CompTIA CASP+ CAS-004 Certification Guide

Develop CASP+ skills and learn all the key topics needed to prepare for the certification exam

Mark Birch

Chapter 1

Figure

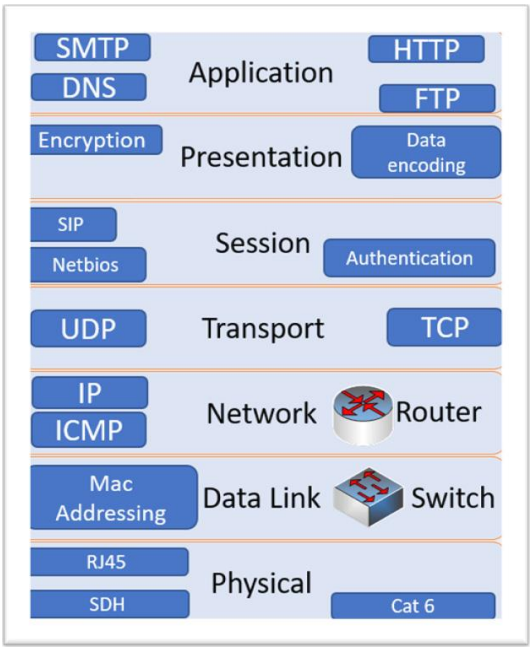


Figure 1.1 – OSI 7-layer model

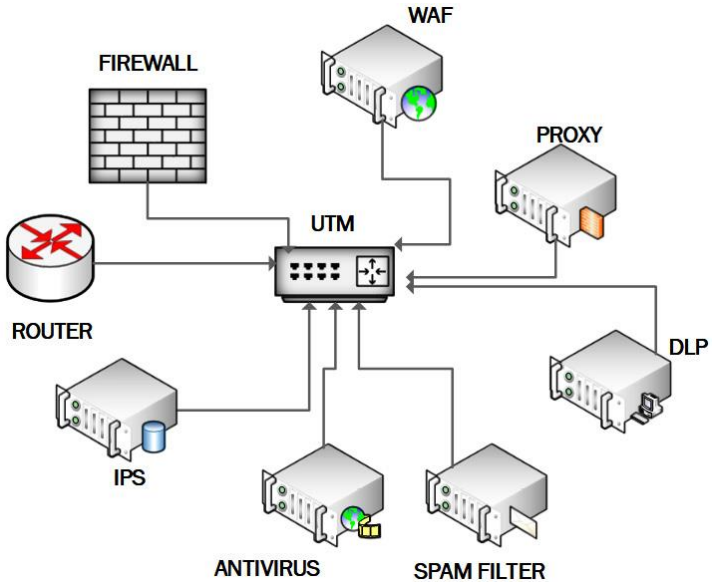


Figure 1.2 – UTM appliance

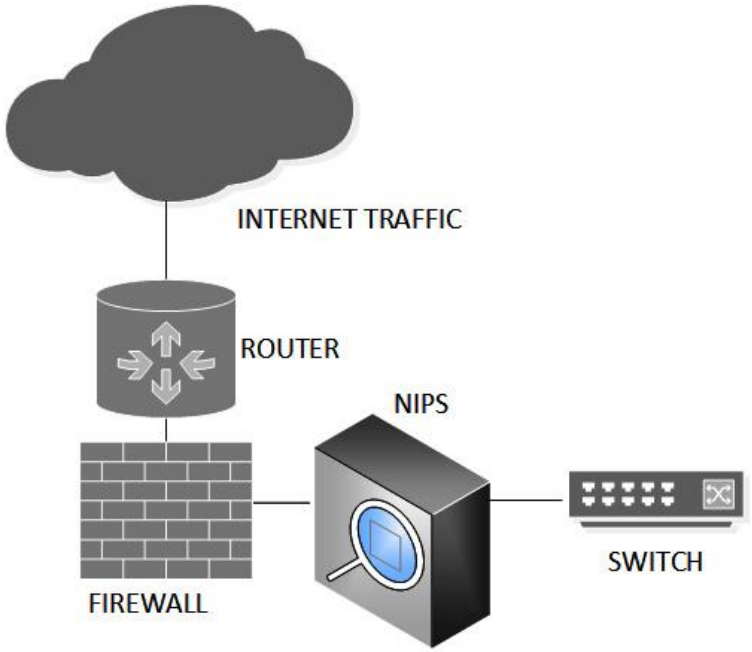


Figure 1.3 – NIPS placement (inline)

