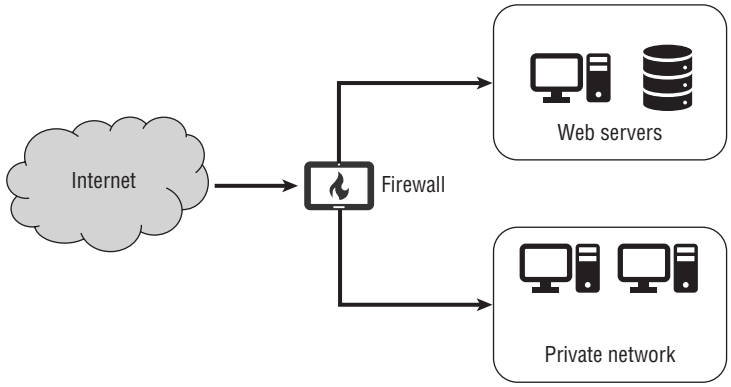


FIGURE 12.3 Screened subnet



ACL Formatting

```
access-list access-list-number dynamic name {permit|deny} [protocol]
{source source-wildcard|any} {destination destination-wildcard|any}
[precedence precedence][tos tos][established] [log|log-input]
[operator destination-port|destination port]
```

TABLE 12.1 Example network ACLs

Rule number	Protocol	Ports	Destination	Allow/deny	Notes
10	TCP	22	10.0.10.0/24	ALLOW	Allow SSH
20	TCP	443	10.0.10.45/32	ALLOW	Inbound HTTPS to web server
30	ICMP	ALL	0.0.0.0/0	DENY	Block ICMP

DMARC Graphic

```
└─$ dig txt _dmarc.sendgrid.net                                                    9 ×

; <<>> DiG 9.16.13-Debian <<>> txt _dmarc.sendgrid.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61837
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;_dmarc.sendgrid.net.           IN      TXT

;; ANSWER SECTION:
_dmarc.sendgrid.net.    5       IN      TXT     "v=DMARC1; p=reject; sp=none; rua=mailto:dmarc_agg@vali.ema
il; rf=afrf; pct=100"

;; Query time: 28 msec
;; SERVER: 192.168.145.2#53(192.168.145.2)
;; WHEN: Sat Aug 05 18:21:33 EDT 2023
;; MSG SIZE  rcvd: 139
```

TABLE 12.2 Secure and unsecure protocols

Unsecure protocol	Original port	Secure protocol option(s)	Secure port	Notes
DNS	UDP/TCP 53	DNSSEC	UDP/TCP 53	
FTP	TCP 21 (and 20)	FTPS	TCP 21 in explicit mode and 990 in implicit mode (FTPS)	Using TLS
FTP	TCP 21 (and 20)	SFTP	TCP 22 (SSH)	Using SSH
HTTP	TCP 80	HTTPS	TCP 443	Using TLS
IMAP	TCP 143	IMAPS	TCP 993	Using TLS
LDAP	UDP and TCP 389	LDAPS	TCP 636	Using TLS
POP3	TCP 110	POP3	TCP 995 – Secure POP3	Using TLS
RTP	UDP 16384-32767	SRTP	UDP 5004	
SNMP	UDP 161 and 162	SNMPv3	UDP 161 and 162	
Telnet	TCP 23	SSH	TCP 22	

FIGURE 12.4 Communications before and after an on-path attack

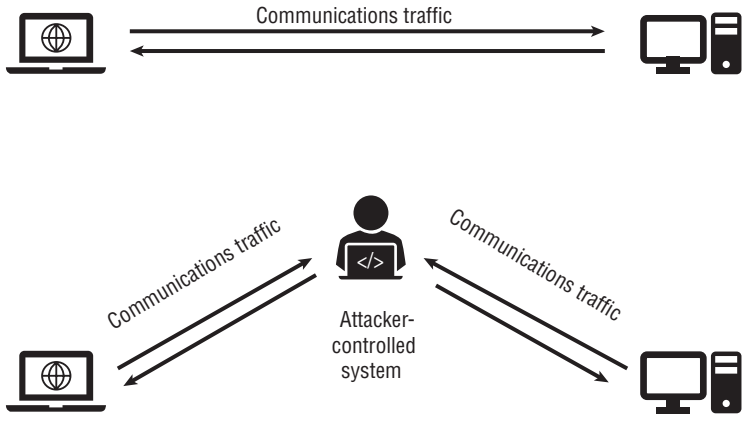
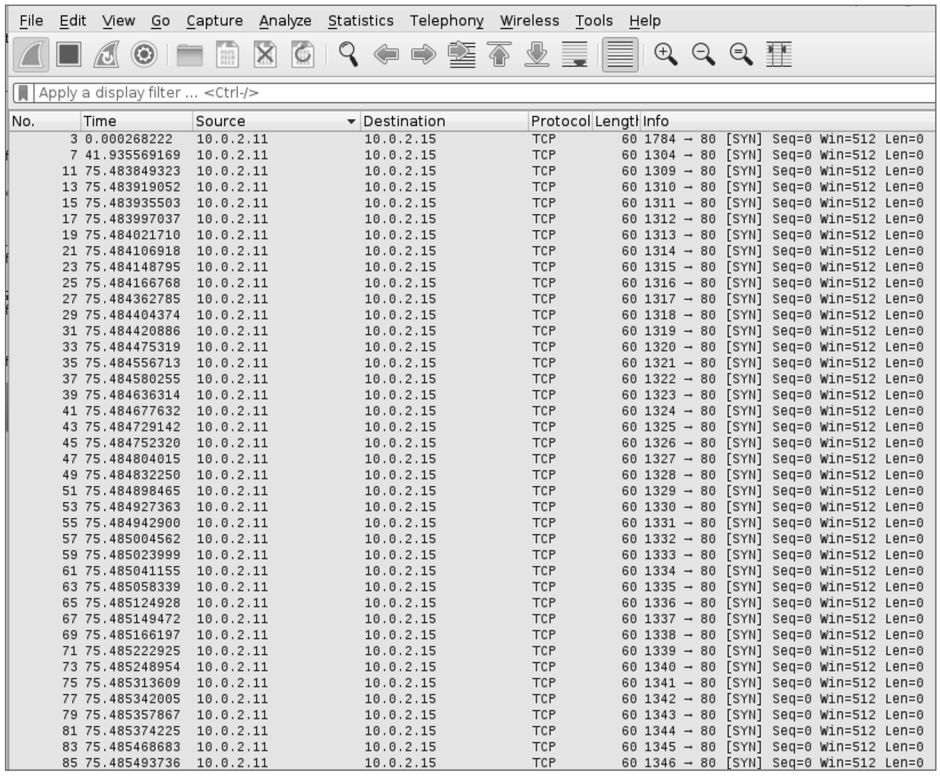


FIGURE 12.5 Reputation data for `gmail.com`

FIGURE 12.6 A SYN flood shown in Wireshark

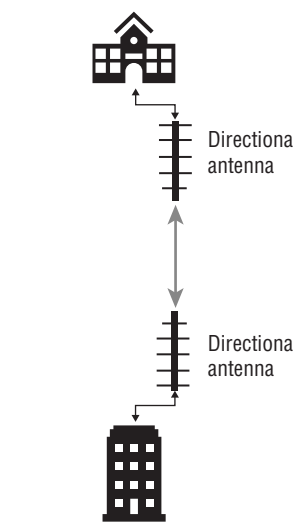


No.	Time	Source	Destination	Protocol	Length	Info
3	0.000268222	10.0.2.11	10.0.2.15	TCP	60	1784 → 80 [SYN] Seq=0 Win=512 Len=0
7	41.935569169	10.0.2.11	10.0.2.15	TCP	60	1304 → 80 [SYN] Seq=0 Win=512 Len=0
11	75.483849323	10.0.2.11	10.0.2.15	TCP	60	1309 → 80 [SYN] Seq=0 Win=512 Len=0
13	75.483919052	10.0.2.11	10.0.2.15	TCP	60	1310 → 80 [SYN] Seq=0 Win=512 Len=0
15	75.483935503	10.0.2.11	10.0.2.15	TCP	60	1311 → 80 [SYN] Seq=0 Win=512 Len=0
17	75.483997037	10.0.2.11	10.0.2.15	TCP	60	1312 → 80 [SYN] Seq=0 Win=512 Len=0
19	75.484021710	10.0.2.11	10.0.2.15	TCP	60	1313 → 80 [SYN] Seq=0 Win=512 Len=0
21	75.484106918	10.0.2.11	10.0.2.15	TCP	60	1314 → 80 [SYN] Seq=0 Win=512 Len=0
23	75.484148795	10.0.2.11	10.0.2.15	TCP	60	1315 → 80 [SYN] Seq=0 Win=512 Len=0
25	75.484166768	10.0.2.11	10.0.2.15	TCP	60	1316 → 80 [SYN] Seq=0 Win=512 Len=0
27	75.484362785	10.0.2.11	10.0.2.15	TCP	60	1317 → 80 [SYN] Seq=0 Win=512 Len=0
29	75.484404374	10.0.2.11	10.0.2.15	TCP	60	1318 → 80 [SYN] Seq=0 Win=512 Len=0
31	75.484420886	10.0.2.11	10.0.2.15	TCP	60	1319 → 80 [SYN] Seq=0 Win=512 Len=0
33	75.484475319	10.0.2.11	10.0.2.15	TCP	60	1320 → 80 [SYN] Seq=0 Win=512 Len=0
35	75.484556713	10.0.2.11	10.0.2.15	TCP	60	1321 → 80 [SYN] Seq=0 Win=512 Len=0
37	75.484580255	10.0.2.11	10.0.2.15	TCP	60	1322 → 80 [SYN] Seq=0 Win=512 Len=0
39	75.484636314	10.0.2.11	10.0.2.15	TCP	60	1323 → 80 [SYN] Seq=0 Win=512 Len=0
41	75.484677632	10.0.2.11	10.0.2.15	TCP	60	1324 → 80 [SYN] Seq=0 Win=512 Len=0
43	75.484729142	10.0.2.11	10.0.2.15	TCP	60	1325 → 80 [SYN] Seq=0 Win=512 Len=0
45	75.484752320	10.0.2.11	10.0.2.15	TCP	60	1326 → 80 [SYN] Seq=0 Win=512 Len=0
47	75.484804015	10.0.2.11	10.0.2.15	TCP	60	1327 → 80 [SYN] Seq=0 Win=512 Len=0
49	75.484832250	10.0.2.11	10.0.2.15	TCP	60	1328 → 80 [SYN] Seq=0 Win=512 Len=0
51	75.484898465	10.0.2.11	10.0.2.15	TCP	60	1329 → 80 [SYN] Seq=0 Win=512 Len=0
53	75.484927363	10.0.2.11	10.0.2.15	TCP	60	1330 → 80 [SYN] Seq=0 Win=512 Len=0
55	75.484942900	10.0.2.11	10.0.2.15	TCP	60	1331 → 80 [SYN] Seq=0 Win=512 Len=0
57	75.485004562	10.0.2.11	10.0.2.15	TCP	60	1332 → 80 [SYN] Seq=0 Win=512 Len=0
59	75.485023999	10.0.2.11	10.0.2.15	TCP	60	1333 → 80 [SYN] Seq=0 Win=512 Len=0
61	75.485041155	10.0.2.11	10.0.2.15	TCP	60	1334 → 80 [SYN] Seq=0 Win=512 Len=0
63	75.485058339	10.0.2.11	10.0.2.15	TCP	60	1335 → 80 [SYN] Seq=0 Win=512 Len=0
65	75.485124928	10.0.2.11	10.0.2.15	TCP	60	1336 → 80 [SYN] Seq=0 Win=512 Len=0
67	75.485149472	10.0.2.11	10.0.2.15	TCP	60	1337 → 80 [SYN] Seq=0 Win=512 Len=0
69	75.485166197	10.0.2.11	10.0.2.15	TCP	60	1338 → 80 [SYN] Seq=0 Win=512 Len=0
71	75.485222925	10.0.2.11	10.0.2.15	TCP	60	1339 → 80 [SYN] Seq=0 Win=512 Len=0
73	75.485248954	10.0.2.11	10.0.2.15	TCP	60	1340 → 80 [SYN] Seq=0 Win=512 Len=0
75	75.485313609	10.0.2.11	10.0.2.15	TCP	60	1341 → 80 [SYN] Seq=0 Win=512 Len=0
77	75.485342005	10.0.2.11	10.0.2.15	TCP	60	1342 → 80 [SYN] Seq=0 Win=512 Len=0
79	75.485357867	10.0.2.11	10.0.2.15	TCP	60	1343 → 80 [SYN] Seq=0 Win=512 Len=0
81	75.485374225	10.0.2.11	10.0.2.15	TCP	60	1344 → 80 [SYN] Seq=0 Win=512 Len=0
83	75.485468683	10.0.2.11	10.0.2.15	TCP	60	1345 → 80 [SYN] Seq=0 Win=512 Len=0
85	75.485493736	10.0.2.11	10.0.2.15	TCP	60	1346 → 80 [SYN] Seq=0 Win=512 Len=0

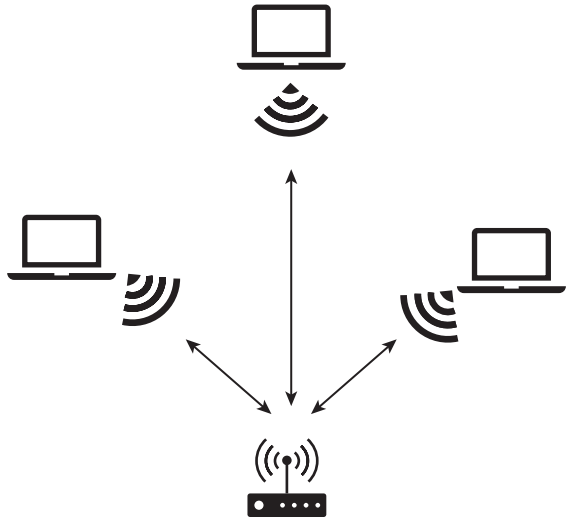
TABLE 13.1 Wi-Fi standards, maximum theoretical speed, and frequencies

Wi-Fi standard	Generation name	Maximum speed	Frequencies
802.11b		11 Mbit/s	2.4 GHz
802.11a		54 Mbit/s	5 GHz
802.11g		54 Mbit/s	2.4 GHz
802.11n	Wi-Fi 4	600 Mbit/s	2.4 GHz and 5 GHz
802.11ac	Wi-Fi 5	6.9 Gbit/s	5 GHz
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s	2.4 GHz, 5 GHz, 6 GHz
802.11be	Wi-Fi 7	40+ Gbit/s	2.4 GHz, 5 GHz, 6 GHz

FIGURE 13.1 Point-to-point and point-to-multipoint network designs



Point to point wireless network



Point to multipoint wireless network

FIGURE 13.2 Evil twin pretending to be a legitimate access point

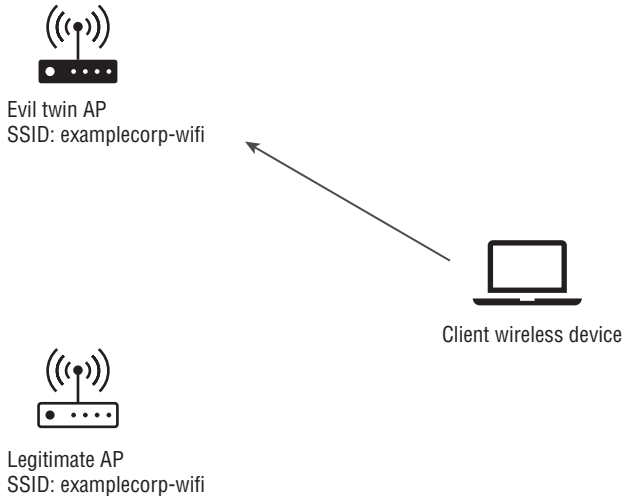


FIGURE 13.3 A wireless heatmap showing the wireless signal available from an access point

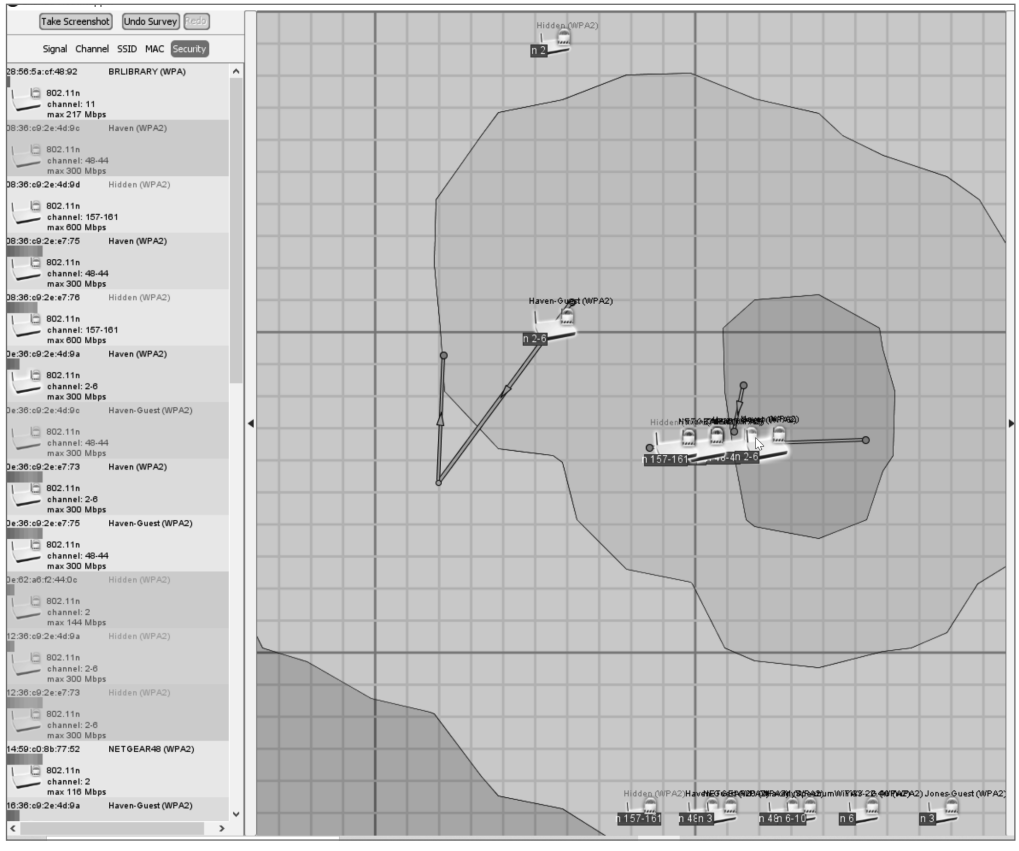


FIGURE 13.4 Overlap map of the North American 2.4 GHz Wi-Fi channels

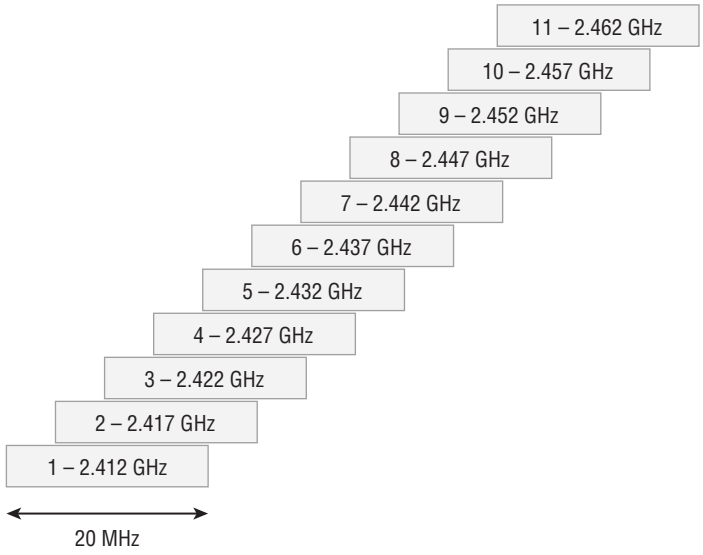


TABLE 13.2 Mobile device deployment and management options

	Who owns the device	Who controls and maintains the device	Description
BYOD			
Bring your own device	The user	The user	The user brings their own personally owned device. This provides more user freedom and lower cost to the organization, but greater risk since the organization does not control, secure, or manage the device.
CYOD			
Choose your own device	The organization	The organization	The organization owns and maintains the device, but allows the user to select it.
COPE			
Corporate-owned, personally enabled	The organization	The organization	Corporate-provided devices allow reasonable personal use while meeting enterprise security and control needs.
Corporate-owned	The organization	The organization	Corporate-owned provides the greatest control but least flexibility.

FIGURE 14.1 The incident response cycle

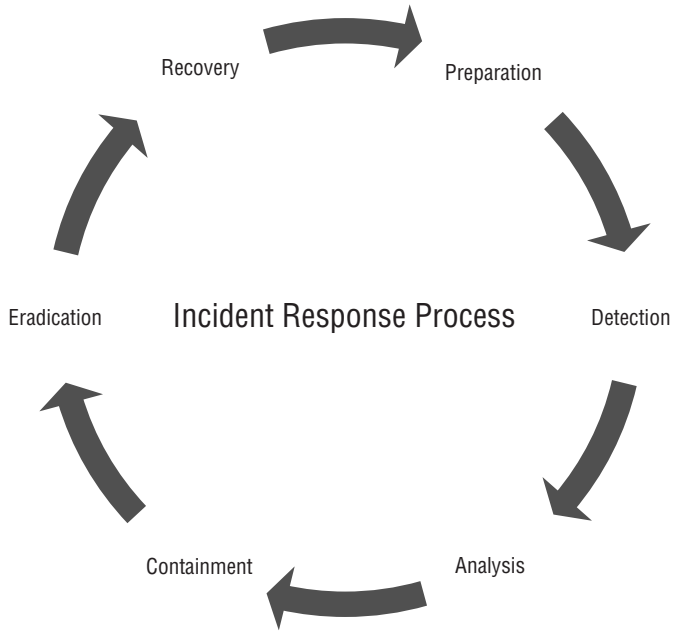


FIGURE 14.2 MITRE's ATT&CK framework example of attacks against cloud instances

Cloud Instance Metadata API

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.[1]

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, attackers may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows the attacker to gain access to the sensitive information via a request to the Instance Metadata API.[2]

The de facto standard across cloud service providers is to host the Instance Metadata API at `http[:]//169.254.169.254`.

ID: T1522
Tactic: Credential Access
Platform: AWS, GCP, Azure
Permissions Required: User
Data Sources: Azure activity logs, AWS CloudTrail logs, Authentication logs
Contributors: Praetorian
Version: 1.0

Mitigations

Mitigation	Description
Filter Network Traffic	Limit access to the Instance Metadata API using a host-based firewall such as iptables. A properly configured Web Application Firewall (WAF) may help prevent external adversaries from exploiting Server-side Request Forgery (SSRF) attacks that allow access to the Cloud Instance Metadata API. [2]

Detection

- Monitor access to the Instance Metadata API and look for anomalous queries.
- It may be possible to detect adversary use of credentials they have obtained. See Valid Accounts for more information.

References

1. AWS. (n.d.). Instance Metadata and User Data. Retrieved July 18, 2019.
2. Higashi, Michael. (2018, May 15). Instance Metadata API: A Modern Day Trojan Horse. Retrieved July 16, 2019.

FIGURE 14.3 The AlienVault SIEM default dashboard

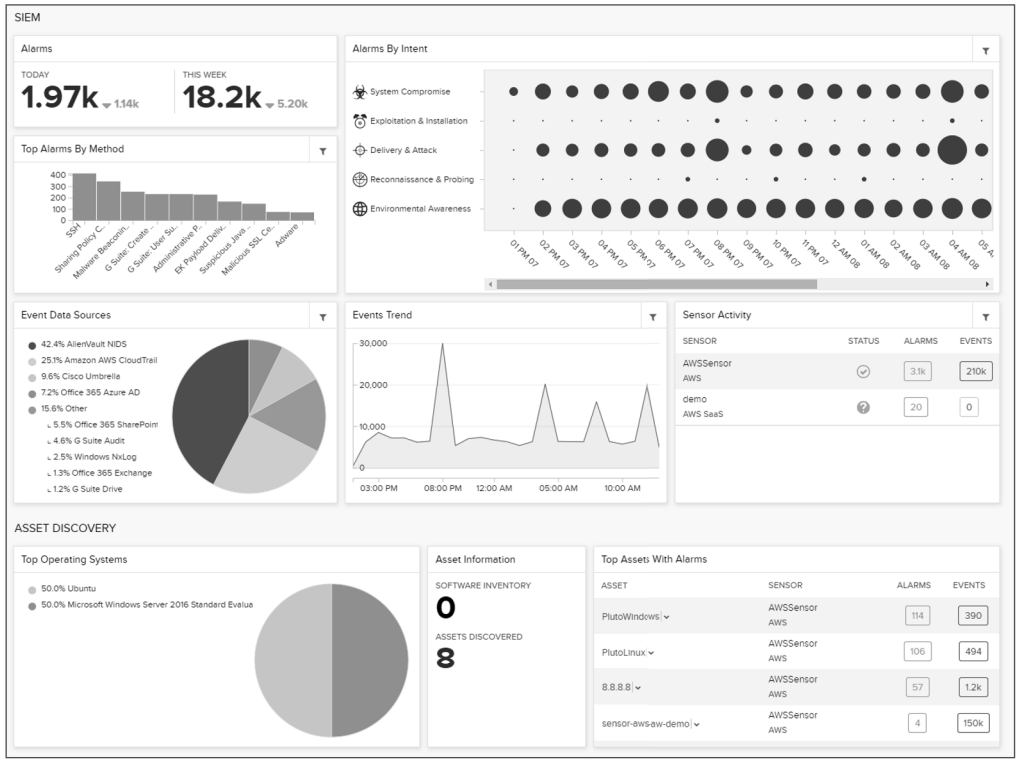


FIGURE 14.4 Trend analysis via a SIEM dashboard

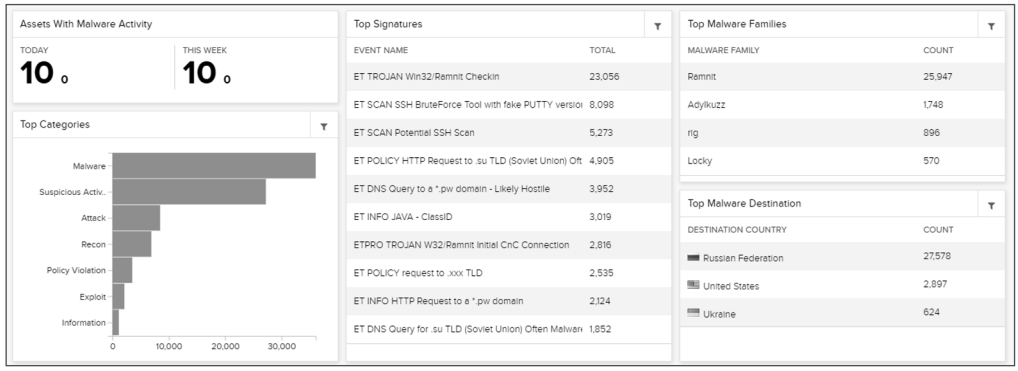


FIGURE 14.5 Alerts and alarms in the AlienVault SIEM

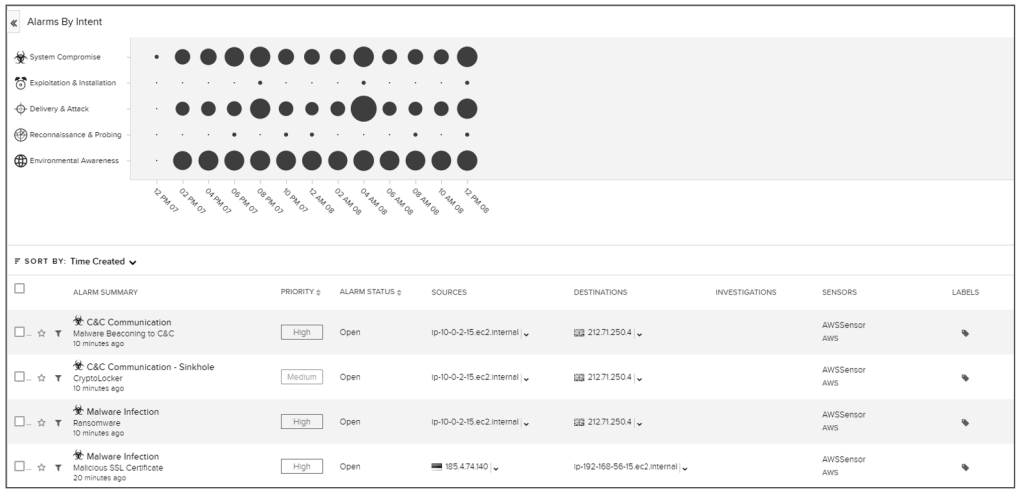


FIGURE 14.6 Rule configuration in AlienVault

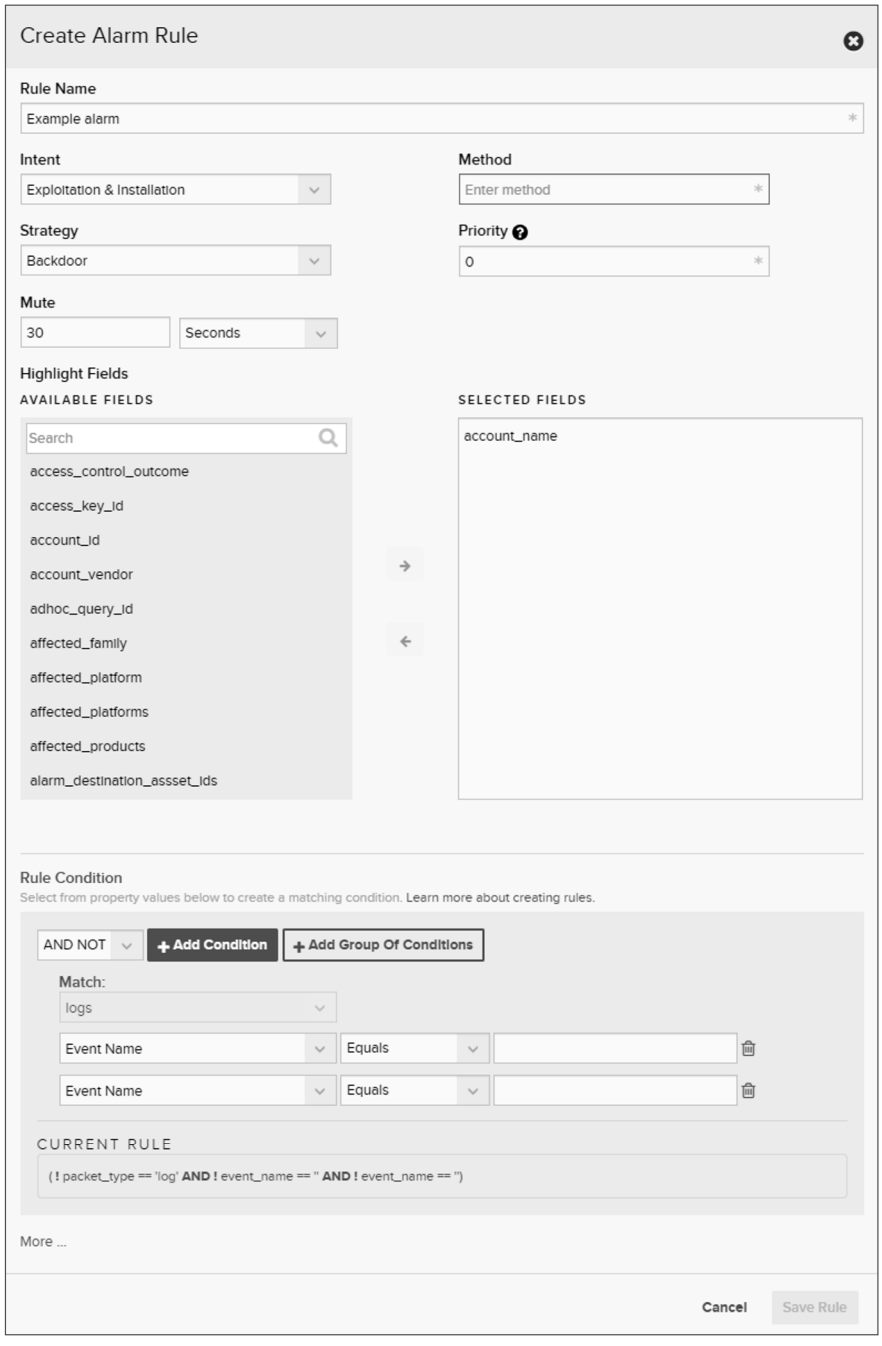
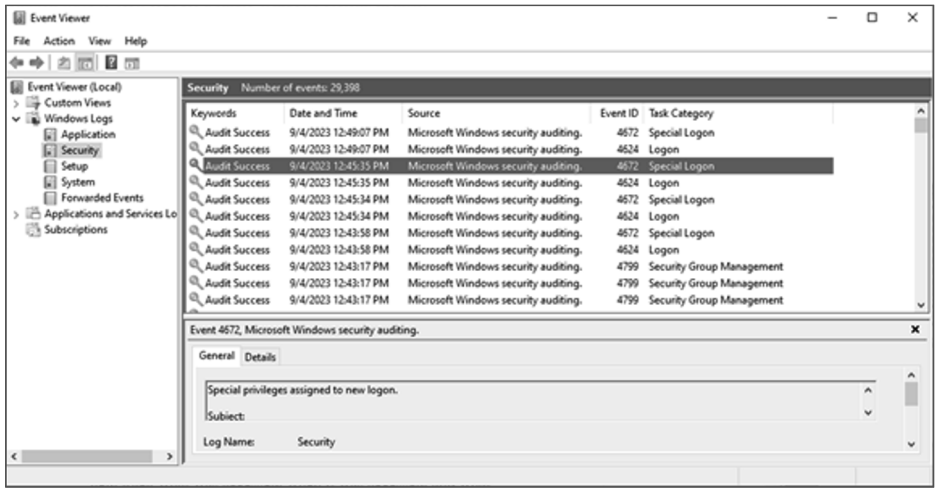


FIGURE 14.7 The Windows Event Viewer showing a security log with an audit event



Going with the Flow Graphic

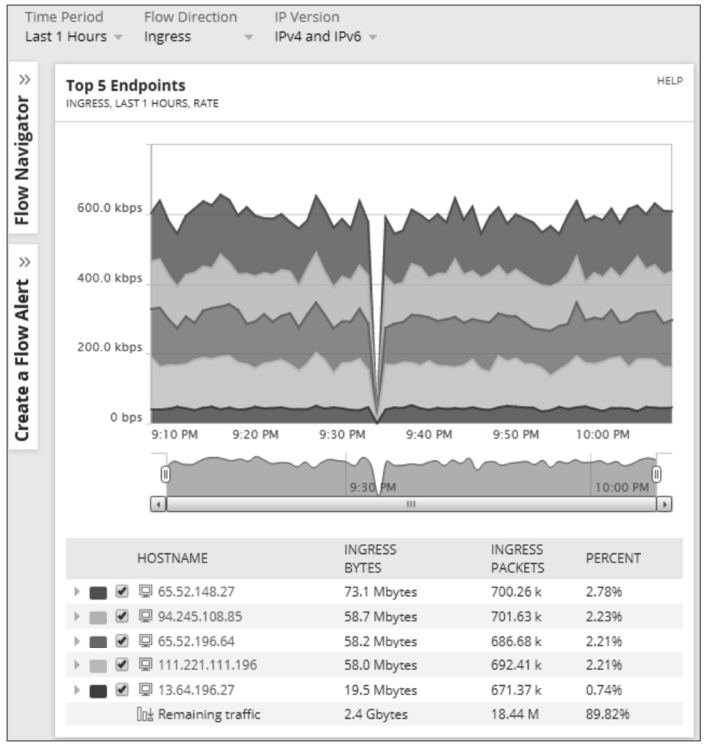
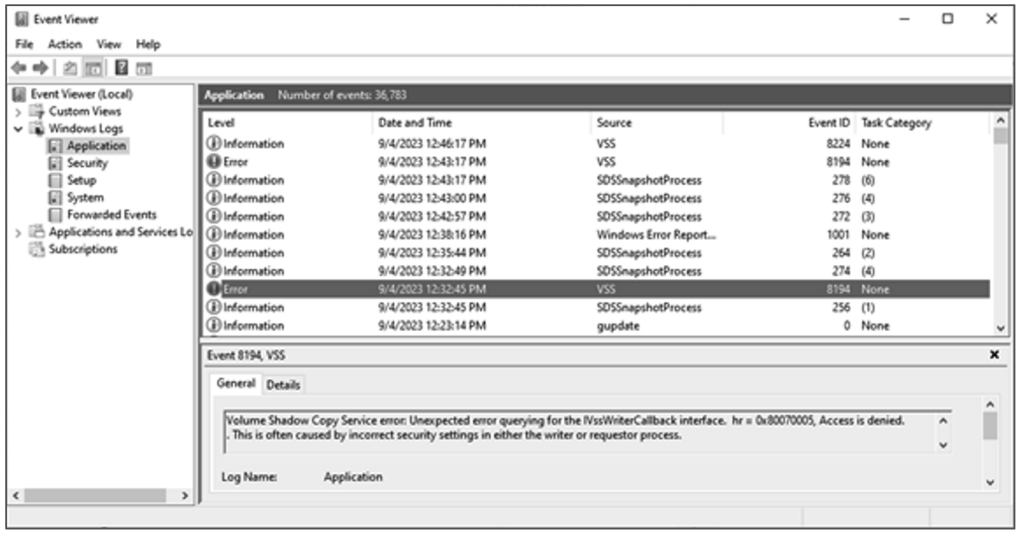


FIGURE 14.8 The Windows Event Viewer showing an application log event



Selected Metadata Recovered from a Photo Coding

```
File Size                       : 2.0 MB
File Modification Date/Time     : 2009:11:28 14:36:02-05:00
Make                            : Canon
Camera Model Name               : Canon PowerShot A610
Orientation                     : Horizontal (normal)
X Resolution                    : 180
Y Resolution                    : 180
Resolution Unit                 : inches
Modify Date                     : 2009:08:22 14:52:16
Exposure Time                   : 1/400
F Number                        : 4.0
Date/Time Original              : 2009:08:22 14:52:16
Create Date                     : 2009:08:22 14:52:16
Flash                           : Off, Did not fire
Canon Firmware Version          : Firmware Version 1.00
```

Chapter 14 Review: Security and Incident Response Cycle Figure (Question 1)