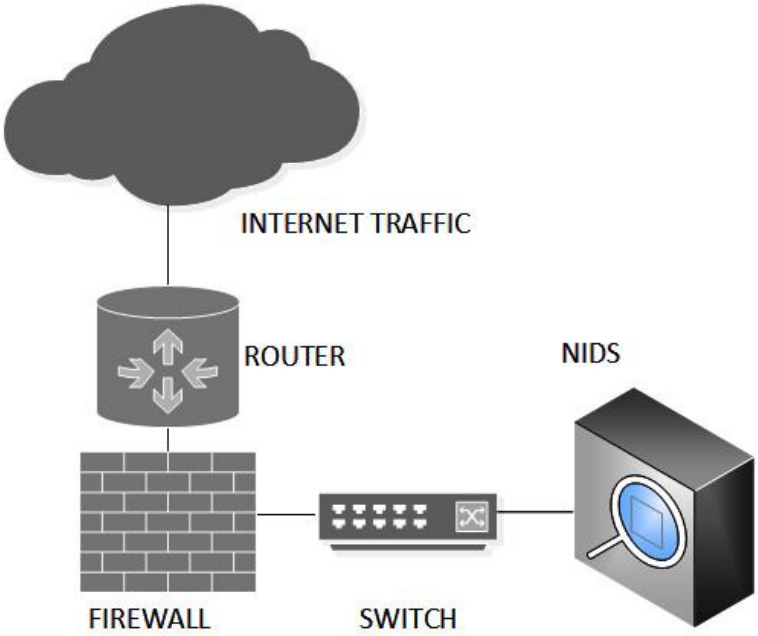


Figure 1.4 – NIDS placement

Figure 1.5 – INE device

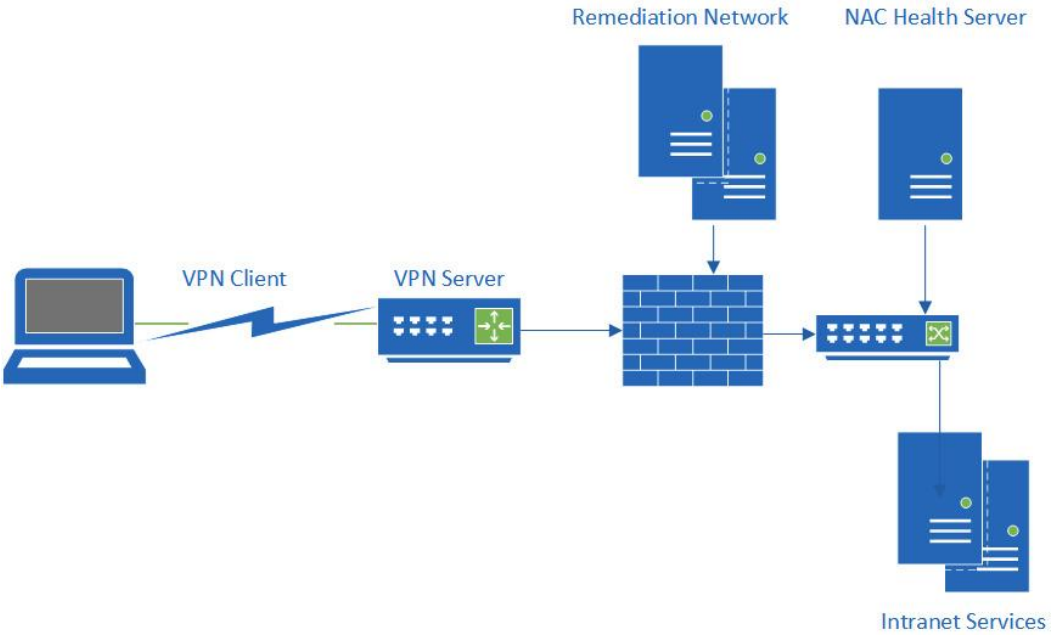


Figure 1.6 – NAC

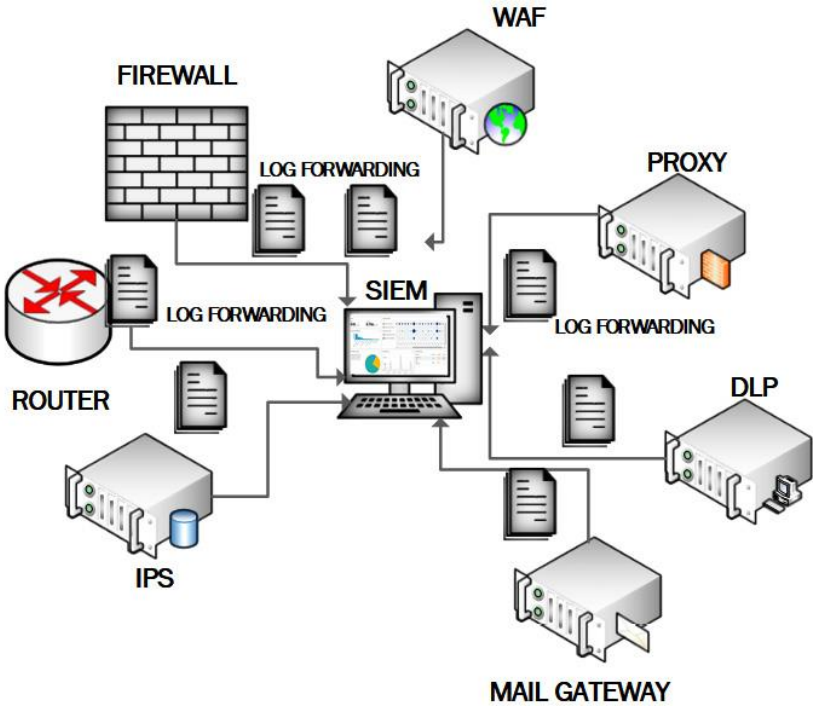


Figure 1.7 – SIEM architecture

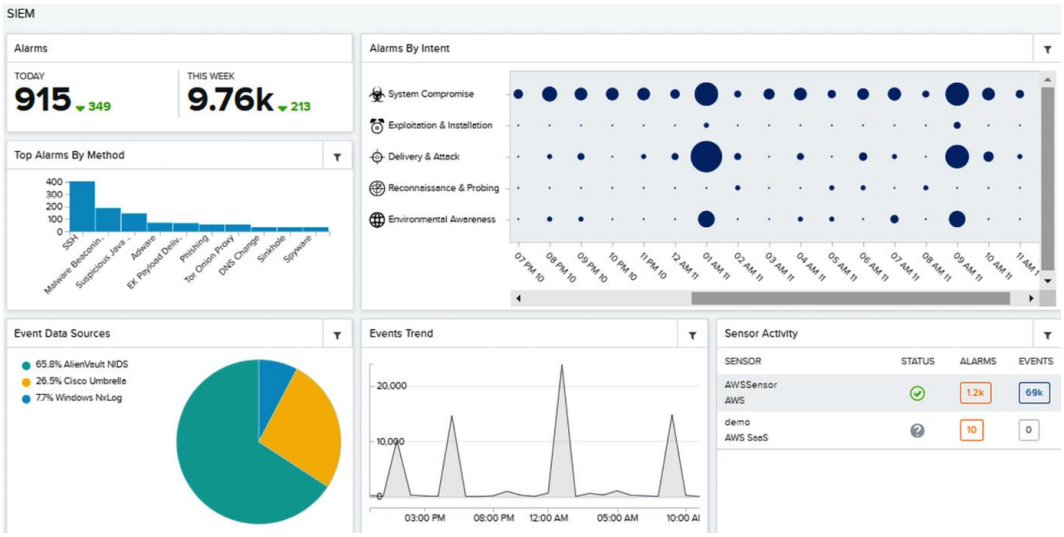


Figure 1.8 – AlienVault/AT&T SIEM dashboard

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0005.5e2e.9319    DYNAMIC     Gig0/1
   1    0060.2f1c.6359    DYNAMIC     Gig0/1
   1    0060.7004.101c    DYNAMIC     Fa0/4
   1    00d0.58b1.3abd    DYNAMIC     Gig0/1
   1    00d0.9719.2339    DYNAMIC     Gig0/1
Switch>
```

Figure 1.9 – Switch table

NETWORK DESTINATION	NETMASK	GATEWAY	INTERFACE	METRIC
0.0.0.0	0.0.0.0	10.0.0.1	10.0.0.254	20
172.16.0.0	255.255.0.0	172.30.0.1	172.30.0.254	30
172.17.0.0	255.255.0.0	172.30.0.1	172.30.0.254	30
172.18.0.0	255.255.0.0	172.30.0.1	172.30.0.254	30

Figure 1.10 – Routing table

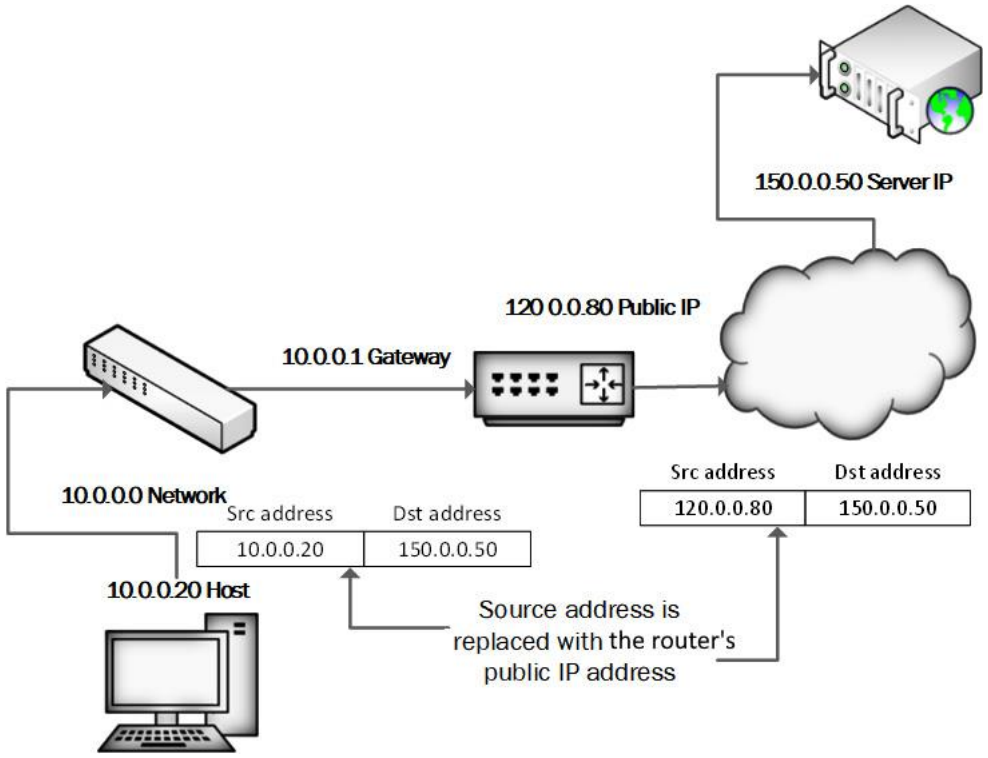


Figure 1.11 – NAT routing

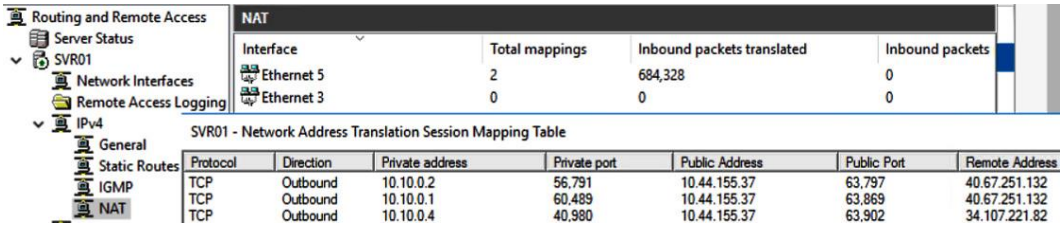


Figure 1.12 – Microsoft Routing and Remote Access Service (RRAS) with connected clients

Figure 1.13 – MicroSD HSM

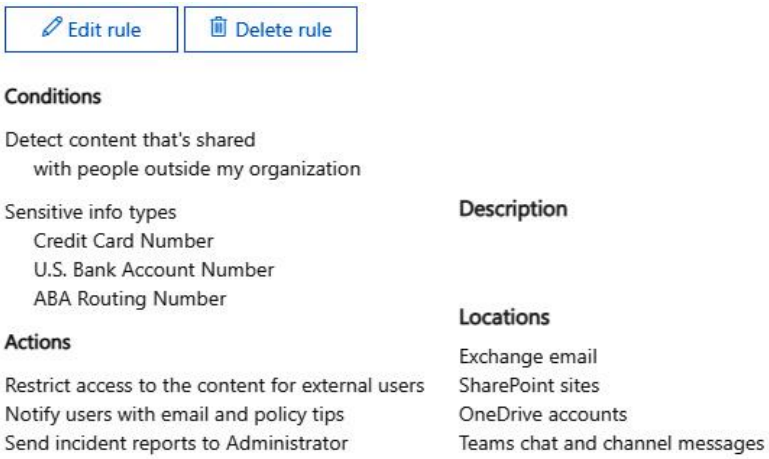


Figure 1.14 – Microsoft 365 DLP rule

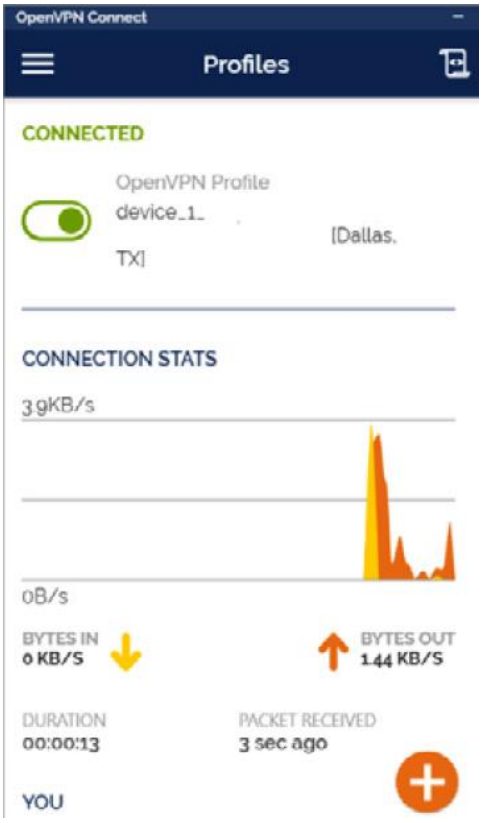


Figure 1.16 – OpenVPN client

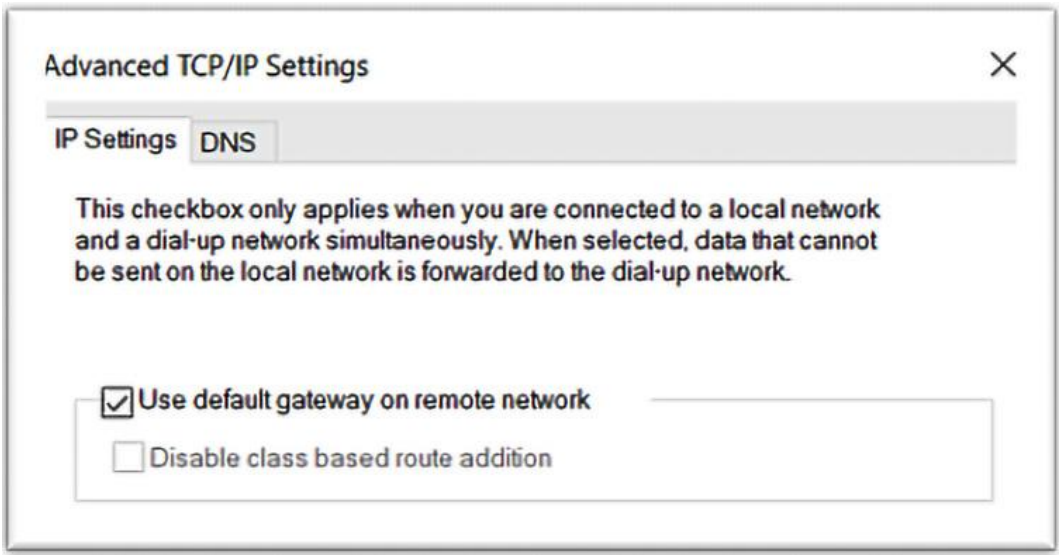


Figure 1.17 – Full-tunnel configuration

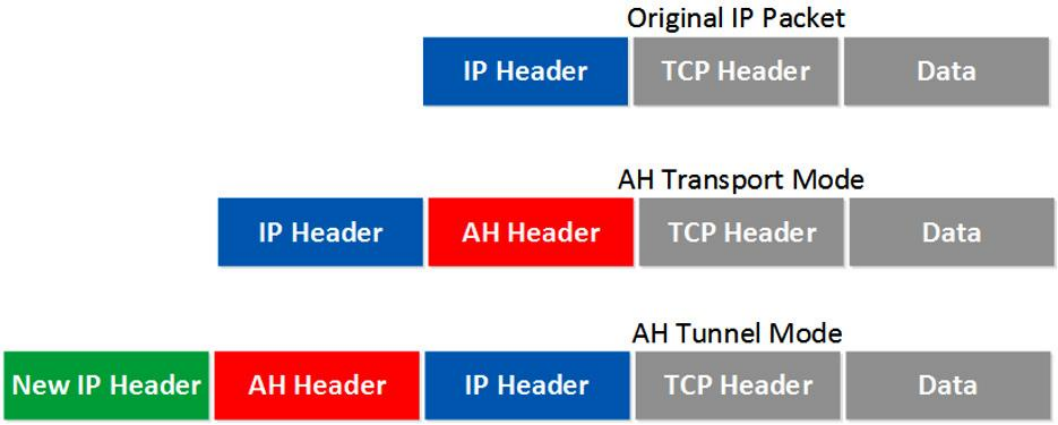


Figure 1.18 – IPsec modes

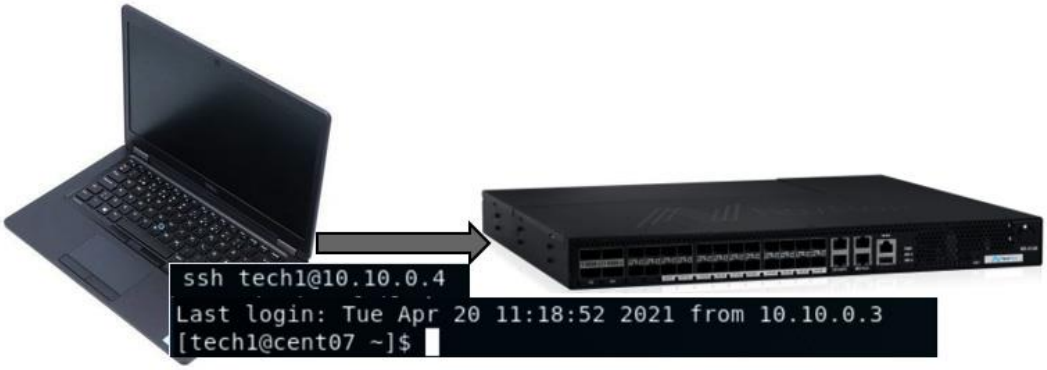


Figure 1.19 – SSH remote security

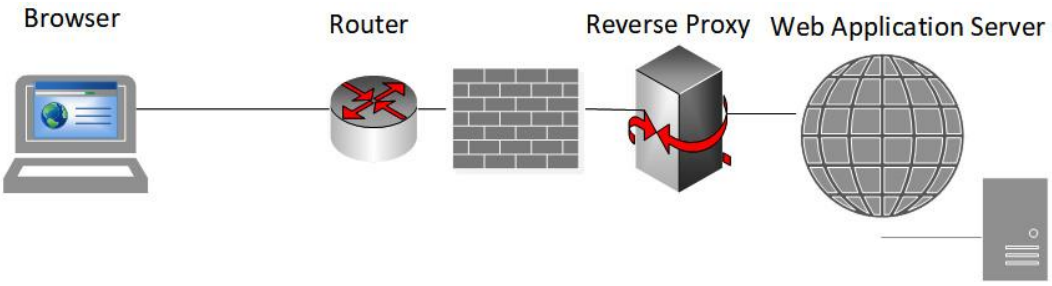


Figure 1.20 – Reverse proxy

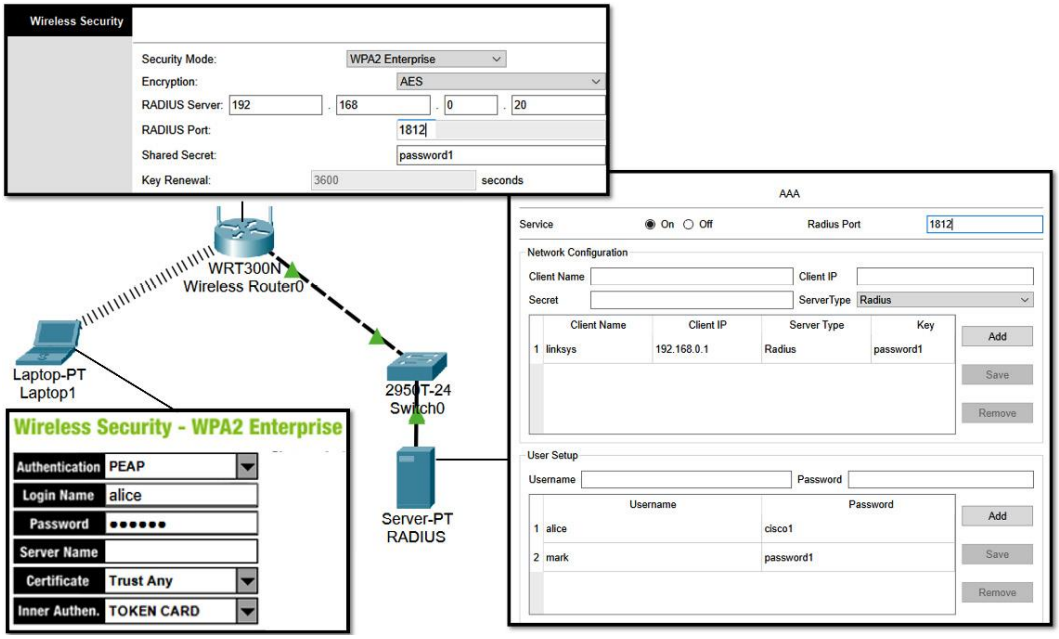


Figure 1.21 – Network authentication

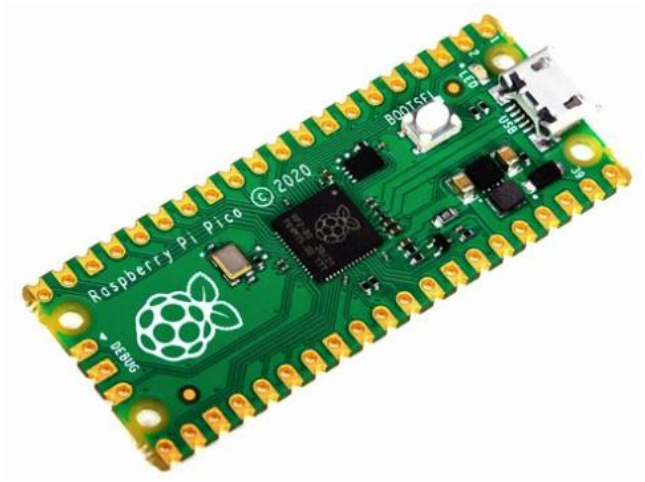


Figure 1.22 – Raspberry Pi

Figure 1.23 – Temperature monitoring sensor

Figure 1.24 – Unsecured IP cameras

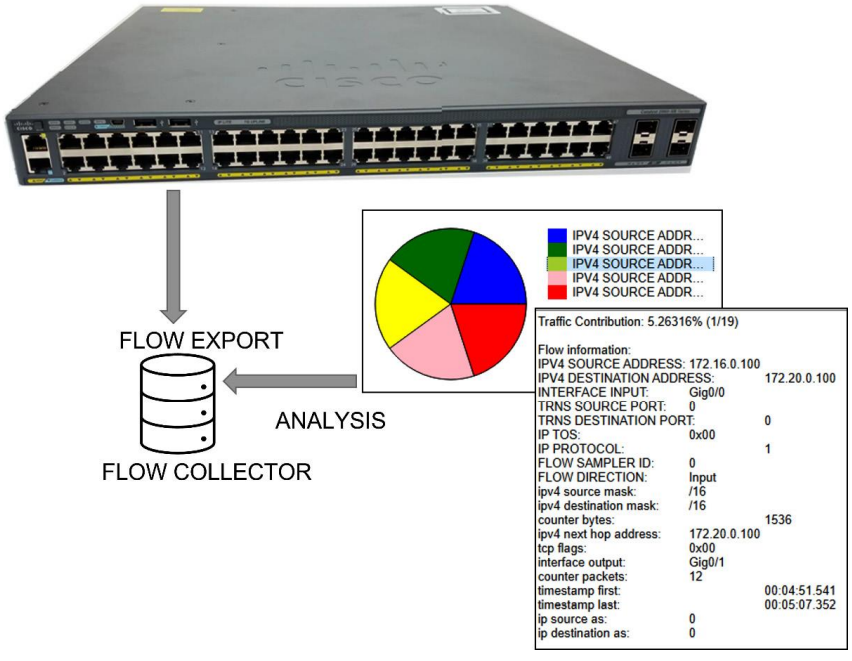


Figure 1.25 – NetFlow

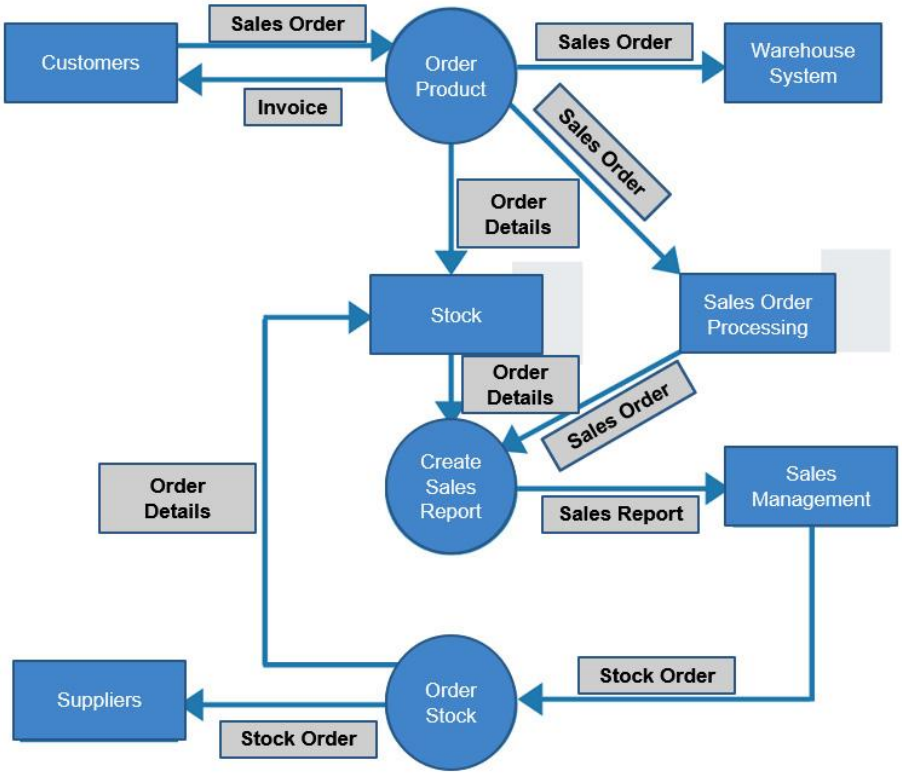


Figure 1.26 – DFD

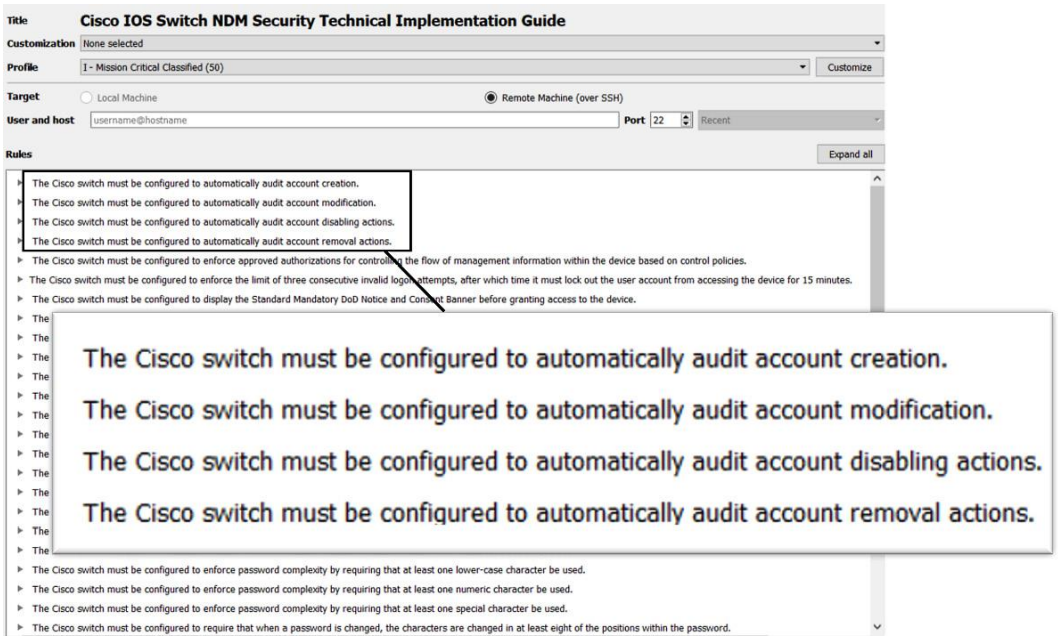


Figure 1.27 – Cisco IOS Switch security baseline

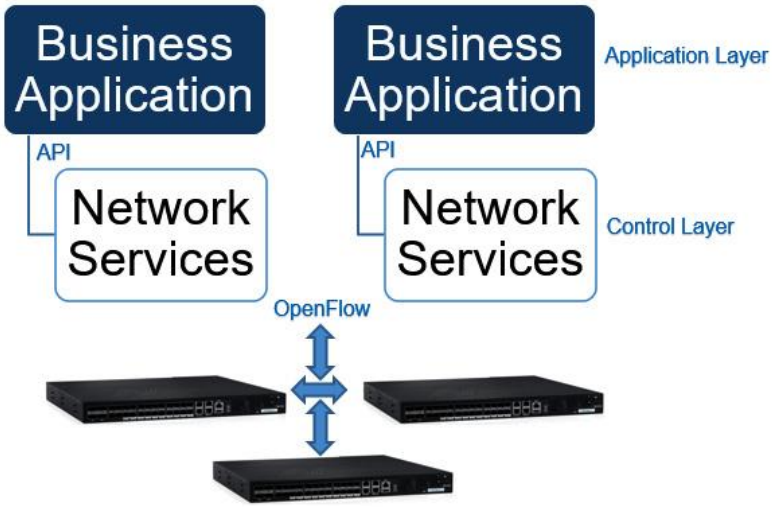


Figure 1.28 – SDN

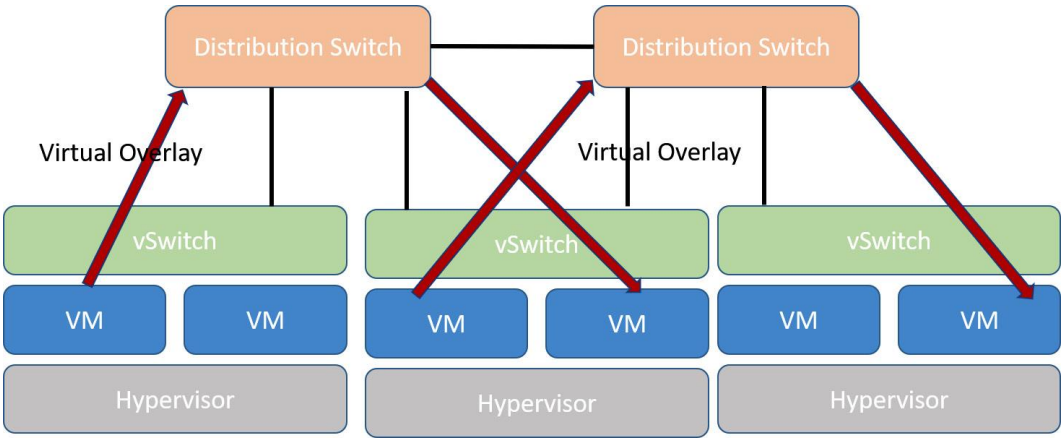


Figure 1.29 – SDN overlay

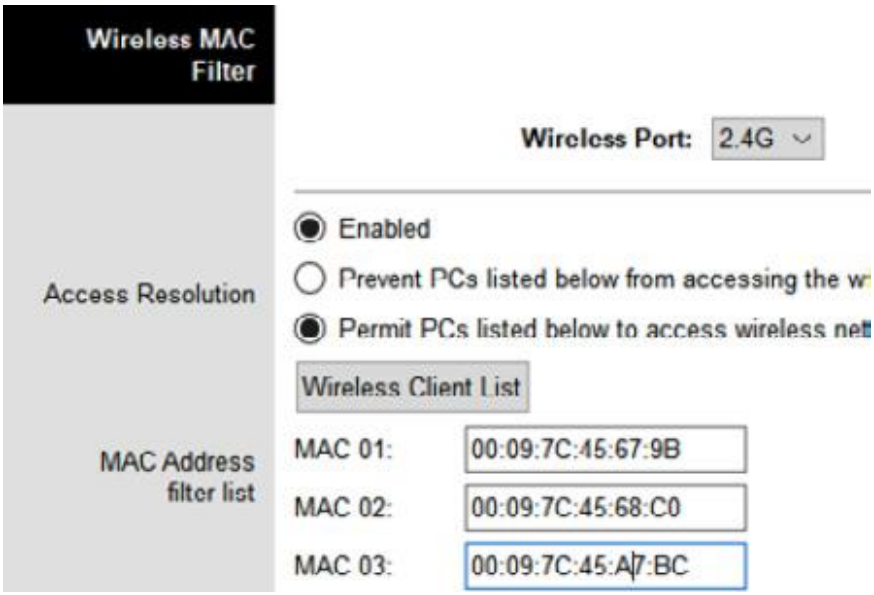


Figure 1.30 – Wireless ACL

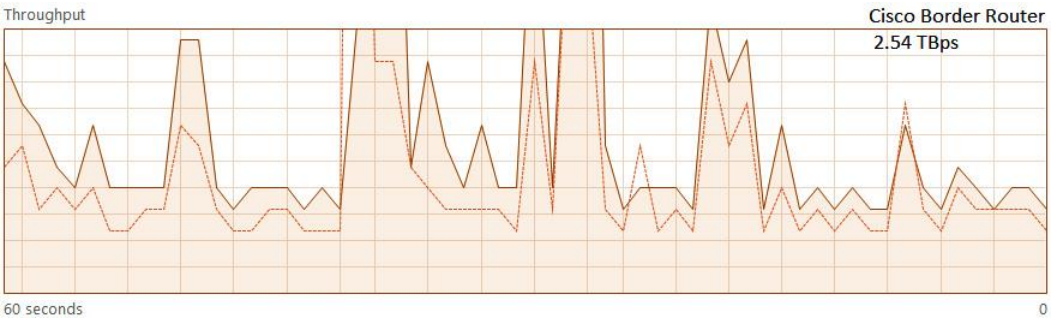


Figure 1.31 – DDoS attack traffic

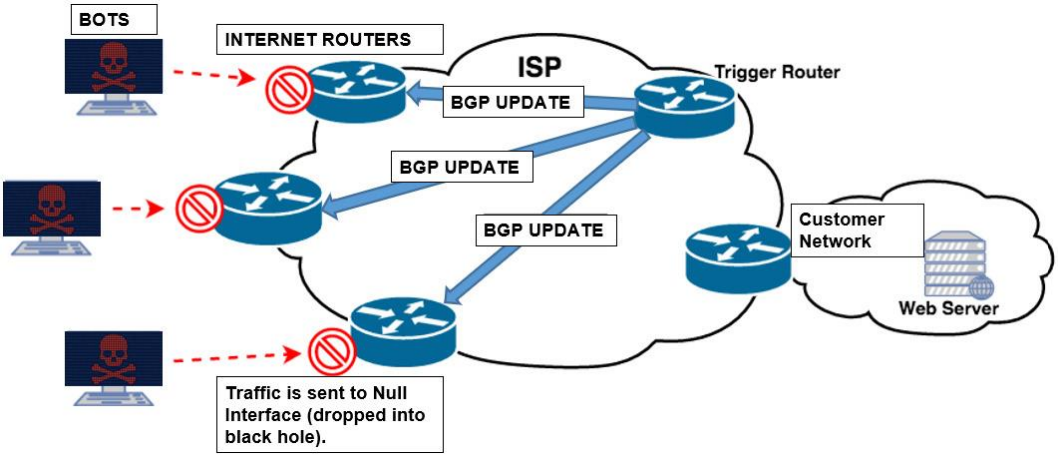


Figure 1.32 – RTBH

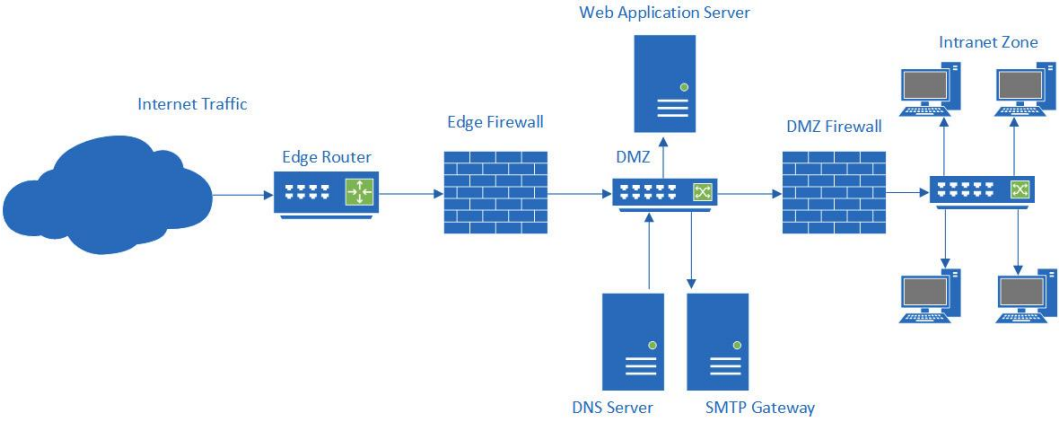


Figure 1.33 – DMZ network zone

Links

Critical infrastructure tools, tactics, and protocols are documented by MITRE (see the following link: https://tinyurl.com/mitreics). For more information on the Ukrainian power grid attack, please go to this link: https://tinyurl.com/icspowerattack

In 2018, the NSA was attacked and suffered a significant data breach due to an unauthorized Raspberry Pi device connected to the agency's network. To read more about this published incident, see this link: https://tinyurl.com/nasapihack.

Questions

Here are a few questions to test your understanding of the chapter:

1. Which is the security module that would store an e-commerce server's private key?
    A. DLP
    B. HSM
    C. DPI
    D. 802.1x
2. How can I mitigate the threat of data leakage?
    A. Through DLP
    B. Through HSM
    C. Through DPI
    D. Through 802.1x
3. What type of IDS would I be using if I needed to update my definition files?
    A. Anomaly
    B. Behavior
    C. Heuristics
    D. Signature
4. What is the purpose of iptables on a host computer?
    A. Routing
    B. Firewall
    C. Switching
    D. Encryption
5. Which protocol would be used to manage a router securely from a technician's laptop?
    A. Telnet
    B. RDP
    C. SSH
    D. FTP

6. How should I protect my management interface on a switch when I need to configure it remotely? Choose two answers.

   A. OSPF

   B. OOB management

   C. Strong password

   D. RIP v2

7. What is an Ethernet standard for port access protocol, used for protecting networks via authentication?

   A. 802.11

   B. 802.3

   C. 802.1x

   D. 802.5

8. What type of connectivity will allow key personnel to maintain communication with one another and key network resources when the main network is under attack?

   A. Email

   B. OOB

   C. Teams

   D. VNC

9. What is a disadvantage when using a **virtual desktop infrastructure** (**VDI**)?

   A. Reliance on networks

   B. Better use of hardware resources

   C. Enhanced security

   D. Standard operating environment (SOE)

10. What is used when my contractors use a tablet or thin client to access a Windows 10 desktop in my data center?

    A. OOB

    B. MDM

    C. VDI

    D. SSH

11. What type of routing will help to mitigate a DDoS attack?
    A. OSPF
    B. RTBH
    C. RIP
    D. EIGRP
12. What is it when SOC staff are failing to respond to alerts due to excessive levels of alerts?
    A. False positive
    B. Alert fatigue
    C. False negative
    D. True positive
13. What will I need to support on my network device in order to forward truncated network traffic to a network monitoring tool?
    A. NetFlow
    B. sFlow
    C. SIEM
    D. System Logging Protocol (Syslog)
14. What type of security would I use on my layer 2 switch to isolate the finance network from the development network?
    A. VPN
    B. IPsec
    C. VLAN
    D. RTBH
15. What type of servers would the security team place on the DMZ network?
    A. Web Application server
    B. SMTP Gateway
    C. Intranet File Server
    D. Finance Department Payoll Server
16. What type of security label would CISA assign to the chemical sector and communications sector?

A. Regulated industry

B. Protected infrastructure

C. SCADA

D. Critical infrastructure

17. What will protect my Wi-Fi network against common threats, including evil-twin/rogue APs and DDoS?

A. 802.1x

B. Host-based IPS (HIPS)

C. Firewall

D. WIPS

18. What should I configure on mobile users' laptop computers to ensure they will not be vulnerable to sniffing/eavesdropping when accessing the hotel's Wi-Fi network?

A. Anti-malware

B. Shielding

C. Cable locks

D. VPN

19. Which edge security appliance should be recommended for an organization that has no dedicated security team and needs multiple security protection functions?

A. Router

B. WAF

C. UTM

D. DLP

20. What should be used to connect a remote government agency across public networks (note that it needs to support the NSA suite of encryption protocols)?

A. VPN

B. HAIPE

C. VLAN

D. Protected distribution

Case study

You are employed as **chief information security officer** (**CISO**) for MORD Motor Cars U.K. You are meeting with the network team to discuss the proposed plan for the new data center. A new customer-facing e-commerce site will be run from a brand-new office and data center in Coventry, **United Kingdom** (**UK**).

The data center will also allow collaboration with a Chinese manufacturing company, through the addition of **business-to-business** (**B2B**) portals.

Place each device in the position that will offer the best security for the network. For bonus points, which ports need to be opened on the firewall?

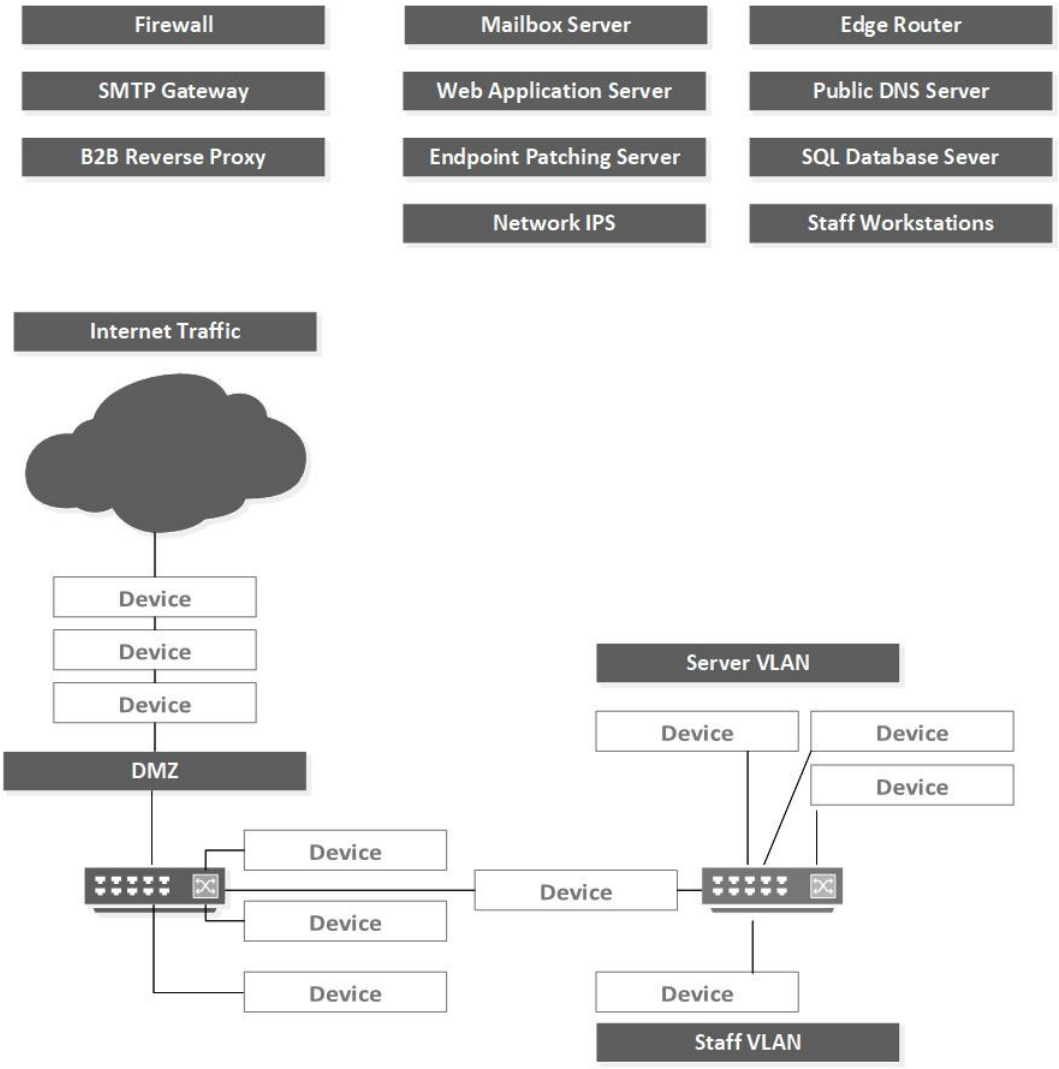


Figure 1.34 – Case study

Answers

1. B
2. A

3. D
4. B
5. C
6. B and C
7. C
8. B
9. A
10. C
11. B
12. B
13. B
14. C
15. A and B
16. D
17. D
18. D
19. C
20. B

Case study answer

The following placement will ensure a strong security posture for our network, although there are additional controls that would further enhance the organization's security, such as DLP, SIEM, and **DNS Security Extensions** (**DNSSEC**):

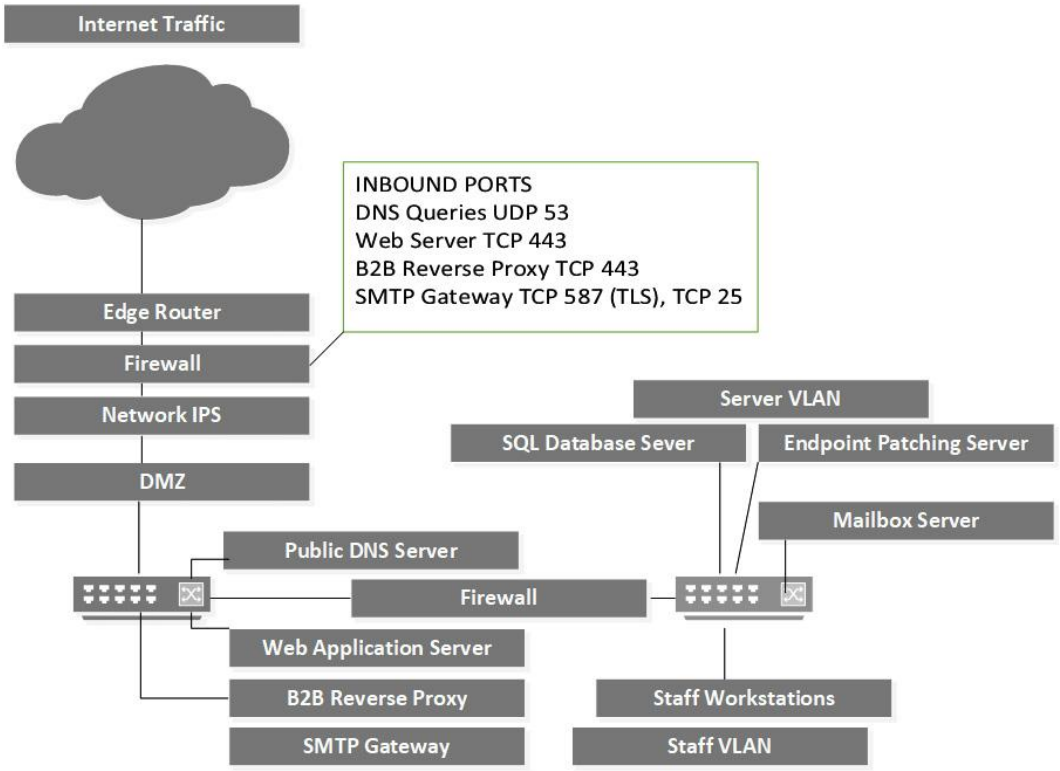


Figure 1.35 – Case study (answer)

Chapter 2

Figure

Figure 2.1 – SDLC process

ID #	Description	Source	Objective	Method
Webapp-01	Ensure all data is encrypted in transit	Design team	Test encryption method used	Data flow analysis using Wireshark
Webapp-02	Ensure all data inputs are validated	Design team	Ensure correct data inputs and exception handling	Fuzzing tool

Figure 2.2 – SRTM

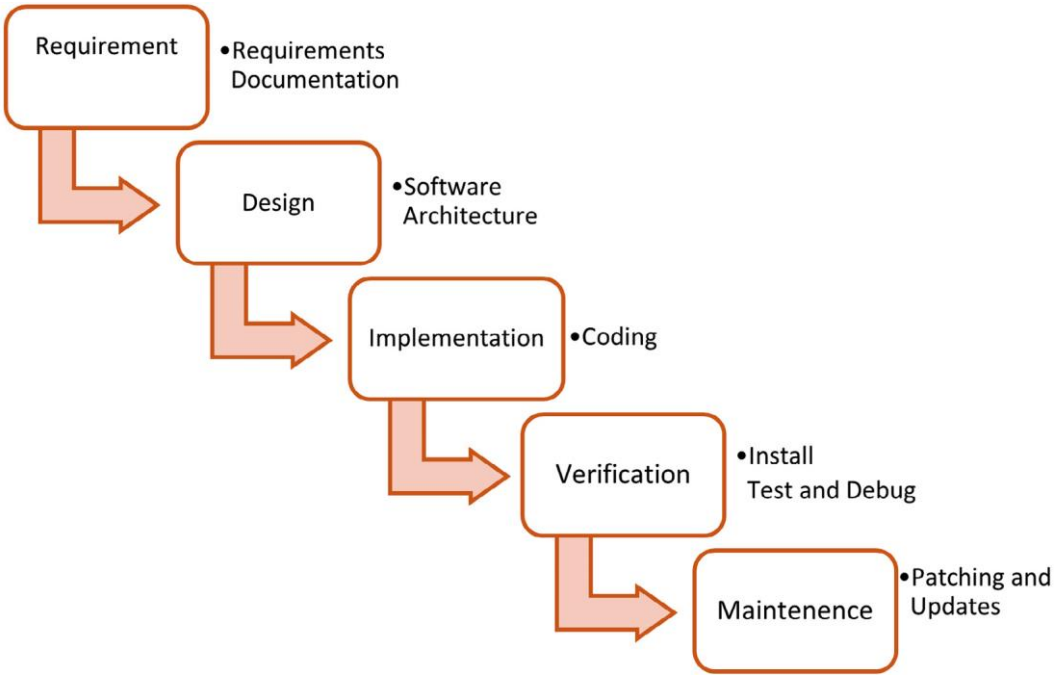


Figure 2.3 – Waterfall Methodology

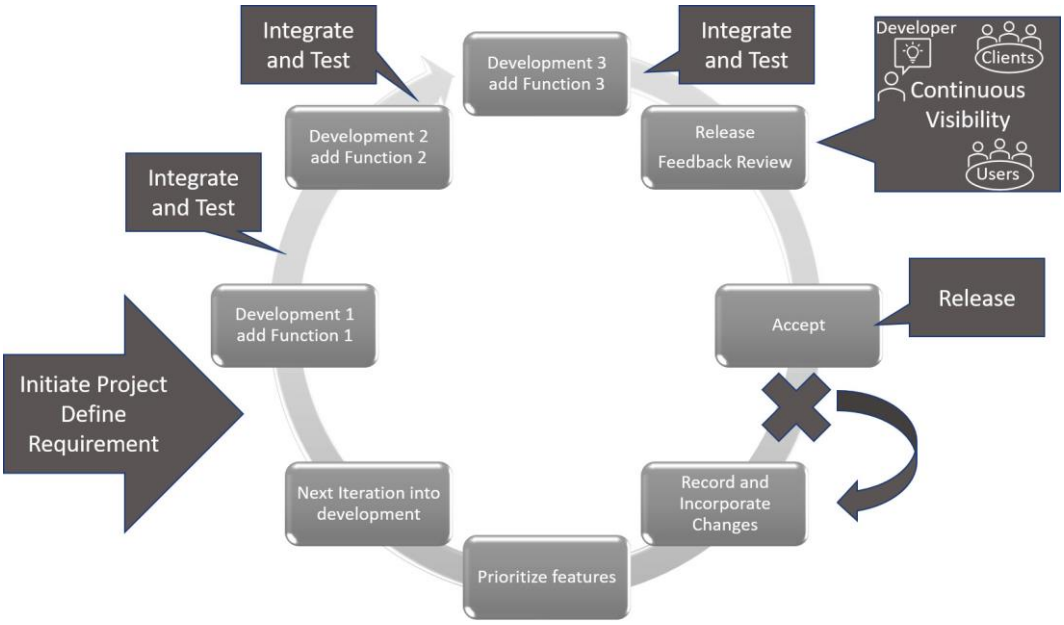


Figure 2.4 – Agile development cycle

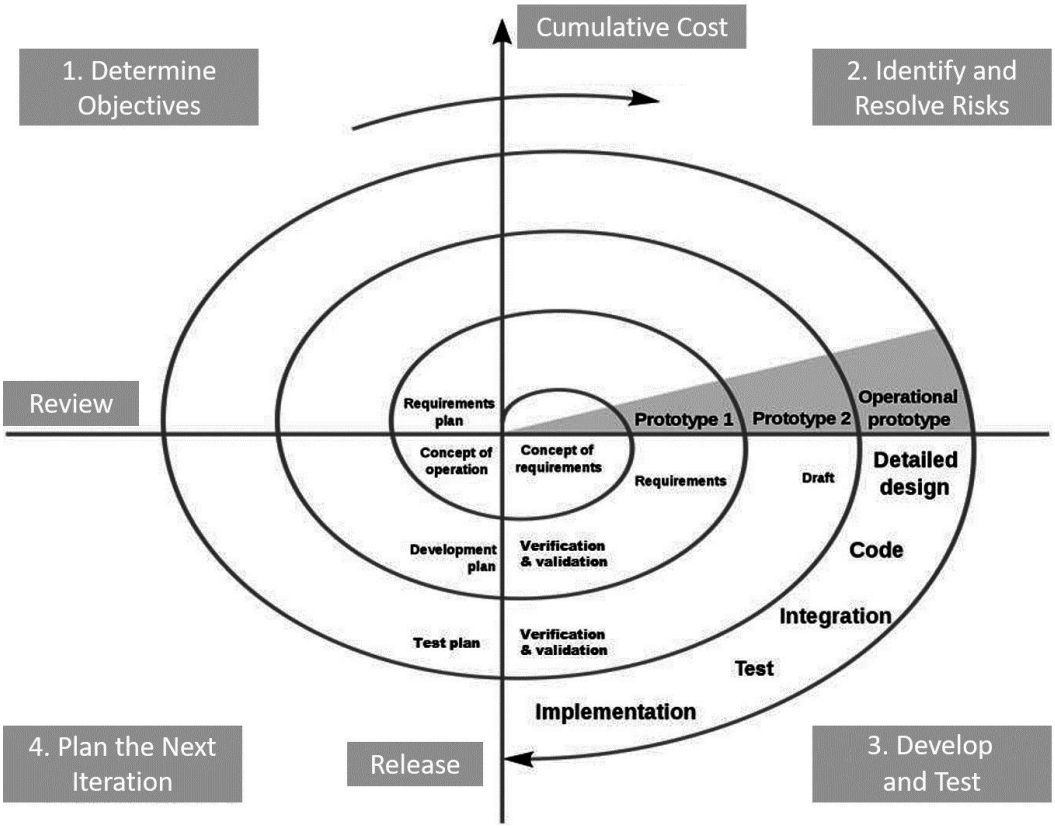


Figure 2.5 – Spiral model

Figure 2.6 – Versioning

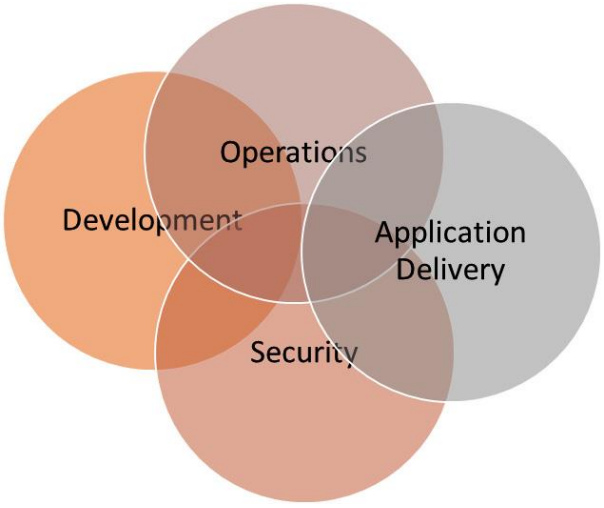


Figure 2.7 – SecDevOps

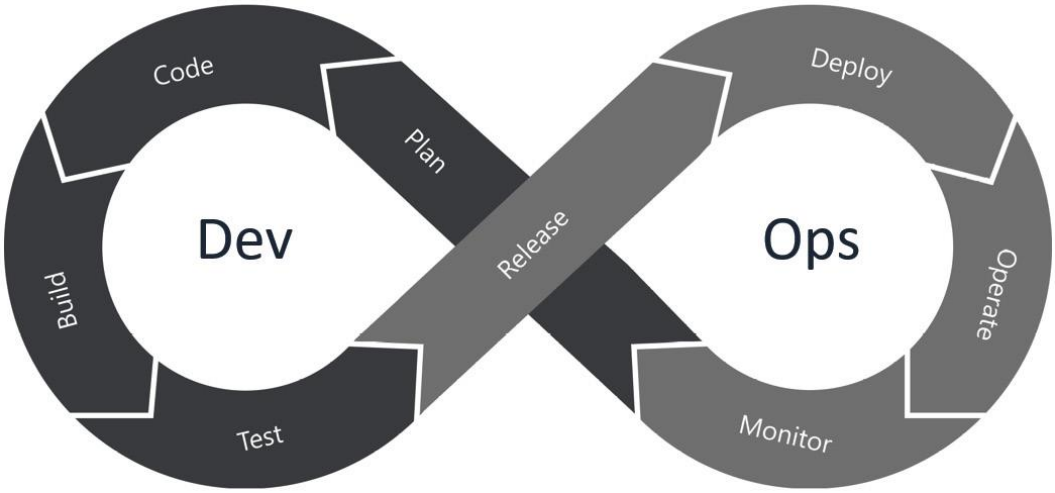
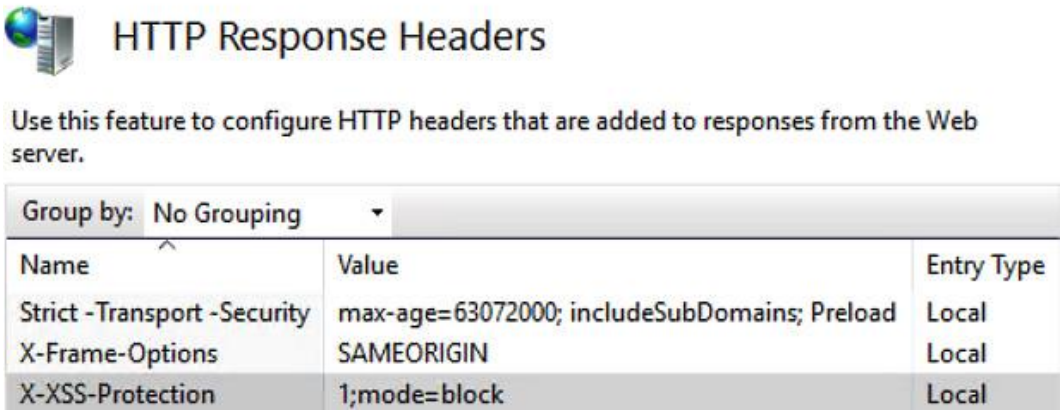


Figure 2.8 – DevOps pipeline



HTTP Response Headers

Use this feature to configure HTTP headers that are added to responses from the Web server.

Group by: No Grouping

Name	Value	Entry Type
Strict -Transport -Security	max-age=63072000; includeSubDomains; Preload	Local
X-Frame-Options	SAMEORIGIN	Local
X-XSS-Protection	1;mode=block	Local

Figure 2.9 – Securing HTTP response headers

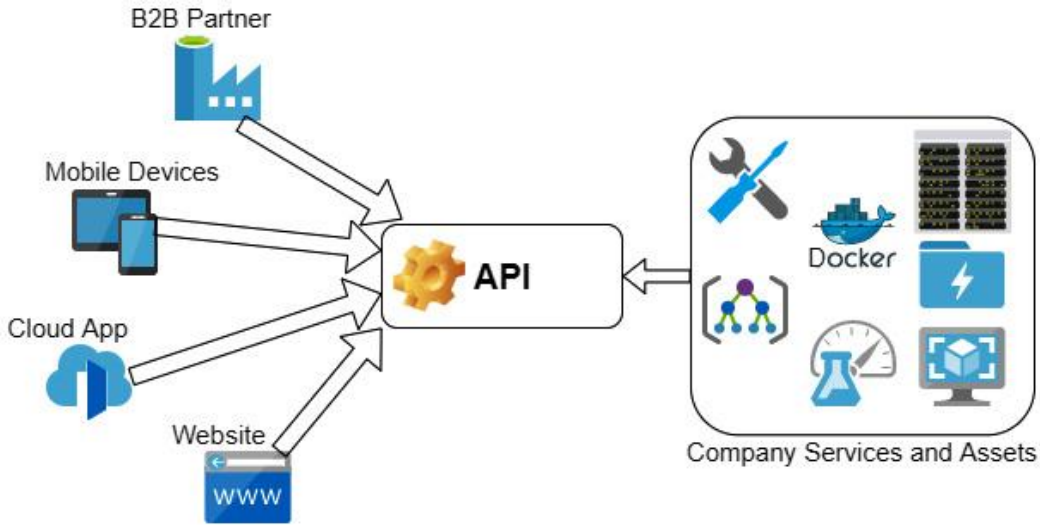


Figure 2.10 – Management API

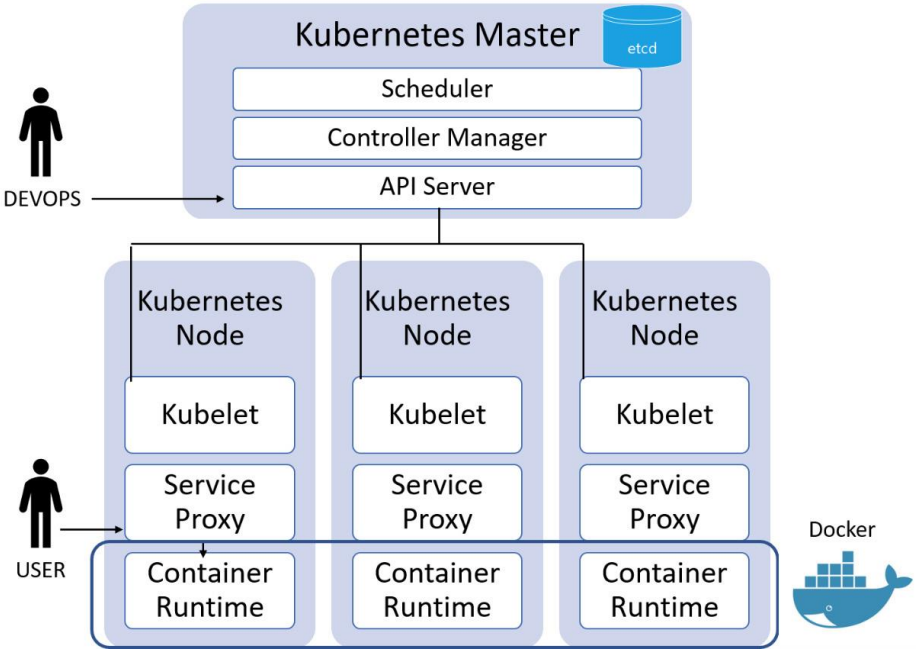


Figure 2.11 – Kubernetes orchestration

Figure 2.12 – CRM components

Figure 2.13 – ERP components

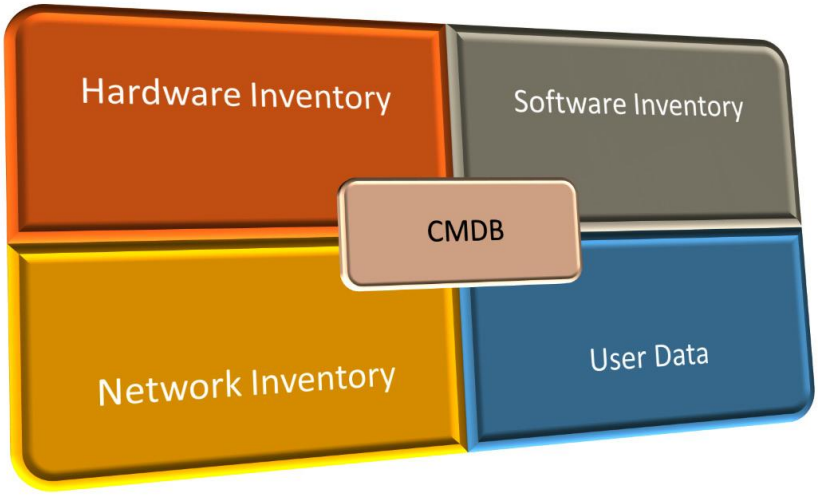


Figure 2.14 – CMDB components

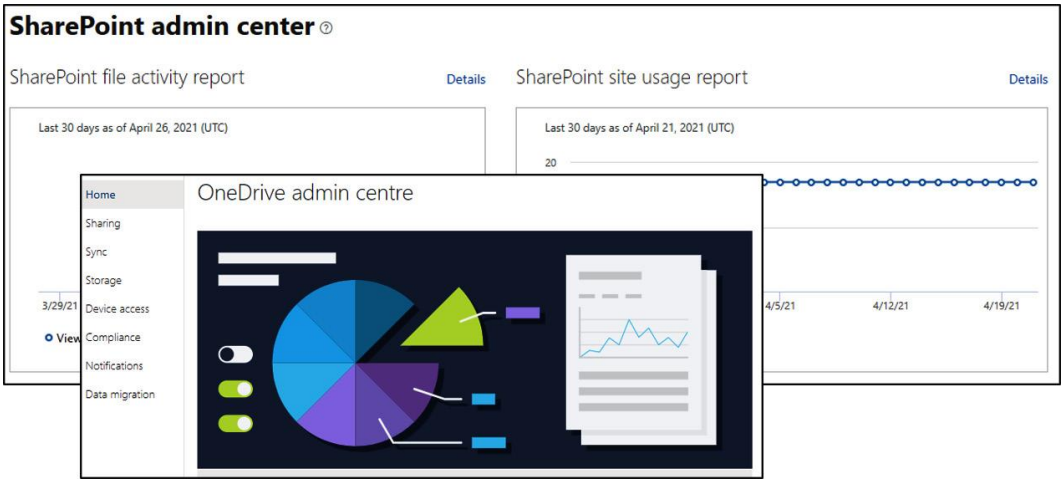


Figure 2.15 – Microsoft SharePoint

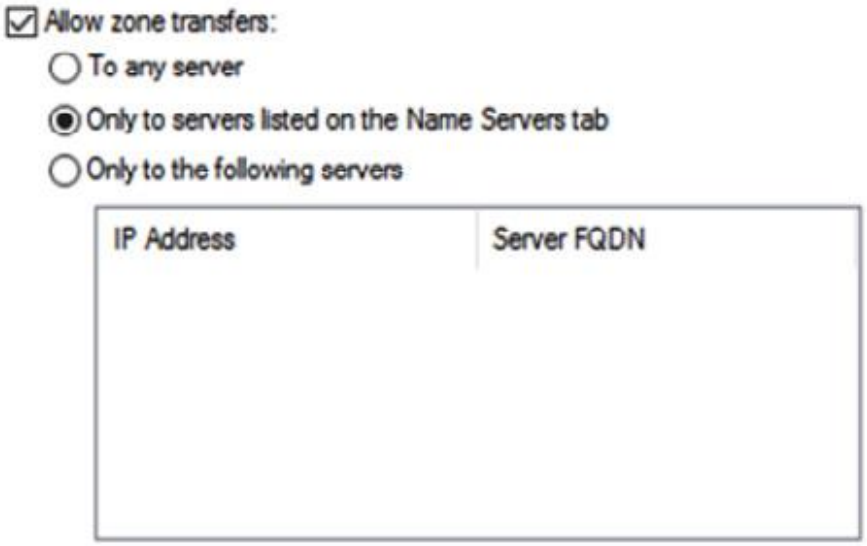


Figure 2.16 – DNS ACL

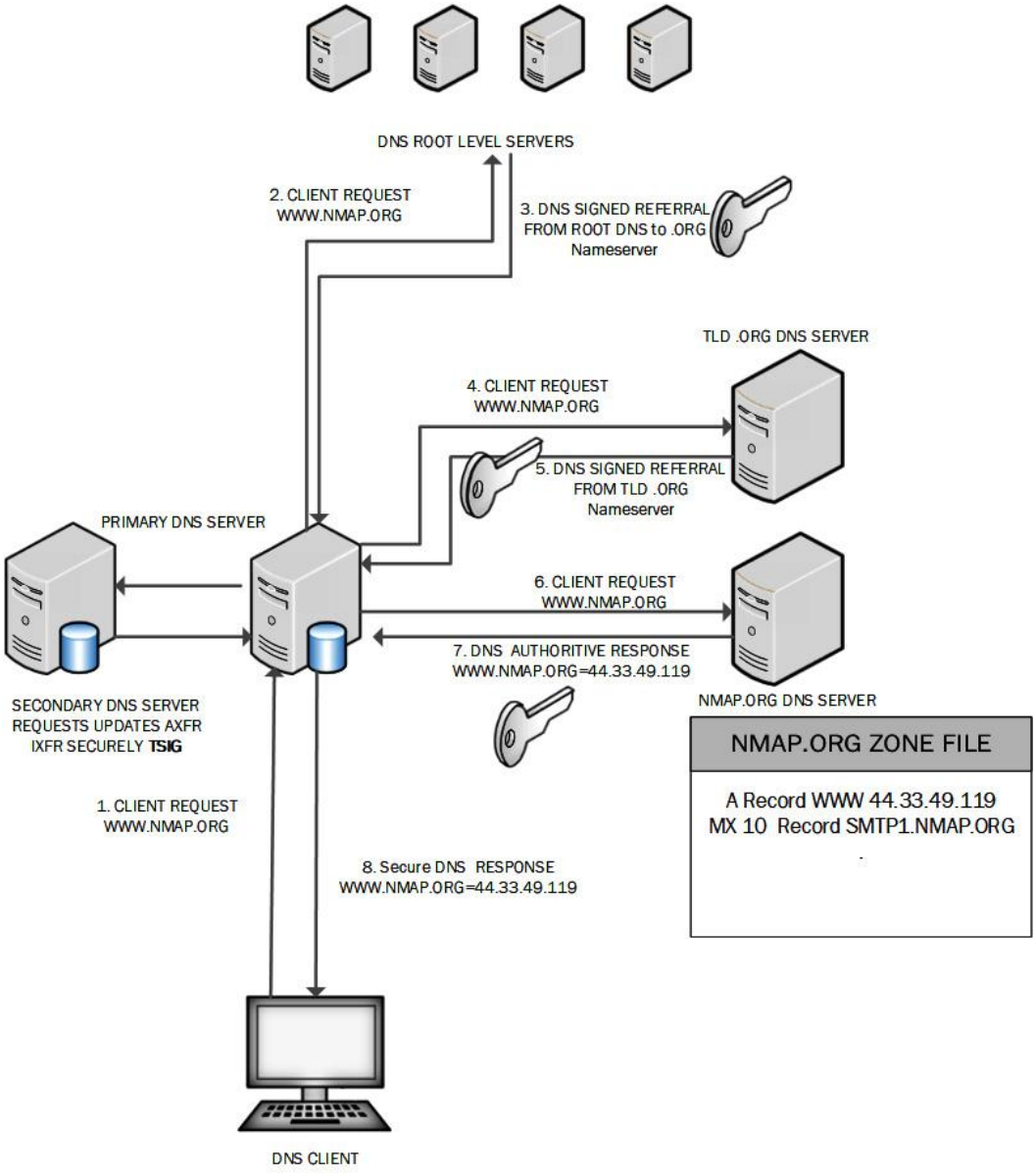


Figure 2.18 – DNSSEC processing

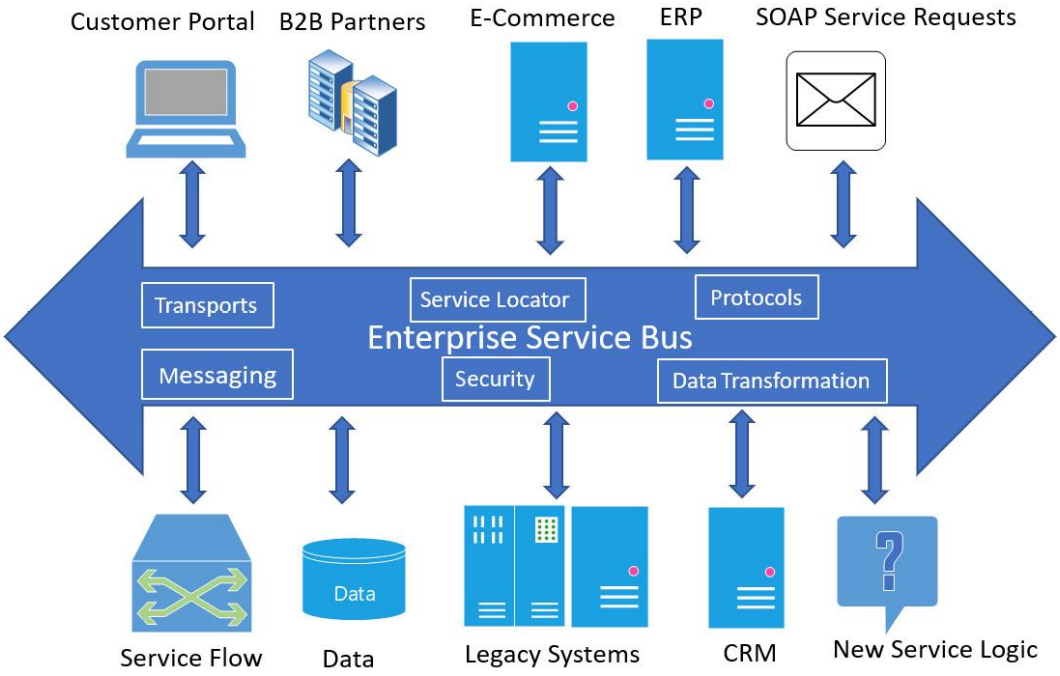


Figure 2.19 – ESB

Code

Code 2.1: XSS-Protection

This HTTP security header ensures that the connecting client uses the functionality of the built-in filter on the web browser. It should be configured as follows:

```
X-XSS-Protection "1; mode=block"
```

The **X-Frame-Options** (**XFO**) security header helps to protect your customers against clickjacking exploits. The following is the correct configuration for the header:

```
X-Frame-Options "SAMEORIGIN"
```

Code 2.2: Strict-Transport-Security

The **Strict-Transport-Security** (**HSTS**) header instructs client browsers to always connect via HTTPS. Without this setting, there may be the opportunity for the transmission of unencrypted traffic, allowing for sniffing or MITM exploits. The following is the suggested configuration for the header:

```
Strict-Transport-Security: max-age=315360000
```

Links

Five NCSC categories (also available at https://www.ncsc.gov.uk/collection/cyber-security-design-principles

For additional reading on security tools, there is a very useful blog from the Carnegie Mellon University Software Engineering Institute at https://tinyurl.com/seiblog.

A PDF document with more detail on the OWASP 10 threats can be downloaded from the following link: https://tinyurl.com/owasptoptenpdf.

More information about their work and contribution toward secure coding standards can be found at the following link:

https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

There are many free tools provided for developers including plugins for Microsoft Visual Studio: https://www.microsoft.com/en-us/securityengineering/sdl/resources

There is a useful site dedicated to all things related to DNS security at https://www.dnssec.net/.

Questions

Here are a few questions to test your understanding of the chapter:

1. Which of the following is a container API?
    A. VMware
    B. Kubernetes
    C. Hyper-V
    D. Docker
2. Why would a company adopt secure coding standards? Choose all that apply.
    A. To ensure most privilege
    B. To adhere to the principle of least privilege
    C. To sanitize data sent to other systems
    D. To practice defense in depth
    E. To deploy effective QA techniques
3. Why does Microsoft have an application-vetting process for Windows Store applications?
    A. To ensure products are marketable
    B. To ensure applications are stable and secure
    C. To make sure patches will be made available
    D. To ensure HTTP is used instead of HTTPS
4. What is most important for a development team validating third-party libraries? Choose two.

A. Third-party libraries may have vulnerabilities.

B. Third-party libraries may be incompatible.

C. Third-party libraries may not support DNSSEC.

D. Third-party libraries may have licensing restrictions.

5. What is the advantage of using the DevOps pipeline methodology?

A. Long lead times

B. Extensive pre-deployment testing

C. Continuous delivery

D. Siloed operations and development environments

6. What is the importance of software code signing?

A. Encrypted code modules

B. Software QA

C. Software integrity

D. Software agility

7. Which of the following is a common tool used to perform **Dynamic Application Security Testing** (**DAST**)?

A. Network enumerator

B. Sniffer

C. Fuzzer

D. Wi-Fi analyzer

8. What type of code must we have to perform **Static Application Security Testing** (**SAST**)?

A. Compiled code

B. Dynamic code

C. Source code

D. Binary code

9. What will my sales team use to manage sales opportunities?

A. CRM

B. ERP

C. CMDB

D. DNS

10. What would be a useful tool to integrate all business functions within an enterprise?

A. CRM

B. ERP

C. CMDB

D. DNS

11. What would be a useful tool to track all configurable assets within an enterprise?

A. CRM

B. ERP

C. CMDB

D. DNS

12. How can I ensure content is made accessible to the appropriate users through my web-based portal?

A. CRM

B. CMS

C. CMDB

D. CCMP

13. How can I protect my DNS servers from cache poisoning?

A. DMARC

B. DNSSEC

C. Strict Transport Security

D. IPSEC

14. What is it called when software developers break up code into modules, each one being an independently functional unit?

A. SOA

B. ESB

C. Monolithic architecture

D. Legacy architecture

15. What is the most important consideration when planning for system end of life?

    A. To ensure systems can be re-purposed

    B. To ensure there are no data remnants

    C. To comply with environmental standards

    D. To ensure systems do not become obsolete

16. What type of software testing is used when there has been a change within the existing environment?

    A. Regression testing

    B. Pen testing

    C. Requirements validation

    D. Release testing

17. What is it called when the development and operations teams work together to ensure that code released to the production environment is secure?

    A. DevOps

    B. Team-building exercises

    C. Tabletop exercises

    D. SecDevOps

18. What software development approach would involve regular meetings with the customer and developers throughout the development process?

    A. Agile

    B. Waterfall

    C. Spiral

    D. Build and Fix

19. What software development approach would involve meetings with the customer and developers at the end of a development cycle, allowing for changes to be made for the next iteration?

    A. Agile

    B. Waterfall

    C. Spiral

    D. Build and Fix

20. What software development approach would involve meetings with the customer and developers at the definition stage and then at the end of the development process?
    A. Agile
    B. Waterfall
    C. Spiral
    D. Build and Fix
21. Where will we ensure the proper HTTP headers are configured?
    A. Domain Controller
    B. DNS server
    C. Web server
    D. Mail server

Answers

1. B
2. B, C, D and E
3. B
4. A and D
5. C
6. B
7. C
8. C
9. A
10. B
11. C
12. B
13. B
14. A
15. B
16. A

17. D

18. A

19. C

20. B

21. C

Chapter 3

Figure

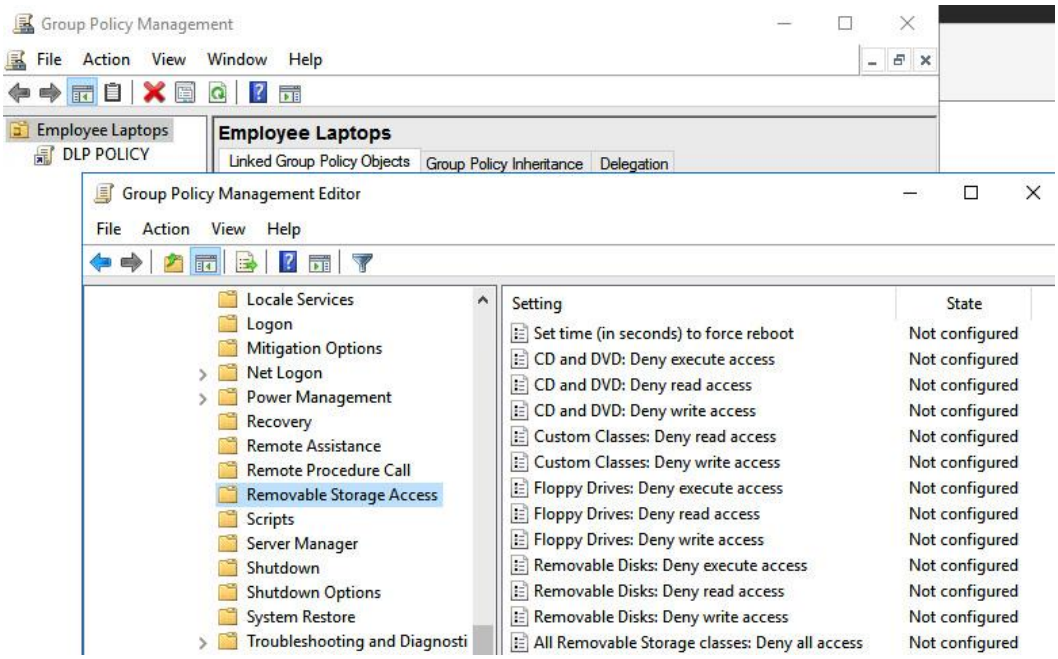


Figure 3.1 – Group Policy for controlling removable storage

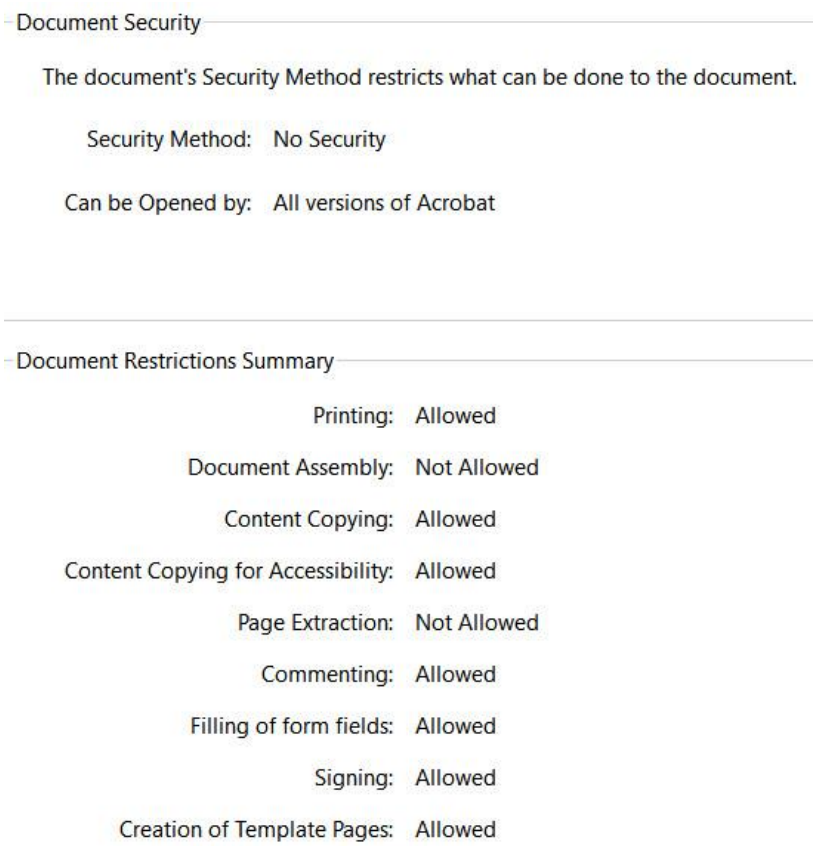


Figure 3.2 – DRM controls

Figure 3.3 – Remote Desktop controls

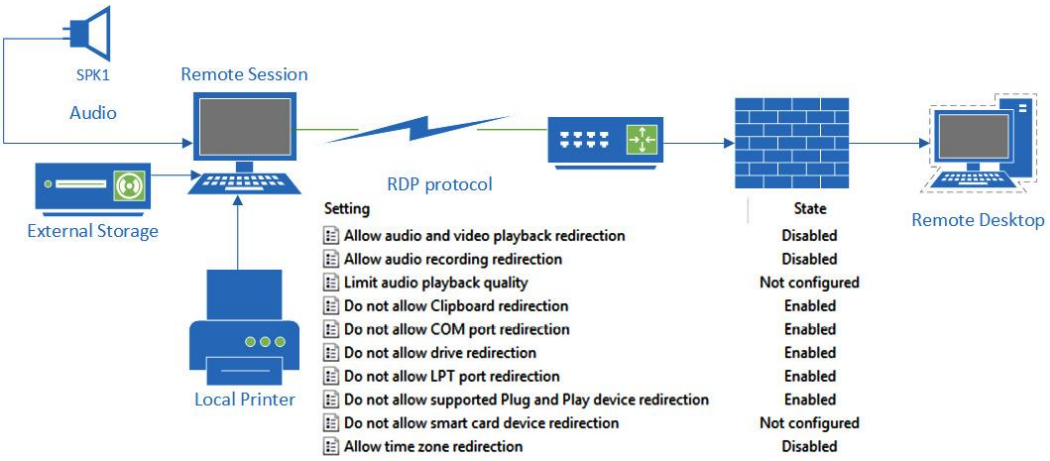


Figure 3.4 – Restricted VDI implementation

ACME CORPORATION

MARKETING CAMPAIGN – QUARTER 4 2021

Figure 3.5 – Watermarking

- ☐ EU Debit Card Number
- ☐ EU Driver's License Number
- ☐ EU National Identification Number
- ☐ EU Passport Number
- ☐ EU Social Security Number (SSN) or Equivalent ID
- ☐ EU Tax Identification Number (TIN)

Figure 3.6 – Data type tagging

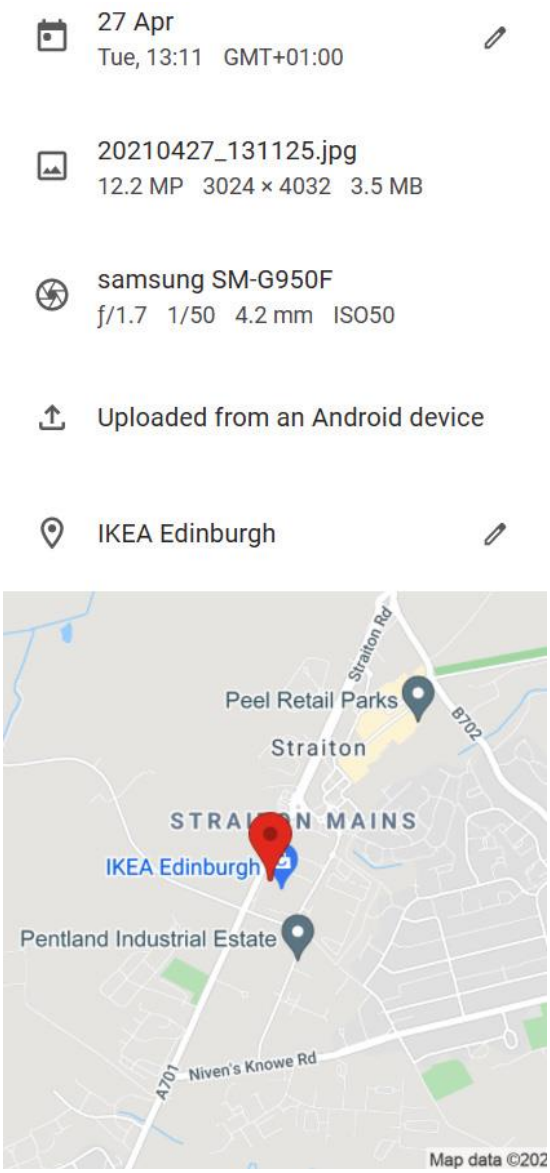


Figure 3.7 – Metadata store alongside an image file

Figure 3.8 – Document attributes

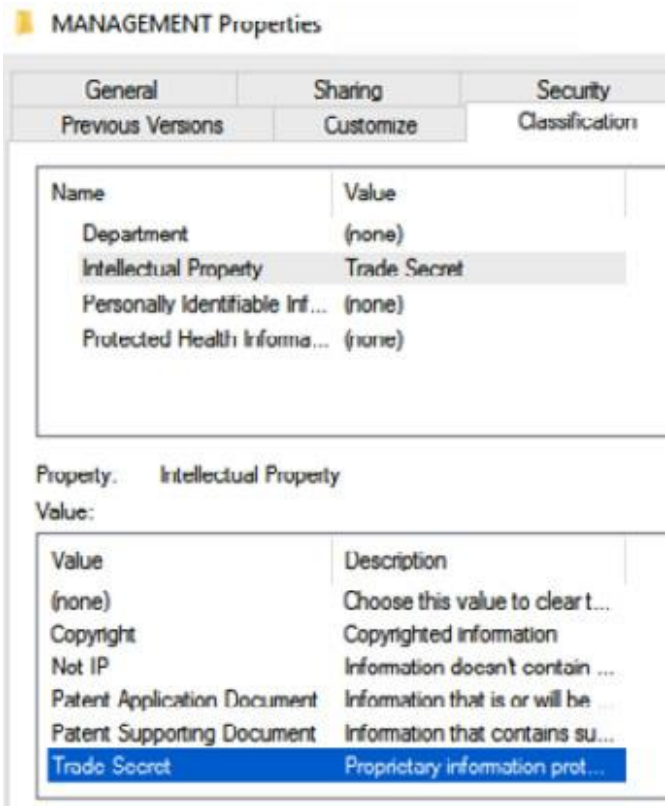


Figure 3.9 – Data labeling

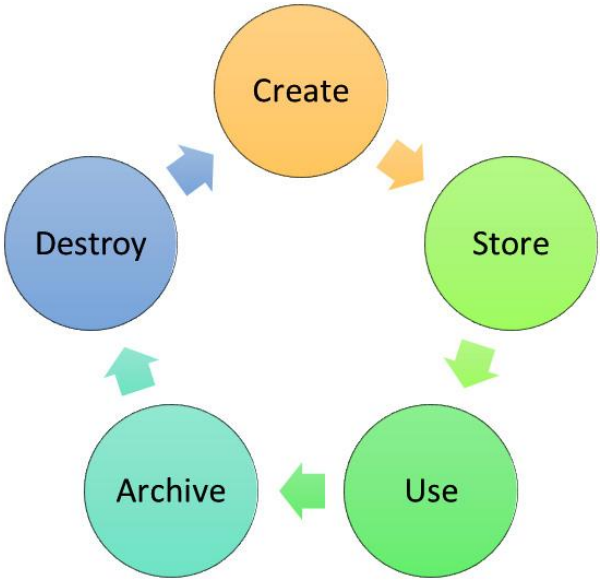


Figure 3.10 – Data life cycle

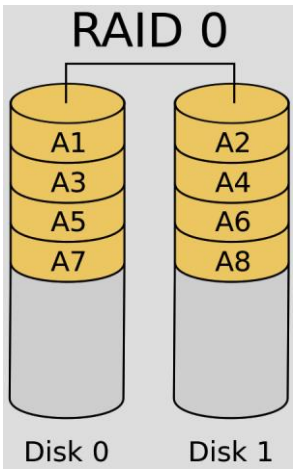


Figure 3.11 – RAID 0 disk striping

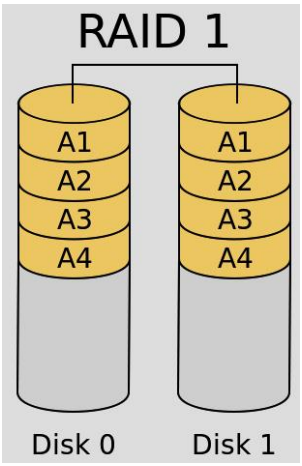


Figure 3.12 – RAID 1 disk mirroring

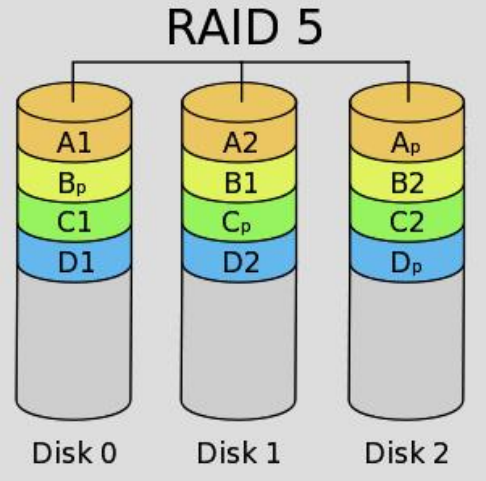


Figure 3.13 – RAID 5 striping with parity

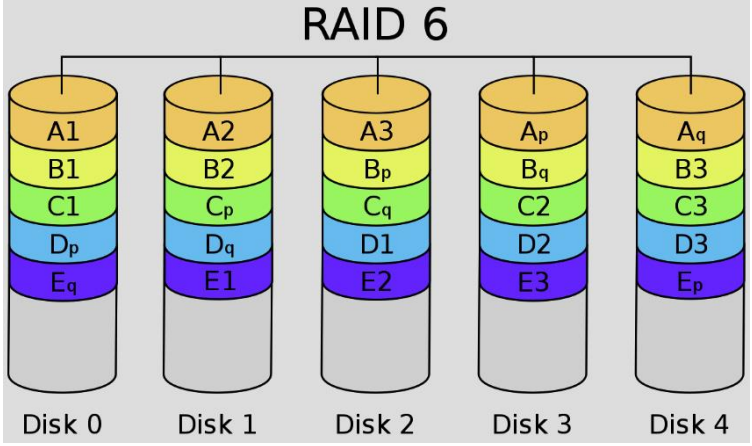


Figure 3.14 – RAID 6 dual stripe with parity

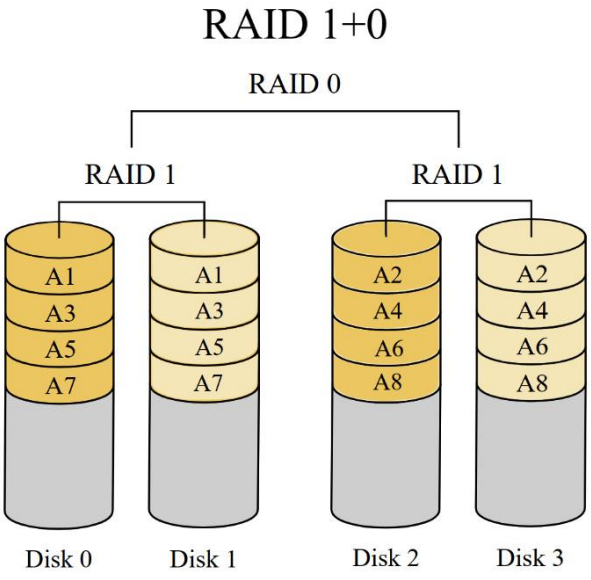


Figure 3.15 – RAID 10 nested raid 1 + 0

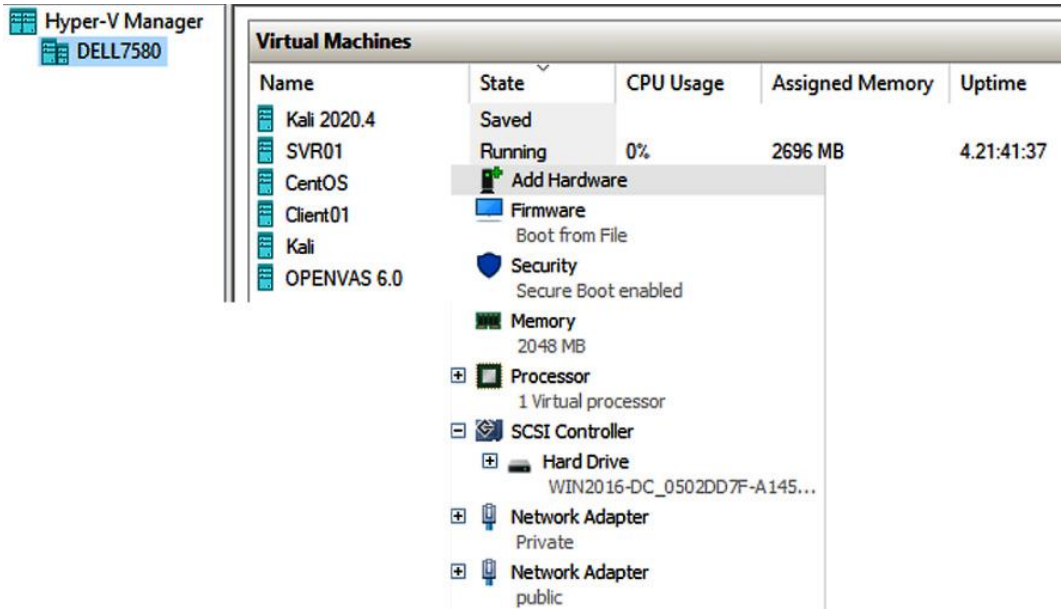


Figure 3.16 – Microsoft Hyper-V

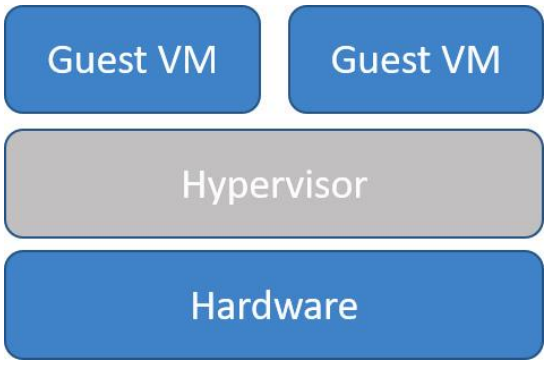


Figure 3.17 – Type 1 hypervisor

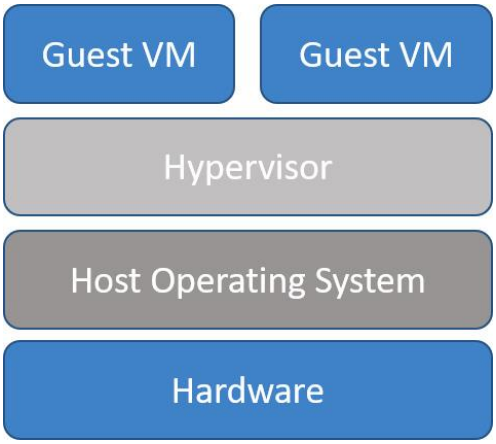


Figure 3.18 – Type 2 hypervisor

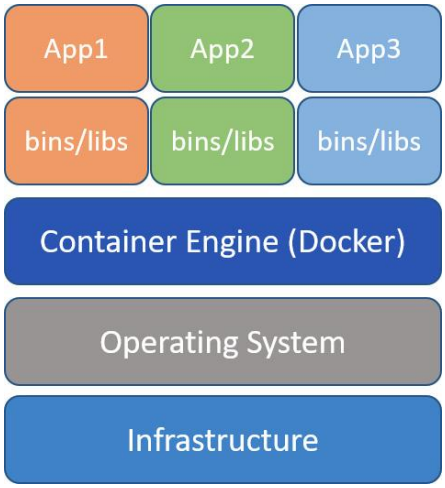


Figure 3.19 – Containers

```
┌──(mark dell7580)-[~]
└─$ help
GNU bash, version 5.1.0(1)-rc2 (x86_64-pc-linux-gnu)
These shell commands are defined internally.  Type `help' to see this list.
Type `help name' to find out more about the function `name'.
Use `info bash' to find out more about the shell in general.
Use `man -k' or `info' to find out more about commands not in this list.