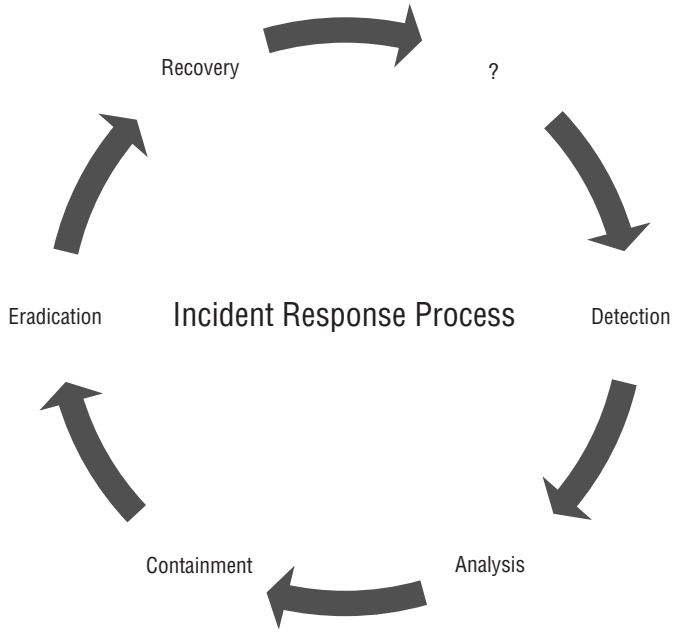


FIGURE 15.1 The order of volatility

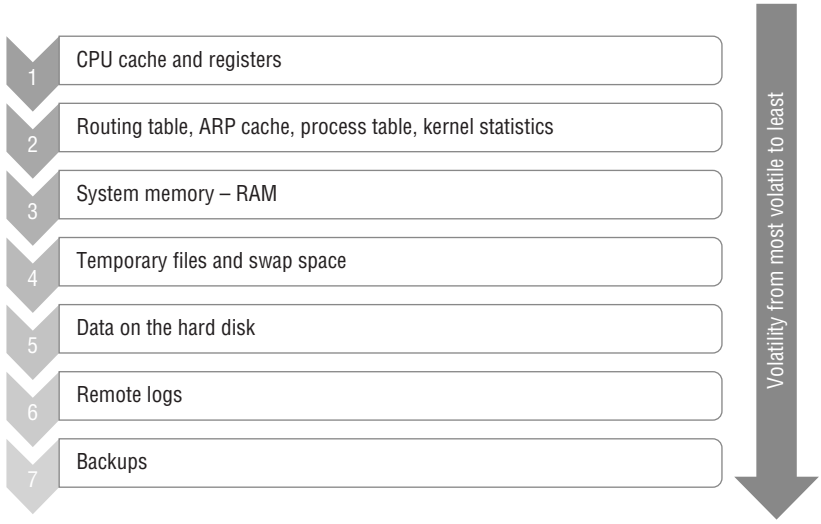


FIGURE 15.2 A sample chain-of-custody form

Case Number: _____ Item Number:_____
Evidence Description: _____
_____
_____
Collection method:_____
_____
Evidence storage method: _____
How is evidence secured? _____
Collected by: (Name/ID#) _____
Signature of collector:_____

Copy History		
Date	**Copied method**	**Disposition of original and all copies**

Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

FIGURE 15.3 Output from a completed FTK Imager image

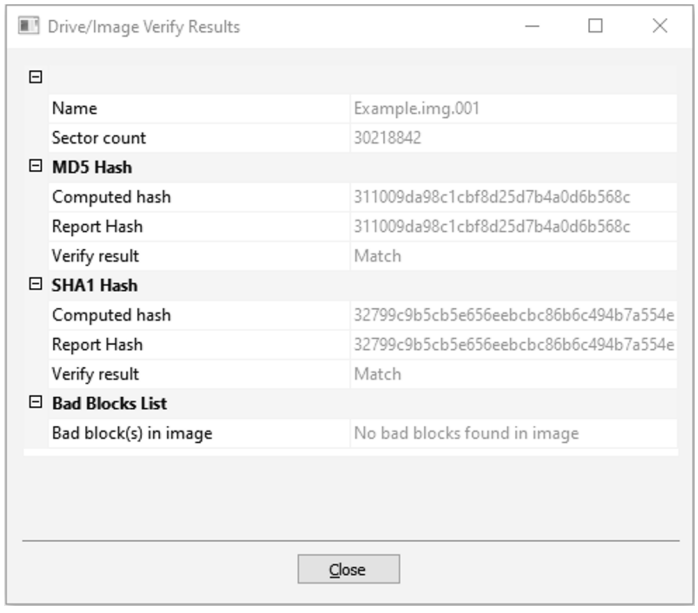


FIGURE 15.4 FTK Imager's Memory Capture dialog box

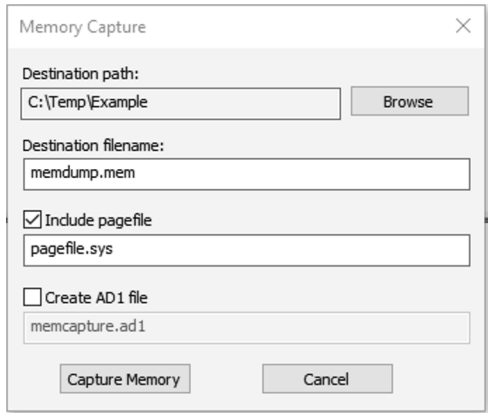


FIGURE 15.5 FTK Imager's evidence item documentation

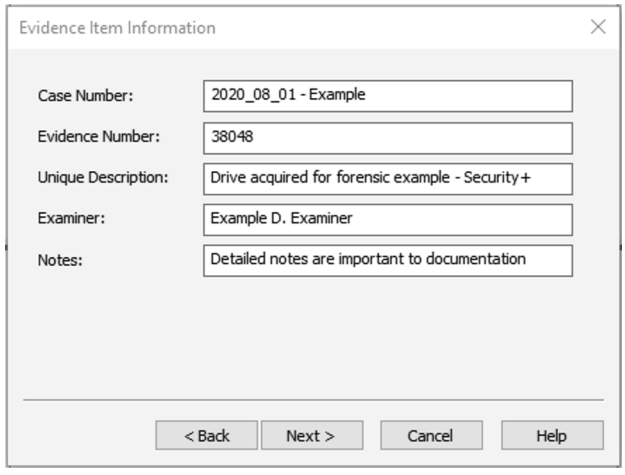


FIGURE 15.6 Selecting the type of image or data to import

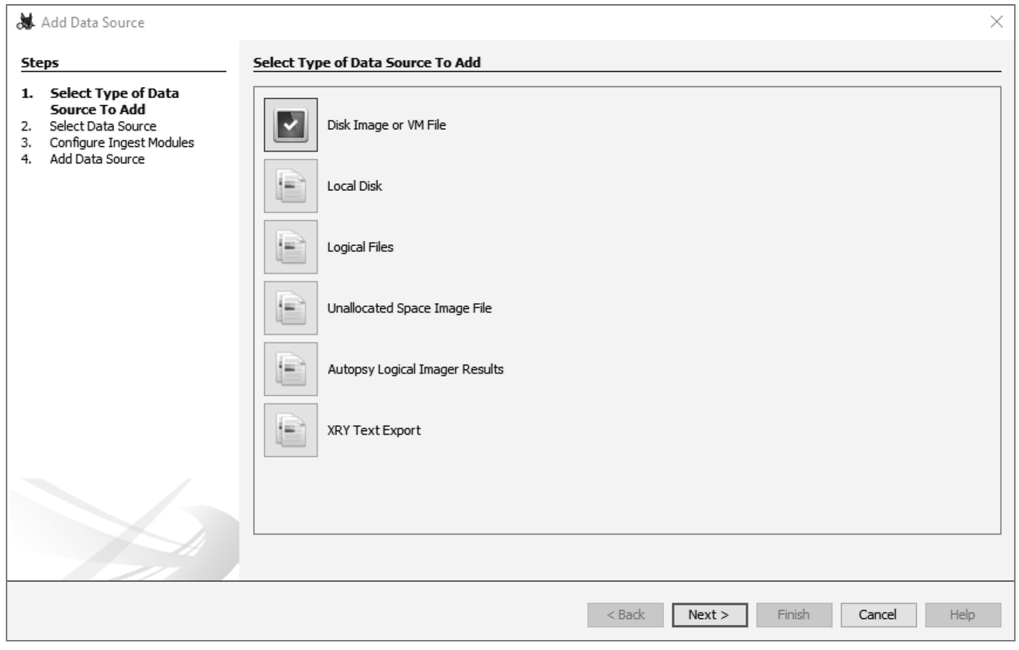


FIGURE 15.7 Ingestion modules in Autopsy

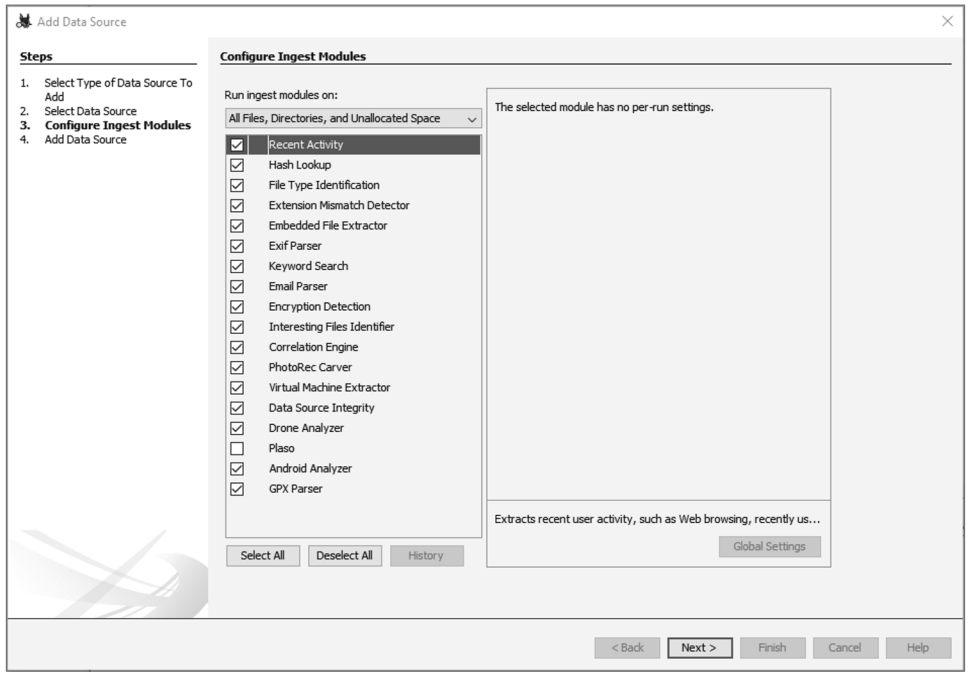


FIGURE 15.8 Using the Autopsy file discovery tool to identify images in an investigation

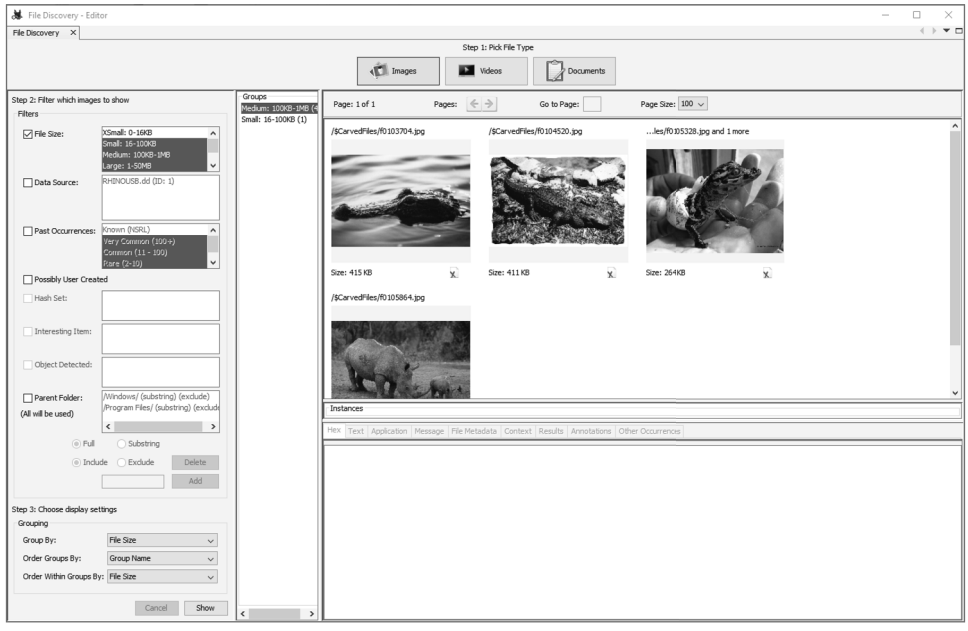


FIGURE 15.9 Timelining in Autopsy to identify events related to the investigation

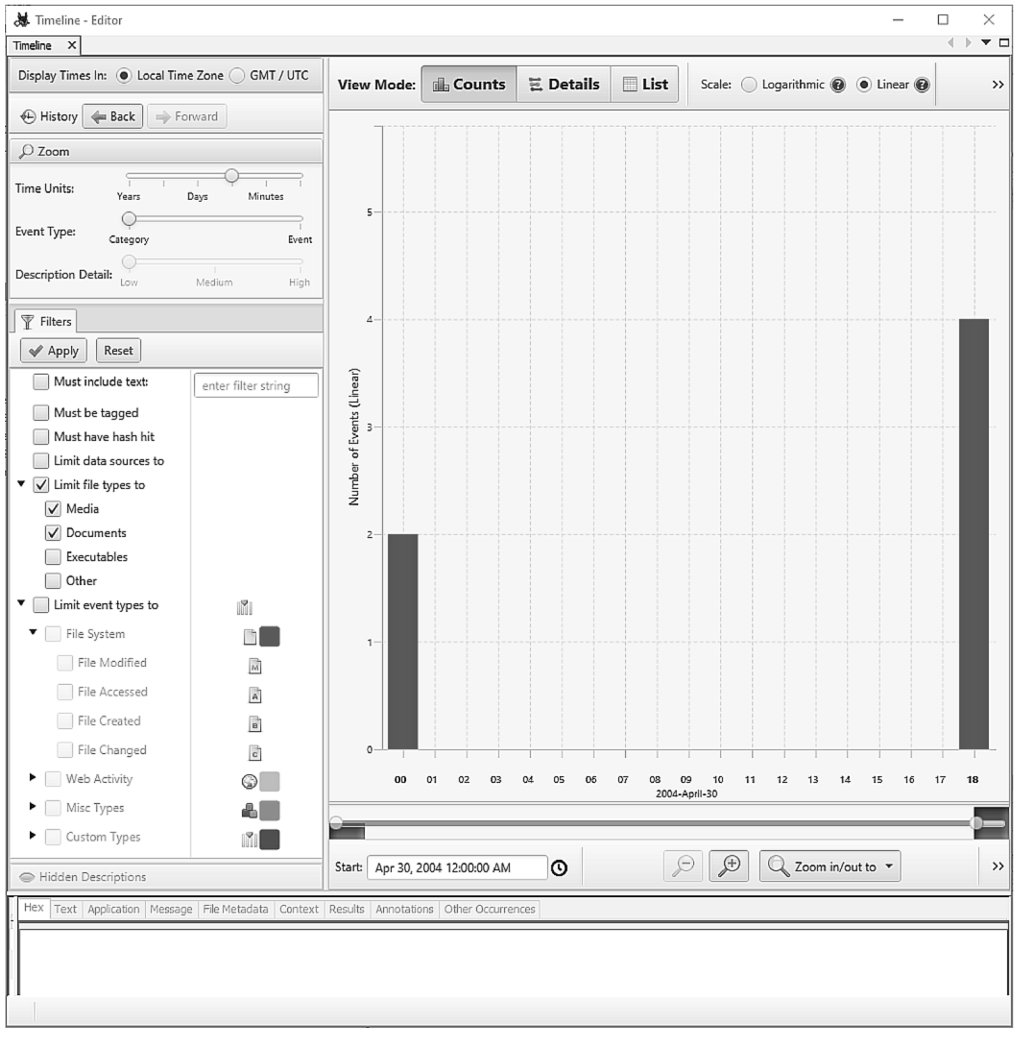


FIGURE 16.1 Typical corporate governance model

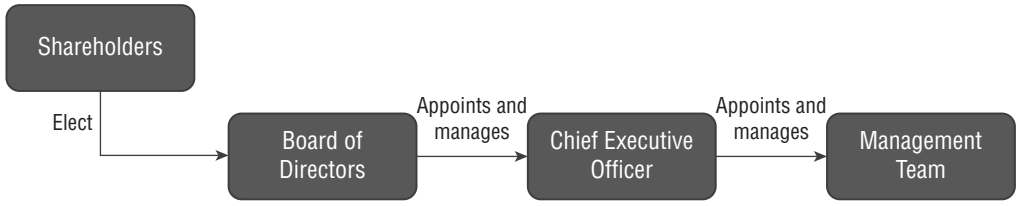
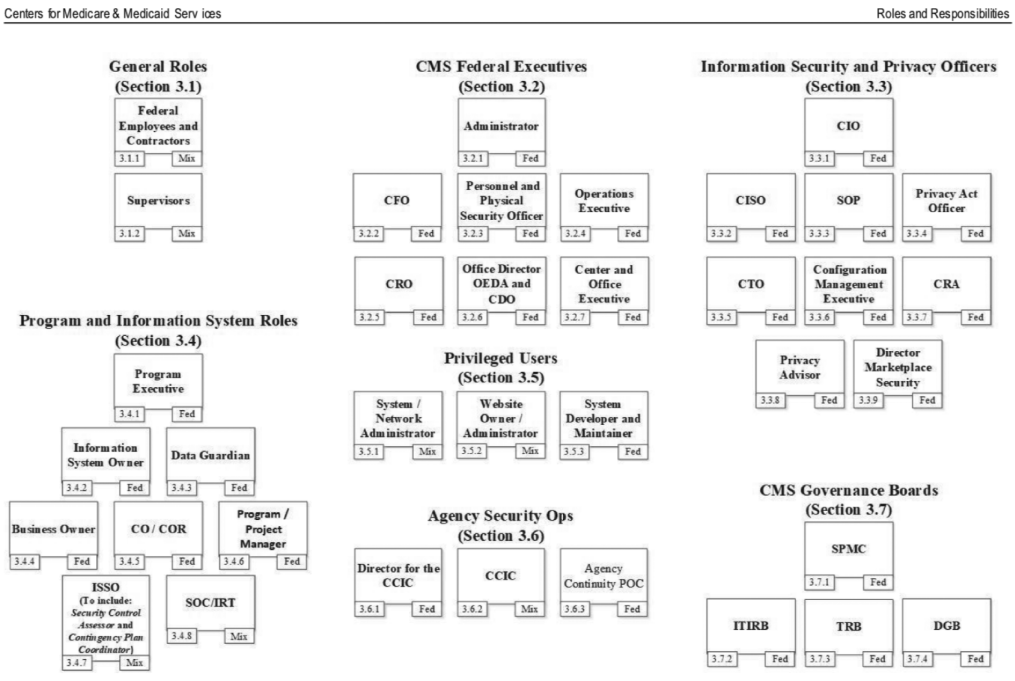


FIGURE 16.2 Excerpt from CMS roles and responsibilities chart



Source: Centers for Medicare and Medicaid Services Information Systems Security and Privacy Policy, May 21, 2019. (www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/CMS-IS2P2.pdf)

FIGURE 16.3 Excerpt from UC Berkeley Minimum Security Standards for Electronic Information

MSSEI Controls	DPL 0 (TBD)	DPL 1 Individual	DPL 1 Privileged	DPL 1 Institutional	DPL 2 Individual	DPL 2 Privileged	DPL 2 Institutional	DPL 3 (TBD)	Guidelines
1.1 Removal of non-required covered data		o	√	√	√	√	√		see secure deletion guideline and UCOP disposition schedules database
1.2 Covered system inventory			√	√		√	√		1.2 guideline
1.3 Covered system registration			+	√		√	√		1.3 guideline
1.4 Annual registration renewal			√	√		√	√		1.4 guideline
2.1 Managed software inventory			+	√	o	√	√		2.1 guideline
3.1 Secure configurations		o	+	√	√	√	√		3.1 guideline
4.1 Continuous vulnerability assessment & remediation			+	√		√	√		4.1 guideline

Source: University of California at Berkeley Minimum Security Standards for Electronic Information

FIGURE 16.4 Web server and database server

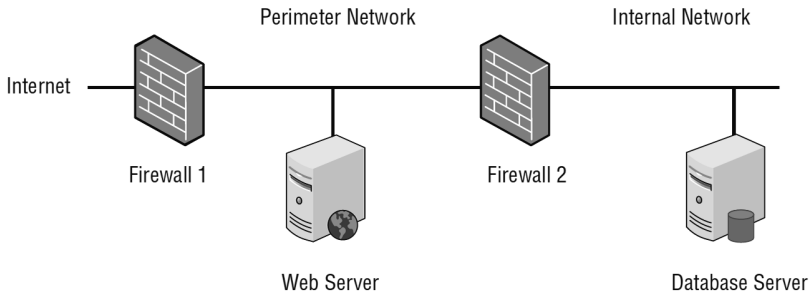
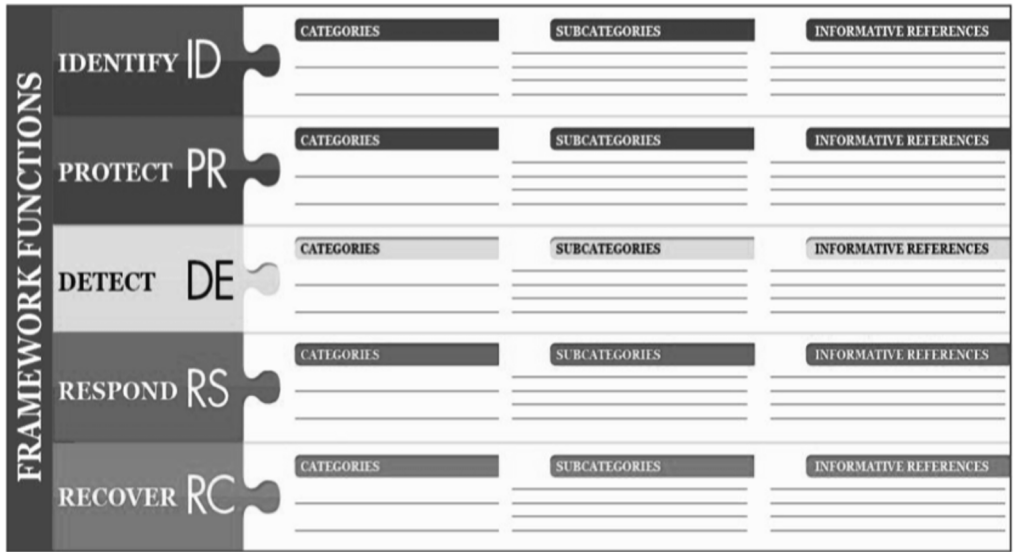


FIGURE 16.5 NIST Cybersecurity Framework Core Structure



Source: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology (`http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf`)

TABLE 16.1 NIST Cybersecurity Framework implementation tiers

Tier	Risk management process	Integrated risk management program	External participation
Tier 1: Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.	There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.	The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organization-wide policy.	There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.	Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both.
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy.	There is an organization-wide approach to manage cybersecurity risk.	The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks.
Tier 4: Adaptive	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.	The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks.

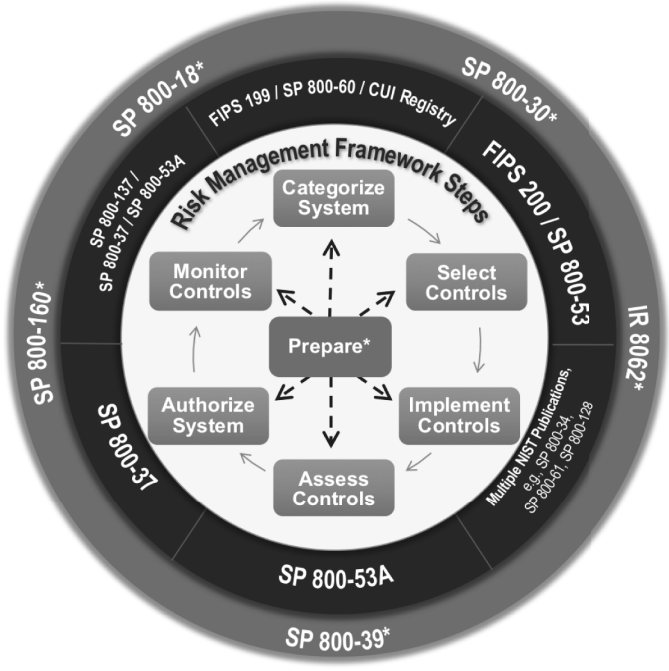
Source: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology

FIGURE 16.6 Asset Management Cybersecurity Framework

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

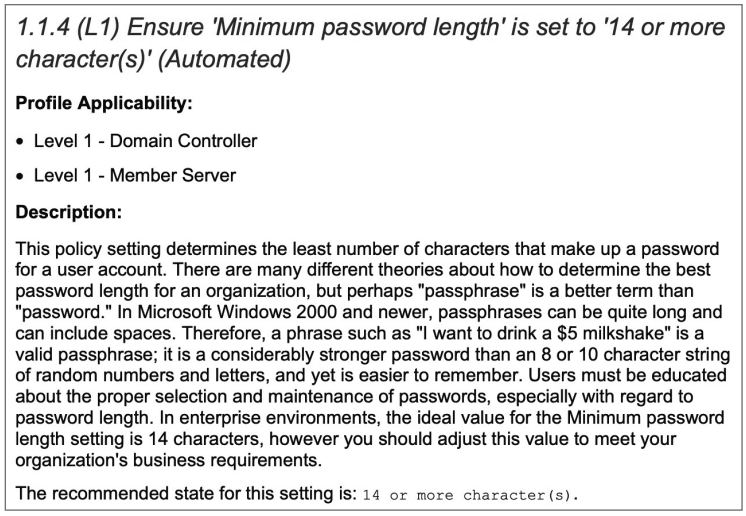
Source: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology (`http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf`)

FIGURE 16.7 NIST Risk Management Framework



Source: FISMA Implementation Project Risk Management Framework (RMF) Overview, National Institute of Standards and Technology `http://csrc.nist.gov/projects/risk-management/rmf-overview`

FIGURE 16.8 Windows Server 2022 Security Benchmark Excerpt



1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

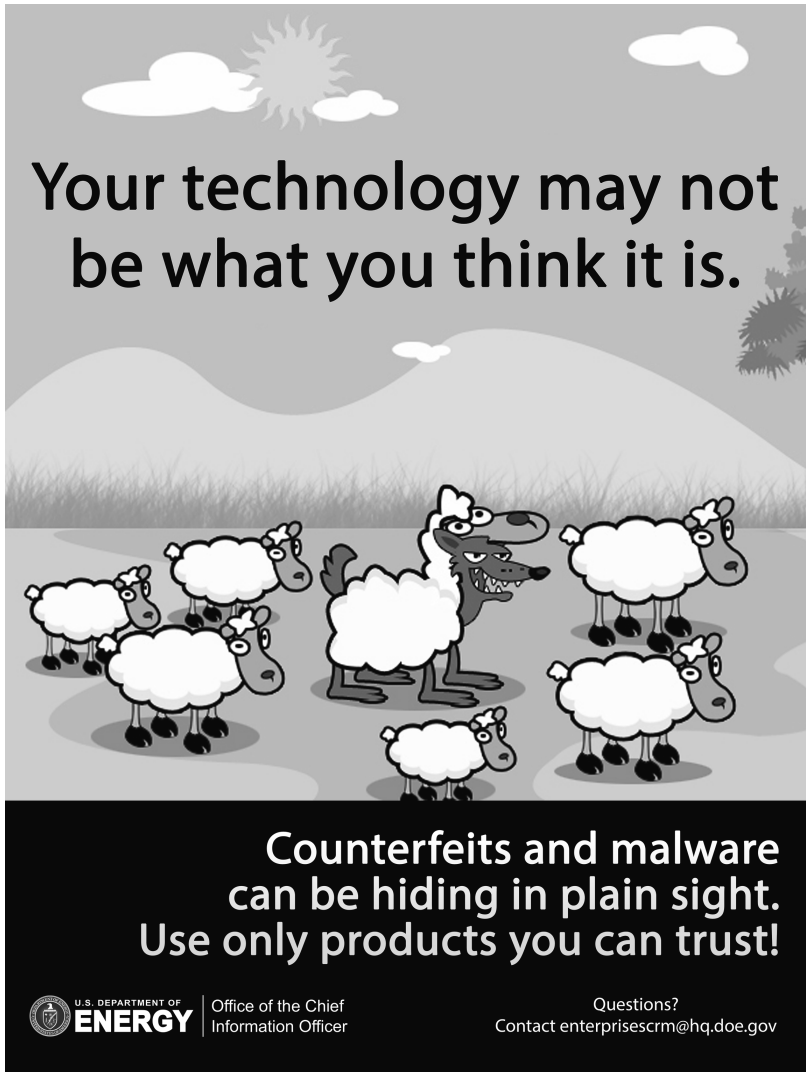
Description:

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements.

The recommended state for this setting is: `14 or more character(s).`

Source: Center for Internet Security (CIS) (`http://cisecurity.org/cis-benchmarks`)

FIGURE 16.9 Security awareness poster



Source: U.S. Department of Energy

FIGURE 17.1 Risk exists at the intersection of a threat and a corresponding vulnerability.

FIGURE 17.2 Qualitative risk analyses use subjective rating scales to evaluate probability and magnitude.

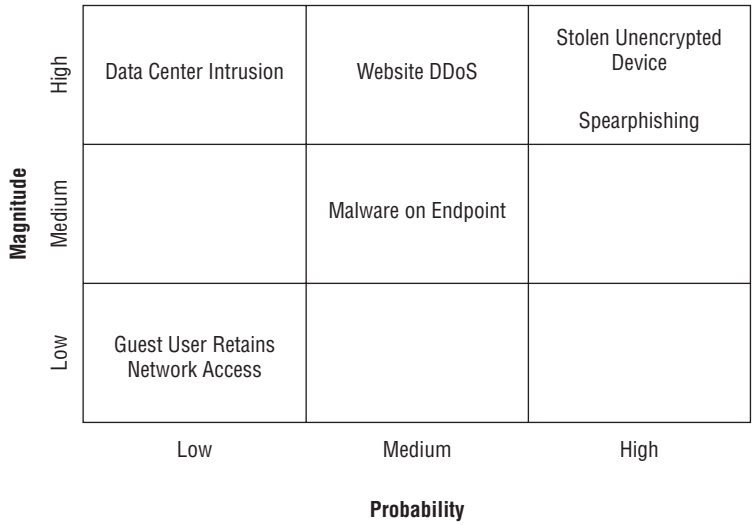


FIGURE 17.3 (a) STOP tag attached to a device. (b) Residue remaining on device after attempted removal of a STOP tag.

(a) (b)

FIGURE 17.4 Risk register excerpt

ID	Risk Statement	Risk Causes	Risk Impacts	Likelihood	Impact	Score
20	No coordinated vetting and review process for third-party or cloud-computing services used to store, process, or transmit institutional data	Lack of senior management support; lack of communication of central vetting process to staff/employees; failure to understand the need to protect institutional data	Multiple redundant services in place (inefficient and costly for the institution); institution unaware who its business partners are; institution unaware if institutional data are held by third parties; institution unable to ensure that third parties are following compliance requirements	1	2	2
21	Failure to create and maintain sufficient and current policies and standards to protect the confidentiality, integrity, and availability of institutional data and IT resources (e.g., hardware, devices, data, and software)	Lack of senior management support; failure to understand information security concepts; lack of funding to support policy development activities; lack of funding for training; lack of user training	Improper use of university IT systems and institutional data; failure of users to protect critical institutional data when using IT resources (leading to data breach); institution subject to regulatory violations and fines; institutional reputation loss; poor perception/reputation of IT	2	3	6
22	Data breach or leak of sensitive information (e.g., academic, business, or research data)	Lack of senior management support; complex regulatory environments impacting higher education IT systems and data (e.g., FERPA, HIPAA, GLBA, PCI, accessibility, export controls, etc.); complexity of IT systems, infrastructure, and services; lack of funding for data handling training; lack of user training; intentional user malfeasance; unintentional user error; hacking or infiltration by third parties	Institution subject to regulatory violations and fines; costs of breach notification; costs of redress for individuals; loss of alumni donations; loss of research data; costs to mitigate underlying breach event; institutional reputation loss; poor perception/reputation of IT	3	3	9

Source: EDUCAUSE IT Risk Register (`http://library.educause.edu/resources/2015/10/it-risk-register`)

FIGURE 17.5 Risk matrix

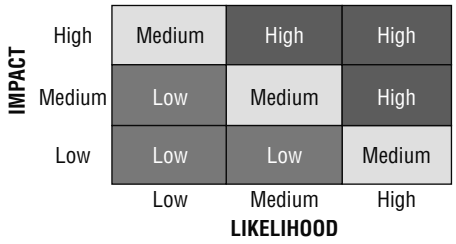
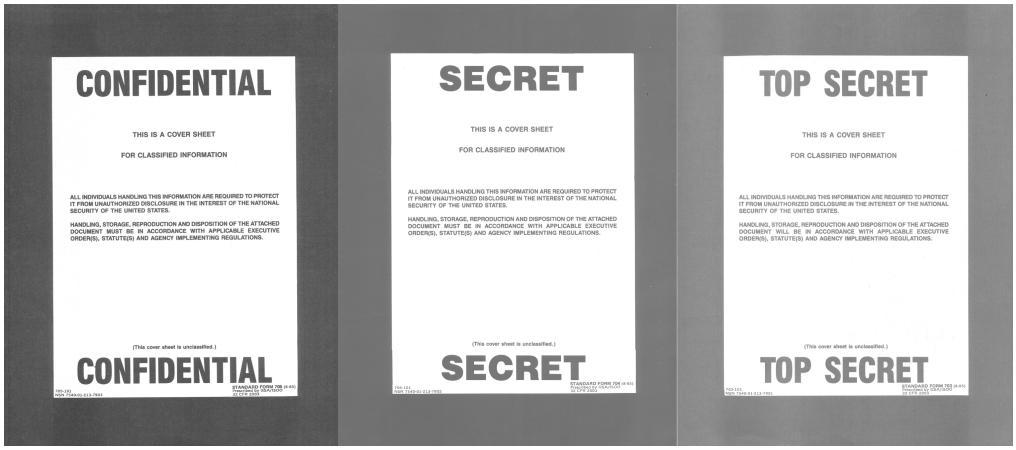
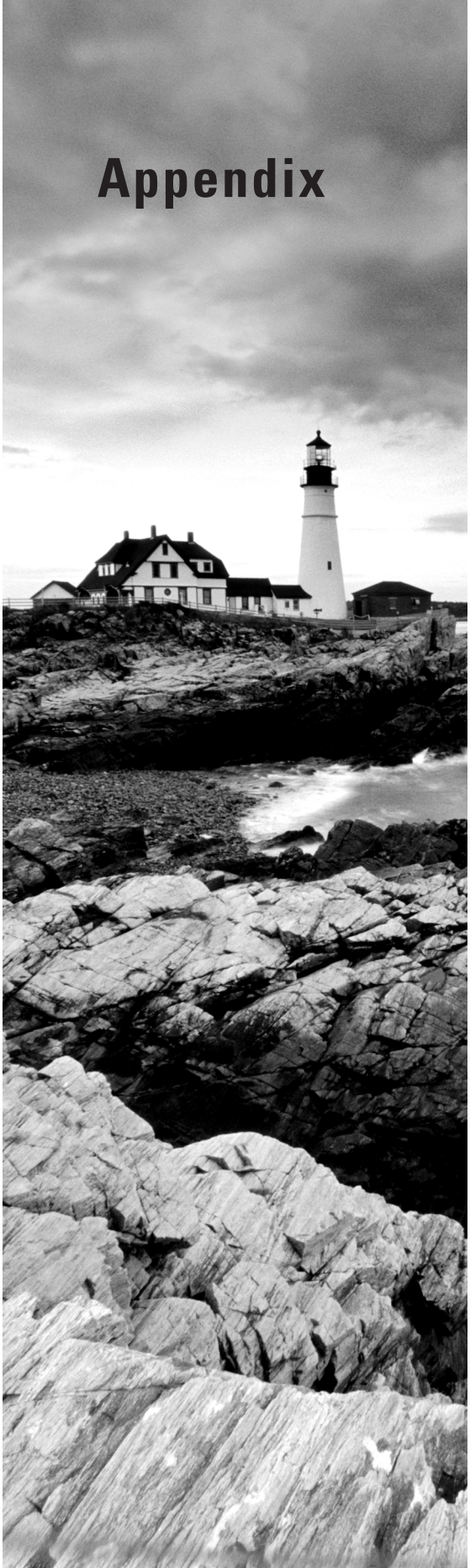


FIGURE 17.6 Cover sheets used to identify classified U.S. government information





Appendix

Answers to Review Questions

Chapter 1: Today's Security Professional

1. D. Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Threat assessment is an example of one of these activities.

2. B. The breach of credit card information may cause many different impacts on the organization, including compliance, operational, and financial risks. However, in this scenario, Jade's primary concern is violating PCI DSS, making his concern a compliance risk.

3. C. The defacement of a website alters content without authorization and is, therefore, a violation of the integrity objective. The attackers may also have breached the confidentiality or availability of the website, but the scenario does not provide us with enough information to draw those conclusions.

4. B. In this case, the first 12 digits of the credit card have been removed and replaced with asterisks. This is an example of data masking.

5. D. Deterrent controls are designed to prevent an attacker from attempting to violate security policies in the first place. Preventive controls would attempt to block an attack that was about to take place. Corrective controls would remediate the issues that arose during an attack. Detective controls detect issues or indicators of issues.

6. D. In this case, Greg must use a network-based DLP system. Host-based DLP requires the use of agents, which would not be installed on guest systems. Greg may use watermarking and/or pattern recognition to identify the sensitive information, but he must use network-based DLP to meet his goal.

7. B. Data being sent over a network is data in transit. Data at rest is stored data that resides on hard drives, tapes, in the cloud, or on other storage media. Data in processing, or data in use, is data that is actively in use by a computer system.

8. A. Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.

9. D. The three primary goals of cybersecurity attackers are disclosure, alteration, and denial. These map directly to the three objectives of cybersecurity professionals: confidentiality, integrity, and availability.

10. A. The risk that Tony is contemplating could fit any one of these categories. However, his primary concern is that the company may no longer be able to do business if the risk materializes. This is a strategic risk.

11. C. Although it is possible that a frequent flyer account number, or any other account number for that matter, could be used in identity theft, it is far more likely that identity thieves would use core identity documents. These include drivers' licenses, passports, and Social Security numbers.

12. A. As an organization analyzes its risk environment, technical and business leaders determine the level of protection required to preserve the confidentiality, integrity, and availability of their information and systems. They express these requirements by writing the control

objectives that the organization wishes to achieve. These control objectives are statements of a desired security state.

13. D. This question is a little tricky. The use of an actual guard dog could be considered a deterrent, physical, or detective control. It could even be a compensating control in some circumstances. However, the question asks about the presence of a *sign* and does not state that an actual dog is used. The sign only has value as a deterrent control. Be careful when facing exam questions like this to read the details of the question.

14. D. Encryption technology uses mathematical algorithms to protect information from prying eyes, both while it is in transit over a network and while it resides on systems. Encrypted data is unintelligible to anyone who does not have access to the appropriate decryption key, making it safe to store and transmit encrypted data over otherwise insecure means.

15. D. The use of full-disk encryption is intended to prevent a security incident from occurring if a device is lost or stolen. Therefore, this is a preventive control gap.

16. A. Although a health-care provider may be impacted by any of these regulations, the Health Insurance Portability and Accountability Act (HIPAA) provides direct regulations for the security and privacy of protected health information and would have the most direct impact on a health-care provider.

17. C. The disclosure of sensitive information to unauthorized individuals is a violation of the principle of confidentiality.