A star (*) next to a name means that the command is disabled.

 job_spec [&]                                history [-c] [-d offset] [n] or history -a>
 (( expression ))                            if COMMANDS; then COMMANDS; [ elif COMMAND>
 . filename [arguments]                      jobs [-lnprs] [jobspec ...] or jobs -x com>
 :                                           kill [-s sigspec | -n signum | -sigspec] p>
 [ arg... ]                                  let arg [arg ...]
 [[ expression ]]                            local [option] name[=value] ...
 alias [-p] [name[=value] ... ]              logout [n]
 bg [job_spec ...]                           mapfile [-d delim] [-n count] [-O origin] >
 bind [-lpsvPSVX] [-m keymap] [-f filename] > popd [-n] [+N | -N]
 break [n]                                   printf [-v var] format [arguments]
 builtin [shell-builtin [arg ...]]           pushd [-n] [+N | -N | dir]
 caller [expr]                               pwd [-LP]
 case WORD in [PATTERN [| PATTERN]...) COMMA> read [-ers] [-a array] [-d delim] [-i text>
 cd [-L|[-P [-e]] [-@]] [dir]                readarray [-d delim] [-n count] [-O origin>
```

Figure 3.20 – Windows 10 Linux Bash shell (emulation)

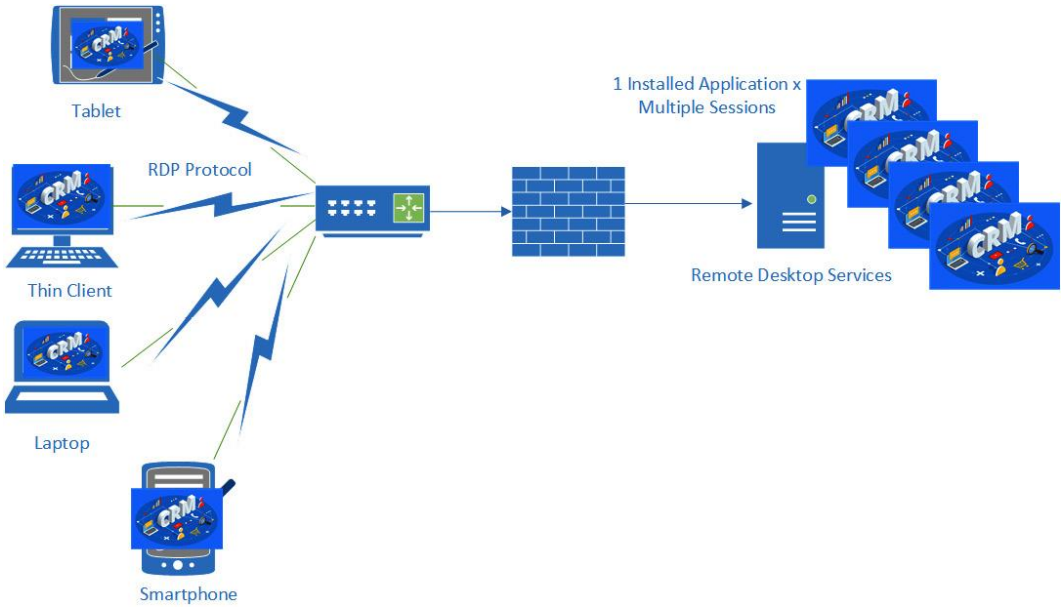


Figure 3.21 – Application virtualization

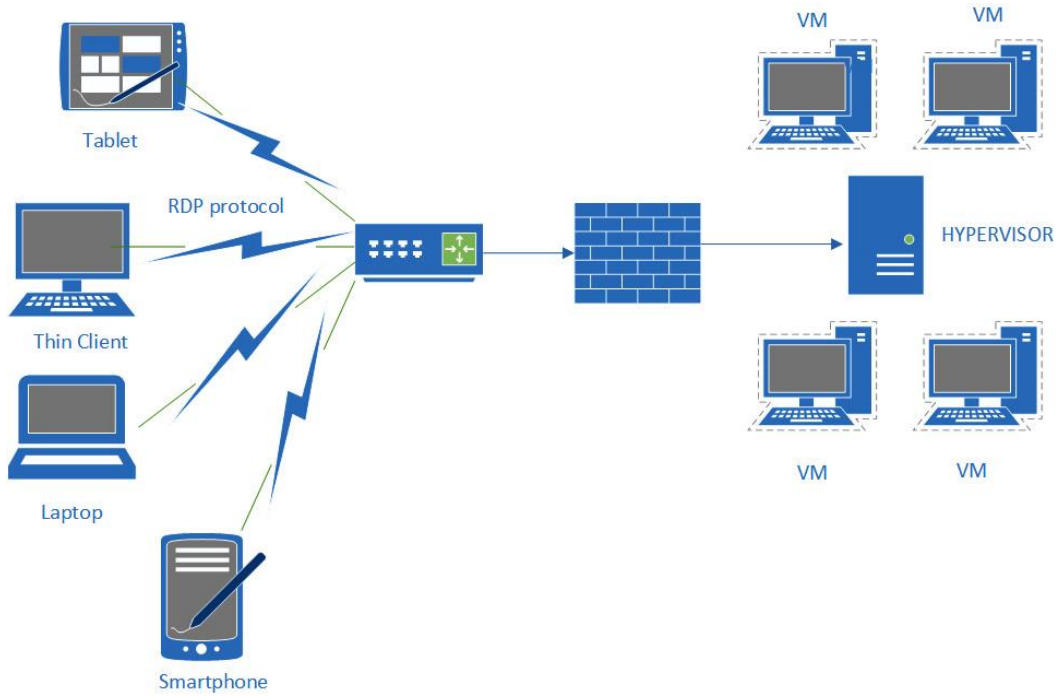


Figure 3.22 – VDI environment

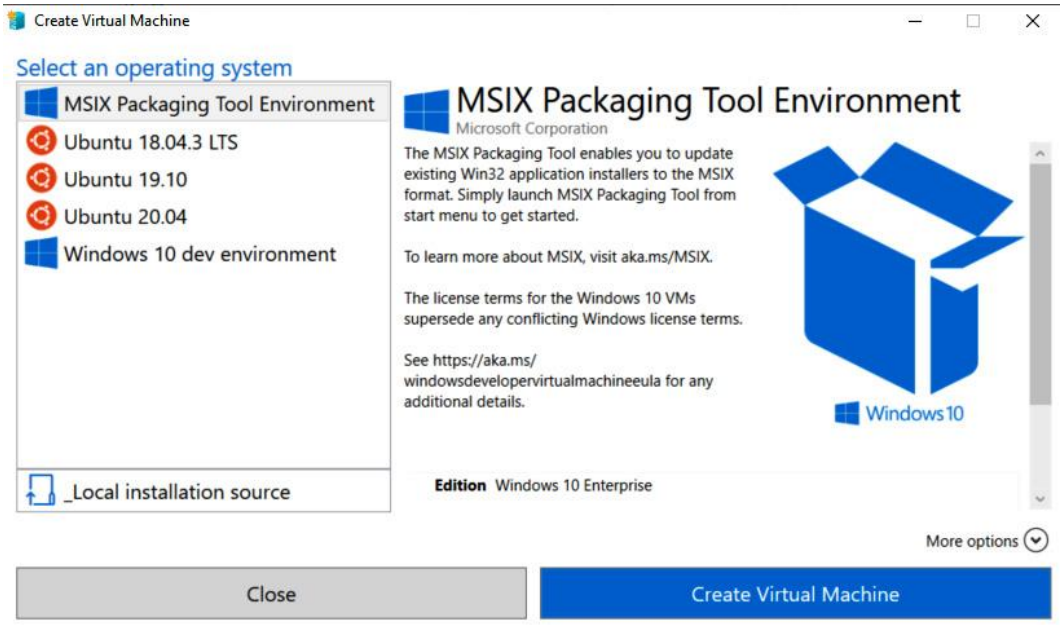


Figure 3.23 – VM provisioning

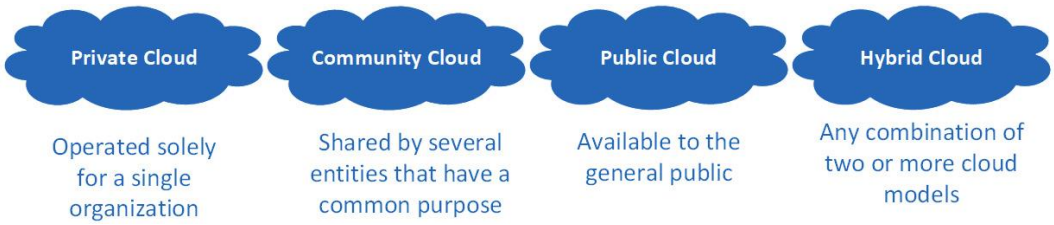


Figure 3.24 – Cloud deployment models

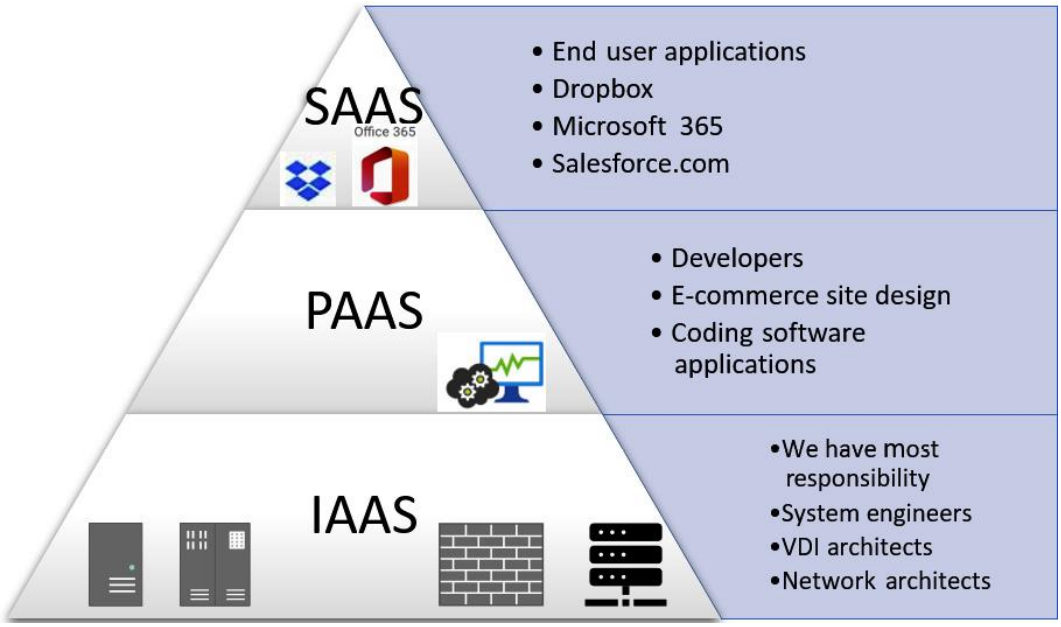


Figure 3.25 – Cloud service model

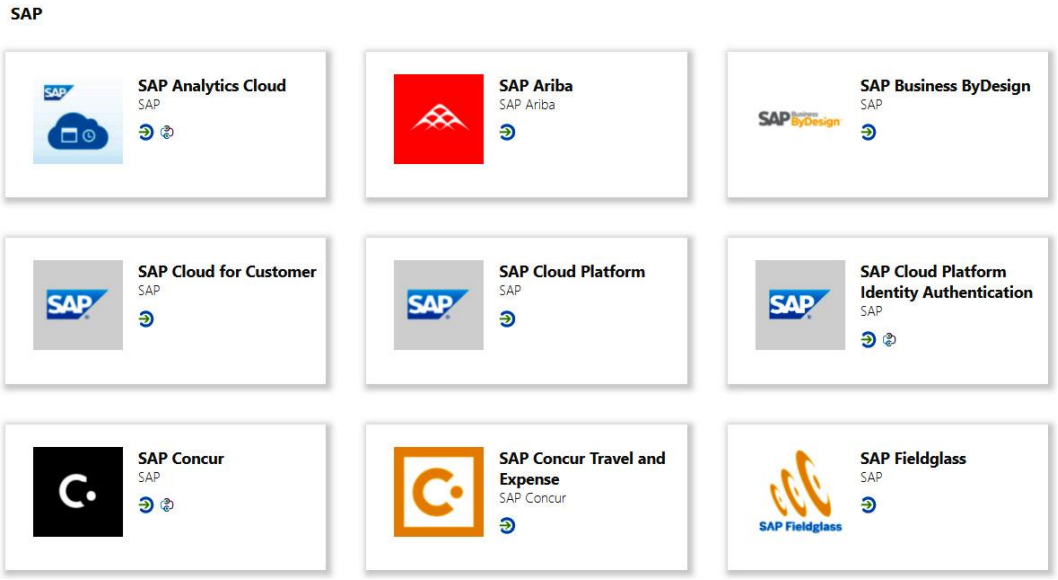


Figure 3.26 – SaaS catalog

Service	Examples	Applications	Middleware	Virtualization	Data	Operating System	Networking	Runtime	Servers	Storage
SAAS	Adobe Connect, CRM, Microsoft 365, Moodle	CSP	CSP	CSP	CSP	CSP	CSP	CSP	CSP	CSP
PAAS	AWS Lambda, Redhat OpenShift, IBM Cloud Foundry	CR	CR	CSP	CSP	CSP	CSP	CSP	CSP	CSP
IAAS	Amazon Web Services (AWS), Microsoft Azure, Oracle Cloud Infrastructure (OCI)	CR	CR	CR	CR	CR	CR	CR	CSP	CSP
Key	CR = Customer's responsibility			CSP = Cloud Service Provider's responsibility						

Figure 3.27 – Cloud shared responsibility matrix

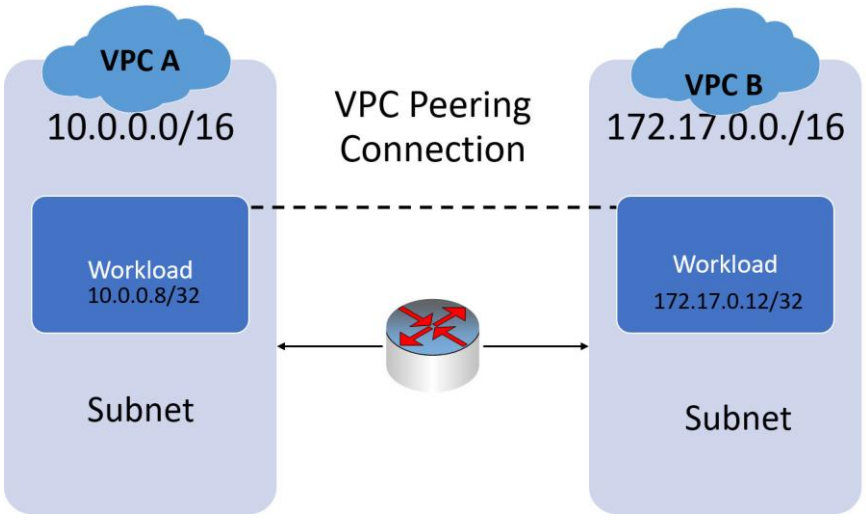


Figure 3.28 – VPC peering

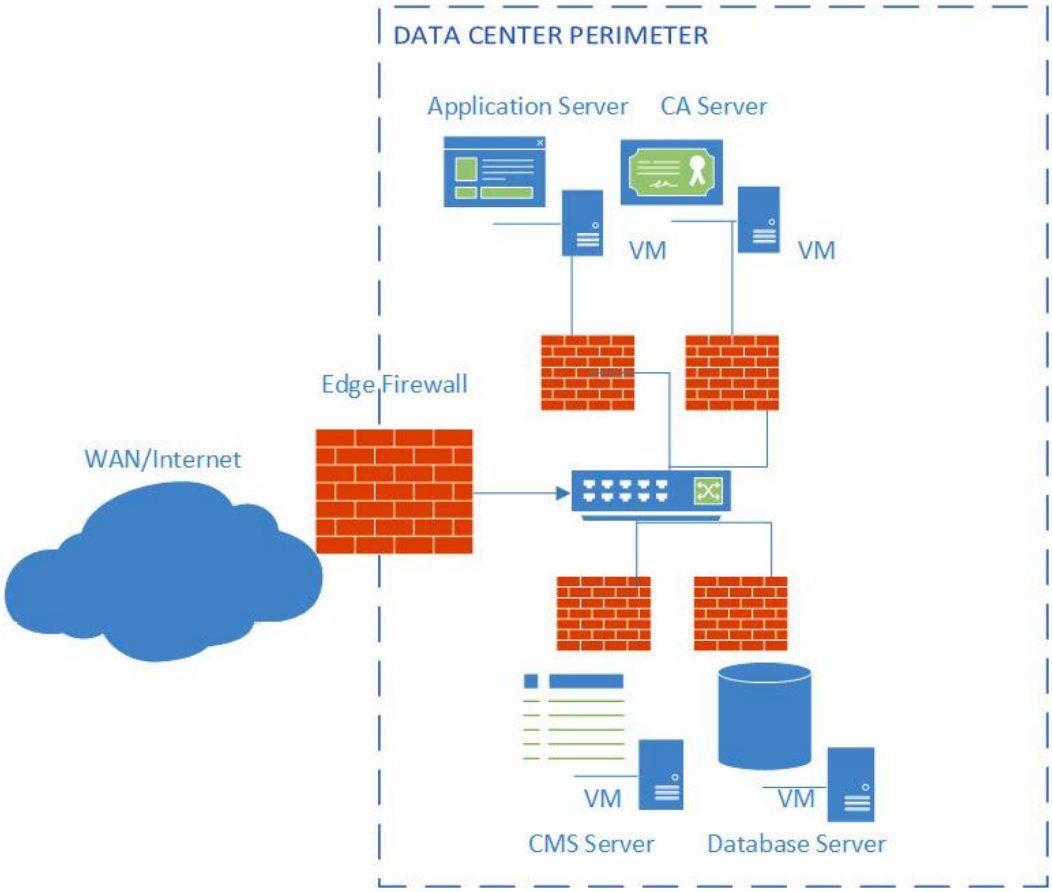


Figure 3.29 – Application-level micro-segmentation

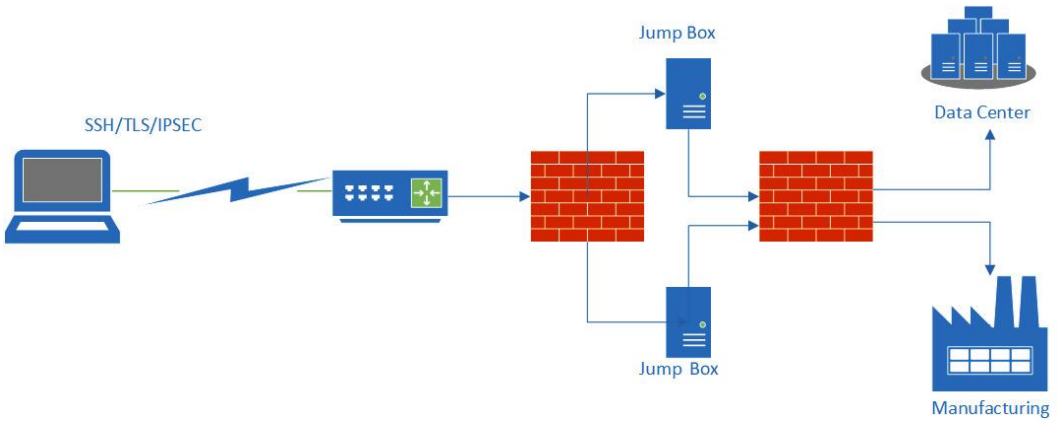


Figure 3.30 – Remote administration using a jump box

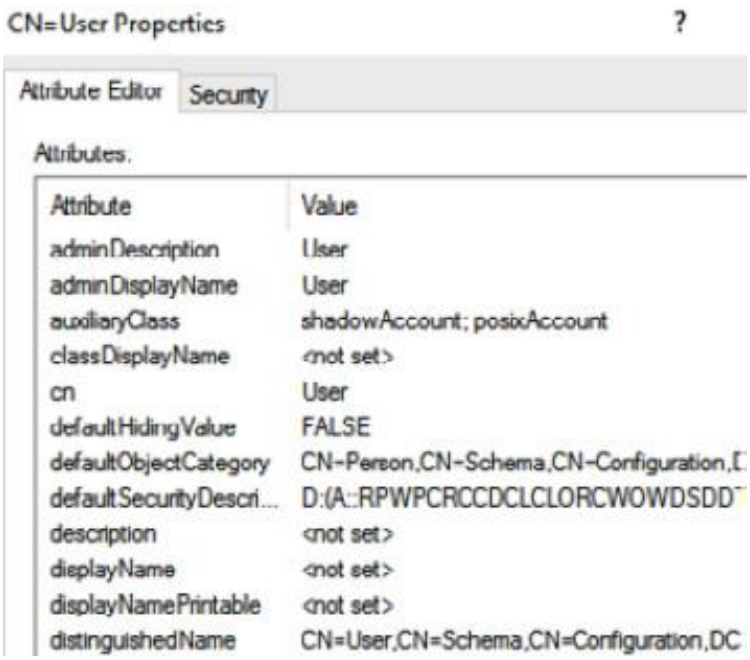


Figure 3.31 – Schema object and attributes

Links

To allow a CSP to prepare for this process, there are baseline security audit requirements and additional documentation available through the following link:
https://www.fedramp.gov/documents-templates/

Questions

Here are a few questions to test your understanding of the chapter:

1. What security setting is it when Group Policy prevents my flash drive from being recognized by my Windows computer?

   A. Watermarking

   B. Blocking the use of external media

   C. Print blocking

   D. Data classification blocking

2. What stops me from capturing bank account details using my mobile banking app?

   A. Watermarking

   B. Blocking the use of external media

   C. Print blocking

   D. Data classification blocking

3. What stops me from printing on my home printer when accessing my work computer using RDP?

    A. Watermarking

    B. Blocking the use of external media

    C. Restricted VDI

    D. Data classification blocking

4. Ben has asked a colleague to collaborate on a project by connecting remotely to his desktop. What would prevent this from happening?

    A. Remote Desktop

    B. Protocol (RDP) blocking

    C. Clipboard privacy controls

    D. Web Application Firewall

5. How can you reduce the risk of administrators installing unauthorized applications during RDP admin sessions?

    A. Remote Desktop

    B. Protocol (RDP) blocking

    C. Clipboard privacy controls

    D. Web Application Firewall

6. How can I ensure that my sales team can send quotations and business contracts out to customers, but not send confidential company data?

    A. Data classification blocking

    B. Data loss detection

    C. Watermarking

    D. Clipboard privacy controls

7. The CISO needs to know who has been sharing *signed-out* company confidential documents on a public web server. How can this be done?

    A. Data classification blocking

    B. Data loss detection

    C. Watermarking

    D. Clipboard privacy controls

8. Jenny wants to share a useful business-related video file with her colleague, but when Charles attempts to play it using the same player and codecs it cannot be viewed. What is the most likely cause?

    A. DRM

    B. Deep packet inspection

    C. Network traffic analysis

    D. Watermarking

9. What allows a forensics investigator to discover the time and location that a digital image was taken?

    A. Metadata

    B. Obfuscation

    C. Tokenization

    D. Scrubbing

10. What may have allowed a rogue administrator to remove evidence from the access logs?

    A. Scrubbing

    B. Metadata

    C. Obfuscation

    D. Tokenization

11. What stops the bank support desk personnel from accessing Ben's 16-digit VISA card number and CVC code?

    A. Metadata

    B. Obfuscation

    C. Key pairs

    D. Masking

12. What ensures that medical researchers cannot unwittingly share PHI data from medical records?

    A. Anonymization

    B. Encryption

    C. Metadata

    D. Obfuscation

13. What allows an organization to manage business data from the moment it is stored to final destruction?

    A. Data life cycle

    B. Containers

    C. Metadata

    D. Storage area network

14. What is another name for a *bare-metal* hypervisor deployed in a data center?

    A. Type 1

    B. Emulation

    C. Type 2

    D. Containers

15. What allows the isolation of workloads, allowing easy migration between vendor platforms?

    A. Type 1

    B. Emulation

    C. Type 2

    D. Containers

16. What allows Amy to play 16-bit Nintendo console games on her Windows desktop computer?

    A. Emulation

    B. Middleware

    C. PaaS

    D. Database storage

17. What allows a legacy Microsoft office application to run on Ben's desktop alongside Microsoft Office 365 applications?

    A. Application virtualization

    B. Database storage

    C. Middleware

    D. PaaS

18. How can we make sure that when a user leaves the organization, we can re-assign their software licenses to the new user?

    A. Deprovisioning

    B. IaaS

    C. Emulation

    D. Off-site backups

19. What type of data is used to provide information about data?

    A. Metadata

    B. Indexes

    C. Emulation

    D. Off-site backups

20. What is the primary reason that a small family coffee shop business would choose a public cloud model?

    A. Cost

    B. Scalability

    C. Resources

    D. Location

21. What type of cloud customer am I likely supporting if I am offering a private cloud and customers require that I have the **Federal Risk and Authorization Management Program** (**FedRAMP**) attestation?

    A. Government

    B. Finance

    C. Utility company

    D. Small online retailer

22. What is used to describe the situation when multiple customers are hosted on a common hardware platform?

    A. Multi-tenant

    B. Platform sharing

    C. Single tenant

    D. Service model

23. What type of cloud service model would be used when buying 50 licenses to access a **customer relationship management** (**CRM**) application?

    A. SaaS

    B. PaaS

    C. IaaS

    D. Security as a service (SecaaS)

24. What type of cloud service model would be used when I need to host my in-house **enterprise resource planning** (**ERP**) suite with a CSP?

    A. SaaS

    B. PaaS)

    C. IaaS

    D. SecaaS

25. What type of cloud service model would be used when the Acme corporation needs to deploy and manage 500 VDI instances across four geographical regions?

    A. SaaS

    B. PaaS

    C. IaaS

    D. SecaaS

26. What will my CSP configure so that I have direct communication between multiple instances of VPC?

    A. IPSEC tunnel

    B. VPN

    C. Inter-domain routing

    D. VPC peering

27. What kind of storage model would be best for images, files, video, and audio streams?

    A. File-based storage

    B. Database storage

    C. Block storage

    D. Blob storage

E. Key/value pairs

28. What kind of storage model would be provided on a **storage area network** (**SAN**)?

    A. File-based storage

    B. Database storage

    C. Block storage

    D. Blob storage

    E. Key/value pairs

29. What kind of storage model would be useful when performing a compliance scan and the database could contain a series of identifiers and the actual value it is expecting to be set?

    A. File-based storage

    B. Database storage

    C. Block storage

    D. Blob storage

    E. Key/value pairs

30. What is used when a customer is considering their responsibilities when buying in-cloud services.

    A. A coud-shared responsibility matrix

    B. A cloud-shared cost matrix

    C. FedRAMP

    D. Platform sharing

Answers

1. B
2. C
3. C
4. B
5. C
6. A
7. C

8. A
9. A
10. A
11. D
12. A
13. A
14. A
15. D
16. A
17. A
18. A
19. A
20. A
21. A
22. A
23. A
24. B
25. C
26. D
27. D
28. C
29. E
30. A

Chapter 4

Figures

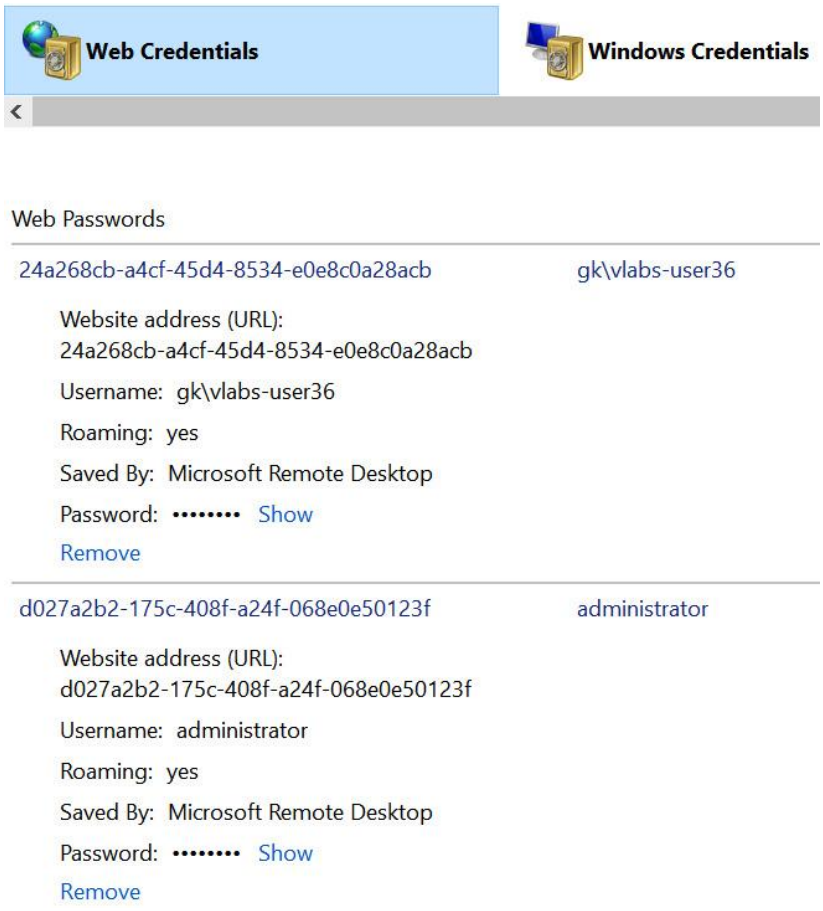


Figure 4.1 – Microsoft Windows Credential Manager

Figure 4.2 – Hardware key manager

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Figure 4.3 – Microsoft Group Policy password settings