18. B. The three primary objectives of cybersecurity professionals are confidentiality, integrity, and availability.

19. A. Tokenization techniques use a lookup table and are designed to be reversible. Masking and hashing techniques replace the data with values that can't be reversed back to the original data if performed properly. Shredding, when conducted properly, physically destroys data so that it may not be recovered.

20. A. PCI DSS compensating controls must be "above and beyond" other PCI DSS requirements. This specifically bans the use of a control used to meet one requirement as a compensating control for another requirement.

Chapter 2: Cybersecurity Threat Landscape

1. B. Although higher levels of detail can be useful, they aren't a common measure used to assess threat intelligence. Instead, the timeliness, accuracy, and relevance of the information are considered critical to determining whether you should use the threat information.

2. C. Hacktivists are defined by the motivation behind their actions—advancing their political or philosophical beliefs. They engage in cyberattacks that they believe will advance their causes.

3. A. Attacks that are conducted as part of an authorized penetration test are white-hat hacking attacks, regardless of whether they are conducted by internal employees or an external firm. Kolin is, therefore, engaged in white-hat hacking. If he were acting on his own, without authorization, his status would depend on his intent. If he had malicious intent, his activity would be considered black-hat hacking. If he simply intended to report vulnerabilities to the hospital, his attack would be considered gray hat and he would likely be semi-authorized.

4. A. Advanced persistent threats (APTs) are most commonly associated with nation-state actors. It is unlikely that an APT group would leverage the unsophisticated services of an unskilled script kiddie type attacker. It is also unlikely that a hacktivist would have access to APT resources. Although APTs may take advantage of insider access, they are most commonly associated with nation-state actors.

5. D. The U.S. government created the Information Sharing and Analysis Centers (ISACs). ISACs help infrastructure owners and operators share threat information, and provide tools and assistance to their members.

6. A. Nation-state actors are government sponsored, and they typically have the greatest access to resources, including tools, money, and talent.

7. A. Email is the most common threat vector exploited by attackers who use phishing and other social engineering tactics to gain access to an organization. The other vectors listed here, direct access, wireless, and removable media, all require physical proximity to an organization and are not easily executed from a remote location.

8. D. The Chinese military and U.S. government are examples of nation-state actors and advanced persistent threats (APTs). The Russian mafia is an example of a criminal syndicate. Anonymous is the world's most prominent hacktivist group.

9. A. Behavioral assessments are very useful when you are attempting to identify insider threats. Since insider threats are often hard to distinguish from normal behavior, the context of the actions performed—such as after-hours logins, misuse of credentials, logins from abnormal locations, or abnormal patterns—and other behavioral indicators are often used.

10. D. Supply chain attacks are typically associated with vendors and suppliers that provide technology infrastructure or services that may be compromised. This would include hardware and software providers as well as managed service providers (MSPs). Talent providers, who help with staffing solutions, are generally not considered common avenues for supply chain attacks.

11. A. Tampering with equipment before it reaches the intended user is an example of a supply chain threat. It is also possible to describe this attack as a direct access attack because it involved physical access to the device, but supply chain is a more relevant answer. You should be prepared to select the best possible choice from several possible correct answers when you take the exam. Security+ questions often use this type of misdirection.

12. B. All of these resources might contain information about the technical details of TLS, but Internet Request for Comments (RFC) documents are the definitive technical standards for Internet protocols. Consulting the RFCs would be Ken's best option.

13. C. All of these items could be concerning, depending on the circumstances. However, API keys should *never* be found in public repositories because they may grant unauthorized individuals access to information and resources.

14. A. Threat maps are graphical tools that display information about the geographic locations of attackers and their targets. These tools are most often used as interesting marketing gimmicks, but they can also help identify possible threat sources.

15. B. Specific details of attacks that may be used to identify compromises are known as indicators of compromise (IoCs). This data may also be described as an adversary tactics, techniques, and procedures (TTP), but the fact that it is a set of file signatures makes it more closely match the definition of an IoC.

16. A. The developers in question are using unapproved technology for business purposes. This is the classic definition of shadow IT. It is possible to describe this as data exfiltration, but there is no indication that the data security has been compromised, so shadow IT is a better description here. Remember, you will often be asked to choose the best answer from multiple correct answers on the exam.

17. A. Tom's greatest concern should be that running unsupported software exposes his organization to the risk of new, unpatchable vulnerabilities. It is certainly true that they will no longer receive technical support, but this is a less important issue from a security perspective. There is no indication in the scenario that discontinuing the product will result in the theft of customer information or increased costs.

18. C. Port scans are an active reconnaissance technique that probe target systems and would not be considered open source intelligence (OSINT). Search engine research, DNS lookups, and WHOIS queries are all open source resources.

19. A, C. As a government contractor, Snowden had authorized access to classified information and exploited this access to make an unauthorized disclosure of that information. This clearly makes him fit into the category of an insider. He did so with political motivations, making him fit the category of hacktivist as well.

20. C. Renee was not authorized to perform this security testing, so her work does not fit into the category of white-hat hacking, or authorized hacking. However, she also does not have malicious intent, so her work cannot be categorized as an unauthorized, or black-hat attack. Instead, it fits somewhere in between the two extremes and would best be described as semi-authorized, or gray-hat hacking.

Chapter 3: Malicious Code

1. B. Logic bombs are embedded in code, so Ryan's organization would get the most benefit from a code review process for any code that goes into production. Antivirus and EDR are unlikely to detect logic bombs created by staff in Ryan's organization.

2. C. Rootkits are intended to be stealthy, and a pop-up demanding ransom works against that purpose. File hashes, command and control details, and behavior-based identifiers are all useful IoCs likely to be relevant to a rootkit.

3. A. Nathan should check the staff member's computer for a keylogger, which would have captured their username and password. A student could have then used the staff member's credentials to make the changes described. A rootkit would be used to retain access, spyware

gathers a variety of data but is not specifically aimed at capturing keystrokes like this, and logic bombs have specific events or triggers that cause them to take action.

4. A. Amanda has most likely discovered a botnet's command and control channel, and the system or systems she is monitoring are probably using IRC as the command and control channel. Spyware is likely to simply send data to a central server via HTTP/HTTPS, worms spread by attacking vulnerable services, and a hijacked web browser would probably operate on common HTTP or HTTPS ports (80/443).

5. D. Remote access to a system is typically provided by a backdoor. Backdoors may also appear in firmware or even in hardware. None of the other items listed provide remote access by default, although they may have a backdoor as part of a more capable malware package.

6. A. Bloatware is typically not a significant security threat, but it consumes resources like disk space, CPU, and memory. Unfortunately, some bloatware can be vulnerable and may not get regularly patched, meaning it's both useless and a potential risk!

7. C. Spyware is specifically designed to gather information about users and systems and to send that data back to a central collector. Trojans pretend to be useful software and include malicious components, bloatware is preinstalled software that isn't needed, and rootkits are used to conceal malicious software and retain a foothold on compromised systems.

8. D. One of the challenges security practitioners can face when attempting to identify malware is that different antivirus and antimalware vendors will name malware packages and families differently. This means that Matt may need to look at different names to figure out what he is dealing with.

9. D. While keyloggers often focus on keyboard input, other types of input may also be captured, meaning Nancy should worry about any user input that occurred while the keylogger was installed. Keyloggers typically do not target files on systems, although if Nancy finds a keylogger, she may want to check for other malware packages with additional capabilities.

10. C. Ransomware demands payment to be made while typically using encryption to make data inaccessible. Worms, viruses, and rootkits are not defined by behavior like this.

11. B. Rootkits are designed to hide from antimalware scanners and can often defeat locally run scans. Mounting the drive in another system in read-only mode or booting from a USB drive and scanning using a trusted, known good operating system can be an effective way to determine what malware is on a potentially infected system.

12. C. Jaya's former employee is describing a logic bomb, malicious code that will cause harm when a trigger or specific action occurs. In this case, the former employee is claiming that the trigger is them not being employed at the company. Jaya will need to assess all of the code that the employee wrote to determine if a logic bomb exists. Ransomware is a type of malicious software that typically uses encryption to extort a ransom. Extortionware is not a commonly used term. Trojans appear to be useful or desirable software but contain malicious code.

13. B. In most malware infection scenarios, wiping the drive and reinstalling from known good media is the best option available. If the malware has tools that can infect the system BIOS/UEFI, even this may not be sufficient, but BIOS/UEFI resident malware is relatively uncommon. Multiple antivirus and antimalware tools, even if they are set to delete malware,

may still fail against unknown or advanced malware packages. Destroying systems is uncommon, expensive, and unlikely to be acceptable to most organizations as a means of dealing with a malware infection.

14. B. The key difference between worms and viruses is how they spread. Worms spread themselves, whereas viruses rely on human interaction.

15. B. Python is an interpreted rather than a compiled language, so Ben doesn't need to use a decompiler. Instead, his best bet is to open the file and review the code to see what it does. Since it was written by an employee, it is unlikely that it will match an existing known malicious package, which means antivirus and antimalware tools and sites will be useless.

16. B. Trojans are often found in application stores where they appear to be innocuous but desirable applications or are listed in confusingly similar ways to legitimate applications. Many organizations choose to lock down the ability to acquire applications from app stores to prevent this type of issue. Since Trojans do not self-spread and rely on user action, patching typically won't prevent them. While users may try to transfer files via USB, this isn't the most common means for modern Trojans to spread.

17. C. Worms often spread via networks, taking advantage of vulnerabilities to install themselves on targeted systems and then to propagate further. Trojans require human interaction to install software that appears desirable. Logic bombs are embedded in code and perform actions when triggers like a date or event occur. Rootkits are used to hide malware and to conceal attacker's actions.

18. D. Unwanted, typically preinstalled programs are known as bloatware. They take up space and resources without providing value, and many organizations either uninstall them or install clean operating system images to avoid them. There is no indication of malicious activity in the question, so these are most likely not viruses, Trojans, or spyware.

19. A. Bots connect to command and control (C&C) systems, allowing them to be updated, controlled, and managed remotely. Worms spread via vulnerabilities, and drones and vampires aren't common terms for malware.

20. A. Randy knows that viruses spread through user interaction with files on thumb drives. A worm would spread itself, a Trojan would look like a useful or desirable file, and there is no indication of spyware in the question.

Chapter 4: Social Engineering and Password Attacks

1. B. This email is an attempt to get account information and is a phishing email. Joseph did not enter the URL himself, which is the behavior that a typosquatter relies on. A smishing attack relies on SMS, and a watering hole attack uses a frequently visited website.

2. D. Vishing is a form of phishing done via voice phones call or voicemail. Whaling focuses on targeting important targets for phishing attacks, whereas spoofing is a general term that means faking things. Spooning is not a technical term used for security practices.

3. A. Michele has discovered a brute-force attack, which relies on trying a large number of passwords, often combined with a list of usernames to try. Shoulder surfing attacks involve an attacker watching as a user enters information like a password or credit card data. On-path attacks intercept data sent via a network, and pretexting is a social engineering attack that relies on a believable reason for attackers to need a victim to take action.

4. C. Password spraying involves the use of the same password to attempt to log into multiple accounts. Joanna should search for uses of the same password for different accounts.

5. B. Susan has most likely discovered a business email compromise and should reach out to the impacted organization to inform them of the potentially compromised account. Smishing would occur via SMS, there is nothing in the question to indicate a disinformation campaign was part of this, and there is no URL mentioned and thus typosquatting can be dismissed as well.

6. A. Watering hole attacks rely on compromising or infecting a website that targeted users frequently visit, much like animals will visit a common watering hole. Vishing is phishing via voice, whaling is a targeted phishing attack against senior or important staff, and typosquatting registers similar URLs that are likely to be inadvertently entered in order to harvest clicks or conduct malicious activity.

7. D. The source IP or hostname; the failed login logs with time, date, username, and other information; and the password that was used for each failed attempt would be useful for watching for brute-force attempts. Knowing where the system being logged into is located isn't useful when tracking brute-force attempts. Logging failed passwords can be problematic as it can reveal actual passwords by allowing log reviewers to see failures driven by typos, so Ben may want to avoid that sort of log even though it can be useful!

8. B. The caller is using pretexting, providing Melissa with a story that relies on urgency and perceived authority to get her to take actions she might normally question. This social engineering attack is not a phishing attack aimed at gathering information or credentials, it does not involve business email accounts being compromised, and carding is not a topic covered in the Security+ exam outline.

9. B. Password spraying attempts try to use a single common password for many user accounts. Determining if a single password is being used over and over can help catch basic password spraying attempts. The time, source IP, or number of failed attempts do not indicate password spraying.

10. A. Misinformation and disinformation campaigns are primarily associated with nation-state actors, but are increasingly used by other organizations and even individuals as well. Watering hole attacks, business email compromise, and password spraying are broadly used attacks.

11. C. Typosquatting uses misspellings and common typos of websites to redirect traffic for profit or malicious reasons. Fortunately in reality, if you visit `smazon.com`, you'll be redirected to the actual `amazon.com` website, as Amazon knows about and works to prevent this type of issue. DNS hijacking and hosts file modifications both attempt to redirect traffic to actual URLs or hostnames to different destinations, and pharming does redirect legitimate traffic to fake sites, but typosquatting is the more specific answer.

12. B. Devon is conducting a watering hole attack that leverages a frequently visited site to deploy malware. There is no description of misinformation or disinformation in the question, and there is not a typo described that would lead to a typosquatting attack being successful.

13. C. Brand impersonation attacks are designed to appear to be from a company that recipients are likely to be familiar with, and thus are more likely to elicit a response. While these are a type of phishing, the more specific answer of brand impersonation is the best answer. Pretexting is a social engineering concept that provides a reason for the request. Pharming attacks redirect traffic intended to be sent to a legitimate site to a fake website typically designed to simulate the real one.

14. C. This is an example of an impersonation attack. The pentester impersonated the head of IT in order to achieve their goals. The good news is that it was a penetration tester! Smishing is phishing via SMS, vishing is phishing via voice or voicemail, and pretexting provides a reason that the target should perform an action. Here the attack relied on the authority that Amanda believed the caller had.

15. C. Smishing attacks are SMS-based. Impersonation attacks could use texts but don't specifically rely on them. Watering hole attacks use frequently visited websites, whereas business email compromise attacks focus on gaining access to business email accounts to use in follow-up attacks.

16. D. Sharif has discovered a spraying attack that uses the same password—often a default or common password—with many usernames. Credential harvesting is the process of gathering credentials like usernames and passwords. Impersonation is a social engineering technique used when an attacker pretends to be someone else. BEC, or business email compromise, involves attackers posing as a trusted individual and asking for actions to be performed.

17. B. Smishing is a type of phishing that occurs via text (SMS) message.

18. B. While it's nearly impossible to prevent typosquatting, purchasing and registering the most common typos (typo-domains) related to your organization's domain and redirecting them to your real domain is the most effective option available. Copyrighting or trademarking the domain name does not prevent typosquatting, and typo resolution is not a feature or capability that is available.

19. B. Using an organization's brand in this way is an example of brand impersonation. While this is also an impersonation attack, the more specific description is the best answer here. Misbranding and crypto-phishing were both made up for this question and aren't commonly used terms.

20. C. Disinformation campaigns are used to shift public opinion or to accomplish other goals. They are not limited to nation-state actors but are an increasingly heavily used social engineering tactic at a broad scale. Smishing relies on SMS messages, pretexting involves using a reason that creates urgency or importance in a request from a social engineer, and spraying is a type of password brute forcing.

Chapter 5: Security Assessment and Testing

1. C. Threat hunting is an assessment technique that makes an assumption of compromise and then searches the organization for indicators of compromise that confirm the assumption. Vulnerability scanning, penetration testing, and war driving are all assessment techniques that probe for vulnerabilities but do not assume that a compromise has already taken place.

2. D. Credentialed scans only require read-only access to target servers. Renee should follow the principle of least privilege and limit the access available to the scanner.

3. C. Ryan should first run his scan against a test environment to identify likely vulnerabilities and assess whether the scan itself might disrupt business activities.

4. C. An attack complexity of "low" indicates that exploiting the vulnerability does not require any specialized conditions.

5. A. A false positive error occurs when the vulnerability scanner reports a vulnerability that does not actually exist.

6. B. By allowing students to change their own grades, this vulnerability provides a pathway to unauthorized alteration of information. Brian should recommend that the school deploy integrity controls that prevent unauthorized modifications.

7. C. Nmap is a port scanning tool used to enumerate open network ports on a system. Nessus is a vulnerability scanner designed to detect security issues on a system. Nslookup is a DNS information gathering utility. All three of these tools may be used to gather information and detect vulnerabilities. Metasploit is an exploitation framework used to execute and attack and would be better suited for the Attacking and Exploiting phase of a penetration test.

8. A. This vulnerability is corrected by a patch that was released by Microsoft in 2017. A strong patch management program would have identified and remediated the missing patch.

9. B. Intrusion detection systems do not detect vulnerabilities; they detect attacks. The remaining three tools could all possibly discover a cross-site scripting (XSS) vulnerability, but a web application vulnerability scanner is the most likely to detect it because it is specifically designed to test web applications.

10. A. Moving from one compromised system to other systems on the same network is known as lateral movement. Privilege escalation attacks increase the level of access that an attacker has to an already compromised system. Footprinting and OSINT are reconnaissance techniques.

11. A. Audits performed to validate an organization's financial statements are very formal audits that are performed by independent third-party auditors. This makes them external audits. Internal audits may be more or less formal than external audits but they are generally done only to provide assurance to internal parties and not to investors. Penetration tests may be done as part of an audit but they are not audits themselves.

12. C. Bug bounty programs are designed to allow external security experts to test systems and uncover previously unknown vulnerabilities. Bug bounty programs offer successful testers financial rewards to incentivize their participation.

13. D. Backdoors are a persistence tool, designed to make sure that the attacker's access persists after the original vulnerability is remediated. Kyle can use this backdoor to gain access to the system in the future, even if the original exploit that he used to gain access is no longer effective.

14. C. WHOIS lookups use external registries and are an example of open source intelligence (OSINT), which is a passive reconnaissance technique. Port scans, vulnerability scans, and footprinting all require active engagement with the target and are, therefore, active reconnaissance.

15. B. Common Vulnerabilities and Exposures (CVE) provides a standard nomenclature for describing security-related software flaws. Common Platform Enumeration (CPE) provides a standard nomenclature for describing product names and versions. The Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security-related software flaws. Common Configuration Enumeration (CCE) provides a standard nomenclature for discussing system configuration issues.

16. C. Known environment tests are performed with full knowledge of the underlying technology, configurations, and settings that make up the target. Unknown environment tests are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems like an attacker would. Partially known environment tests are a blend of unknown environment and known environment testing. Detailed environment tests are not a type of penetration test.

17. C. The rules of engagement provide technical details on the parameters of the test. This level of detail would not normally be found in a contract or statement of work (SOW). The lessons learned report is not produced until after the test.

18. B. All of these techniques might provide Grace with information about the operating system running on a device. However, footprinting is a technique specifically designed to elicit this information.

19. B. Vulnerabilities with CVSS base scores between 4.0 and 6.9 fit into the medium risk category. Vulnerability scores between 0.1 and 3.9 would be low, between 7.0 and 8.9 would be high, and those between 9.0 and 10.0 would be in the critical risk category.

20. C. The privileges required (PR) metric indicates the type of system access that an attacker must have to execute the attack.

Chapter 6: Application Security

1. B. Adam is conducting static code analysis by reviewing the source code. Dynamic code analysis requires running the program, and both mutation testing and fuzzing are types of dynamic analysis.

2. C. Charles should perform user input validation to strip out any SQL code or other unwanted input. Secure session management can help prevent session hijacking, logging may provide useful information for incident investigation, and implementing TLS can help protect network traffic, but only input validation helps with the issue described.

3. A. A parameterized query (sometimes called a prepared statement) uses a prebuilt SQL statement to prevent SQL-based attacks. Variables from the application are fed to the query, rather than building a custom query when the application needs data. Encoding data helps to prevent cross-site scripting attacks, as does input validation. Appropriate access controls can prevent access to data that the account or application should not have access to, but they don't use precompiled SQL statements. Stored procedures are an example of a parameterized query implementation.