```
123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345
1234567890
123123
000000
iloveyou
1234
1q2w3e4r5t
qwertyuiop
123
monkey
dragon
```

Figure 4.4 – Password wordlist

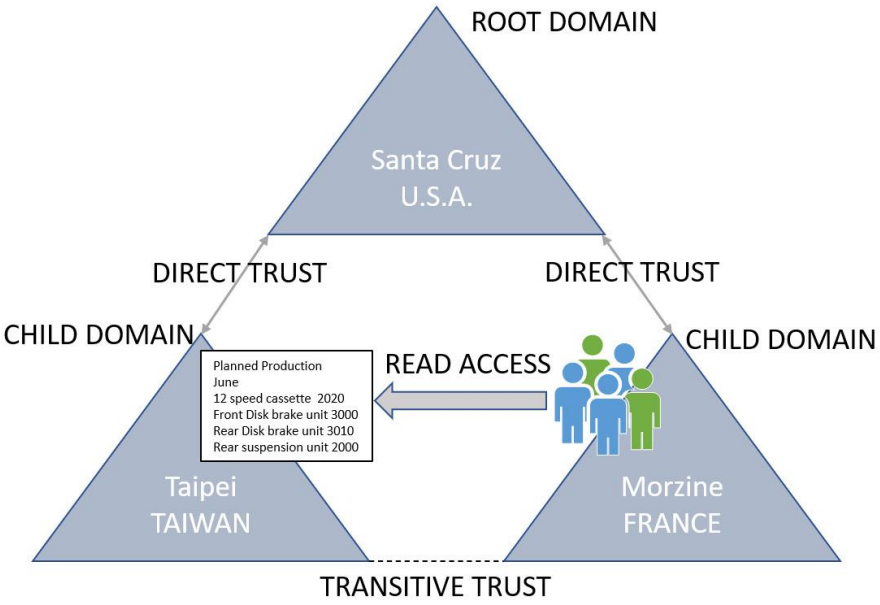
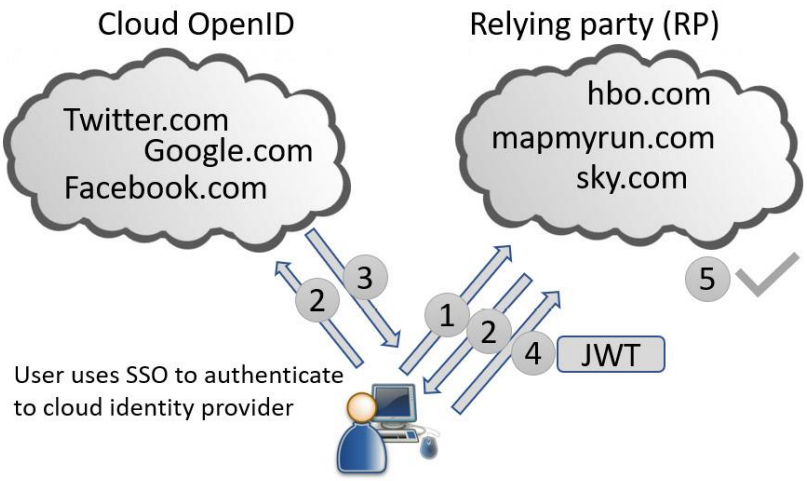
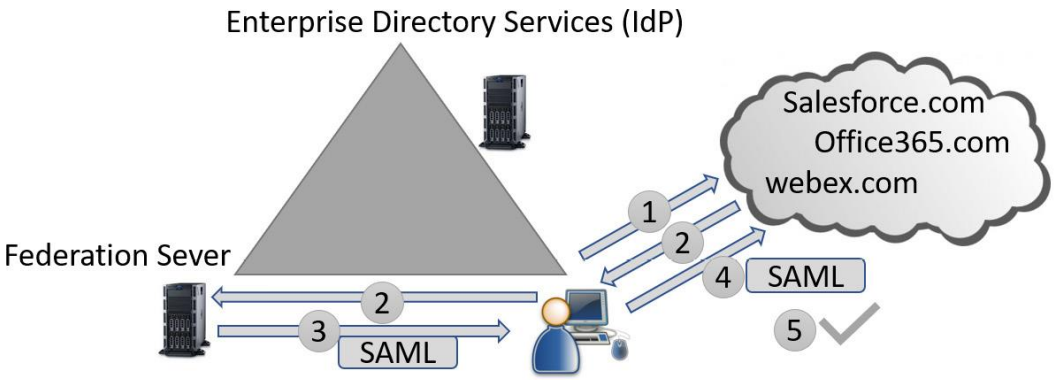


Figure 4.5 – Transitive trust



1. User accesses cloud portal
2. Users' browser is redirected back to OpenID provider
3. OpenID provider creates JWT (user is not prompted, they already signed in)
4. Token is sent to relying party (RP)
5. JWT is validated, and access granted

Figure 4.6 – OpenID process



1. User accesses cloud portal **FEDERATION SERVICES**
2. Users' browser is redirected back to IdP Federation Server
3. Federation Server creates SAML token (user is not prompted, they already signed in)
4. Token is sent to SP (Service Provider)
5. Token is validated and access granted

Figure 4.7 – SAML

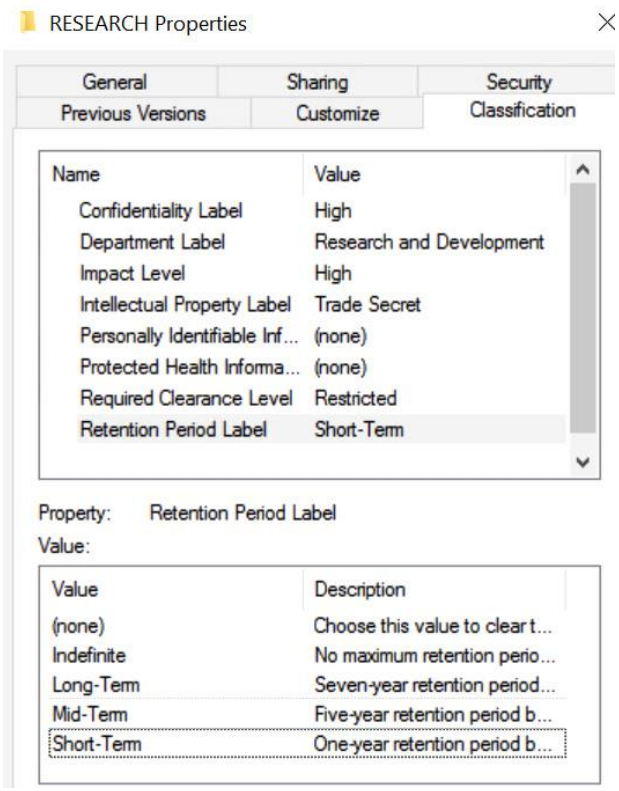


Figure 4.8 – MAC

Name: C:\Users\MarkBirch\OneDrive - MARKBIRCH.BIZ\Documents\Mycode.PS1

Owner: MarkBirch (AzureAD\MarkBirch) Change

Permissions | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	Bill (DELL7580\Bill)	Read & execute	None
Allow	MarkBirch (AzureAD\MarkBirch)	Full control	None
Allow	Mary (DELL7580\Mary)	Read & execute	None

Figure 4.9 – DAC

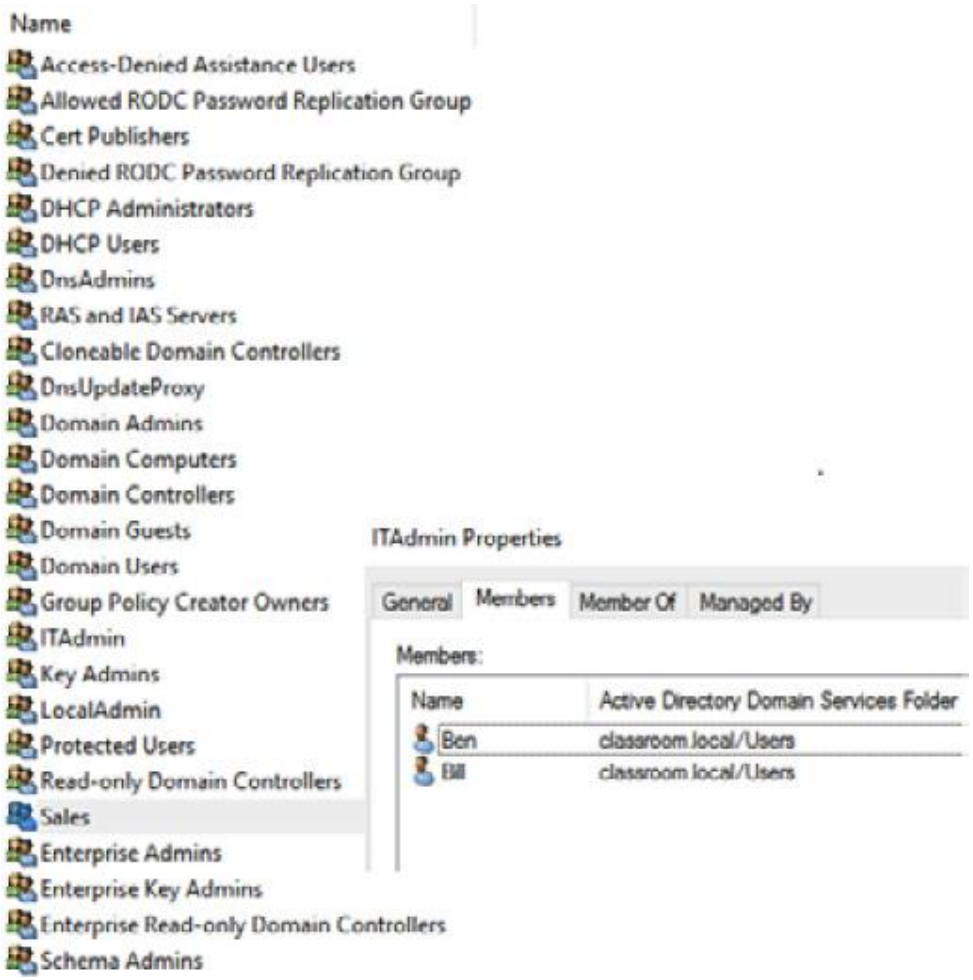


Figure 4.10 – Role-based access control

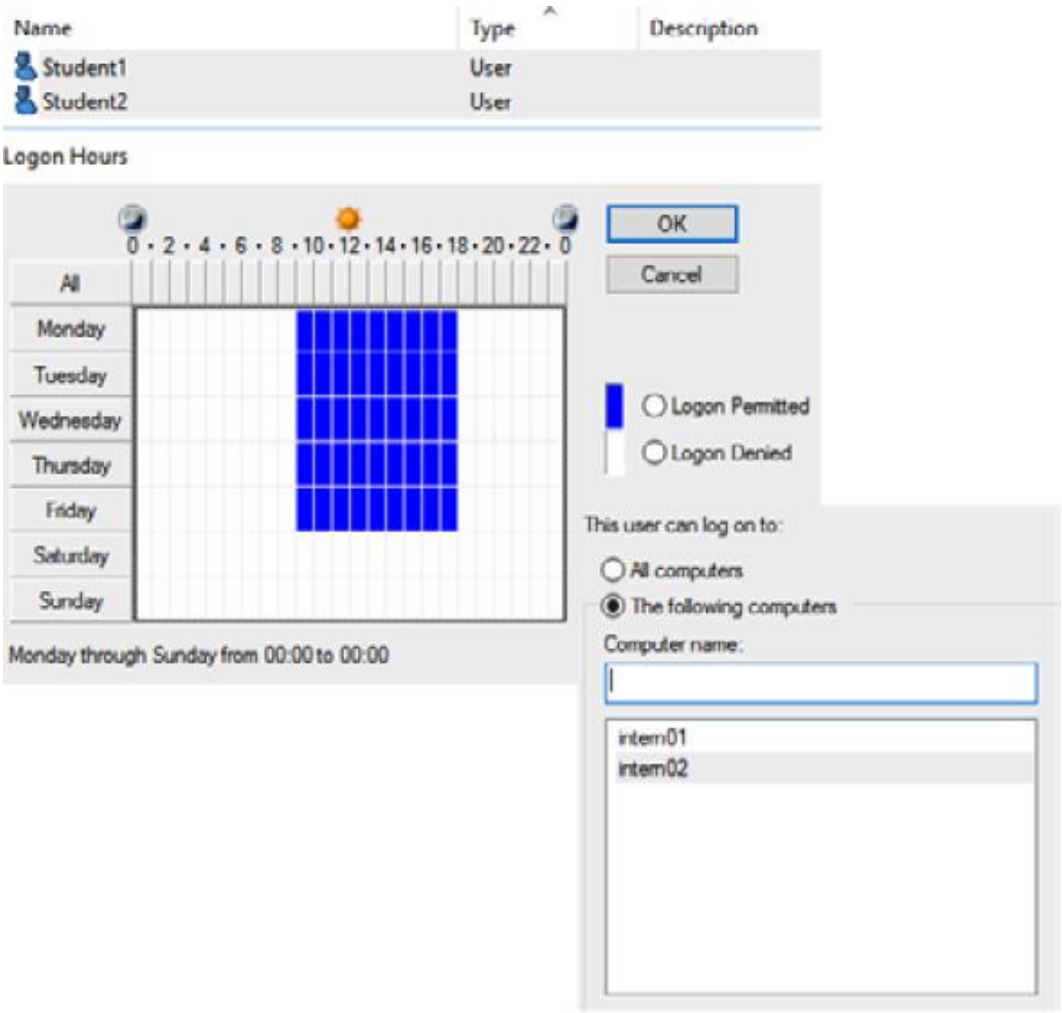


Figure 4.11 – Rule-based access control

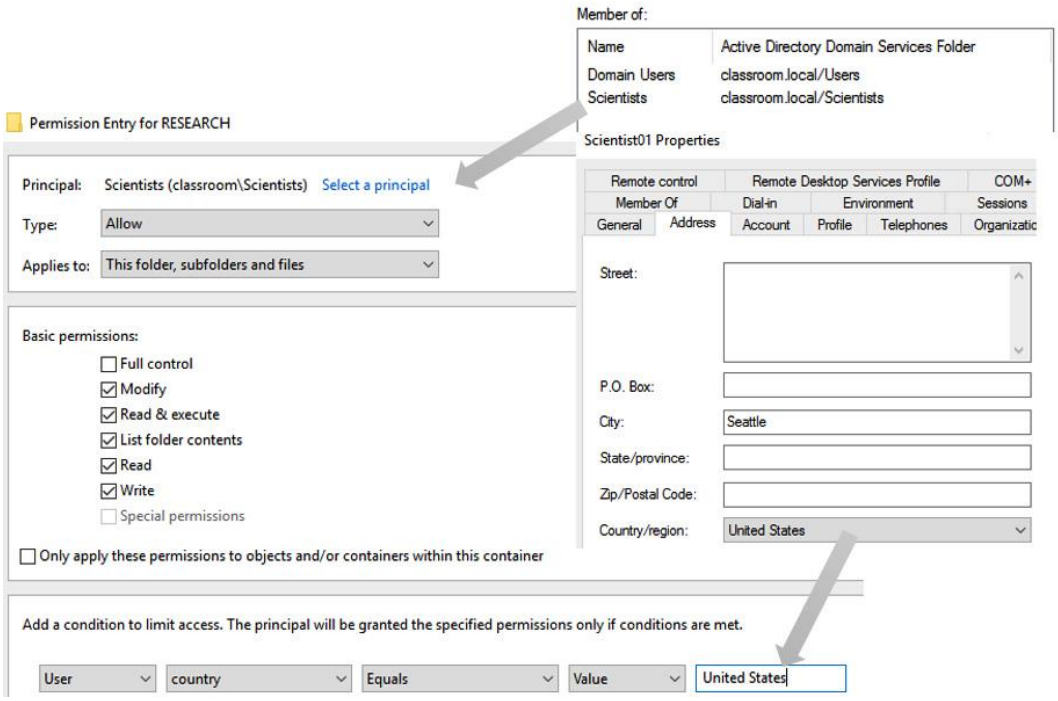


Figure 4.12 – Attribute-based access control

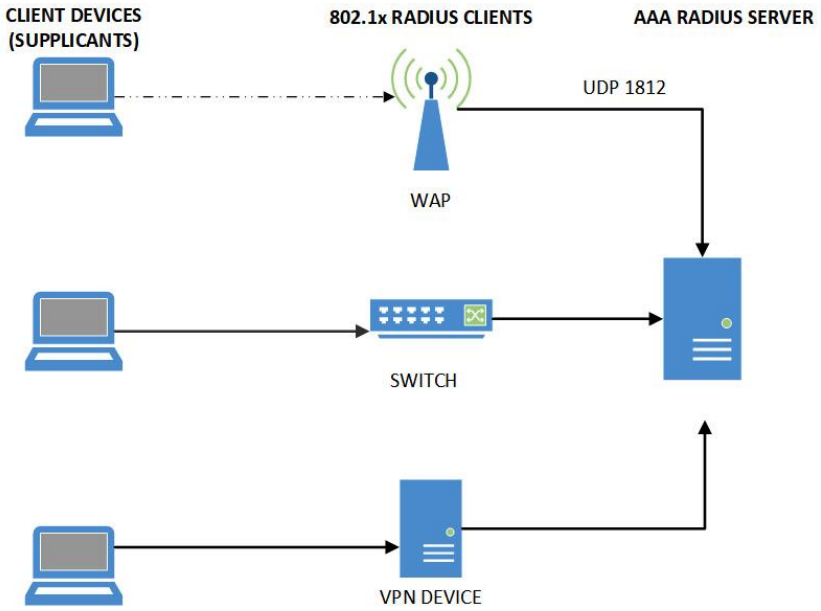


Figure 4.13 – AAA services

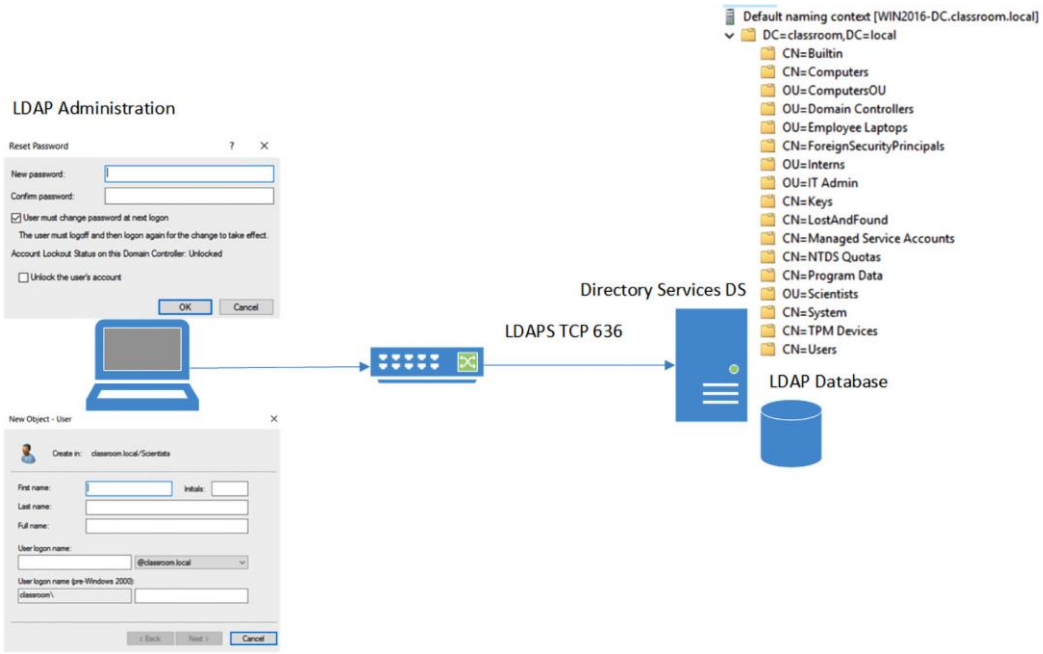


Figure 4.14 – LDAP services

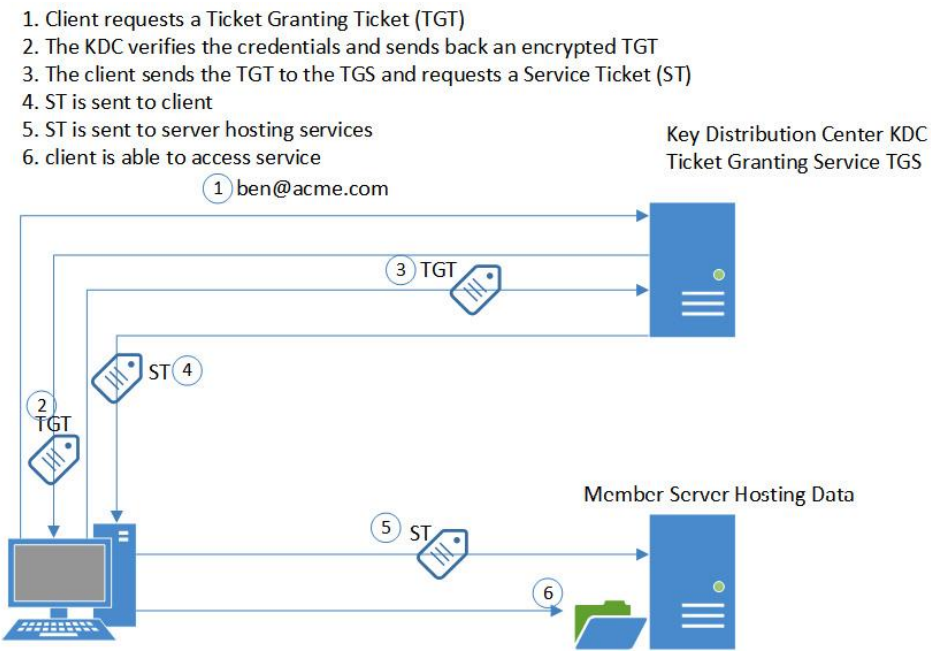


Figure 4.15 – Kerberos authentication

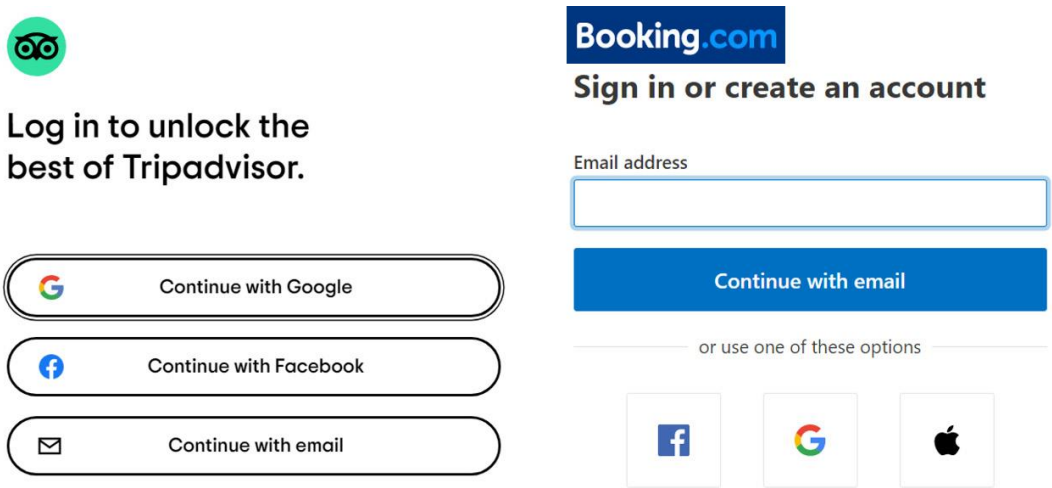


Figure 4.16 – OAuth SSO dialogs

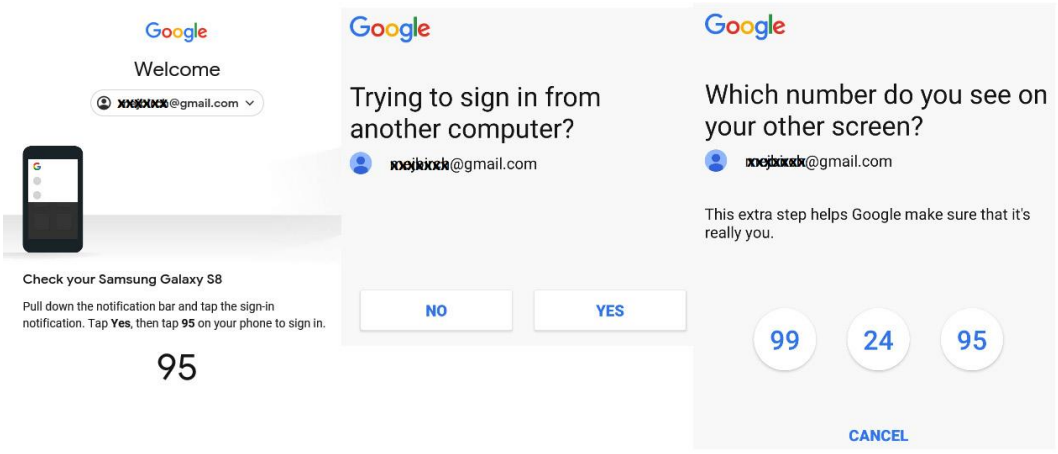


Figure 4.17 – Two-step verification

Figure 4.18 – RSA SecurID token ("File:RSA SecurID Token Old.jpg" by Alexander Klink is licensed with CC BY 3.0: https://creativecommons.org/licenses/by/3.0)

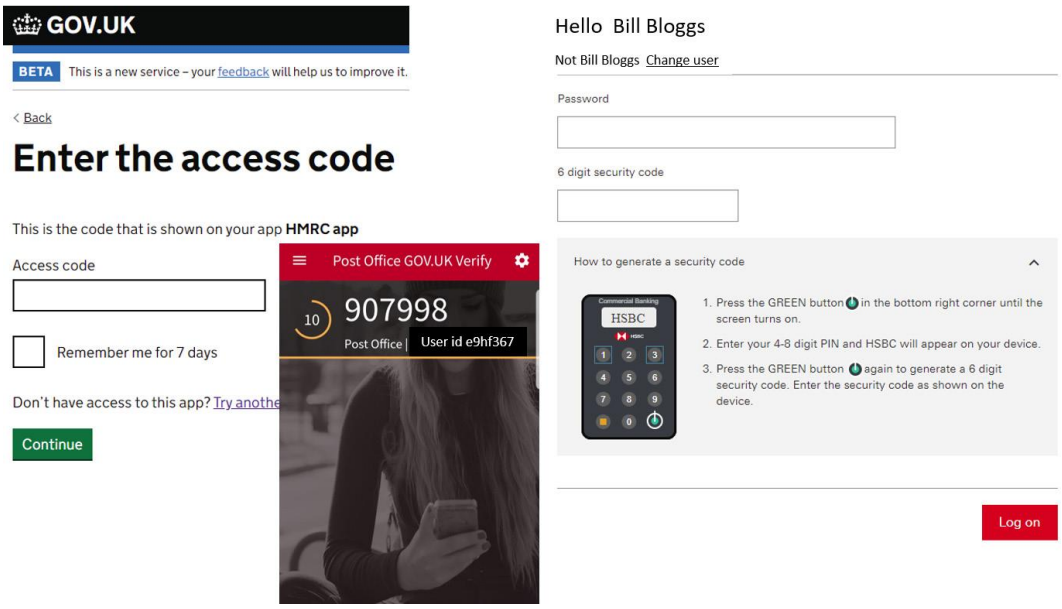


Figure 4.19 – MFA using TOTP

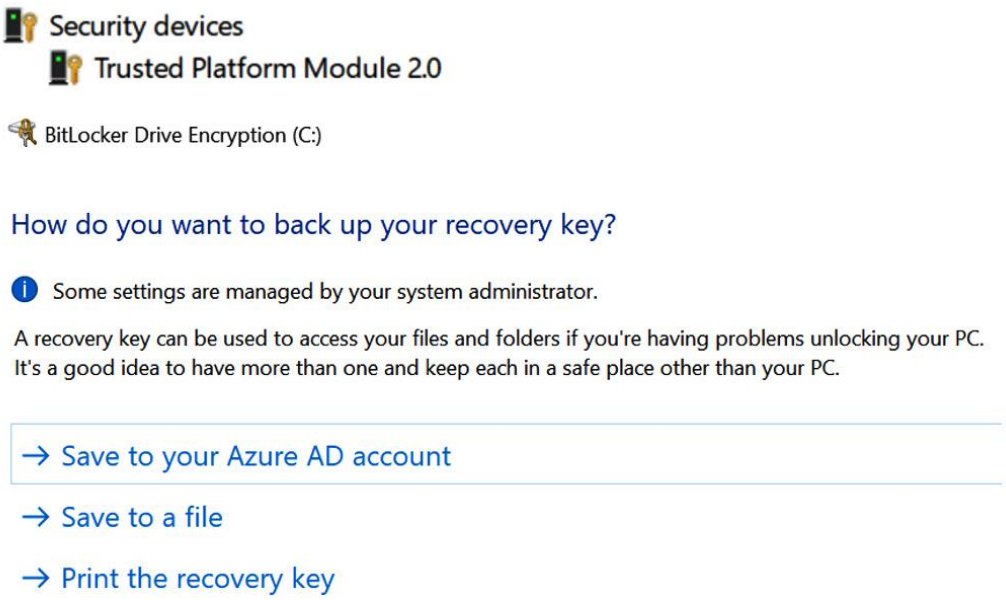


Figure 4.20 – Hardware root of trust

Links

The **National Cyber Security Center** (**NCSC**) has listed 100,000 passwords taken from https://haveibeenpwned.com. The list can be found at the following link: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

Questions

Here are a few questions to test your understanding of the chapter:

1. What is the container on a Windows operating system that allows the secure storage of user credentials and passwords?
    A. Password repository application
    B. Credential Manager
    C. iCloud Keychain
    D. End user password storage
2. What security would be provided for the storage of passwords in a cloud repository? Choose three.
    A. Advanced access control
    B. Behavioral analytics
    C. Continuous validation
    D. Reversible encryption
3. What type of device allows the secure retention of user passwords?
    A. Hardware key manager
    B. Removable storage
    C. Password policies
    D. iCloud Keychain
4. What management solution allows auditing of privileged accounts and *checkout* of these credentials?
    A. Password policies
    B. Privileged access management
    C. Password complexity

D. Password auditing

5. What password policy will ensure a password cannot be reused? Choose two.

   A. Password length

   B. Password reuse

   C. Password complexity

   D. Password history

6. What password policy would most likely force Bill to change his password from `flowerpot` to `F10w€rPot`?

   A. Password length

   B. Password reuse

   C. Password complexity

   D. Password history

7. What password policy will ensure Mary cannot spend her lunch break resetting her password 24 times to make it the original password?

   A. Minimum password age

   B. Maximum password age

   C. Password complexity

   D. Password history

8. How can you detect the use of a poor password that may match dictionary words?

   A. Password spraying

   B. Password auditing

   C. Password guessing

   D. Password reset

9. What is required for CHAP authentication, when setting a password requirements policy?

   A. Strong encryption

   B. Reversible encryption

   C. Forward encryption

   D. Complexity

10. What is the term used when credentials can be used with a third party utilizing SSO?

A. Identity proofing

B. Identity federation

C. Identity cloud

D. Identity trust

11. What XML federation service will most like be used to access third-party cloud-based corporate portals?

A. Shibboleth

B. SAML

C. OAuth

D. OpenID

12. Which federation service will most like be used to access third-party cloud-based digital services?

A. OAuth

B. SAML

C. Kerberos

D. LDAP

13. What access control will offer the most security for a government agency?

A. MAC

B. DAC

C. Role-based access control

D. Rule-based access control

14. What access control will offer the most flexibility for de-centralized administration?

A. MAC

B. DAC

C. Role-based access control

D. Rule-based access control

15. What access control will allow for access based upon *country* and *department*?

A. MAC

B. DAC

C. Role-based access control

D. Attribute-based access control

16. Which AAA service offers the widest support across vendor networking equipment?

A. RADIUS

B. TACACS+

C. Circumference

D. HP proprietary

17. How can I administer my directory services securely?

A. LDAP using TLS

B. Kerberos

C. OAuth

D. Out-of-band

18. What can I use to authenticate securely to directory services, preventing replay and MITM attacks?

A. IPsec

B. Kerberos

C. CHAP

D. PAP

19. What Ethernet standard allows networking appliances to authenticate connection attempts?

A. 802.11

B. 802.1X

C. 802.3

D. 802.1s

20. What is the framework that allows many different authentication protocols?

A. PAP

B. EAP

C. CHAP

D. PEAP

21. What will I need to support if users need to present an RFID card, iris scan, and pin?

    A. MFA

    B. 2FA

    C. Two-step verification

    D. In-band authentication

22. What is being used when my bank sends me a confirmation code via SMS?

    A. In-band authentication

    B. OOBA

    C. Bandwidth

    D. Out-of-bounds

23. What type of password is not already known to the user?

    A. Forgotten password

    B. OTP

    C. PIN

    D. KBA question

24. What will I need to support if users need to present a password, memorable secret, and pin?

    A. MFA

    B. 2FA

    C. Two-step verification

    D. Single-factor authentication

25. What type of password will my Microsoft Authenticator application generate?

    A. HOTP

    B. TOTP

    C. Hardware root of trust

    D. JWT

26. What is called it when I sign on to directory services and can use my internal email without being prompted to sign in a second time?

    A. SSO

B. JWT

C. Attestation and identity proofing

D. TPM

Answers

1. B
2. A, B and C
3. A
4. B
5. B and D
6. C
7. A
8. B
9. B
10. B
11. B
12. A
13. A
14. B
15. D
16. A
17. A
18. B
19. B
20. B
21. A
22. B
23. B

24. D

25. B

26. A

Chapter 5

Figures

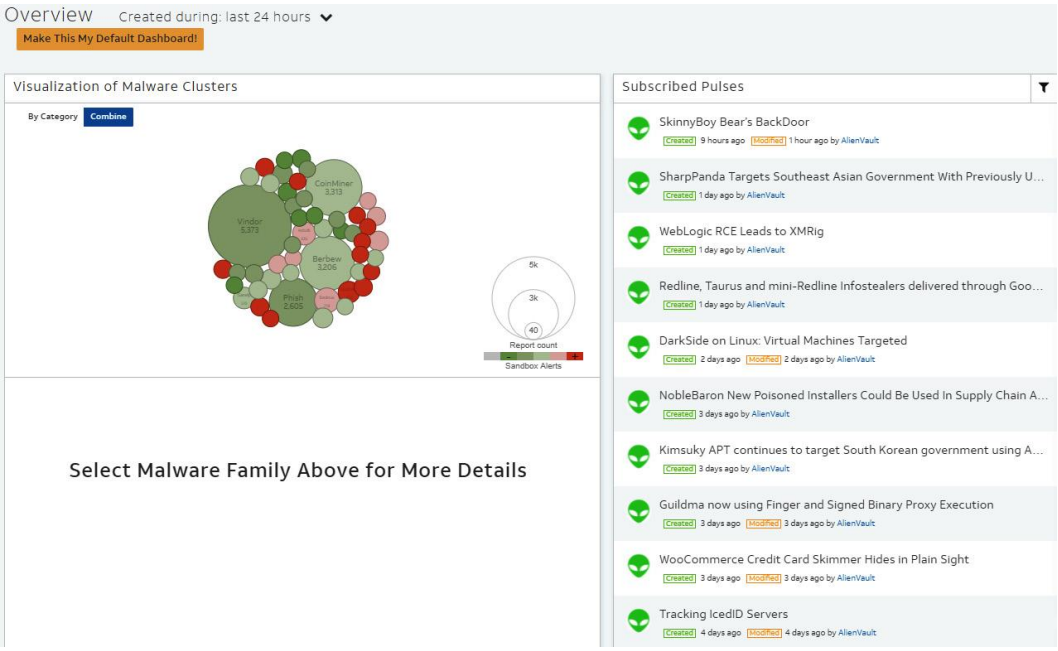


Figure 5.1 – Threat feed

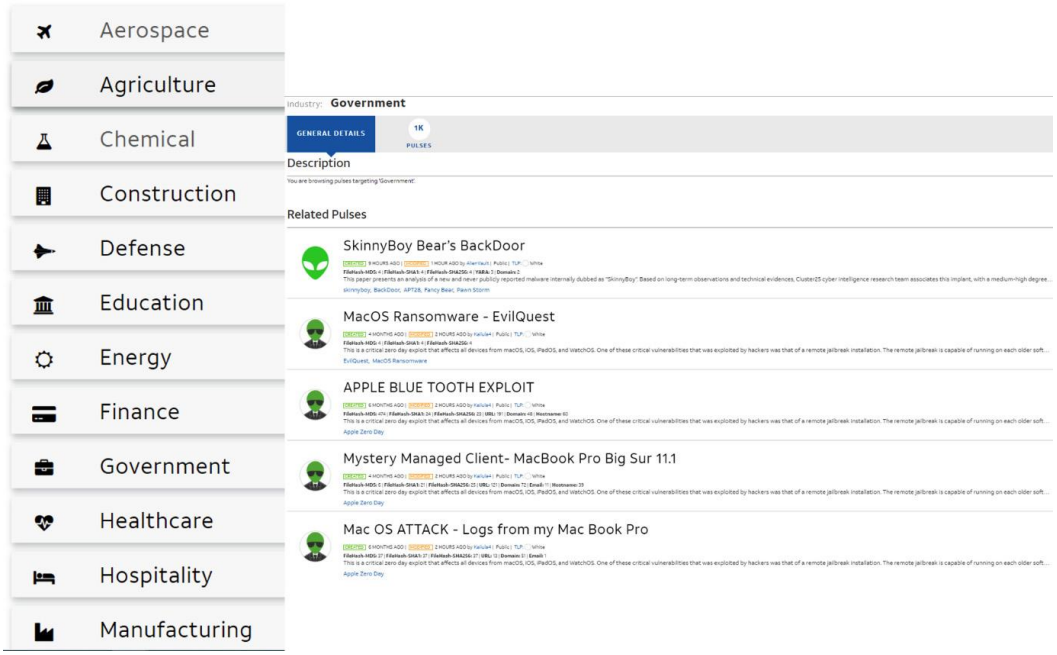


Figure 5.2 – Industry-specific threat feed

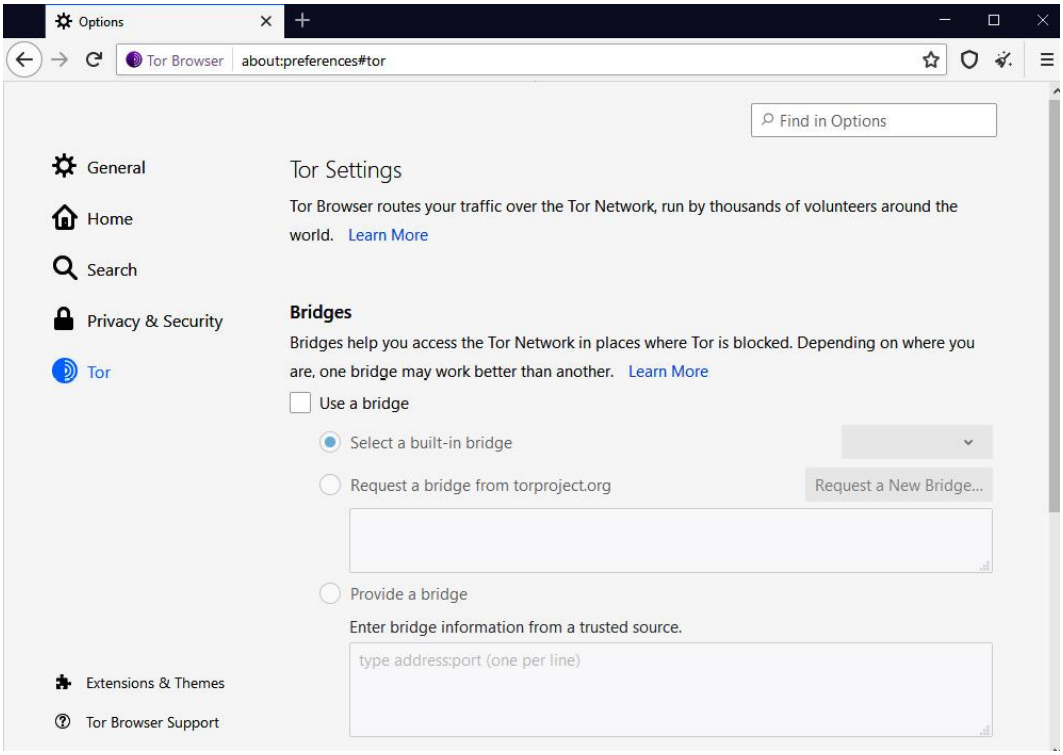


Figure 5.3 – Tor browser

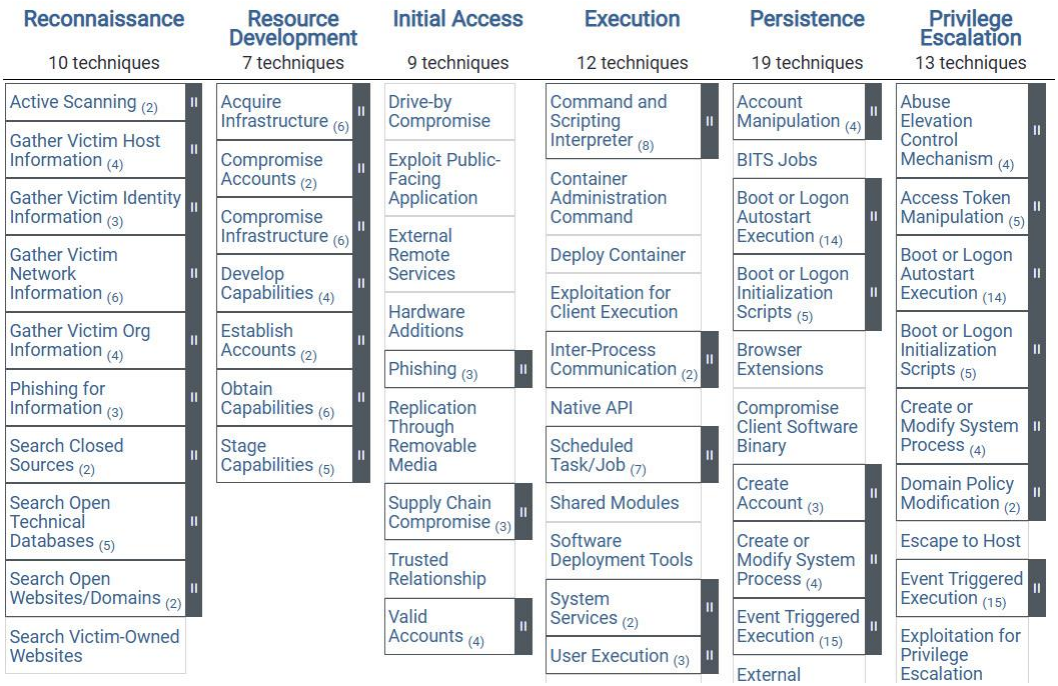


Figure 5.4 – MITRE Att&ck framework (© 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation)

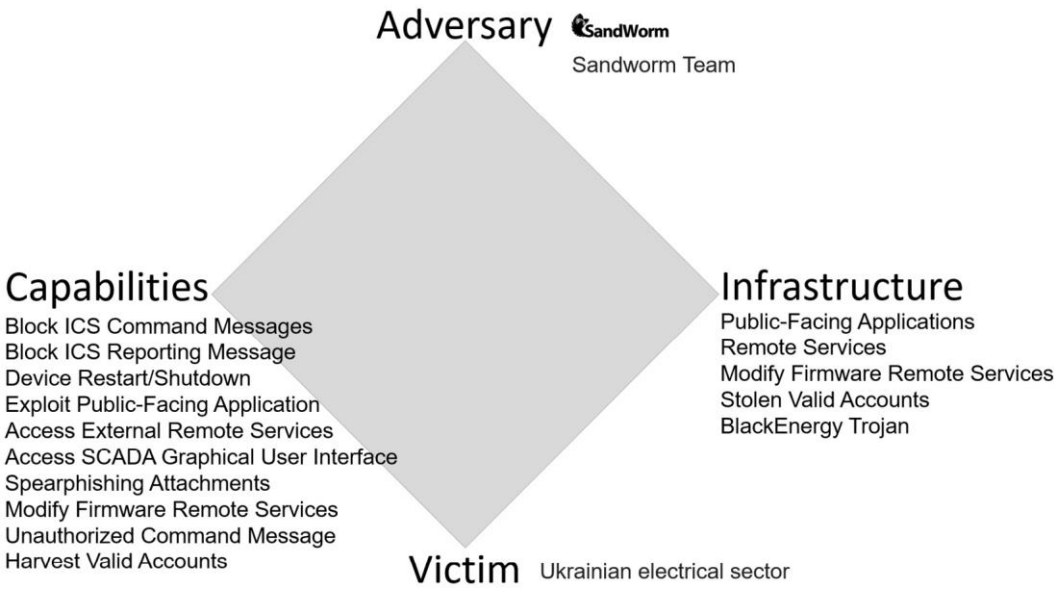


Figure 5.5 – The Diamond model of intrusion analysis

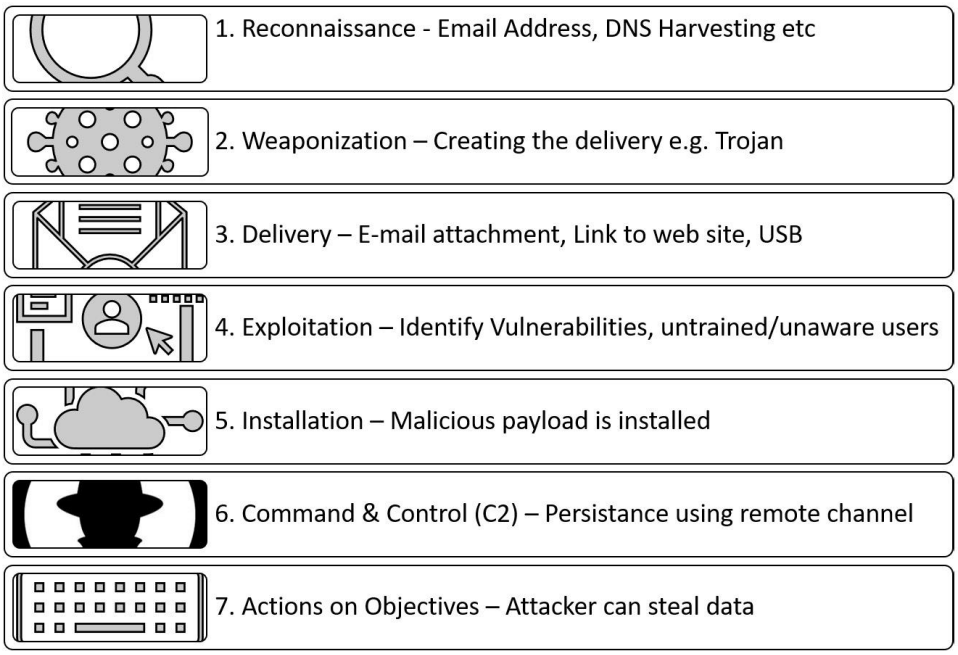


Figure 5.6 – Cyber Kill Chain

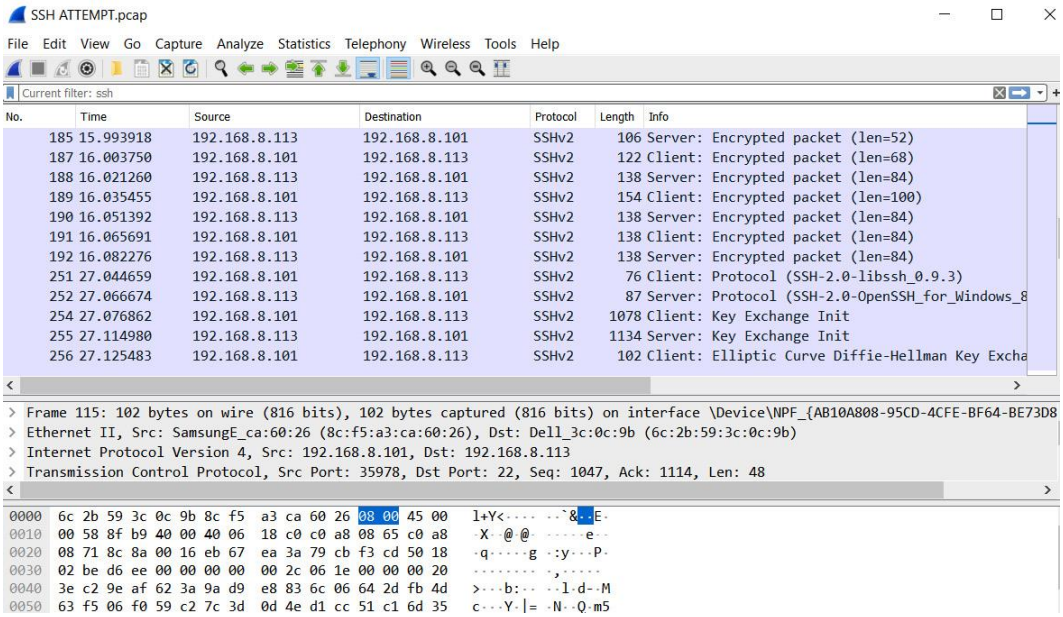


Figure 5.7 – PCAP file

Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Cron subsystem
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16–23	local0 – local7	Locally used facilities

Figure 5.8 – Syslog facility codes

```
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2021-06-08 09:53:51 ALLOW UDP 192.168.8.101 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE
2021-06-08 09:53:51 ALLOW UDP 192.168.8.101 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE
2021-06-08 09:54:03 ALLOW UDP 192.168.8.113 192.168.8.1 64254 53 0 - - - - - - - SEND
2021-06-08 09:54:03 ALLOW UDP 192.168.8.113 172.217.16.238 54523 443 0 - - - - - - - SEND
2021-06-08 09:54:06 ALLOW UDP 192.168.8.113 192.168.8.1 58463 53 0 - - - - - - - SEND
2021-06-08 09:54:06 ALLOW TCP 192.168.8.113 52.113.205.4 1746 443 0 - 0 0 0 - - - SEND
2021-06-08 09:54:06 ALLOW TCP 192.168.8.101 192.168.8.113 55978 22 0 - 0 0 0 - - - RECEIVE
2021-06-08 09:54:25 ALLOW UDP 192.168.8.113 192.168.8.1 55181 53 0 - - - - - - - SEND
2021-06-08 09:54:25 ALLOW TCP 192.168.8.113 52.0.218.127 1042 443 0 - 0 0 0 - - - SEND
2021-06-08 09:54:46 ALLOW TCP 192.168.8.113 52.104.18.41 1045 443 0 - 0 0 0 - - - SEND
2021-06-08 09:54:46 ALLOW TCP 192.168.8.113 52.104.18.41 1046 443 0 - 0 0 0 - - - SEND
2021-06-08 09:55:23 ALLOW UDP 192.168.8.113 239.255.255.250 57174 1900 0 - - - - - - - SEND
2021-06-08 09:55:23 ALLOW UDP 192.168.8.113 172.217.16.238 52108 443 0 - - - - - - - SEND
2021-06-08 09:55:32 ALLOW UDP 192.168.8.113 192.168.8.1 49664 53 0 - - - - - - - SEND
2021-06-08 09:55:32 ALLOW UDP 192.168.8.113 216.58.212.227 61629 443 0 - - - - - - - SEND
2021-06-08 09:55:40 ALLOW UDP 192.168.8.113 192.168.8.1 53393 53 0 - - - - - - - SEND
2021-06-08 09:55:40 ALLOW TCP 192.168.8.113 172.217.169.69 1025 443 0 - 0 0 0 - - - SEND
2021-06-08 09:56:11 ALLOW TCP 192.168.8.113 52.97.208.18 1027 443 0 - 0 0 0 - - - SEND
2021-06-08 09:56:19 ALLOW ICMP fe80::2a64:b0ff:fe50:bb7 ff02::1 - - 0 - - - - 134 0 - RECEIVE
2021-06-08 09:56:23 ALLOW UDP 192.168.8.113 172.217.16.238 53097 443 0 - - - - - - - SEND
2021-06-08 09:56:39 ALLOW UDP 192.168.8.113 224.0.0.253 60080 3544 0 - - - - - - - SEND
2021-06-08 09:56:54 ALLOW TCP 192.168.8.113 192.168.8.1 1026 80 0 - 0 0 0 - - - SEND
2021-06-08 09:56:54 ALLOW TCP 192.168.8.113 192.168.8.1 13851 80 0 - 0 0 0 - - - SEND
2021-06-08 09:56:55 ALLOW UDP 192.168.8.113 192.168.8.1 54102 53 0 - - - - - - - SEND
2021-06-08 09:57:15 ALLOW UDP 192.168.8.113 192.168.8.1 57089 53 0 - - - - - - - SEND
2021-06-08 09:57:15 ALLOW UDP 192.168.8.113 142.250.178.3 49312 443 0 - - - - - - - SEND
2021-06-08 09:57:23 ALLOW UDP 192.168.8.113 239.255.255.250 64038 1900 0 - - - - - - - SEND
2021-06-08 09:57:23 ALLOW UDP 192.168.8.113 192.168.8.1 52951 53 0 - - - - - - - SEND
2021-06-08 09:57:23 ALLOW UDP 192.168.8.113 192.168.8.1 52952 53 0 - - - - - - - SEND
2021-06-08 09:57:23 ALLOW TCP 192.168.8.113 51.141.116.70 13853 443 0 - 0 0 0 - - - SEND
2021-06-08 09:57:23 ALLOW TCP 192.168.8.113 51.141.116.70 13852 443 0 - 0 0 0 - - - SEND
2021-06-08 09:57:23 ALLOW UDP 192.168.8.113 192.168.8.1 63436 53 0 - - - - - - - SEND
2021-06-08 09:57:23 ALLOW UDP 192.168.8.113 142.250.180.10 60235 443 0 - - - - - - - SEND
```

Figure 5.9 – Network firewall logs

Figure 5.10 – Vulnerability log

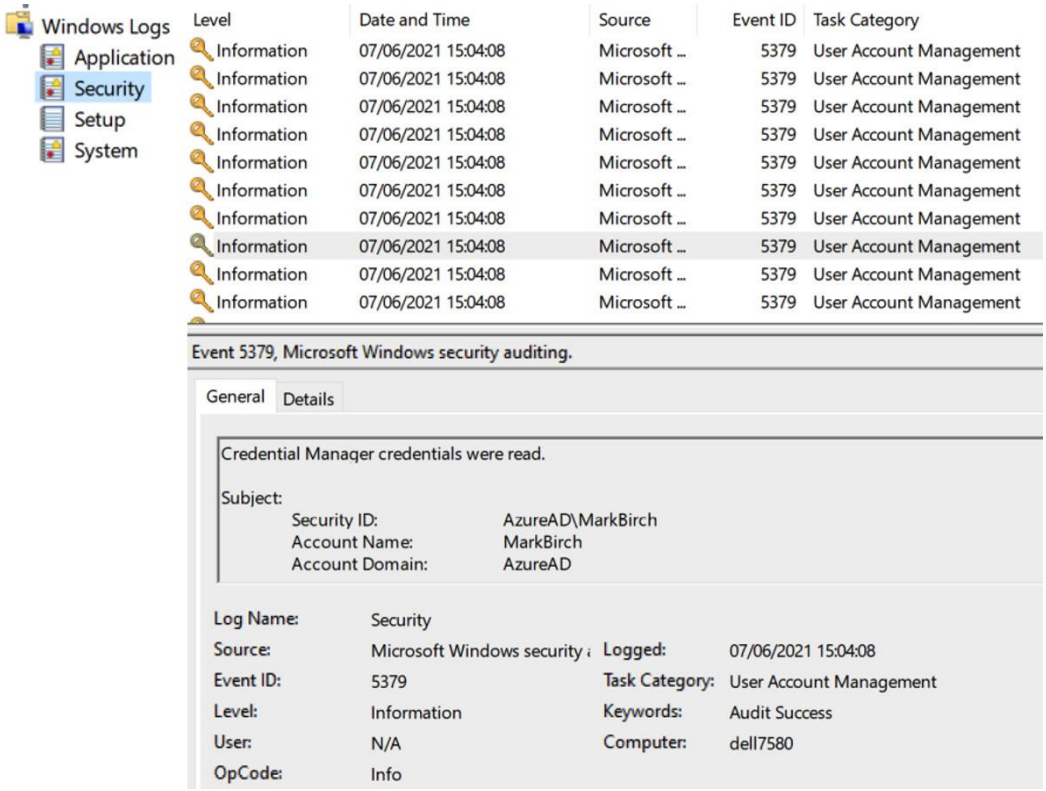


Figure 5.11 – Windows operating system security log

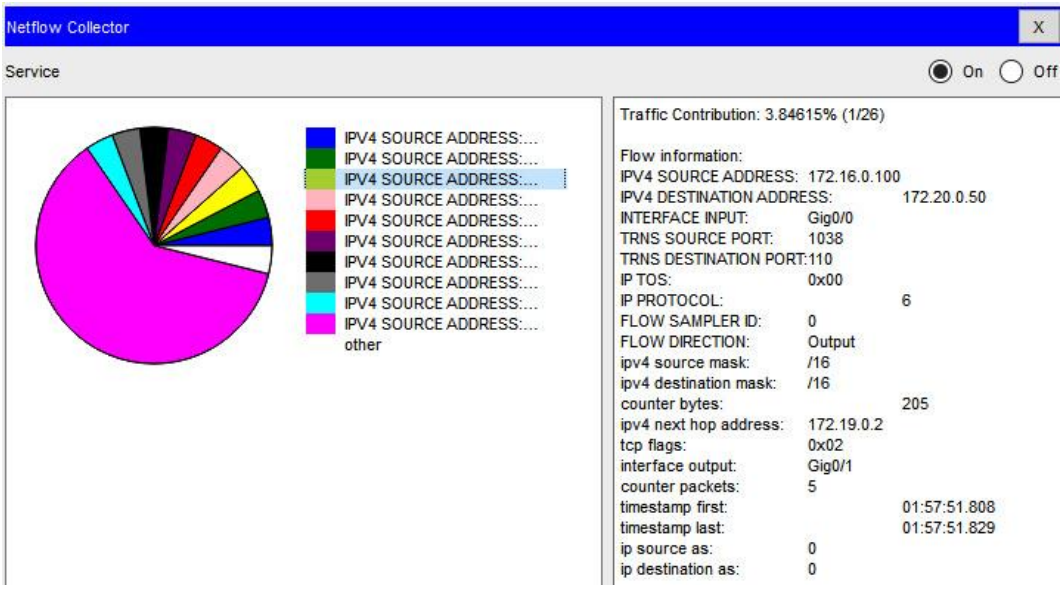


Figure 5.12 – Cisco NetFlow collector

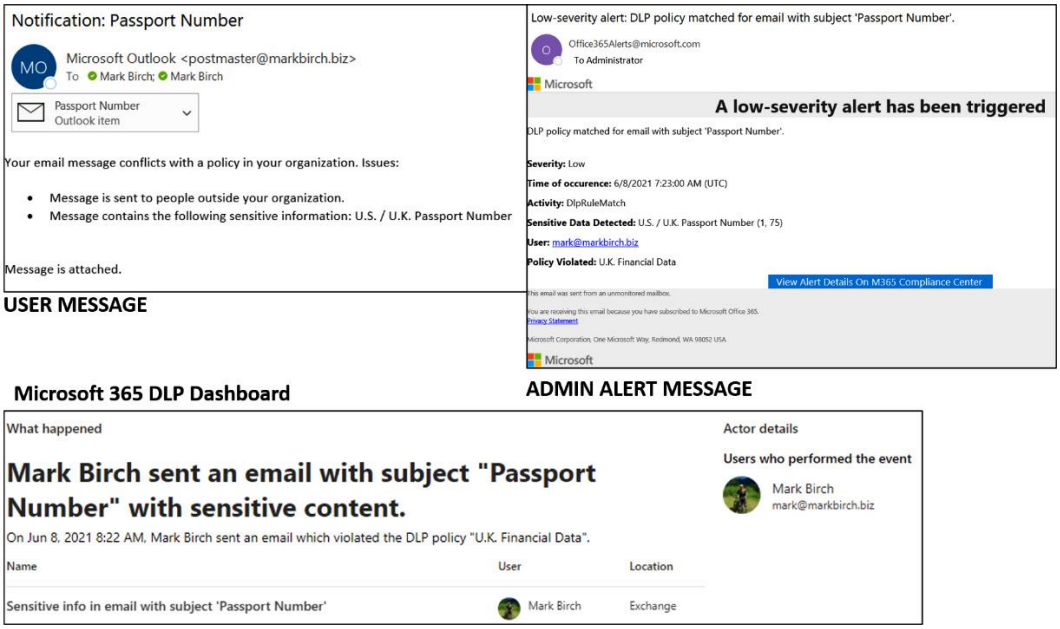


Figure 5.13 – Microsoft 365 DLP alert

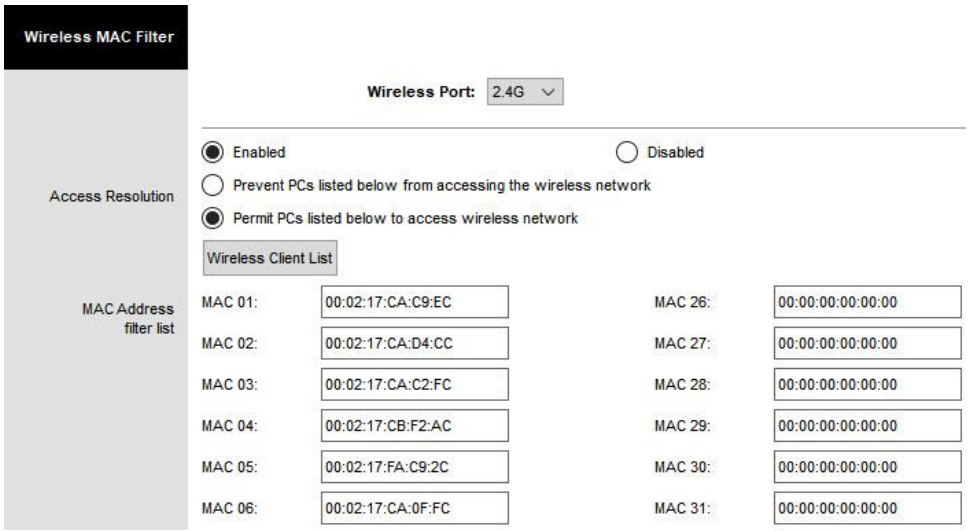


Figure 5.14 – MAC address ACL

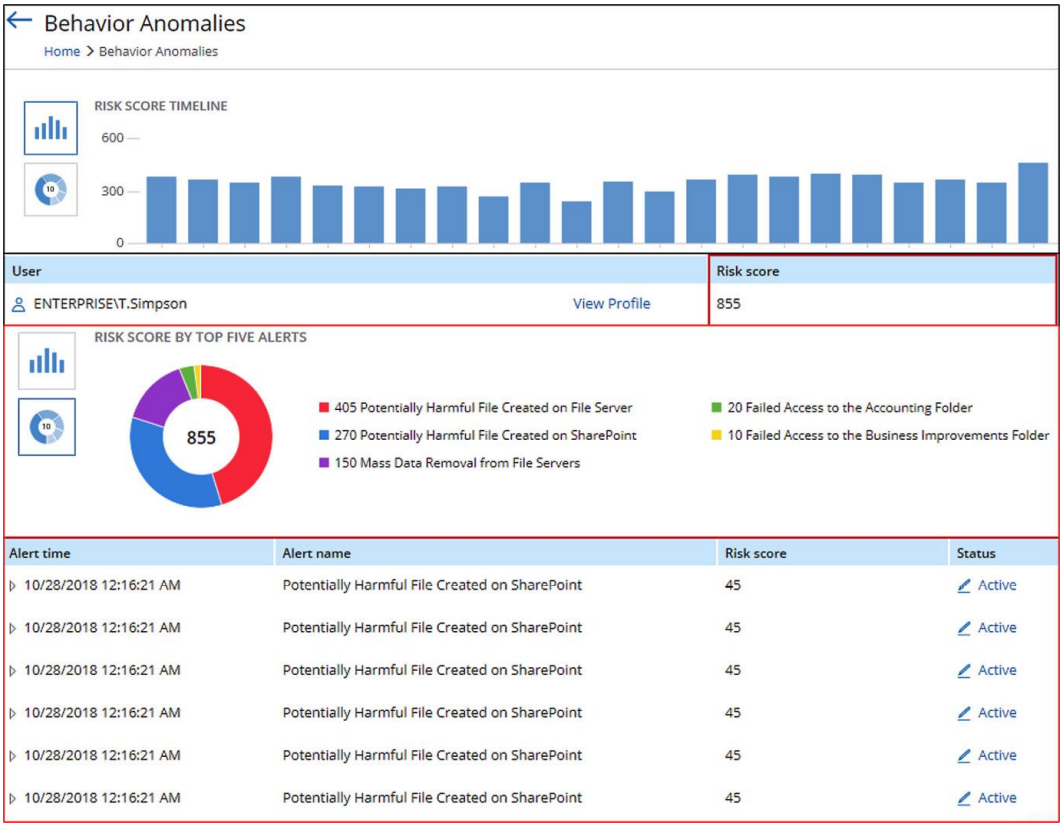


Figure 5.16 – User behavior analytics reporting

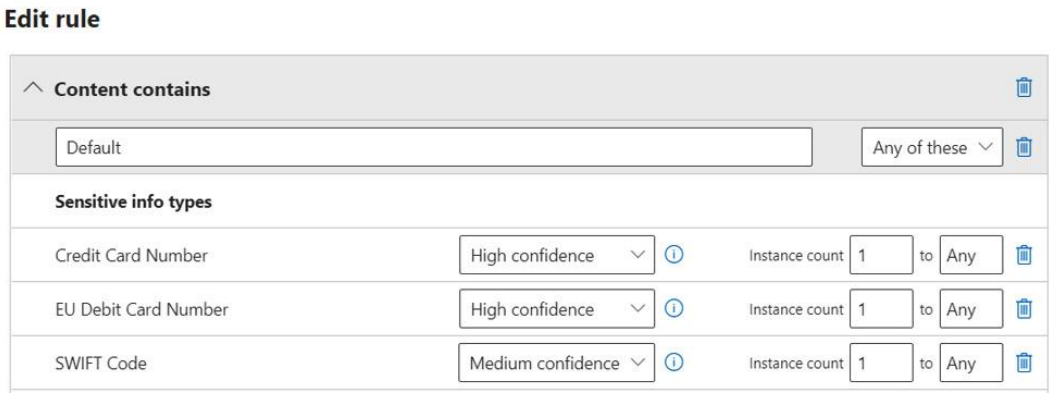


Figure 5.17 – Microsoft 365 DLP rules

Code

Code 5.1

A signature could be a hash match for a known malicious file. For example, the **European Institute for Computer Antivirus Research** (**EICAR**) test file was developed to allow security personnel to check if antivirus software is functional. It uses a well-known string of characters:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Figure 5.15 – EICAR test file

the signature for this string would be as follows:

```
SHA1 3395856ce81f2b7382dee72602f798b642f14140
```

Links

See the following link for more intelligence on APT30 activities:

https://attack.mitre.org/versions/v9/groups/G0013/

For an up-to-date list, follow this URL:

https://www.fireeye.com/current-threats/apt-groups.html

Massachusetts Institute of Technology Research and Engineering (**MITRE**) also publishes a list of APT threat actors:

https://attack.mitre.org/versions/v9/groups/

Recently, the group targeted tech billionaire Elon Musk in retaliation for his activity concerning cryptocurrency. See the following link for more information: https://tinyurl.com/anonymoustarget

The FBI has estimated the cost worldwide to be in excess of $4.2 trillion for 2020, and this is predicted to grow to over $10 trillion by 2025, according to reports in this *Cybercrime Magazine* article: https://tinyurl.com/cybercrimegrowth

For more details on the SolarWinds attack, see the following link:
https://www.bbc.co.uk/news/technology-55321643

There is a good example hosted by spamhaus.com, which can be found at the following link:
https://www.spamhaus.com/threat-map/

A good example of an all-round cyber threat feed can be found at the following link:
https://otx.alienvault.com/preview

The Enterprise Matrix can be found at the following link:
https://attack.mitre.org/versions/v9/matrices/enterprise/

For more information on Sandworm team, see the following link:
https://attack.mitre.org/groups/G0034/

More information can be found at https://tinyurl.com/uebarules.

The ICS matrix can be found at the following link:
https://collaborate.mitre.org/attackics/index.php/Main_Page

The seven stages documented by Lockheed Martin are: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#Resources

This is fully documented in **RFC 5424**. Full documentation can be found at the following URL:
https://datatracker.ietf.org/doc/html/rfc5424

Questions

Here are a few questions to test your understanding of the chapter:

1. Which of the following intelligence types focuses on the threat actor and the reason for the attack?

   A. Tactical

   B. Strategic

   C. Targeted

   D. Operational

2. What is used as a common vector to launch a broad range of attacks?

   A. Tactical

   B. Strategic

   C. Commodity malware

   D. Targeted attacks

3. What type of attack would use spear-phishing against engineers in the Ukraine electricity supply industry with the goal of gaining user credentials?

   A. Deep web

   B. Proprietary

   C. Commodity malware

   D. Targeted attacks

4. Which of the following intelligence types focuses on the technical and automated discovery of everyday threats, threat actors, and the reason for the attack?

   A. Tactical

   B. Strategic

   C. Commodity malware

   D. Targeted attacks

5. Which of the following intelligence types uses forensics and historical logs to identity threats?

   A. Tactical

   B. Strategic

   C. Commodity malware

   D. Operational threat intelligence

6. What framework could a forensics team use to document a specific adversary, victim, capabilities, and infrastructure?

   A. Threat emulation

   B. Threat hunting

   C. Diamond model

   D. STIX

7. What is the most likely threat actor if your router firmware has been tampered with over a period of two years, without being detected?

   A. Advanced persistent threat

   B. Competitor

   C. Hacktivist

   D. Script kiddie

8. What is the most likely threat actor if your electrical power delivery capabilities are attacked?

   A. Nation-state

   B. Insider threat

   C. Hacktivist

   D. Script kiddie

9. What threat actor will most likely steal your intellectual property?

   A. Advanced persistent threat

   B. Competitor

   C. Hacktivist

   D. Script kiddie

10. What is the threat when vulnerabilities are present on your network due to misconfiguration by poorly trained technicians?

    A. Advanced persistent threat

    B. Insider threat

    C. Script kiddie

    D. Organized crime

11. What is the threat when vulnerabilities are present due to the use of third-party libraries in our code base?

    A. Advanced persistent threat

    B. Supply Chain

    C. Insider threat

    D. Organized crime

12. What is the likely threat actor when thousands of systems are targeted with crypto malware followed up with a demand for $5,000 in bitcoin?

    A. Advanced persistent threat

    B. Supply chain

    C. Insider threat

    D. Organized crime

13. What is the public network that hosts unindexed and unsearchable content that may be used for unlawful activities?

    A. World Wide Web

    B. Intranet

    C. Deep web

    D. Proprietary networks

14. What type of intelligence gathering would involve DNS record harvesting?

    A. Intelligence feeds

    B. Deep web

    C. Open source intelligence (OSINT)

    D. Human intelligence (HUMINT)

15. What type of intelligence gathering would involve physical reconnaissance?

    A. Intelligence feeds

    B. Deep Web

    C. Open source intelligence (OSINT)

    D. Human intelligence (HUMINT)

16. What framework would be the best choice to build up a picture of threat actors and their tactics and techniques for a water treatment plant?

    A. MITRE ATT&CK

    B. ATT&CK for industrial control system (ICS)

    C. Diamond model of intrusion analysis

    D. Cyber kill chain

17. What framework would be used to understand the capabilities of APT29 and how they will target your enterprise information systems?

    A. MITRE (ATT&CK)

    B. ATT&CK for industrial control system (ICS)

    C. Scripts/regular expressions

    D. SRTM

18. What framework uses seven stages, starting with *reconnaissance* and ending in *actions on objectives*?

    A. MITRE (ATT&CK)

    B. ATT&CK for industrial control system (ICS)

    C. Diamond model of intrusion analysis

    D. Cyber kill chain

19. What file type will allow for the analysis of network traffic captured by Wireshark or tcpdump?

    A. Packet capture (PCAP)

    B. Vulnerability logs

    C. Operating system logs

    D. Portable Data Format (PDF)

20. What can be used to centrally correlate events from multiple sources and raise alerts?

    A. FIM alerts

    B. SIEM alerts

    C. DLP alerts

    D. IDS/IPS alerts

21. What type of logging can be used for accountability?

    A. Vulnerability logs

    B. Operating system logs

    C. Access logs

    D. NetFlow logs

22. What type of logging can identify the source of most *noise* on a network?

    A. Vulnerability logs

    B. Operating system logs

    C. Access logs

    D. NetFlow logs

23. How will I know if my critical files have been tampered with?

    A. FIM alerts

    B. SIEM alerts

    C. DLP alerts

    D. IDS/IPS alerts

24. George has tried to email his company credit card details to his **Gmail** account. The security team has contacted him and reminded him this is not acceptable use. How were they informed?

    A. FIM alerts

    B. SIEM alerts

    C. DLP alerts

    D. IDS/IPS alerts

25. An attacker has had their session reset after they successfully logged on to the **Private Branch Exchange** (**PBX**) after three unsuccessful attempts using SSH. What is the reason for this?

    A. FIM alerts

    B. Firewall alerts

    C. DLP rules

    D. IPS rules

26. The Acme corporation needs to block the exfiltration of United States medical-related data due to a new regulatory requirement. What is most likely going to get updated?

    A. ACL rules

    B. Signature rules

    C. Behavior rules

    D. DLP rules

27. Bill the network technician has been tasked with updating security based upon a threat exchange update. Five known bad actor IP addresses must be blocked. What should be updated?

    A. Firewall rules

    B. Signature rules

    C. Behavior rules

    D. DLP rules

28. What is used to search for character strings in my DLP solution?

    A. Signature rules

    B. Behavior rules

    C. Firewall rules

    D. Regular expressions

29. What type of rule will alert administrators that Colin is deleting significant amounts of sensitive company data?

    A. Signature rules

    B. Behavior rules

    C. Firewall rules

    D. Regular expressions

30. What will alert the SOC team to IOCs detected in logs of multiple network appliances?

    A. SIEM alerts

    B. Behavior alerts

    C. DLP alerts

    D. Syslogs

31. What type of rule will alert administrators about a known malware variant that has the following checksum:

```
sha1 checksum 29386154B7F99B05A23DC9D04421AC8B0534CBE1?
```

    A. ACL rules

    B. Signature rules

    C. Behavior rules

    D. DLP rules

32. Charles notices several endpoints have been infected by a recently discovered malware variant. What has allowed Charles to receive this information?

    A. SIEM alerts

    B. Antivirus alerts

    C. DLP alerts

    D. Syslogs

Answers

1. A
2. C
3. D
4. A
5. D
6. C
7. A
8. A
9. B
10. B
11. B
12. D
13. C
14. C

15. D
16. B
17. A
18. D
19. A
20. B
21. C
22. D
23. A
24. C
25. D
26. D
27. A
28. D
29. B
30. A
31. B
32. B

Chapter 6

Figures

SCAN 1. Report

Windows IExpress Untrusted Search Path Vulnerability	9.3 (High)
Wireshark Security Updates (wnpa-sec-2017-43_wnpa-sec-2017-42)-Windows	7.8 (High)
Wireshark Security Updates (wnpa-sec-2018-34_wnpa-sec-2018-41) Windows	7.8 (High)
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)
Wireshark Denial of Service Vulnerability (Windows)	7.5 (High)
MS Windows HID Functionality (Over USB) Code Execution Vulnerability	6.9 (Medium)
Wireshark Security Updates (wnpa-sec-2018-05 to -14) Windows	5.0 (Medium)

SCAN 2. Report

Windows IExpress Untrusted Search Path Vulnerability	9.3 (High)
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)
MS Windows HID Functionality (Over USB) Code Execution Vulnerability	6.9 (Medium)

Figure 6.1 – Critical ranked vulnerabilities

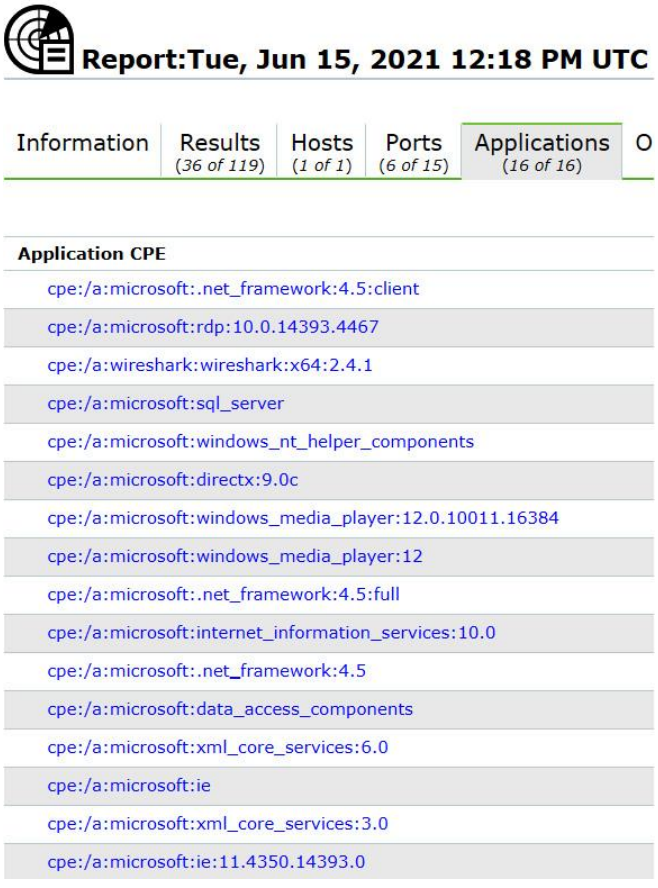


Figure 6.2 – List of discovered CPE items

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score

Select values for all base metrics to generate score

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Vector String - select values for all base metrics to generate a vector

Temporal Score

Select values for all base metrics to generate score

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Figure 6.3 – CVSS calculator

VMware Guest to Host Escape Vulnerability (CVE-2012-1516)

Vulnerability

Due to a flaw in the handler function for Remote Procedure Call (RPC) commands, it is possible to manipulate data pointers within the Virtual Machine Executable (VMX) process. This vulnerability may allow a user in a Guest Virtual Machine to crash the VMX process resulting in a Denial of Service (DoS) on the host or potentially execute code on the host.

Attack

A successful exploit requires an attacker to have access to a Guest Virtual Machine (VM). The Guest VM needs to be configured to have 4GB or more of memory. The attacker would then have to construct a specially crafted remote RPC call to exploit the VMX process.

The VMX process runs in the VMkernel that is responsible for handling input/output to devices that are not critical to performance. It is also responsible for communicating with user interfaces, snapshot managers, and remote console. Each virtual machine has its own VMX process which interacts with the host processes via the VMkernel.

The attacker can exploit the vulnerability to crash the VMX process resulting in a DoS of the host or potentially execute code on the host operating system.

CVSS v3.1 Base Score: 9.9

Metric	Value	Comments
Attack Vector	Network	VMX process is bound to the network stack and the attacker can send RPC commands remotely.
Attack Complexity	Low	The only required condition for this attack is for virtual machines to have 4GB of memory. Virtual machines that have less than 4GB of memory are not affected.
Privileges Required	Low	The attacker must have access to the guest virtual machine. This is easy in a tenant environment.
User Interaction	None	The attacker requires no user interaction to successfully exploit the vulnerability. RPC commands can be sent anytime.
Scope	Changed	The vulnerable component is a VMX process that can only be accessed from the guest virtual machine. The impacted component is the host operating system which has separate authorization authority from the guest virtual machine.
Confidentiality	High	Full compromise of the host operating system via remote code execution.
Integrity	High	Full compromise of the host operating system via remote code execution.
Availability	High	Full compromise of the host operating system via remote code execution.

Figure 6.4 – Critical vulnerability

Report:Tue, Jun 15, 2021 12:18 PM UTC Done

ID: 6bb9ca4d-7c0f-450a-aaf9-f94aa1d89fa4 Created: Tue, Jun 15, 2021 12:18 PM UTC Modified:

Information | Results (36 of 119) | Hosts (1 of 1) | Ports (6 of 15) | Applications (16 of 16) | Operating Systems (1 of 1) | CVEs (27 of 27) | Closed CVEs (1585 of 1585) | TLS Certificates (4 of 4) | Error Messages (0 of 0) | User Tags (0)

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location
Windows IExpress Untrusted Search Path Vulnerability	9.3 (High)	80 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Security Updates (wnpa-sec-2017-43_wnpa-sec-2017-42)-Windows	7.8 (High)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Security Updates (wnpa-sec-2018-34_wnpa-sec-2018-41) Windows	7.8 (High)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	10.10.0.1	WIN2016-DC.classroom.local	445/tcp
Wireshark Denial of Service Vulnerability (Windows)	7.5 (High)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
MS Windows HID Functionality (Over USB) Code Execution Vulnerability	6.9 (Medium)	80 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Security Updates (wnpa-sec-2018-05 to -14) Windows	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Multiple Vulnerabilities-Nov18 (Windows)	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities Apr18 (Windows)	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Security Updates (wnpa-sec-2017-49_wnpa-sec-2017-47)-Windows	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark Security Updates (wnpa-sec-2018-04_wnpa-sec-2018-03_wnpa-sec-2018-01) Windows	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
Wireshark 'non-NULL DACL' Access Control Vulnerability (Windows)	5.0 (Medium)	97 %	10.10.0.1	WIN2016-DC.classroom.local	general/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	10.10.0.1	WIN2016-DC.classroom.local	636/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	10.10.0.1	WIN2016-DC.classroom.local	443/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	10.10.0.1	WIN2016-DC.classroom.local	3389/tcp

Figure 6.5 – OpenVAS SCAP scan

Wireshark Security Updates (wnpa-sec-2017-43_wnpa-sec-2017-42)-Windows | 7.8 (High) | 97 % | 10.10.0.1 | WIN2016-DC.classroom.local

Summary

This host is installed with Wireshark and is prone to multiple vulnerabilities.

Detection Result

```
Installed version: 2.4.1
Fixed version:     2.4.2
```

Insight

Multiple flaws exist due to:

- The MBIM dissector could crash or exhaust system memory.

- Attribute Protocol dissector could crash.

Detection Method

Checks if a vulnerable version is present on the target host.

Details: Wireshark Security Updates (wnpa-sec-2017-43_wnpa-sec-2017-42)-Windows...,OID: 1.3.6.1.4.1.25623.1.0.811943

Affected Software/OS

Wireshark version 2.4.0 to 2.4.1, 2.2.0 to 2.2.9 on Windows.

Impact

Successful exploitation of this vulnerability will allow remote attackers to make Wireshark crash or exhaust system memory by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file. It may be possible to make Wireshark crash by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.

Solution

Solution Type: Vendorfix
Upgrade to Wireshark version 2.4.2, 2.2.10 or later.

References

CVE CVE-2017-15193
CVE-2017-15192

Figure 6.6 – Vendor fix

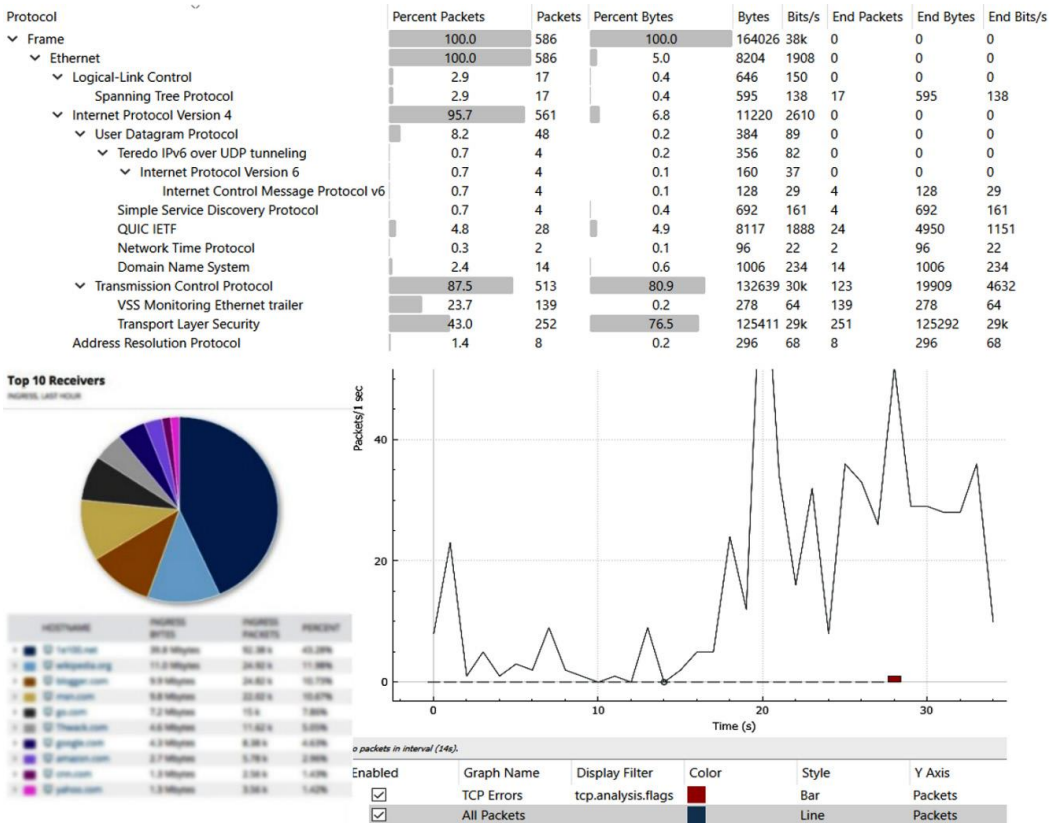


Figure 6.7 – Network traffic flow

10.10.0.1 / 10.10.0.1 port 80

Target IP	10.10.0.1
Target hostname	10.10.0.1
Target Port	80
HTTP Server	Microsoft-IIS/10.0
Site Link (Name)	http://10.10.0.1:80/
Site Link (IP)	http://10.10.0.1:80/

URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: ASP.NET
Test Links	http://10.10.0.1:80/ http://10.10.0.1:80/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'strict -transport -security' found, with contents: max-age=63072000; includeSubDomains; Preload
Test Links	http://10.10.0.1:80/ http://10.10.0.1:80/

URI	/
HTTP Method	GET
Description	Uncommon header 'strict -transport -security' found, with contents: max-age=63072000; includeSubDomains; Preload
Test Links	http://10.10.0.1:80/ http://10.10.0.1:80/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://10.10.0.1:80/ http://10.10.0.1:80/
OSVDB Entries	OSVDB-0

Host Summary

Start Time	2021-06-17 10:53:08
End Time	2021-06-17 10:54:42
Elapsed Time	94 seconds
Statistics	8041 requests, 0 errors, 6 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-host 10.10.0.1 -Format html -output /home/mark/Documents/vreport.htm
Hosts Tested	1
Start Time	Thu Jun 17 10:53:07 2021
End Time	Thu Jun 17 10:54:42 2021
Elapsed Time	95 seconds

Figure 6.8 – Vulnerability scanner

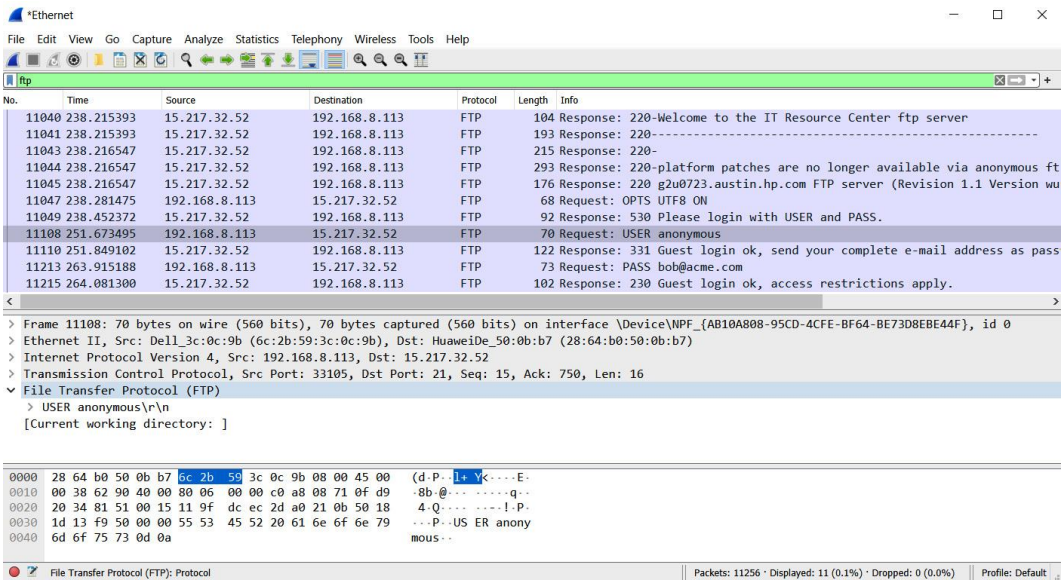


Figure 6.9 – Wireshark protocol analyzer

```
nmap -T4 -A -v 192.168.0.0/24

Initiating SYN Stealth Scan at 11:15
Scanning 192.168.0.8 [1000 ports]
Discovered open port 139/tcp on 192.168.0.8
Discovered open port 445/tcp on 192.168.0.8
Discovered open port 135/tcp on 192.168.0.8
Discovered open port 2179/tcp on 192.168.0.8
Discovered open port 808/tcp on 192.168.0.8
Discovered open port 5357/tcp on 192.168.0.8
Completed SYN Stealth Scan at 11:15, 0.06s elapsed (1000 total ports)
Initiating Service scan at 11:15
Scanning 6 services on 192.168.0.8
Completed Service scan at 11:15, 21.06s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.8
NSE: Script scanning 192.168.0.8.
Initiating NSE at 11:15
Completed NSE at 11:15, 14.34s elapsed
Initiating NSE at 11:15
Completed NSE at 11:15, 0.01s elapsed
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Nmap scan report for 192.168.0.8
Host is up (0.00020s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
808/tcp  open  mc-nmf        .NET Message Framing
2179/tcp open  vmrdp?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 6.10 – NMAP scan

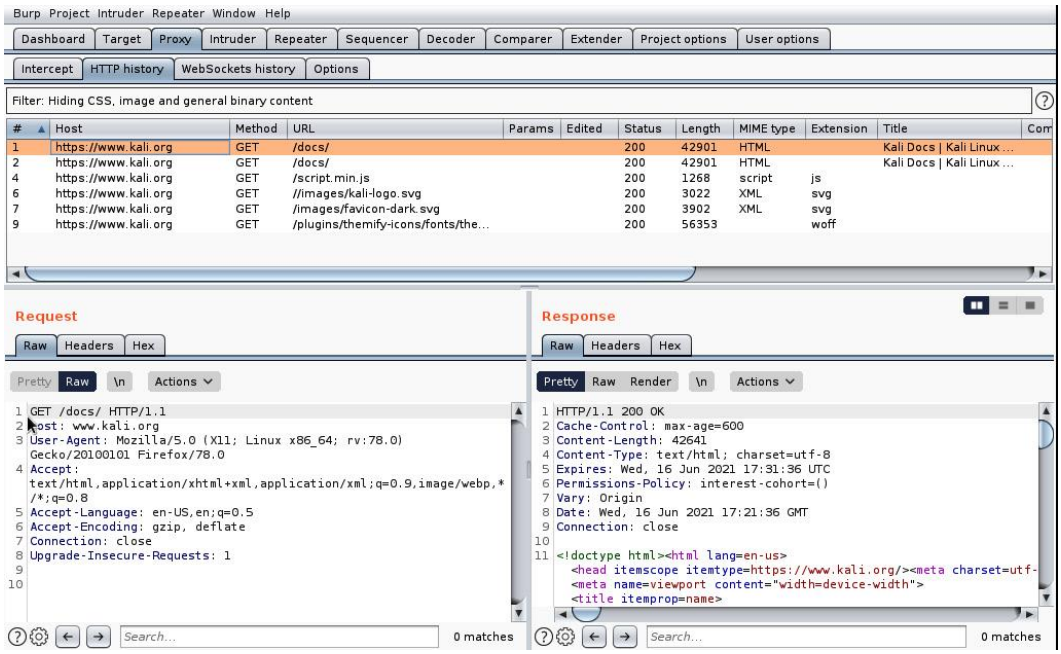


Figure 6.11 – HTTP interceptor

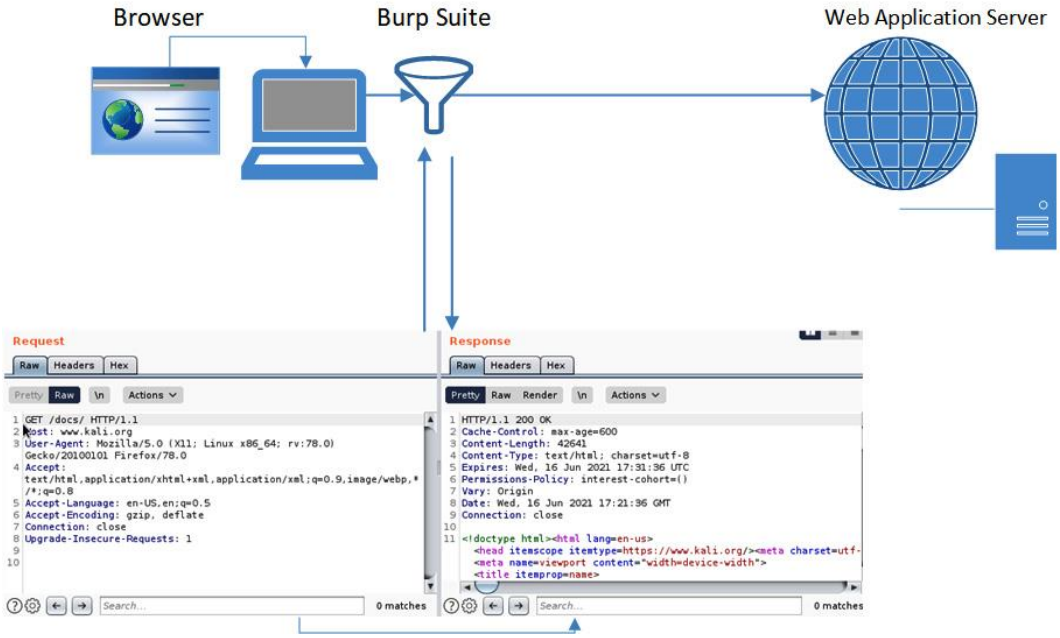


Figure 6.12 – Burp Suite deployment

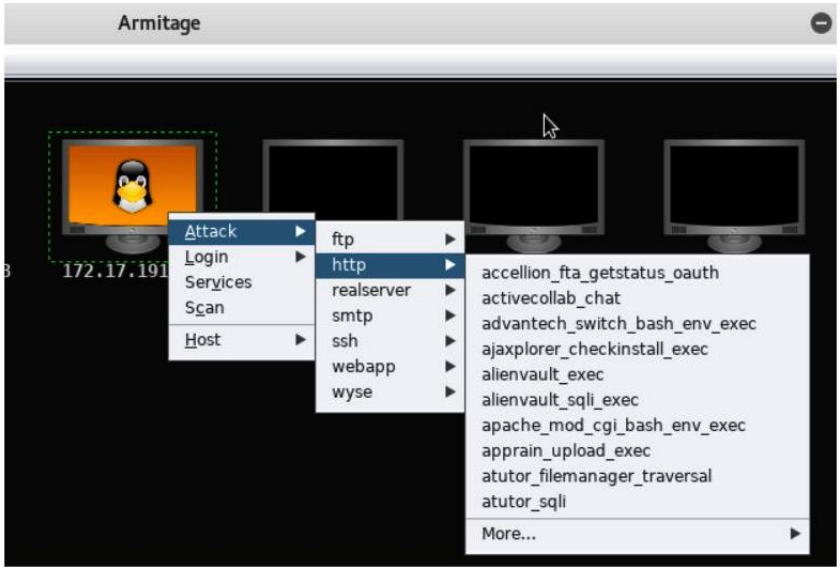


Figure 6.13 – Exploitation framework

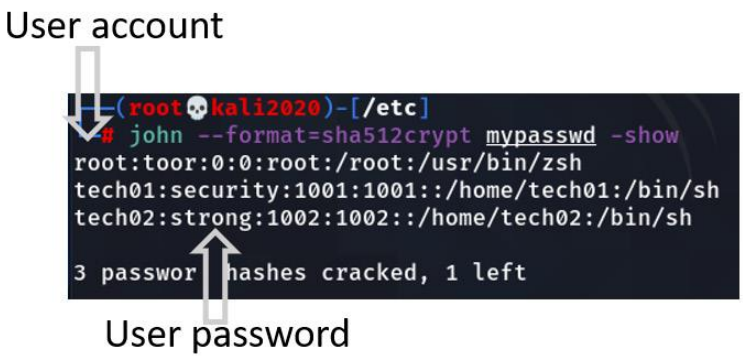


Figure 6.14 – John the Ripper password cracking

Links

More information on STIG be obtained from the following public site: https://public.cyber.mil/stigs/.

CVSS Calculator: https://www.first.org/cvss/calculator/3.1

Some Advisories example site URLs are listed as follows:

- **Cisco**: https://tools.cisco.com/security/center/publicationListing.x
- **VMware**: https://www.vmware.com/security/advisories.html
- **Microsoft**: https://www.microsoft.com/en-us/msrc/technical-security-notifications?rtc=1
- **Hewlett Packard**: https://www.hpe.com/us/en/services/security-vulnerability.html

Examples of vendor security bulletins are listed as follows:

- **Amazon Web Services** (**AWS**): https://tinyurl.com/awsbulletins
- **Google Cloud**: https://cloud.google.com/compute/docs/security-bulletins

Microsoft is one of many vendors who offer their customers access to extensive security guidance and best practices: https://docs.microsoft.com/en-us/security/

For more information concerning ISACs, go to https://www.nationalisacs.org/.

US fuel pipeline 'paid hackers $5m in ransom: https://tinyurl.com/colonialransomware.

10 June 2021: JBS, the world's largest meat processing company, paid out $11 million in bitcoin to regain control of their IT services. Follow the story at this link: https://tinyurl.com/jcbransomware.

IBM chips in with '60s Golfball anniversary: https://tinyurl.com/ibmgolfball.

There are many available online tools to reverse-engineer Java code. One example is https://devtoolzone.com/decompiler/java

For more information on SCA, see the following link: https://tinyurl.com/scaTools/.

The **National Cyber Security Center** (**NCSC**) recommends that United Kingdom government agencies choose a penetration tester that holds one of the following accreditations:

- **CREST**: https://www.crest-approved.org/
- **Tigerscheme**: https://www.tigerscheme.org/
- **Cyber Scheme**: https://www.thecyberscheme.org/

OWASP: More information can be found at the following link: http://www.pentest-standard.org/index.php/Exploitation.

For a comprehensive list of activities in post exploitation, follow this URL: http://www.pentest-standard.org/index.php/Post_Exploitation#Purpose.

MITRE lists 19 techniques, used for peristence, in the **ATT&CK Matrix for Enterprise.** The full list can be found at the following link: https://attack.mitre.org/tactics/TA0003/

For more detail on the nine methods listed by **MITRE ATT&CK Matrix for Enterprise**, follow this URL: https://attack.mitre.org/versions/v9/matrices/enterprise/.

Questions

Here are a few questions to test your understanding of the chapter:

1. When performing a SCAP scan on a system, which of the following types of scans will be most useful?

   A. Credentialed

   B. Non-credentialed

   C. Agent-based

   D. Intrusive

2. What would be most important when monitoring security on ICS networks, where latency must be minimized?

   A. Group Policy

   B. Active scanning

   C. Passive scanning

   D. Continuous integration

3. What is the protocol that allows for the automation of security compliance scans?

   A. SCAP

   B. CVSS

   C. CVE

   D. ARF

4. What standard would support the creation of XML-format configuration templates?

   A. XCCDF

   B. CVE

   C. CPE

   D. NMAP

5. What standard allows a vulnerability scanner to detect the host operating system and installed applications?

A. XCCDF

B. CVE

C. CPE

D. SCAP

6. What standard supports a common reporting standard for vulnerability scanning?

A. XCCDF

B. CVE

C. OVAL

D. STIG

7. What information type can be found at MITRE and NIST NVD that describes a known vulnerability and gives information regarding remediation?

A. CVE

B. CPE

C. CVSS

D. OVAL

8. What is used to calculate the criticality of a known vulnerability?

A. CVE

B. CPE

C. CVSS

D. OVAL

9. If my organization is preparing to host publicly available SaaS services in the data center, what kind of assessment would be best?

A. Self-assessment

B. Third-party assessment

C. PCI compliance

D. Internal assessment

10. When we download patches from Microsoft, where should they be tested *first*?

A. Staging network

B. Production network

C. DMZ network

D. IT administration network

11. Where can security professionals go to remain aware of vendor-published security updates and guidance? (Choose all that apply.)