4. A. Improper error handling often exposes data to users and possibly attackers that should not be exposed. In this case, knowing what SQL code is used inside the application can provide an attacker with details they can use to conduct further attacks. Code exposure is not one of the vulnerabilities we discuss in this book, and SQL code being exposed does not necessarily mean that SQL injection is possible. While this could be caused by a default configuration issue, there is nothing in the question to point to that problem.

5. B. The application has a race condition, which occurs when multiple operations cause undesirable results due to their order of completion. De-referencing accesses or uses a memory pointer, an insecure function would have security issues in the function itself, and improper error handling would involve an error and how it was displayed or what data it provided.

6. B. Although this example includes continuous integration, the key thing to notice is that the code is then deployed into production. This means that Susan is operating in a continuous deployment environment, where code is both continually integrated and deployed. Agile is a development methodology and often uses CI/CD, but we cannot determine if Susan is using Agile.

7. B. Developers working on active changes to code should always work in the development environment. The test environment is where the software or systems can be tested without impacting the production environment. The staging environment is a transition environment for code that has successfully cleared testing and is waiting to be deployed into production. The production environment is the live system. Software, patches, and other changes that have been tested and approved move to production.

8. B. All of the activities listed here may reduce the risk of the vulnerabilities created by the code. However, Ricky is specifically concerned about the fact that the organization may not be aware of all of the code that it is running. Package monitoring would inventory and monitor these third-party libraries, so that is the best answer here.

9. B. The main benefits of automation are efficiency and time savings, enforcing baselines, standardizing infrastructure configurations, scaling in a secure manner, retaining employees, reducing reaction time, and serving as a workforce multiplier. Technical debt is one of the potential drawbacks of automation.

10. B. This is an example of the guard rails use case for automation. Cybersecurity professionals can use scripting to automatically review user actions and block any that are outside of normal parameters.

11. A. Automation normally increases employee retention. The common drawbacks to automation include complexity, cost, creating single points of failure, incurring technical debt, and creating challenges to ongoing supportability.

12. D. Buffer overflow attacks occur when an attacker manipulates a program into placing more data into an area of memory than is allocated for that program's use. The goal is to overwrite other information in memory with instructions that may be executed by a different process running on the system.

13. A. In an on-path attack, the attacker fools the user into thinking that the attacker is actually the target website and presenting a fake authentication form. They may then authenticate to the website on the user's behalf and obtain the cookie. This is slightly different from a session hijacking attack, where the attacker steals the cookie associated with an active session.

14. A. Code signing provides developers with a way to confirm the authenticity of their code to end users. Developers use a cryptographic function to digitally sign their code with their own private key, and then browsers can use the developer's public key to verify that signature and ensure that the code is legitimate and was not modified by unauthorized individuals.

15. A. This is an example of a reflected attack because the script code is contained within the URL. A persistent or stored attack places the content on a web page or other location where a victim may later access it. DOM-based XSS attacks hide the attack code within the Document Object Model.

16. C. This query string is indicative of a parameter pollution attack. In this case, it appears that the attacker was waging a SQL injection attack and tried to use parameter pollution to slip the attack past content filtering technology. The two instances of the `serviceID` parameter in the query string indicate a parameter pollution attempt.

17. A. The series of thousands of requests incrementing a variable indicate that the attacker was most likely attempting to exploit an insecure direct object reference vulnerability.

18. C. In this case, the `..` operators are the telltale giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the `/etc/passwd` file on the server.

19. B. Websites use HTTP cookies to maintain sessions over time. If Wendy is able to obtain a copy of the user's session cookie, she can use that cookie to impersonate the user's browser and hijack the authenticated session.

20. A. The use of the SQL `WAITFOR` command is a signature characteristic of a timing-based SQL injection attack.

Chapter 7: Cryptography and the PKI

1. D. In symmetric encryption algorithms, both the sender and the receiver use a shared secret key to encrypt and decrypt the message, respectively.

2. A. Downgrade attacks try to remove or lower the strength of encryption to allow the decryption of sensitive information. Birthday attacks find collisions where two different inputs produce the same hash value output, but there is no discussion of that in this scenario. Homomorphic encryption is not an attack but a technology that protects privacy by encrypting data in a way that preserves the ability to perform computation on that data.

3. D. Norm's actions are designed to protect against the unauthorized disclosure of sensitive information. This is a clear example of protecting confidentiality.

4. A. Steganography is the art of using cryptographic techniques to embed secret messages within another file.

5. A. All of these statements are correct except for the statement that all cryptographic keys should be kept secret. The exception to this rule are public keys used in asymmetric cryptography. These keys should be freely shared.

6. C. Stream ciphers operate on one character or bit of a message (or data stream) at a time. Block ciphers operate on "chunks," or blocks, of a message and apply the encryption algorithm to an entire message block at the same time.

7. D. AES is the successor to 3DES and DES and is the best choice for a symmetric encryption algorithm. RSA is a secure algorithm, but it is asymmetric rather than symmetric.

8. C. The Online Certificate Status Protocol (OCSP) provides real-time checking of a digital certificate's status using a remote server. Certificate stapling attaches a current OCSP response to the certificate to allow the client to validate the certificate without contacting the OCSP server. Certificate revocation lists (CRLs) are a slower, outdated approach to managing certificate status. Certificate pinning is used to provide an expected key, not to manage certificate status.

9. C. When the 11th employee joins Acme Widgets, they will need a shared secret key with every existing employee. There are 10 existing employees, so 10 new keys are required.

10. B. In an asymmetric encryption algorithm, each employee needs only two keys: a public key and a private key. Adding a new user to the system requires the addition of these two keys for that user, regardless of how many other users exist.

11. D. Extended validation (EV) certificates provide the highest available level of assurance. The CA issuing an EV certificate certifies that they have verified the identity and authenticity of the certificate subject.

12. C. Wildcard certificates protect the listed domain as well as all first-level subdomains. `dev.www.mydomain.com` is a second-level subdomain of `mydomain.com` and would not be covered by this certificate.

13. A. Root CAs are highly protected and not normally used for certificate issuance. A root CA is usually run as an offline CA that delegates authority to intermediate CAs that run as online CAs.

14. C. The PFX format is most closely associated with Windows systems that store certificates in binary format, whereas the P7B format is used for Windows systems storing files in text format.

15. A. Hardware security modules (HSMs) provide an effective way to manage encryption keys. These hardware devices store and manage encryption keys in a secure manner that prevents humans from ever needing to work directly with the keys.

16. C. A downgrade attack is sometimes used against secure communications such as TLS in an attempt to get the user or system to inadvertently shift to less secure cryptographic modes. The idea is to trick the user into shifting to a less secure version of the protocol, one that might be easier to break.

17. C. When encrypting a message using an asymmetric encryption algorithm, the person performing the encryption does so using the recipient's public key.

18. D. In an asymmetric encryption algorithm, the recipient of a message uses their own private key to decrypt messages that they receive.

19. B. The sender of a message may digitally sign the message by encrypting a message digest with the sender's own private key.

20. A. The recipient of a digitally signed message may verify the digital signature by decrypting it with the public key of the individual who signed the message.

Chapter 8: Identity and Access Management

1. D. Angela's organization is acting as an identity provider (IdP). Other members of the federation may act as a service provider or relying party when they allow her users to access their services. Authentication provider is not a named role in typical federation activities.

2. A. Password complexity requirements do not prevent sharing of complex passwords, making it the least effective option from the list. Biometric authentication measures will require the enrolled user to be there, although in some cases such as fingerprint systems, multiple users could each enroll a valid fingerprint for a single account. Both types of one-time passwords could be shared but make it harder and less convenient to share accounts.

3. B. Most cloud services provide identity and authorization tools for their services. Most, although not all, allow customers to set some or even many of the account policies they will use, and most major vendors support some form of multifactor capability.

4. D. Password age is set to prevent users from resetting their password enough times to bypass reuse settings. Complexity, length, and expiration do not influence this.

5. B. SMS messages are not secure and could be accessed by cloning a SIM card or redirecting VoIP traffic, among other possible threat models. Both HOTP and TOTP tokens and applications as well as biometric factors are generally considered more secure than an SMS-based factor.

6. A. A USB security key is an example of a hard, or physical, token. An application is an example of a soft token. A biometric factor might be a fingerprint or faceprint. Attestation is a formal verification that something is true. Attestation tokens were made up for this question.

7. B. Picture password asks users to click on specific, self-defined parts of a picture. This means that clicking on those points is something you know. Something you are involves biometric traits, and somewhere you are relies on geographic locations.

8. A. Linux file permissions are read left to right, with the first three characters indicating read, write, and execute permissions (`rwx`) for the owner of the file, the second three apply to the group, and the last three to all other users. Any indicated with a – are not allowed for that set.

9. C. Role-based access control (RBAC) sets permissions based on an individual's role, which is typically associated with their job. Attribute-based access control (ABAC) is typically matched to other attributes than the job role. Discretionary access control (DAC) and mandatory access control (MAC) are commonly implemented at the operating system level.

10. D. Fingerprint scanners are found on many mobile devices and laptops, making them one of the most broadly deployed biometric technologies. Facial recognition is also broadly deployed, but it is not mentioned in this question or offered as an option.

11. B. Password length has the largest impact on preventing password cracking. When paired with a strong password hash algorithm and proper use of technology like salting, long passwords are much harder to crack. Complexity is the next most important option, as preventing simple repeated characters and similar problematic passwords helps reduce the probability of easily cracked passwords being used. Reuse limitations and preventing common words are less useful.

12. A. PINs and passwords are both examples of something you know. Something you set is not a type of factor. Biometric factors are an example of something you are, and a physical USB token would be a common example of something you have.

13. C. Password vaulting, which stores passwords for use with proper authentication and rights, is the most appropriate solution for Marie's needs. Ephemeral accounts and just-in-time permissions are typically used under normal circumstances to provide least privilege access as needed. Token-based authentication is not specifically a PAM solution.

14. D. Jill is able to make decisions about the rights she grants on her files, meaning this is a discretionary access control system. A mandatory access control system relies on labels to set access control rules. Rule-based access control systems rely on rules to define access, and attribute-based access control systems grant access based on attributes like job roles or locations.

15. B. OAuth is an authentication protocol that allows services to receive authentication tokens from an identity provider without needing the user's password. LDAP is a directory service and is often used as part of SSO processes. MITRE is a nonprofit organization, and RADIUS is an authentication technology.

16. C. Kyle can assume that his government-issued ID is being used as part of an identity proofing process to validate that he is who he claims to be. Biometric enrollment typically requires interaction with an enrollment process to scan or capture biometric information. Just-in-time permission creation is done when access is requested and does not require government ID, and federation connects identity providers with service providers, which is not described here.

17. A. The principle of least privilege means that users should only be given the permissions necessary to perform their role. Best practice is a general term describing commonly recommended and accepted industry practices. Temporal accounts are ephemeral, or short-lived accounts. Mandatory access control is an access control scheme.

18. C. Without other factors that would require the account to be retained, deprovisioning accounts that belonged to users who have left the organization is a best practice. Transferring accounts or reprovisioning them may expose data to new users or provide them with rights that they should not have.

19. C. A person's name, age, location, job title, and even things like their height or their hair color are all attributes that may be associated with a person's identity. None of these describe biometric factors used for authentication, and identity factors are something you are, something you have, or somewhere you are. Account permissions determine what you can do, not attributes like these.

20. C. Linux users can change who can read, write, or execute files and directories they own, which is discretionary access control (DAC). Mandatory access control (MAC) would enforce settings set by the systems administrator without users having the rights to make their own decisions. While role-based access control is involved, DAC best describes the access control scheme. ABAC is not a default method for setting rights for the Linux filesystem.

Chapter 9: Resilience and Physical Security

1. A. Naomi should select a load balancing solution. Load balancers allow multiple systems or services to appear like a single resource and can take systems out of the load-balanced pool to allow for upgrades or changes in resources required. Clustering is used to allow groups of computers to perform the same task, but without a load balancer cannot provide the same transparent service appearing as the same system. Geographic diversity and hot sites are concepts used to provide resilience but don't provide this capability.

2. D. Differential backups back up the changes since the last full backup. Incremental backups back up changes since the last backup, and snapshots are a live copy of a system. This is not a full backup, because it is capturing changes since a full backup.

3. B. Warm sites have systems, connectivity, and power but do not have the live or current data to immediately take over operations. A hot site can immediately take over operations, whereas a cold site has space and power, and likely connectivity, but will require that systems and data be put in place to be used. Cloud sites are not one of the three common types of recovery sites.

4. C. Testing that involves an actual failover to another site or service is failover testing. Parallel processing runs both sites or services at the same time; simulation and tabletops both review what would happen without making the actual change.

5. B. Virtual machine snapshots capture the machine state at a point in time and will allow Felix to clone the system. A full backup and a differential backup can be used to capture the disk for the machine but typically will not capture the memory state and other details of the system state. Live boot media allows you to boot and run a nonpersistent system from trusted media.

6. A. A documented restoration order helps ensure that systems and services that have dependencies start in the right order and that high-priority or mission-critical services are restored first. TOTP and HOTP are types of one-time password technology, and last-known good configurations are often preserved with a snapshot or other technology that can allow a system to return to a known good status after an issue such as a bad patch or configuration change.

7. D. Bollards are physical security controls that prevent vehicles from accessing or ramming doors or other areas. They may look like pillars, planters, or other innocuous objects. An air gap is a physical separation of technology environments; a hot aisle is the aisle where systems in a datacenter exhaust warm air; and unlike in movies, robotic sentries are not commonly deployed and aren't ready to stop vehicles in most current circumstances.

8. D. Encryption is commonly used to ensure that backup media or data that is exposed is not accessible to third parties. This does mean that Alecia must carefully secure the encryption keys for the backup. Hashing that data would not keep it secure, and if only hashes were stored the data would be unrecoverable. Security guards are expensive and not a complete solution if data is inadvertently exposed, and offsite, secure storage locations are a useful and common solution for organizations that want to have remote backups.

9. C. Offsite journaling will allow transactions to be recorded and to remain available if a significant event occurred that involved his datacenter. Snapshots are useful at a point in time but do not retain a transaction log between snapshots.

10. A. Resilience requires capacity planning to ensure that capacity—including staff, technology, and infrastructure—is available when is needed. Although a generator, UPS, various RAID levels, and backups have their place in disaster recovery and contingency planning, they are not the primary focus of resiliency and capacity planning.

11. A. Synchronous replication occurs in real time, whereas asynchronous replication occurs after the fact but more regularly than a backup. Journaled and snapshot-based replication are not specific types of replication.

12. C. Security guards can be one of the costliest physical security controls over time, making the cost of guards one of the most important deciding factors guiding when and where they will be employed. Reliability, training, and the potential for social engineering are all possible issues with security guards, but none of these is the major driver in the decision process.

13. A. Infrared sensors balance lower cost with the ability to detect humans entering and moving in a space. Microwave sensors are more expensive but can provide better coverage, including traveling through some barriers. Ultrasonic sensors are rarely used for this purpose, and pressure sensors are limited to the pad where they are deployed, making them expensive and challenging to use for rooms or larger spaces.

14. C. Fences, lighting, and video surveillance can all help discourage potential malicious actors from entering an area, although a determined adversary will ignore or bypass all three. Platform diversity can help make it harder for attackers to succeed, but this is primarily a resilience tactic, and remains more costly to maintain and implement.

15. D. Technology diversity helps ensure that a single failure—due to a vendor, vulnerability, or misconfiguration—will not impact an entire organization. Technology diversity does have additional costs, including training, patch management, and configuration management.

16. D. Scott has implemented an offsite backup scheme. His backups will take longer to retrieve because they are at a remote facility and will have to be sent back to him, but they are likely to survive any disaster that occurs in his facility or datacenter. Onsite backups are kept immediately accessible, whereas nearline backups can be retrieved somewhat more slowly than online backups but faster than offline backups. "Safe backups" is not an industry term.

17. A. Security guards who can monitor for and understand the signs of a physical brute-force attempt are the most useful control listed. Locks may show signs of attempts but require careful inspection, access badges would require log review and additional information to detect brute-force attacks, and an IDS is useful for network attacks.

18. B. A tabletop exercise is the least disruptive form of exercise. Even simulations have some risk if an employee does not fully realize that the scenario is simulated and takes action. Failover, even partial, involves the potential for disruption.

19. B. An access control vestibule uses a pair of doors. When an individual enters, the first door must be closed and secured before the second door can be opened. This helps prevent tailgating, since the person entering will notice anybody following them through the secured area. A Faraday cage is used to stop electromagnetic interference (EMI), a bollard prevents vehicular traffic, and an air gap is a physical separation of networks or devices.

20. C. Geographic dispersion helps ensure that a single natural or human-made disaster does not disable multiple facilities. This distance is not required by law; latency increases with distance; and though there may be tax reasons in some cases, this is not a typical concern for a security professional.

Chapter 10: Cloud and Virtualization Security

1. C. This is an example of adding additional capacity to an existing server, which is also known as vertical scaling. Kevin could also have used horizontal scaling by adding additional web servers. Elasticity involves the ability to both add and remove capacity on demand, and though it does describe this scenario, it's not as good a description as vertical scaling. There is no mention of increasing the server's availability.

2. C. Type I hypervisors, also known as bare-metal hypervisors, run directly on top of the physical hardware and, therefore, do not require a host operating system.

3. D. The cloud service provider bears the most responsibility for implementing security controls in an SaaS environment and the least responsibility in an IaaS environment. This is due to the division of responsibilities under the cloud computing shared responsibility model.

4. A. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a reference document designed to help organizations understand the appropriate use of cloud security controls and map those controls to various regulatory standards. NIST SP 500-292 is a reference model for cloud computing and operates at a high level. ISO 27001 is a general standard for cybersecurity, and PCI DSS is a regulatory requirement for organizations involved in processing credit card transactions.

5. A. This approach may be described as client-server computing, but that is a general term that describes many different operating environments. The better term to use here is edge computing, which involves placing compute power at the client to allow it to perform preprocessing before sending data back to the cloud. Fog computing is a related concept that uses IoT gateway devices that are located in close physical proximity to the sensors.

6. C. One of the key characteristics of cloud computing is that customers can access resources on-demand with minimal service provider interaction. Cloud customers do not need to contact a sales representative each time they wish to provision a resource but can normally do so on a self-service basis.

7. B. Helen is using IaaS services to create her payroll product. She is then offering that payroll service to her customers as a SaaS solution.

8. D. Hybrid cloud environments blend elements of public, private, and/or community cloud solutions. A hybrid cloud requires the use of technology that unifies the different cloud offerings into a single, coherent platform.

9. A. Customer relationship management (CRM) packages offered in the cloud would be classified as software-as-a-service (SaaS), since they are not infrastructure components. Storage, networking, and computing resources are all common IaaS offerings.

10. C. Infrastructure as code (IaC) is any approach that automates the provisioning, management, and deprovisioning of cloud resources. Defining resources through JSON or YAML is IaC, as is writing code that interacts with an API. Provisioning resources through a web interface is manual, not automated, and therefore does not qualify as IaC.

11. D. API-based CASB solutions interact directly with the cloud provider through the provider's API. Inline CASB solutions intercept requests between the user and the provider. Outsider and comprehensive are not categories of CASB solutions.

12. C. Customers are typically charged for server instances in both IaaS environments, where they directly provision those instances, and PaaS environments, where they request the number of servers needed to support their applications. In an SaaS environment, the customer typically has no knowledge of the number of server instances supporting their use.

13. A. Cloud providers offer resource policies that customers may use to limit the actions that users of their accounts may take. Implementing resource policies is a good security practice to limit the damage caused by an accidental command, a compromised account, or a malicious insider.

14. A. Cloud providers offer VPC endpoints that allow connections of VPCs to each other using the cloud provider's secure network. Cloud transit gateways extend this model even further, allowing the direct interconnection of cloud VPCs with on-premises VLANs for hybrid cloud operations. Secure web gateways (SWGs) provide a layer of application security for cloud-dependent organizations. Hardware security modules (HSMs) are special-purpose computing devices that manage encryption keys and also perform cryptographic operations in a highly efficient manner.

15. D. Virtual machine (VM) escape vulnerabilities are the most serious issue that can exist in a virtualized environment, particularly when a virtual host runs systems of differing security levels. In an escape attack, the attacker has access to a single virtual host and then manages to leverage that access to intrude upon the resources assigned to a different virtual machine. The hypervisor is supposed to prevent this type of access by restricting a virtual machine's access to only those resources assigned to that machine.

16. A. Controls offered by cloud service providers have the advantage of direct integration with the provider's offerings, often making them cost-effective and user-friendly. Third-party solutions are often more costly, but they bring the advantage of integrating with a variety of cloud providers, facilitating the management of multicloud environments.

17. C. Cloud access security brokers (CASBs) are designed specifically for this situation: enforcing security controls across cloud providers. A secure web gateway (SWG) may be able to achieve Kira's goal, but it would be more difficult to do so. Security groups and resource policies are controls used in IaaS environments.

18. D. The principle of data sovereignty states that data is subject to the legal restrictions of any jurisdiction where it is collected, stored, or processed. In this case, Howard needs to assess the laws of all three jurisdictions.

19. D. Brenda's company is offering a technology service to customers on a managed basis, making it a managed service provider (MSP). However, this service is a security service, so the term managed security service provider (MSSP) is a better description of the situation.

20. A. This is an example of public cloud computing because Tony is using a public cloud provider, Microsoft Azure. The fact that Tony is limiting access to virtual machines to his own organization is not relevant because the determining factor for the cloud model is whether the underlying infrastructure is shared, not whether virtualized resources are shared.

Chapter 11: Endpoint Security

1. B. Legacy hardware is unsupported and no longer sold. End-of-life typically means that the device is no longer being made but is likely to still have support for a period of time. End-of-sales means the device is no longer being sold, but again, may have support for some time. Senescence is not a term typically used in hardware life cycles.

2. C. The services listed are:

- 21—FTP
- 22—SSH

- 23—Telnet
- 80—HTTP
- 443—HTTPS

Of these services, SSH (Port 22) and HTTPS (port 443) are secure options for remote shell access and HTTP. Although secure mode FTP (FTP/S) may run on TCP 21, there is not enough information to know for sure, and HTTPS can be used for secure file transfer if necessary. Thus, Naomi's best option is to disable all three likely unsecure protocols: FTP (port 21), Telnet (port 23), and HTTP (port 80).

3. C. Protecting data using a DLP requires data classification so that the DLP knows which data should be protected and what policies to apply to it. Defining data life cycles can help prevent data from being kept longer than it should be and improves data security by limiting the data that needs to be secured, but it isn't necessary as part of a DLP deployment. Encrypting all sensitive data may mean the DLP cannot recognize it and may not be appropriate for how it is used. Tagging all data with a creator or owner can be useful but is not required for a DLP rollout—instead, knowing the classification of the data is more important.

4. C. Oliver should look for a key management system, or KMS, which will allow him to securely create, store, and manage keys in a cloud environment. TPMs, secure enclaves, and Google's Titan M are all local hardware solutions.

5. C. XDR is similar to EDR but has a broader perspective covering not only endpoints but also cloud services, security platforms, and other components. Thus, the breadth of coverage of the technology stack is broader for XDR solutions.

6. B. A Windows Group Policy Object (GPO) can be used to control whether users are able to install software. Antivirus will not stop this, nor will EDR or a HIPS.

7. A. Endpoint detection and response (EDR) systems provide monitoring, detection, and response capabilities for systems. EDR systems capture data from endpoints and send it to a central repository, where it can be analyzed for issues and indicators of compromise or used for incident response activities. IAM is identity and access management, FDE is full-disk encryption, and ESC is not a commonly used security acronym.

8. D. Network devices as well as many other devices like printers come with default passwords set. Fred should change the default password as part of the process of setting up his new router.

9. B. A host-based intrusion prevention system (HIPS) can detect and prevent attacks against services while allowing the service to be accessible. A firewall can only block based on port, protocol, and IP; encryption won't prevent this; and an EDR is primarily targeted at malicious software and activity, not at network-based attacks on services.

10. A. Unlike computers and mobile devices, switches and other network devices typically do not have additional software that can be removed. Installing patches, placing administrative interfaces on protected VLANs, and changing default passwords are all common hardening techniques for network devices like switches.

11. B. Since the web interfaces are needed to manage the devices, Helen's best option is to place the IoT devices in a protected VLAN. IoT devices will not typically allow additional software to be installed, meaning that adding firewalls or a HIPS won't work.

12. A. Removing unnecessary software helps to reduce the attack surface of the devices. Not all software runs a service or opens a network port, but installed software provides additional opportunities for attackers to find vulnerabilities. That means that reducing firewall rules is not a primary purpose. While removing it may reduce the number of patches required by a device, that is not the primary driver. Finally, while incident response efforts may point to a need for further hardening to prevent future incidents, removing unnecessary software is not a typical step in support of IR activities.

13. A. SCADA (supervisory control and data acquisition) is a system architecture that combines data acquisition and control devices with communications methods and interfaces to oversee complex industrial and manufacturing processes, just like those used in utilities. A SIM (subscriber identity module) is the small card used to identify cell phones; HVAC stands for heating, ventilation, and air-conditioning; and AVAD was made up for this question.

14. D. A real-time operating system (RTOS) is an OS that is designed to handle data as it is fed to the operating system, rather than delaying handling it as other processes and programs are run. Real-time operating systems are used when processes or procedures are sensitive to delays that might occur if responses do not happen immediately. An MFP is a multifunction printer, a HIPS is a host intrusion prevention system, and an SoC is a system on a chip—which is hardware, which might run an RTOS, but the option does not mention what type of OS the SoC is running.

15. B. Embedded systems are available at many price points. Understanding constraints that limited resources create for embedded systems helps security professionals identify appropriate security controls and options.

16. A. Jim knows that once a BitLocker-enabled machine is booted, the drive is unlocked and could be accessed. He would be least worried if the machine were off and was stolen, or if the drive itself were stolen from the machine, since the data would not be accessible in either of those cases.

17. B. Olivia should install a host-based intrusion detection system (HIDS). An HIDS can detect and report on potential attacks but does not have the ability to stop them. A host-based intrusion prevention system (HIPS) can be configured to report only on attacks, but it does have the built-in ability to be set up to block them. Firewalls can block known ports, protocols, or applications, but they do not detect attacks—although advanced modern firewalls blur the line between firewalls and other defensive tools. Finally, a data loss prevention (DLP) tool focuses on preventing data exposures, not on stopping network attacks.

18. B. Group Policy deployed via Active Directory will allow Anita to set security settings across her domain managed systems. EDR and XDR are useful for detecting and responding to malware and malicious actors but not for deploying security configurations. SELinux is a Linux kernel-based security module that provides additional security capabilities and options on top of existing Linux distributions.

19. C. Chris knows that BIOS-based systems do not support either of these modes, and that trusted boot validates every component before loading it, whereas measured boot logs the boot process and sends it to a server that can validate it before permitting the system to connect to the network or perform other actions.

20. A. A degausser is a quick and effective way to erase a tape before it is reused. Wiping a tape by writing 1s, 0s, or a pattern of 1s and 0s to it will typically be a slow operation and is not a common method of destroying data on a tape. Incinerating the tape won't allow it to be reused!

Chapter 12: Network Security

1. C. SNMP traps can be configured to provide additional information, but typical SNMP traps provide information about issues such as links going down, authentication failures, and reboots.

2. C. A honeynet is a group of systems that intentionally exposes vulnerabilities so that defenders can observe attacker behaviors, techniques, and tools to help them design better defenses.

3. B. Telnet provides remote command-line access but is not secure. SSH is the most common alternative to telnet, and it operates on port 22.

4. D. DNS reputation services can provide Jill with an automated feed of malicious sites that she can include in her DNS filter. OSINT (open source intelligence) is gathered without scans but typically won't provide DNS block lists. STP (Spanning Tree Protocol) prevents loops in networks and is not relevant to DNS filtering, and an access control monitoring service will not be either.

5. B. Jump servers are used to provide secure, monitored access to a protected network. Users log in to the jump server, which then has access to the network. Proxies are used to filter or manage traffic and might be used in this scenario, but jump servers are the preferred answer for most organizations and uses. A VLAN (virtual LAN) is used to logically separate network segments. An air gap is a physical disconnection between networks or devices.

6. A. A next-generation firewall (NGFW) device is typically designed and built to be more capable at high speeds and throughput than a universal threat management device. Since UTM devices provide such a wide array of services that consume CPU and memory resources, this performance gap can also sometimes be due to the broad set of services that a UTM device provides. A WAF (web application firewall) is specialized in web traffic, and SD-FW was made up for this question.

7. A. DNSSEC validates both the origin of DNS information and ensures that DNS responses have not been modified, making it the best option to help prevent DNS poisoning attacks. SDNS was made up for this question. SASE is used to secure networks in complex multilocation environments, and SD-WAN allows for dynamic wide area networks defined by software, but neither provides this type of DNS security.

8. C. SD-WAN (software-defined wide area network) is commonly used to replace MPLS (Multiprotocol Label Switching) networks, which are typically higher cost than other connectivity options. IPSec and TLS-based VPNs are used to connect through untrusted networks, but they do not provide the functionality required. SASE uses SD-WAN and other technologies to ensure secure connectivity in complex network infrastructures with endpoints in many locations.

9. D. Transport Layer Security (TLS) is commonly used to wrap (protect) otherwise insecure protocols. In fact, many of the secure protocols simply add TLS to protect them. ISAKMP and IKE are both used for IPSec and can be used to wrap insecure protocols, but they aren't used alone. SSL is no longer used; TLS has almost entirely replaced it, although SSL is still often casually referred to as TLS.

10. D. While many protocols have a secure version, DHCP does not have a secure option, and protection must be handled by using detection and response mechanisms, rather than an encrypted protocol.

11. B. Policy enforcement points communicate with policy administrators to forward requests from subjects and to receive instructions from them about connections to allow or end. Policy administrators are components that establish or remove the communication path between subjects and resources, including creating session-specific authentication tokens or credentials as needed. Policy engines make policy decisions based on both rules and external systems. Policy gateways are not reference components for zero-trust designs.

12. C. End users may use secure POP (POPS), secure IMAP (IMAPS), and secure HTTP (HTTPS) to retrieve email. SPF, DKIM, and DMARC are used to identify and validate email servers, not to access email by end users.

13. A. Physical isolation like an air gap is used when the additional work to manually transfer files is an acceptable trade-off against the potential for a security event caused by potential network-based attackers. Firewall rules, an IPS, or the use of IPSec to protect traffic will not sufficiently address this issue if any services remain accessible on the system.

14. B. Active/active designs spread traffic among active nodes, helping ensure that a single node will not be overwhelmed. Active/passive designs are useful for disaster recovery and business continuity, but they do not directly address heavy load on a single node. There are many load-balancing schemes, but daisy chains and duck-duck-goose are not among them.

15. A. Agent-based, preadmission NAC will provide Isaac with the greatest amount of information about a machine and the most control about what connects to the network and what can impact other systems. Since systems will not be connected to the network, even to a quarantine or preadmission zone, until they have been verified, Isaac will have greater control.

16. D. SASE (Secure Access Service Edge) combines network security and device security by leveraging SD-WAN with security tools like Zero Trust, firewalls, and cloud access security brokers (CASBs). Both UTM and NGFW are advanced firewalls but do not provide this full functionality, and IPSec is a protocol used to provide encryption and authentication for network traffic.

17. B. Browser on-path attacks take advantage of malicious browser plug-ins or proxies to modify traffic at the browser level. They do not involve compromised routers or servers, and a modified hosts file is more likely to be involved in an on-path attack.

18. C. Understanding what services your organization offers to the outside world is an important step in describing the organization's attack surface. Fail open and fail closed describe what happens when devices or systems fail, not vulnerability and service availability information. OSINT is a passive process and scanning is not a passive activity.

19. A. DNSSEC does not encrypt data but does rely on digital signatures to ensure that DNS information has not been modified and that it is coming from a server that the domain owner trusts. DNSSEC does not protect confidentiality, which is a key thing to remember when discussing it as a security option. TLS, an IPSec VPN, or encryption via AES are all potential solutions to protect the confidentiality of network data.

20. C. Out-of-band management places the administrative interface of a switch, router, or other device on a separate network or requires direct connectivity to the device to access and manage it. This ensures that an attacker who has access to the network cannot make changes to the network devices. NAC and port security help protect the network itself, whereas trunking is used to combine multiple interfaces, VLANs, or ports together.

Chapter 13: Wireless and Mobile Security

1. B. The Center for Internet Security (CIS) provides hardening guidelines known as CIS benchmarks that Alyssa can use as a guide to secure her organization's iOS devices. OWASP does not provide these, and NIST provides general guidance, not OS- or device-specific configuration guides.

2. D. Using a containerization system can allow Fred's users to run corporate applications and to use corporate data in a secure environment that cannot be accessed by other applications outside of the container on the device. Containerization schemes for mobile devices typically use encryption and other isolation techniques to ensure that data and applications do not cross over. Biometrics and context-aware authentication are useful for ensuring that the right user is using a device but don't provide this separation. Full-device encryption helps reduce the risk of theft or loss of a device resulting in a data breach.

3. B. Geofencing will allow Michelle to determine what locations the device should work in. The device will then use geolocation to determine when it has moved and where it is. In this case, the correct answer is therefore geofencing—simply having geolocation capabilities would not provide the solution she needs. Context-aware authentication can help by preventing users from logging in when they aren't in the correct location, but a device that was logged in may not require reauthentication. Finally, UEM, much like mobile device management, can be used to enforce these policies, but the most correct answer is geofencing.

4. D. When access points conflict, enterprise wireless network management tools will typically decrease the power for both access points until the issue is resolved. Simply increasing power will cause more conflicts, changing the SSID would not serve typical enterprise models that use a single SSID to allow roaming, and disabling an access point may leave coverage gaps.

5. C. Nearfield communication (NFC) is not typically used for geolocation because of its extremely short range. Geolocation services may use GPS, Wi-Fi, and Bluetooth to identify areas, access points, Bluetooth beacons, and other items that help with location services.

6. A. Simultaneous Authentication of Equals (SAE) is used to establish a secure peering environment and to protect session traffic. Since the process requires additional cryptographic steps, it causes brute-force attacks to be much slower and thus less likely to succeed while also providing more security than WPA2's preshared key (PSK) mode. WPS is Wi-Fi Protected Setup, a quick setup capability; CCMP is the encryption mode used for WPA2 networks. WPA3 moves to 128-bit encryption for Personal mode and can support 192-bit encryption in Enterprise mode.

7. C. Isabelle should select PEAP, which doesn't require client certificates but does provide TLS support. EAP-TTLS provides similar functionality but requires additional software to be installed on some devices. EAP-FAST focuses on quick reauthentication, and EAP-TLS requires certificates to be deployed to the endpoint devices.

8. A. Storage segmentation is the concept of splitting storage between functions or usage to ensure that information that fits a specific context is not shared or used by applications or services outside of that context. Full-device encryption encrypts the entire device, geofencing is used to determine geographic areas where actions or events may be taken by software, and multifactor storage was made up for this question.

9. C. Sideloading is the process of copying files between two devices like a phone and a laptop, desktop, or storage device. Jake's team member has loaded an application without using the Android application store. Sideloading does not necessarily imply malware, rooting, or disabling an MDM, although an MDM may be configured to prevent sideloading.

10. B. SMS (Short Message Service) is used to send text messages, and MMS and RCS provide additional multimedia features. Neither provides phone calls or firmware updates.

11. C. Geotagging places a location stamp in documents and pictures that can include position, time, and date. This can be a serious privacy issue when pictures or other information are posted, and many individuals and organizations disable GPS tagging. Organizations may want to enforce GPS tagging for some work products, meaning that the ability to enable or disable it in an MDM tool is quite useful. Chain of custody is a forensic concept, the ability to support geofencing does not require GPS tagging, and context-aware authentication may need geolocation but not GPS tagging.

12. A. This is an ad-hoc network set up to allow devices to connect to the access point provided by the cellular modem. NFC is a short range, low bandwidth connection method used for payments and similar purposes. Point-to-point connections are used to bridge two networks together or for single connections, this is a multi-device network. RFID uses tags and readers.

13. B. Susan's best options are to use a combination of full-device encryption (FDE) and remote wipe. If a device is stolen and continues to be connected to the cellular network, or reconnects at any point, the remote wipe will occur. If it does not, or if attackers attempt to get data from the device and it is locked, the encryption will significantly decrease the likelihood of the data being accessed. Of course, cracking a passcode, PIN, or password remains a potential threat. NFC and Wi-Fi are wireless connection methods and have no influence on data breaches due to loss of a device. Geofencing may be useful for some specific organizations that want to take action if devices leave designated areas, but it is not a general solution. Containerization may shield data, but use of containers does not immediately imply encryption or other protection of the data but simply that the environments are separated.

14. C. Current mobile device implementations have focused heavily on facial recognition via services like Apple's Face ID and fingerprint recognition like Android's fingerprint scanning and Apple's Touch ID. Gait recognition is not a widely deployed biometric technology and would be difficult for most mobile device users to use. Voice recognition as a biometric authenticator has not been broadly deployed for mobile devices, whereas voice-activated services are in wide usage.

15. B. Jailbreaking will allow Alaina to obtain administrator access to the underlying phone operating system and to modify operating system settings and options as well as to install applications that are not available via the App Store. Deploying an MDM does not permit all of this, keymodding is not a term used in this context, and installing a third-party OS would allow access but would change the OS.

16. D. Jerome should deploy a captive portal that requires users to provide information before being moved to a network segment that allows Internet access. WPS capture mode was made up for this question, Kerberos is used for enterprise authentication, and WPA2 supports open, enterprise, or PSK modes but does not provide the capability Jerome needs by itself.

17. C. Amanda wants to create a heatmap, which shows the signal strength and coverage for each access point in a facility. Heatmaps can also be used to physically locate an access point by finding the approximate center of the signal. This can be useful to locate rogue access points and other unexpected or undesired wireless devices. PSK stands for preshared key, a channel overlay is not a commonly used term (although channel overlap is a concern for channels that share bandwidth), and SSID chart was made up for this question.

18. D. Managing applications won't help protect a misplaced phone from being accessed. PINs, device encryption, and remote wipe will all help keep her organization's data and devices secure.

19. B. Gurvinder's requirements fit the COPE (corporate-owned, personally enabled) mobile device deployment model. Choose your own device (CYOD) allows users to choose a device but then centrally manages it. BYOD allows users to use their own device, rather than have the company provide it, and MOTD means message of the day, and is not a mobile device deployment scheme.

20. C. Bluesnarfing is the theft of information from a Bluetooth enabled device. If Octavia left Bluetooth on and had not properly secured her device, then an attacker may have been able to access her contact list and download its contents. A bluejacking attack occurs when

unwanted messages are sent to a device via Bluetooth. Evil twins are malicious access points configured to appear to be legitimate access points, and an evil maid attack is an in-person attack where an attacker takes advantage of physical access to hardware to acquire information or to insert malicious software on a device.

Chapter 14: Monitoring and Incident Response

1. D. The first item in the incident response cycle used by the Security+ exam is preparation.

2. C. Packet capture will allow Michael to see all the content of packets that are captured to analyze them. NetFlow simply shows source, destination, protocol, and traffic volume. Syslog and a SIEM don't capture packet content, and instead focus on logs and events.

3. C. A SIEM with correlation rules for geographic IP information as well as user IDs and authentication events will accomplish Susan's goals. An IPS may detect attacks, but it isn't well suited to detecting impossible travel. OS logs would need to be aggregated, and vulnerability scan data won't show this at all.

4. C. Application allow lists are used to ensure that only allowed applications are installable on systems. A deny list specifically identifies programs that aren't allowed. A SIEM doesn't provide application management capabilities, and sFlow is a flow tool like NetFlow.

5. D. The primary concern for analysts who deploy sFlow is often that it samples only data, meaning some accuracy and nuance can be lost in the collection of flow data. Sampling, as well as the implementation methods for sFlow, means that it scales well to handle complex and busy networks. Although vulnerabilities may exist in sFlow collectors, a buffer overflow is not a primary concern for them.

6. B. Mark has isolated the system by removing it from the network and ensuring that it cannot communicate with other systems. Containment would limit the impact of the incident and might leave the system connected but with restricted or protected access. Segmentation moves systems or groups of systems into zones that have similar purposes, data classification, or other restrictions on them.

7. C. Ben's organization is conducting a tabletop exercise. Tabletop exercises are conducted with more flexibility—team members are given a scenario and asked how they would respond and what they would do to accomplish tasks they believe would be relevant. Checklist exercises are not a specific type of exercise. A simulation exercise attempts to more fully re-create an actual incident to test responses. Fail-over exercises are conducted by actually failing a datacenter over to a hot location.

8. C. If the photo includes GPS data, it will be included in the photo's metadata. Madhuri can use a tool like ExifTool to review the metadata for useful information. None of the other options are places where data is stored for a PNG image as a normal practice.

9. A. Alyssa's has quarantined the machine, ensuring it cannot reach other systems or impact the rest of her organization. Segmentation would involve putting the system in protected network zone. Agentless tools are used to send data without a separate program or agent deployed to allow that. Deny lists are used to prevent specific programs or files from being used or deployed to systems.

10. C. Missing logs are often associated with an attacker attempting to hide evidence of their actions. Log rotation will typically remove the oldest log items and replace them with new log items rather than wiping a log, or will archive the old log file and create a new one. A newly deployed system typically has at least some logs from booting and running. Encrypting logs would leave a file in place even if it couldn't be read.

11. B. Ian's first step should be changing the sensitivity for his alerts. Adjusting the alerts to ignore safe or expected events can help reduce false positives. Correlation rules may then need to be adjusted if they are matching unrelated items. Dashboards are used to visualize data, not for alerting, and trend analysis is used to feed dashboards and reports.

12. C. Members of management or organizational leadership act as a primary conduit to senior leadership for most incident response teams. They also ensure that difficult or urgent decisions can be made without needing escalated authority. Communications and PR staff focus on internal and external communications but are typically not the direct conduit to leadership. Technical and information security experts do most of the incident response work itself.

13. D. This is an example of out-of-cycle logging, or logging that occurs at a different time than expected. This may be because an attacker is using the backup tool to acquire data. Unexpected logs are not an indicator found on the Security+ exam outline. There is no indication of resource consumption or inaccessibility in the question.

14. C. Red Hat Enterprise uses journalctl to view journal logs that contain application information. Jim should use journalctl to review the logs for the information he needs. The tool also provides functionality that replicates what `head` and `tail` can do for logs. Syslog-ng is a logging infrastructure, and though logs may be sent via syslog-ng, it is not mentioned here. `logger` is a logging utility used to make entries in the system log.

15. B. Benchmarks often include logging settings and configurations. SIEM is used to gather and analyze logs. Syslog is a standard for logging and sending logs. Agents are used to send logs for systems that don't have a logging capability.

16. B. The Windows Security log records logon events when logon auditing is enabled. The Application and System logs do not contain these events.

17. A. Five whys, event analysis, and diagramming are all common methods of performing root cause analysis. Root/branch review is not a typical process for this.

18. A. Containment activities focus on preventing further malicious actions or attacks. In this case, Hitesh might opt to prevent the malware from spreading but leave the system online due to a critical need or a desire to preserve memory and other artifacts for investigation. Isolation walls a system or systems off from the rest of the world, whereas segmentation is frequently used before incidents occur to create zones or segments of a network or system with different security levels and purposes.

19. D. The Analysis phase focuses on using various techniques to analyze events to identify potential incidents. Preparation focuses on building tools, processes, and procedures to respond to incidents. Eradication involves the removal of artifacts related to the incident, and containment limits the scope and impact of the incident.

20. C. Vulnerability scans are the best way to find new services that are offered by systems. In fact, many vulnerability scanners will flag new services when they appear, allowing administrators to quickly notice unexpected new services. Registry information is not regularly dumped or collected in most organizations. Firewall logs and flow logs could show information about the services being used by systems whose traffic passes through them, but this is a less useful and accurate way of identifying new services and would work only if those services were also being used.

Chapter 15: Digital Forensics

1. C. `dd` is a copying and conversion command for Linux and can be used to create a forensic image that can be validated using an MD5sum or SHA1 hash. The other commands are `df` for disk usage, `cp` for copying files, and `ln` to link files.

2. C. If there are known limitations or issues with the tools used, this should be included in the report. The type of system the tool was installed on may influence performance but should not influence the report or output. Training and certification may be listed as part of a team description but are not required as part of tool description. Finally, patch levels or installed versions are not critical unless there are known issues that would have been described as such.

3. A. If forensic evidence was not properly handled, it may not be admissible in court. Repeating forensic activities won't reverse mishandling, staff can't go back and re-create logs, and noting the issue will not resolve it.

4. B. Mike's best option is to identify the log information available from the provider and to request any additional information knowing that he may not receive more detail unless there is contractual language that specifies it. SaaS vendors typically won't allow installation of forensic tools, law enforcement does not perform forensic acquisition for third parties upon request, and auditors don't provide forensic data acquisition either.

5. C. Creating a snapshot will provide a complete copy of the system, including memory state that can then be analyzed for forensic purposes. Copying a running system from a program running within that system can be problematic, since the system itself will change while it is trying to copy itself. FTK Imager can copy drives and files, but it would not handle a running virtual machine.

6. B. Even though Wireshark is not a dedicated network forensic tool, since network traffic is ephemeral, capturing it with a packet sniffer like Wireshark is Melissa's best option. Forensic suites are useful for analyzing captured images, not capturing network traffic, and dd and WinHex are both useful for packet capture, but not for network traffic analysis.

7. D. Forensic information does not have to include a time stamp to be admissible, but time stamps can help build a case that shows when events occurred. Files without a time stamp may still show other information that is useful to the case or may have other artifacts associated with them that can provide context about the time and date.

8. D. Chain-of-custody documentation tracks evidence throughout its life cycle, with information about who has custody or control and when transfers happened, and continues until the evidence is removed from the legal process and disposed of. The other terms are not used for this practice.

9. B. The most common cause of an hour of difference between two systems in an environment is an incorrectly set time zone. Isaac should check the time zone settings, and then correct his findings based on the time zones set on the systems if necessary.

10. C. Jurisdiction is the legal authority over an area or individuals based on laws that create the jurisdiction. Nexus defines whether a relationship or connection exists, such as a local branch or business location. Non-repudiation ensures that evidence or materials can be connected to their originator. Admissibility determines whether evidence can be used in court.

11. A. Firmware can be challenging to access, but both memory forensic techniques and direct hardware interface access are viable means in some cases. Firmware is not typically stored on the disk and instead is stored in a BIOS or UEFI chip. Removing the chip from the system will leave it unable to run and thus this is not a preferred method. Also, many chips are not removable. Shutting down the device and booting it to the firmware does not provide a means of copying the firmware for most devices. Although the firmware is likely to allow updates, most do not allow downloads or copying.

12. C. Although it may be tempting to use a technical answer, interviewing the individual involved is the best starting point when a person performed actions that need to be reviewed. Charles can interview the staff member, and then move on to technical means to validate their responses. System and event logs may have some clues to what occurred, but normal systems do not maintain a keystroke log. In fact, the closest normal element is the command log used by both Windows and Linux to allow command-line input to be recalled as needed.

13. B. Once a copy is made, hashes for the original and target drive should be compared to ensure that the copy was successful. After that, the chain-of-custody document can be updated to note that a copy was made and will be tracked as it is analyzed while the original is preserved. Wiping either drive after a copy is not part of the process, although a target drive may be wiped after a case is complete.

14. B. Quick-formatting a drive removes the file indexes but leaves the file content on the drive. Recovery tools look for those files on the drive and piece them back together using metadata, headers, and other clues that help to recover the files.

15. B. Contracts commonly include right to audit, choice of jurisdiction, and data breach notification time frame clauses, but a right to forensically examine a vendor's systems or devices is rarely included. Naomi may want to ask about their incident response process and for examples of previous breach notification and incident documentation shared with customers instead.

16. D. Chain of custody tracks who has an item, how it is collected, where it is stored and how, how it is secured or protected, who collected it, and transfers, but it does not typically include how the items were transported because that is not relevant if the other data is provided.

17. C. It is important to ensure that data prepared for e-discovery only contains what it is supposed to, and that information that should not be shared is not included. Time stamps, hashing, chain of custody, and ensuring malicious files are not included are not part of the EDRM model. Validating that a legal hold is valid should happen before preservation, but validating that documented items from the hold are included if they exist should occur.

18. C. Removing information relevant to a legal hold is exactly what the hold is intended to prevent. Theresa's organization could be in serious legal trouble if they were to intentionally purge or change related information.

19. C. Backups are the least volatile of these options according to the order of volatility. Backups will be kept until they are aged out, which may be days, weeks, or even months in some cases. From most to least volatile, these are RAM, data on the hard drive, remote logs, and then backups.

20. A. Although both a checksum and a hash can be used to validate message integrity, a hash has fewer collisions than a checksum and will also provide a unique fingerprint for a file. Checksums are primarily used as a quick means of checking that that integrity is maintained, whereas hashes are used for many other purposes such as secure password validation without retaining the original password. A checksum would not be useful for proving a forensic image was identical, but it could be used to ensure that your work had not changed the contents of the drive.

Chapter 16: Security Governance and Compliance

1. B. The key phrase in this scenario is "one way." This indicates that compliance with the document is not mandatory, so Joe must be authoring a guideline. Policies, standards, and procedures are all mandatory.

2. A. PCI DSS compensating controls must be "above and beyond" other PCI DSS requirements. This specifically bans the use of a control used to meet one requirement as a compensating control for another requirement.

3. C. The General Data Protection Regulation (GDPR) implements privacy requirements for handling the personal information of EU residents. The Health Insurance Portability and Accountability Act (HIPAA) includes security and privacy rules that affect health-care providers, health insurers, and health information clearinghouses. The Family Educational Rights and Privacy Act (FERPA) applies to educational institutions. The Payment Card Industry Data Security Standard (PCI DSS) applies to credit and debit card information.

4. B. The five security functions described in the NIST Cybersecurity Framework are identify, protect, detect, respond, and recover.

5. C. The International Organization for Standardization (ISO) publishes ISO 27701, covering privacy controls. ISO 27001 and 27002 cover cybersecurity, and ISO 31000 covers risk management.

6. D. Policies require approval from the highest level of management, usually the CEO. Other documents may often be approved by other managers, such as the CISO.

7. C. Master service agreements (MSAs) provide an umbrella contract for the work that a vendor does with an organization over an extended period of time. The MSA typically includes detailed security and privacy requirements. Each time the organization enters into a new project with the vendor, they may then create a statement of work (SOW) that contains project-specific details and references the MSA.

8. B. All of these organizations produce security standards and benchmarks. However, only the Center for Internet Security (CIS) is known for producing independent benchmarks covering a wide variety of software and hardware.

9. C. Many organizations use scheduled maintenance windows to coordinate changes to information systems. These windows are preplanned and announced times when all non-emergency changes will take place and often occur on evenings and weekends. A change management process ensures that personnel can perform a security impact analysis. Experts evaluate changes to identify any security impacts before personnel deploy the changes in a production environment. A backout plan allows personnel to undo the change and return the system to its previous state if necessary. Version control ensures that developers and users have access to the latest versions of software and that changes are carefully managed throughout the release process.

10. B. Security policies do not normally contain prescriptive technical guidance, such as a requirement to use a specific encryption algorithm. This type of detail would normally be found in a security standard.

11. C. Alice's exercise is designed to evaluate how well employees can identify phishing messages and, if they fail to do so, redirect them to a training program that is meant to help them get better at recognizing such messages. The exercise is meant for educational purposes and not for penalizing employees. It is intended to help them improve their skills in recognizing phishing emails. While rewarding employees for identifying phishing emails could be a component of a security awareness program, the exercise described is primarily educational and is focused on helping those who fail to recognize the phishing messages. While data might be collected for analysis and understanding areas where improvement is needed, the intention is not to label departments as gullible.

12. B. An organization's acceptable use policy (AUP) should contain information on what constitutes allowable and unallowable use of company resources. This policy should contain information to help guide Tonya's next steps.

13. D. The Payment Card Industry Data Security Standard (PCI DSS) provides detailed rules about the storage, processing, and transmission of credit and debit card information. PCI DSS is not a law but rather a contractual obligation that applies to credit card merchants and service providers.

14. B. As an information security manager, Mike's primary role would be to establish an effective security training and awareness program, promote it within the organization, and ensure it is maintained effectively to foster a security-conscious culture among employees. This aligns with a proactive approach to reducing security incidents. Mike should take an active role in security training and awareness, rather than delegating all responsibilities to another department. While HR may be involved, Mike's expertise is crucial in establishing effective programs. Although security awareness posters and training sessions are two components of security awareness efforts, Mike's role should be much broader, encompassing the establishment, promotion, and maintenance of comprehensive training and awareness programs.

15. D. Mandatory vacations are designed to force individuals to take time away from the office to allow fraudulent activity to come to light in their absence. The other controls listed here (separation of duties, least privilege, and dual control) are all designed to prevent, rather than detect, fraud.

16. D. Guidelines are the only element of the security policy framework that is optional. Compliance with policies, standards, and procedures is mandatory.

17. A. Security training typically involves structured and formal programs where employees learn new security concepts and practices. In contrast, security awareness efforts are more informal and aim to keep security principles top-of-mind for employees through reminders, without requiring them to engage in formal learning. The idea that security training involves giving rewards to employees and awareness efforts involve punishments is not accurate. Security training is meant to educate employees on security concepts and practices, not to serve as a platform for rewards. Similarly, awareness efforts are not punitive; they serve to remind and reinforce security principles among employees. The statement that there is no difference between security training and awareness efforts and that both terms can be used interchangeably is also incorrect. There is a distinct difference between the two in terms of their structure and purpose, as explained in the correct answer. Lastly, the notion that security training is only for security team members while security awareness is for all employees is not true. Security training is important for all employees, depending on their roles and responsibilities, to ensure they understand the security protocols and policies. Security awareness, on the other hand, is a continual reminder for all employees, including the security team, to stay vigilant and informed about security practices.

18. B. Standards describe specific security controls that must be in place for an organization. Allan would not include acceptable mechanisms in a high-level policy document, and this information is too general to be useful as a procedure. Guidelines are not mandatory, so they would not be applicable in this scenario.

19. D. The NIST Cybersecurity Framework is designed to help organizations describe their current cybersecurity posture, describe their target state for cybersecurity, identify and prioritize opportunities for improvement, assess progress, and communicate with stakeholders about risk. It does not create specific technology requirements.

20. C. Requests for an exception to a security policy would not normally include a proposed revision to the policy. Exceptions are documented variances from the policy because of specific technical and/or business requirements. They do not alter the original policy, which remains in force for systems not covered by the exception.

Chapter 17: Risk Management and Privacy

1. C. By applying the patch, Jen has removed the vulnerability from her server. This also has the effect of eliminating this particular risk. Jen cannot control the external threat of an attacker attempting to gain access to her server.

2. C. Installing a web application firewall reduces the probability that an attack will reach the web server. Vulnerabilities may still exist in the web application and the threat of an external attack is unchanged. The impact of a successful SQL injection attack is also unchanged by a web application firewall.

3. C. The asset at risk in this case is the customer database. Losing control of the database would result in a $500,000 fine, so the asset value (AV) is $500,000.

4. D. The attack would result in the total loss of customer data stored in the database, making the exposure factor (EF) 100 percent.

5. C. We compute the single loss expectancy (SLE) by multiplying the asset value (AV) ($500,000) and the exposure factor (EF) (100%) to get an SLE of $500,000.

6. A. Aziz's threat intelligence research determined that the threat has a 5 percent likelihood of occurrence each year. This is an ARO of 0.05.

7. B. We compute the annualized loss expectancy (ALE) by multiplying the SLE ($500,000) and the ARO (0.05) to get an ALE of $25,000.

8. C. Installing new controls or upgrading existing controls is an effort to reduce the probability or magnitude of a risk. This is an example of a risk mitigation activity.

9. B. Changing business processes or activities to eliminate a risk is an example of risk avoidance.

10. D. Insurance policies use a risk transference strategy by shifting some or all of the financial risk from the organization to an insurance company.

11. A. When an organization decides to take no further action to address remaining risk, they are choosing a strategy of risk acceptance.

12. A. Under the GDPR, the data protection officer (DPO) is an individual assigned direct responsibility for carrying out an organization's privacy program.

13. A. In this case, the physicians maintain the data ownership role. They have chosen to outsource data processing to Helen's organization, making that organization a data processor.

14. C. The Recovery Time Objective (RTO) is the amount of time that the organization can tolerate a system being down before it is repaired. That is the metric that Gene has identified in this scenario.

15. B. This is a tricky question, as it is possible that all of these categories of information may be found in patient records. However, they are most likely to contain protected health information (PHI). PHI could also be described as a subcategory of personally identifiable information (PII), but PHI is a better description. It is also possible that the records might contain payment card information (PCI) or personal financial information (PFI), but that is less likely than PHI.

16. C. Organizations should only use data for the purposes disclosed during the collection of that data. In this case, the organization collected data for technical support purposes and is now using it for marketing purposes. That violates the principle of purpose limitation.

17. C. Top Secret is the highest level of classification under the U.S. system and, therefore, requires the highest level of security control.

18. D. Quantitative risk analysis uses numeric data in the analysis, resulting in assessments that allow the very straightforward prioritization of risks. Qualitative risk analysis substitutes subjective judgments and categories for strict numerical analysis, allowing the assessment of risks that are difficult to quantify. A one-time risk assessment offers the organization a point-in-time view of its current risk state. Recurring risk assessments are performed at regular intervals, such as annually or quarterly.

19. B. Data controllers are the entities who determine the reasons for processing personal information and direct the methods of processing that data. This term is used primarily in European law, and it serves as a substitute for the term *data owner* to avoid a presumption that anyone who collects data has an ownership interest in that data.

20. D. The residual risk is the risk that remains after an organization implements controls designed to mitigate, avoid, and/or transfer the inherent risk.

Online Test Bank

To help you study for your CompTIA Security+ certification exam, register to gain one year of FREE access after activation to the online interactive test bank—included with your purchase of this book! All of the chapter review questions and the practice tests in this book are included in the online test bank so you can practice in a timed and graded setting.

Register and Access the Online Test Bank

To register your book and get access to the online test bank, follow these steps:

1. Go to `www.wiley.com/go/sybextestprep`. You'll see the **"How to Register Your Book for Online Access"** instructions.
2. Click "here to register" and then select your book from the list.
3. Complete the required registration information, including answering the security verification to prove book ownership. You will be emailed a pin code.
4. Follow the directions in the email or go to `www.wiley.com/go/sybextestprep`.
5. Find your book on that page and click the "Register or Login" link with it. Then enter the pin code you received and click the "Activate PIN" button.
6. On the Create an Account or Login page, enter your username and password, and click Login or, if you don't have an account already, create a new account.
7. At this point, you should be in the test bank site with your new test bank listed at the top of the page. If you do not see it there, please refresh the page or log out and log back in.

SYBEX®
A Wiley Brand