A. Advisories

B. Bulletins

C. Vendor websites

D. MITRE

12. What allows European critical infrastructure providers to share security-related information?

A. ISACs

B. NIST

C. SCAP

D. CISA

13. What kind of testing would be performed against uncompiled code?

A. Static analysis

B. Dynamic analysis

C. Fuzzing

D. Reverse engineering

14. What type of analysis would allow researchers to measure power usage to predict the encryption keys generated by a crypto-processor?

A. Side-channel analysis

B. Frequency analysis

C. Network analysis

D. Hacking

15. What type of analysis would most likely be used when researchers need to study third-party compiled code?

A. Static analysis

B. Side-channel analysis

C. Input validation

D. Reverse engineering

16. What automated tool would developers use to report on any outdated software libraries and licensing requirements?

    A. Software composition analysis

    B. Side-channel analysis

    C. Input validation

    D. Reverse engineering

17. What is it called when we send pseudo-random inputs to an application, in an attempt to find flaws in the code?

    A. Fuzz testing

    B. Input validation

    C. Reverse engineering

    D. Pivoting

18. What is the term for lateral movement from a compromised host system?

    A. Pivoting

    B. Reverse engineering

    C. Persistence

    D. Requirements

19. When would a penetration tester use a privilege escalation exploit?

    A. Post-exploitation

    B. OSINT

    C. Reconnaissance

    D. Foot printing

20. What is the correct term for a penetration tester manipulating the registry in order to launch a binary file during the boot sequence?

    A. Pivoting

    B. Reverse engineering

    C. Persistence

    D. Requirements

21. What tool would allow network analysts to report on network utilization levels?

    A. Network traffic analyzer

    B. Vulnerability scanner

    C. Protocol analyzer

    D. Port scanner

22. What would be the *best* tool to test the security configuration settings for a web application server?

    A. Network traffic analyzer

    B. Vulnerability scanner

    C. Protocol analyzer

    D. Port scanner

23. With what tool would penetration testers discover live hosts and application services on a network segment?

    A. Network traffic analyzer

    B. Vulnerability scanner

    C. Protocol analyzer

    D. Port scanner

24. What type of tool would perform uncredentialed scans?

    A. Network traffic analyzer

    B. Vulnerability scanner

    C. Protocol analyzer

    D. Port scanner

25. What could be used to reverse engineer a web server API when conducting a zero-knowledge (black box) test?

    A. Exploitation framework

    B. Port scanner

    C. HTTP interceptor

    D. Password cracker

26. What tool could be used by hackers to discover unpatched systems using automated scripts?

A. Exploitation framework

B. Port scanner

C. HTTP interceptor

D. Password cracker

27. What would allow system administrators to discover weak passwords stored on the server?

A. Exploitation framework

B. Port scanner

C. HTTP interceptor

D. Password cracker

28. What documentation would mitigate the risk of pen testers testing the security posture of all regional data centers when the requirement was only for the e-commerce operation center?

A. Requirements

B. Scope of work

C. Rules of engagement

D. Asset inventory

29. What documentation would mitigate the risk of pen testers unintentionally causing an outage on the network during business hours?

A. Requirements

B. Scope of work

C. Rules of engagement

D. Asset inventory

30. What type of security assessment is taking place if the tester needs to perform badge skimming *first*?

A. Network security assessment

B. Corporate policy considerations

C. Facility considerations

D. Physical security assessment

Answers

1. A
2. C
3. A
4. A
5. C
6. C
7. A
8. C
9. B
10. A
11. A, B and C
12. A
13. A
14. A
15. D
16. A
17. A
18. A
19. A
20. C
21. A
22. B
23. D
24. D
25. C
26. A
27. D

28. B

29. C

30. D

Chapter 7

Figures

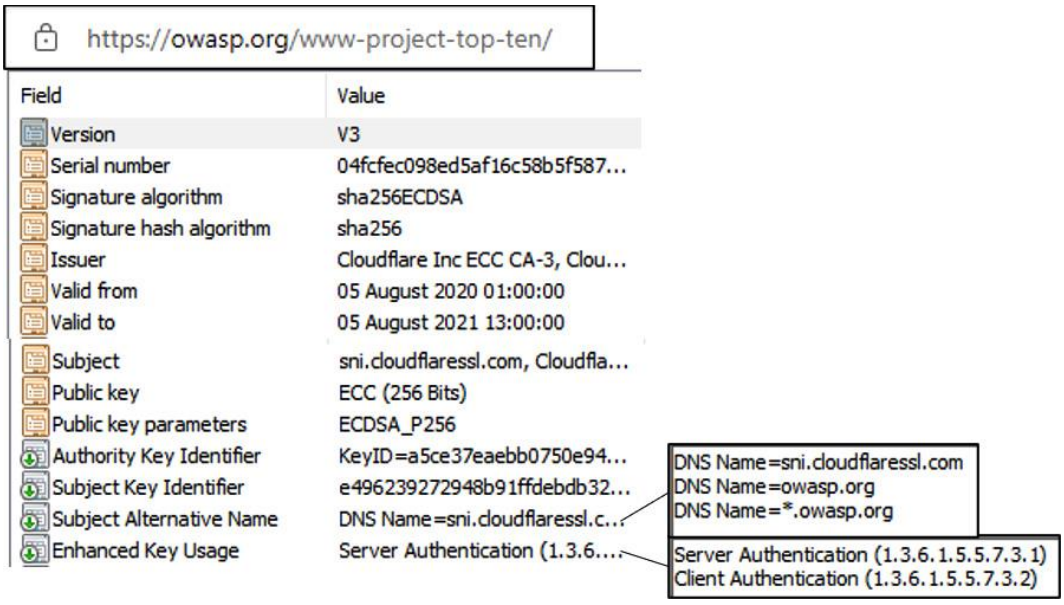


Figure 7.1 – Certificate fields

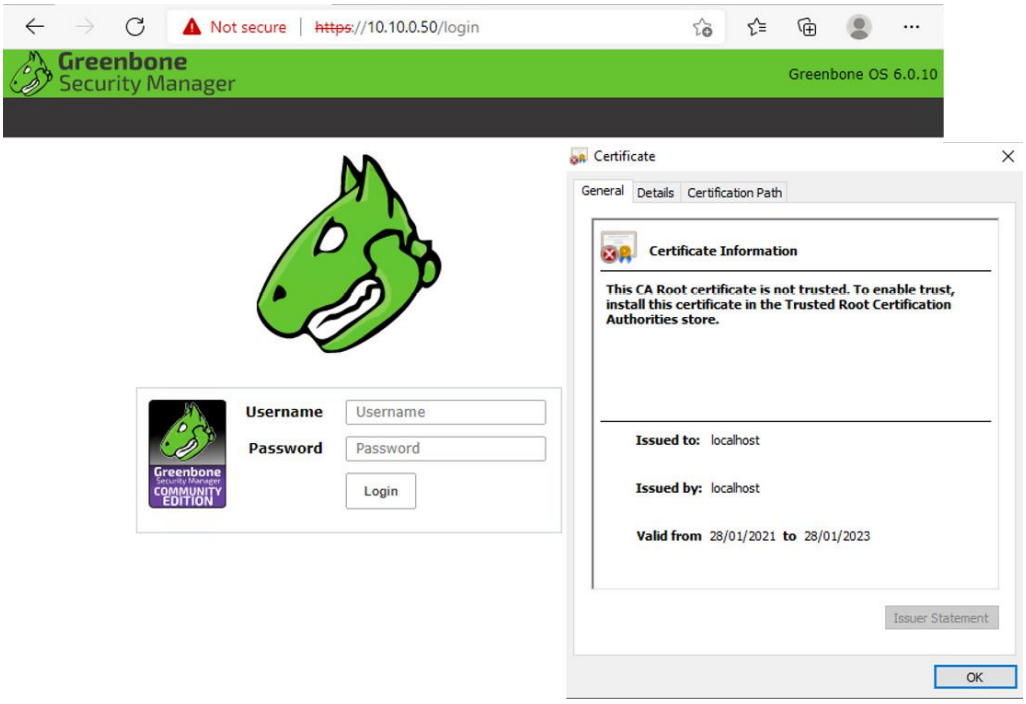
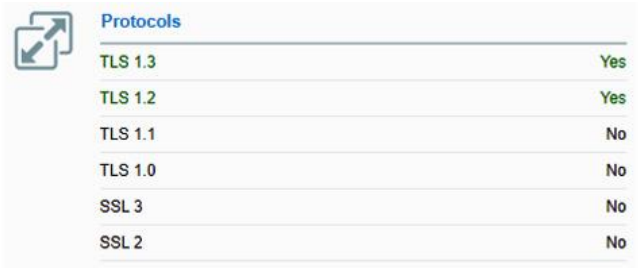


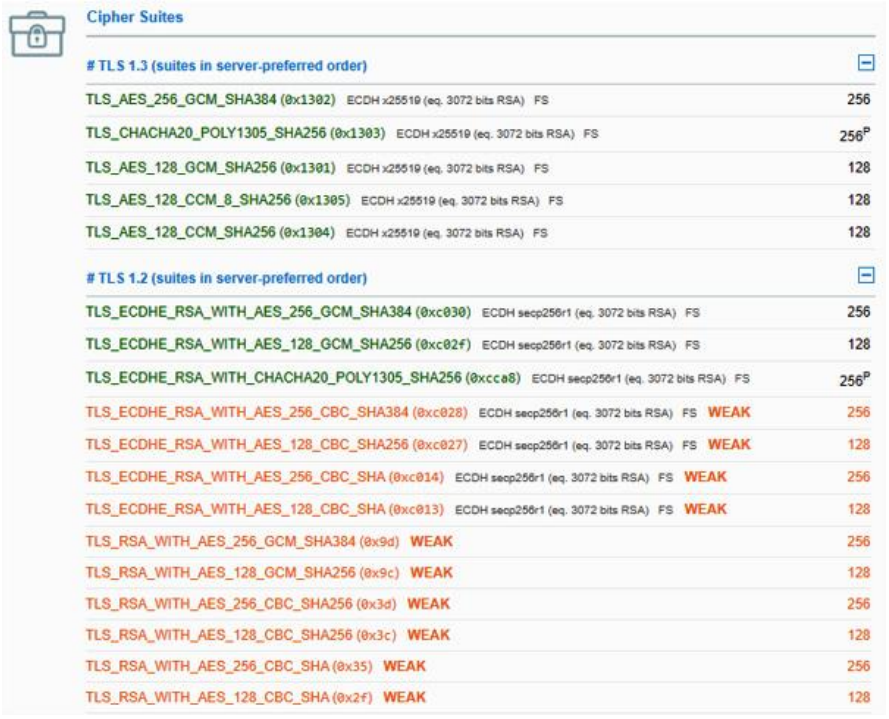
Figure 7.2 – Untrusted web browser connection



Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 7.3 – Secure Transport Layer Security (TLS)



Cipher Suites

# TLS 1.3 (suites in server-preferred order)	
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_8_SHA256 (0x1305) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304) ECDH x25519 (eq. 3072 bits RSA) FS	128
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128

Figure 7.4 – Output from the Qualys SSL Labs vulnerability testing tool

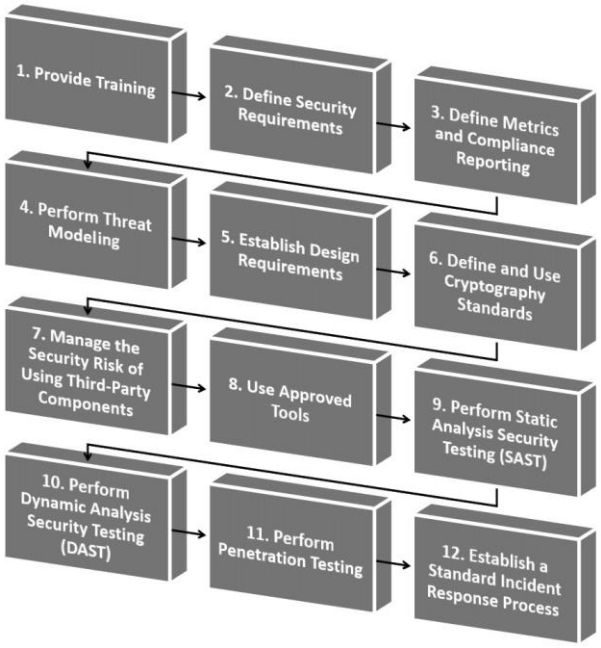


Figure 7.5 – Microsoft SDL framework

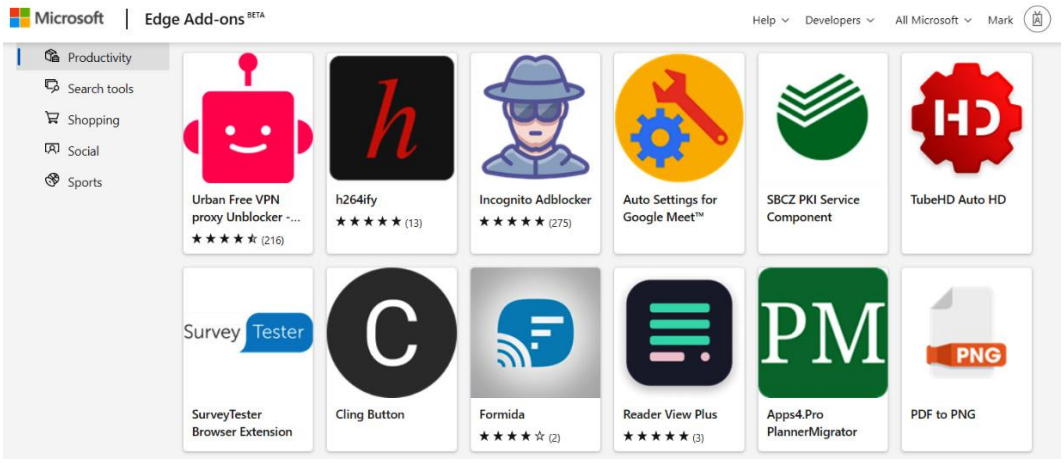


Figure 7.6 – Microsoft Edge extensions

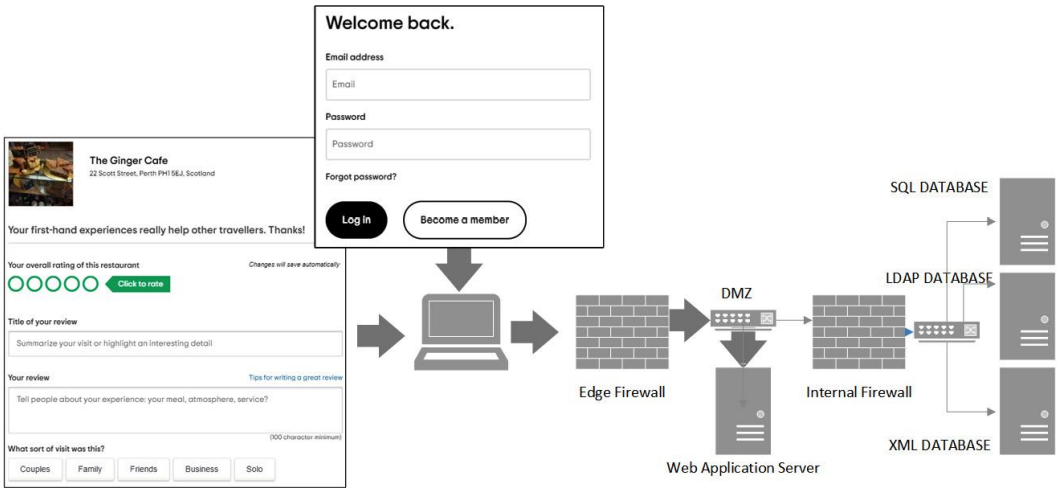


Figure 7.7 – Web application server located in DMZ

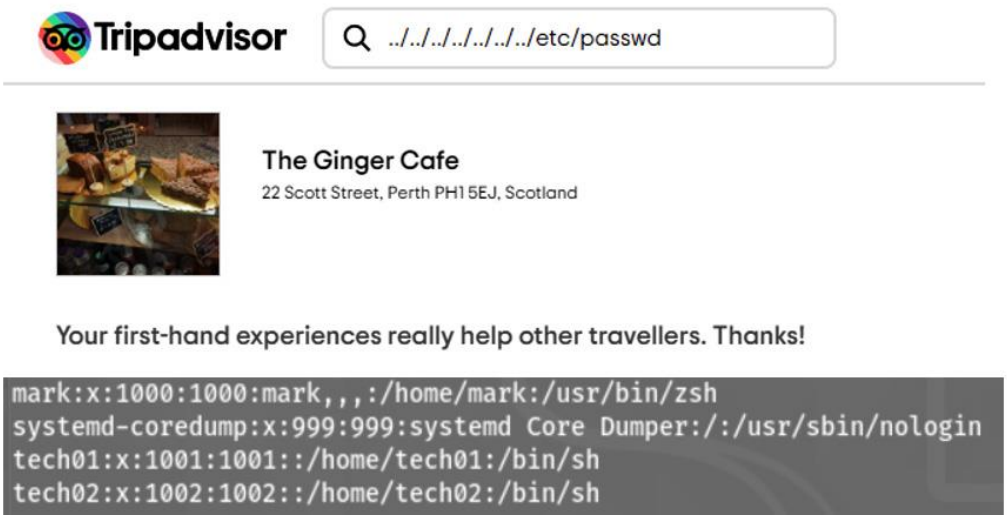


Figure 7.8 – Directory traversal

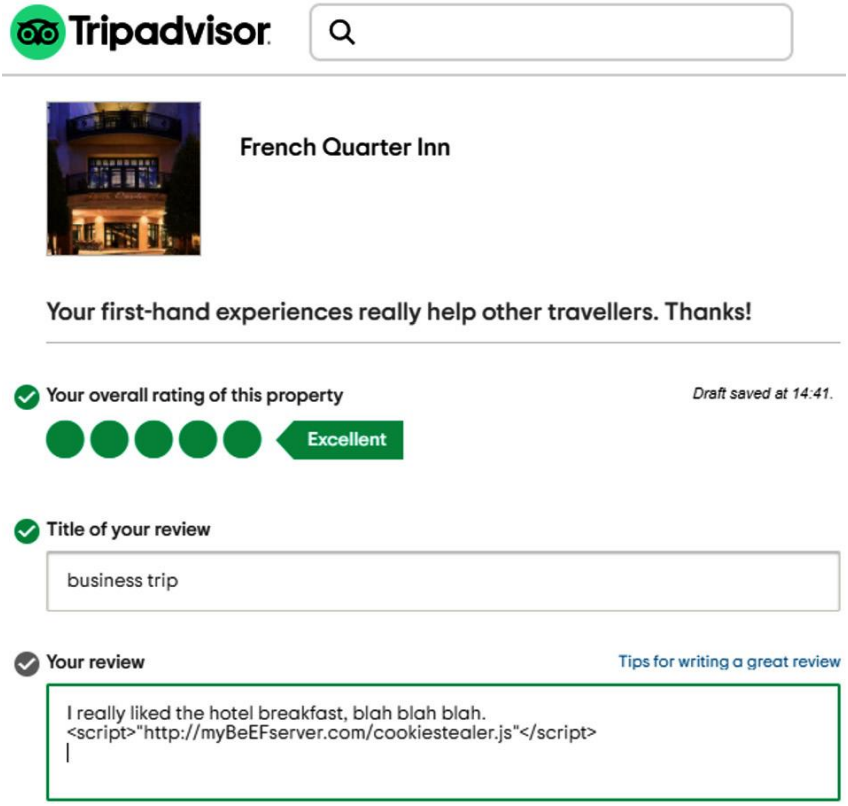


Figure 7.9 – XSS exploit

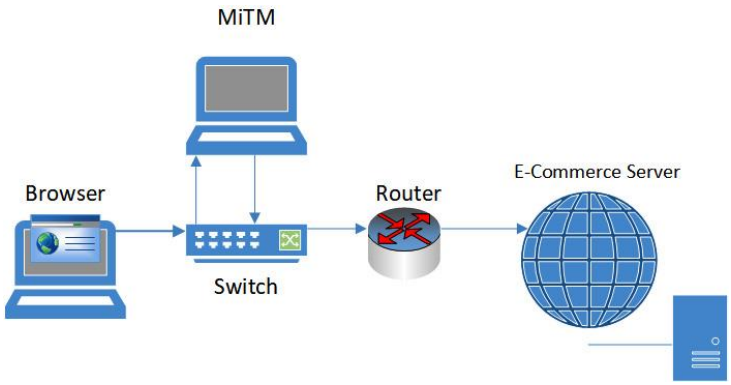


Figure 7.13 – MITM attack

Figure 7.14 – IoT camera

Figure 7.15 – Processing pipeline

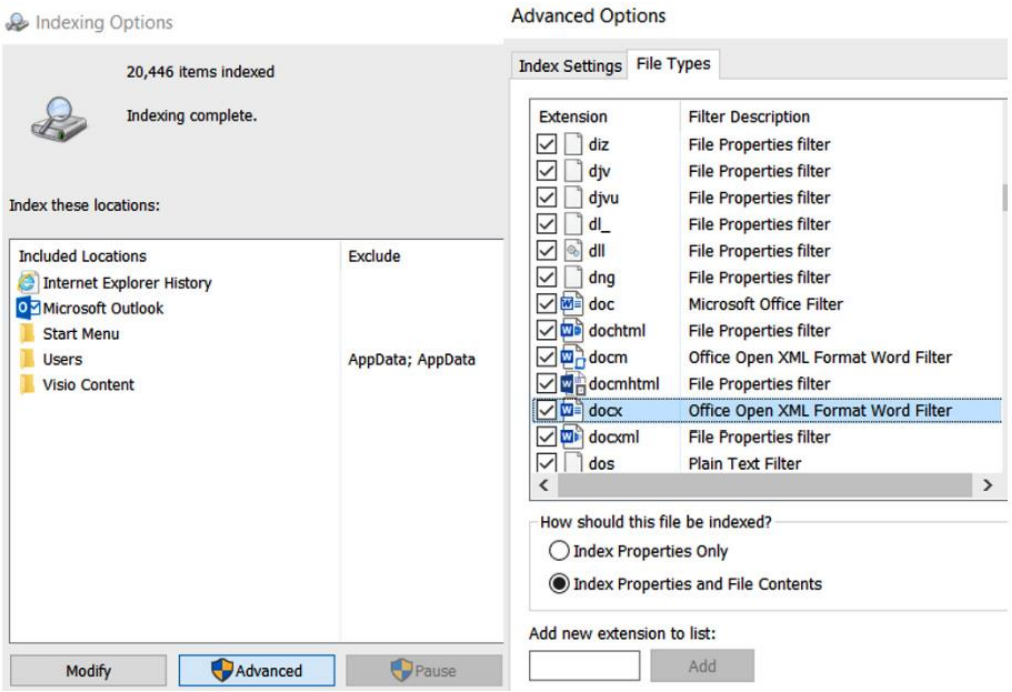


Figure 7.16 – Microsoft Indexing Service

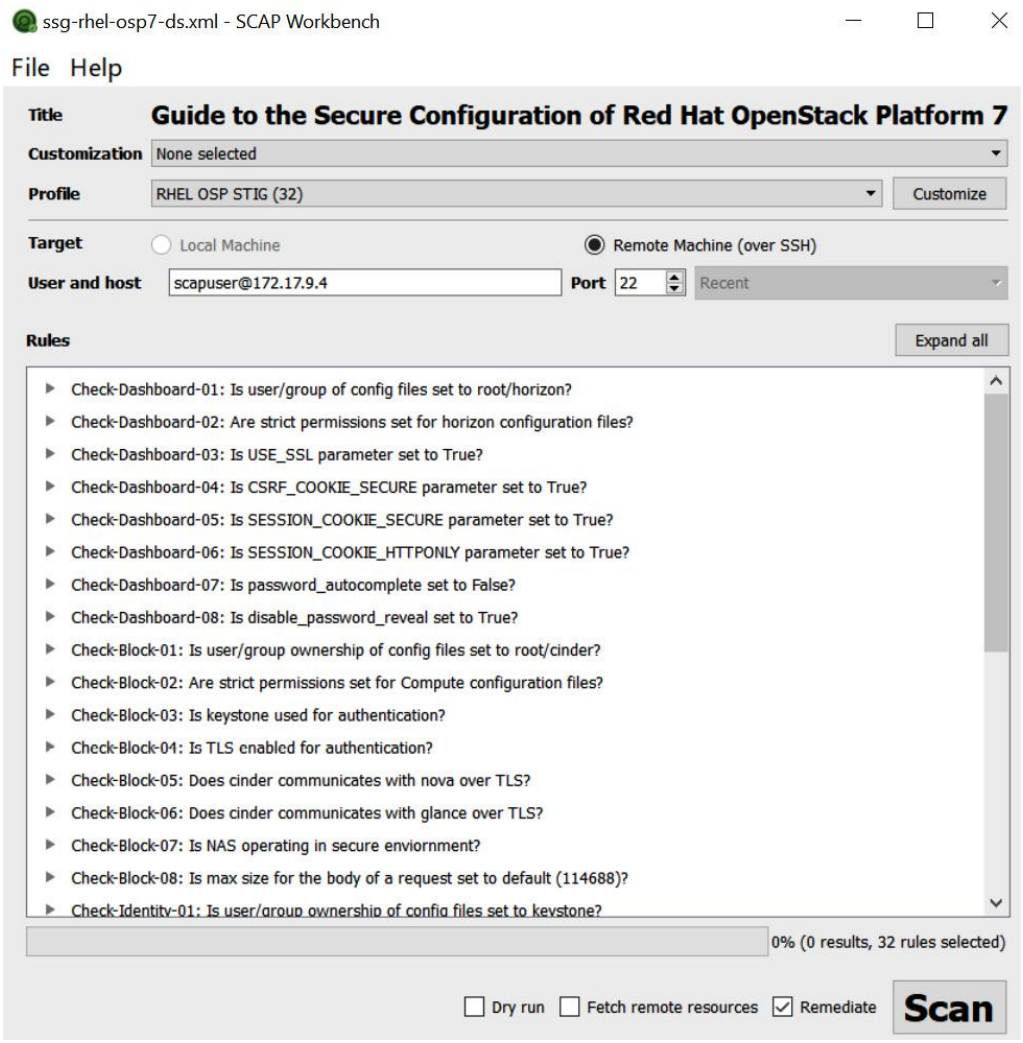


Figure 7.17 – Baseline compliance scan

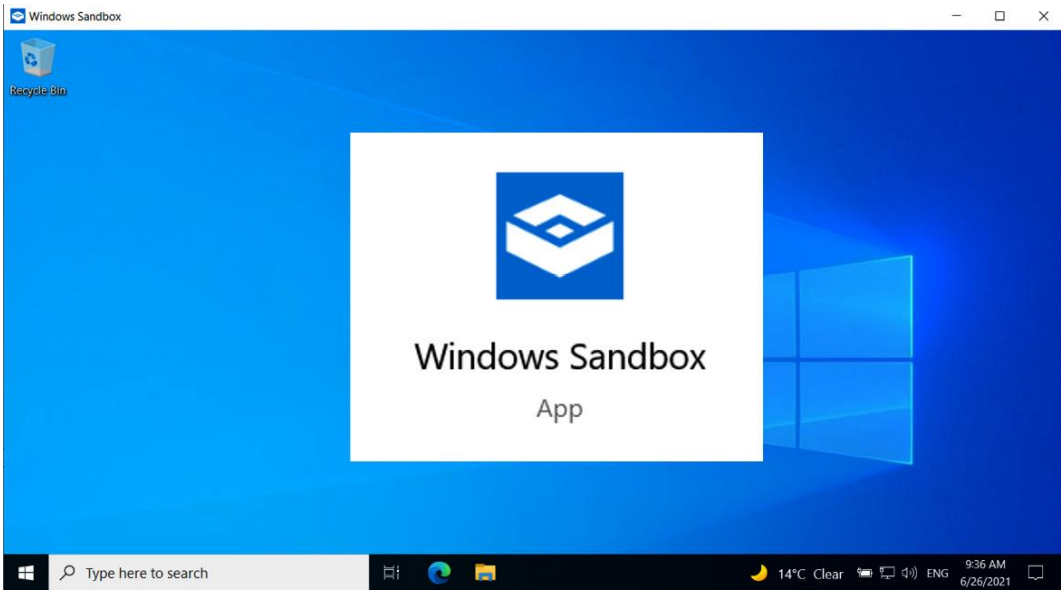


Figure 7.18 – Windows Sandbox

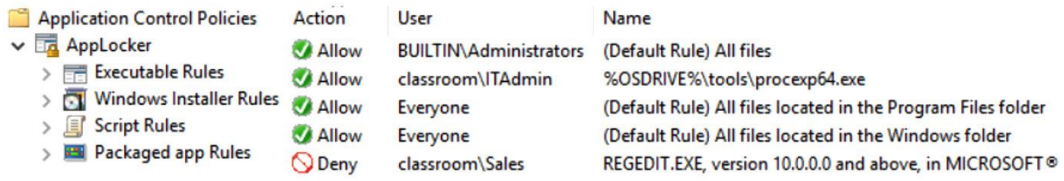


Figure 7.19 – Microsoft Application Control Policy

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

Figure 7.20 – Sample crontab configuration file

```
PS C:\Windows\system32> get-vm

Name        State   CPUUsage(%) MemoryAssigned(M) Uptime            Status             Version
----        -----   ----------- ----------------- ------            ------             -------
CentOS      Saved   0           0                 00:00:00          Operating normally 9.0
Client01    Running 0           3914              1.00:19:50.0350000 Operating normally 9.0
Kali        Off     0           0                 00:00:00          Operating normally 9.0
Kali 2020.4 Running 0           4096              1.00:19:50.7100000 Operating normally 9.0
OPENVAS 6.0 Running 0           4096              1.00:19:51.4140000 Operating normally 9.0
SVR01       Running 0           2346              1.00:19:50.3290000 Operating normally 9.0
```

Figure 7.21 – get-vm displaying a list of VMs

```
PS C:\Windows\system32> Start-VM CentOS
PS C:\Windows\system32> get-vm CentOS

Name   State   CPUUsage(%) MemoryAssigned(M) Uptime           Status             Version
----   -----   ----------- ----------------- ------           ------             -------
CentOS Running 0           4096              00:00:22.4810000 Operating normally 9.0
```

Figure 7.22 – PowerShell Start-VM

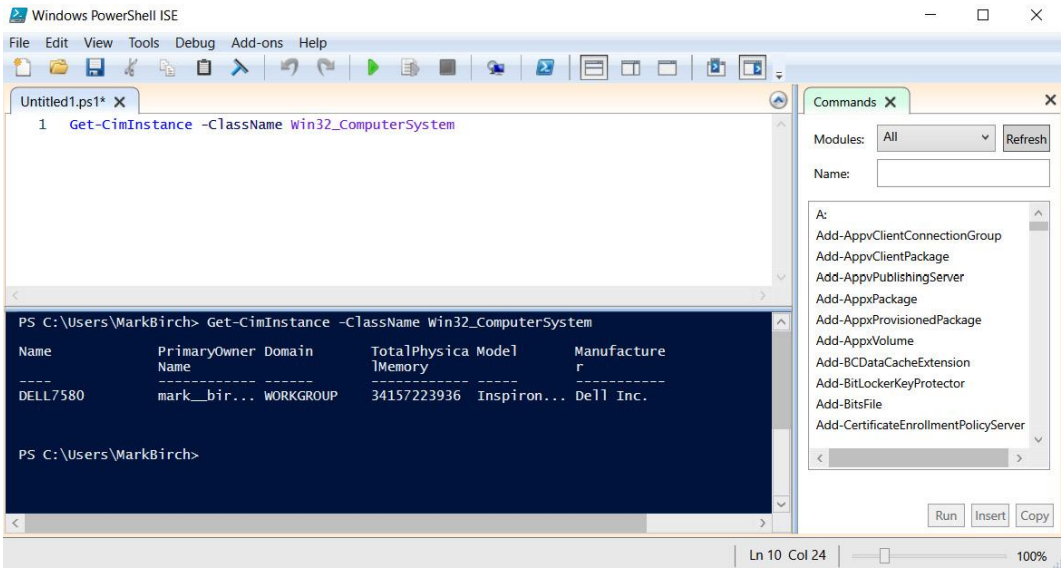


Figure 7.23 – Microsoft Windows ISE

Code

Code 7.1: An example of a JSON key pair would look like the following:

```
{"firstName": "John","lastName":"Jones"}
```

Code 7.2: Cross-site request forgery

In *Figure 7.10*, a victim will load the web page and the script will make a payment into another customer's account:

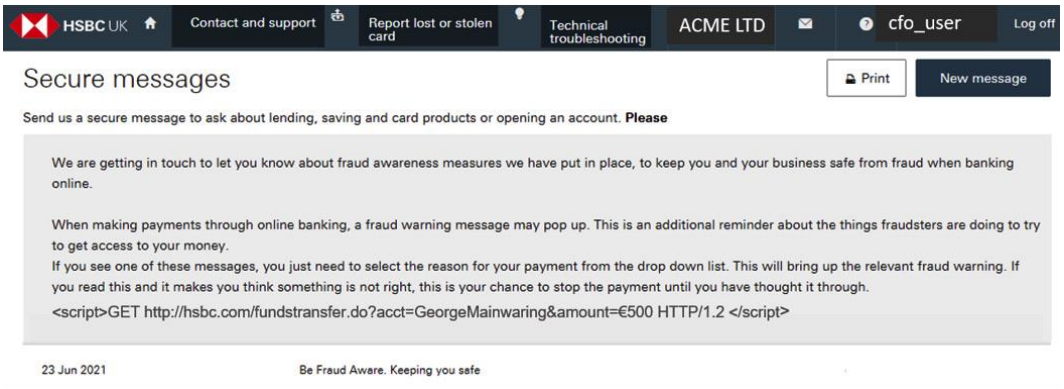


Figure 7.10 – CSRF example

The example script at the bottom of the bank customer's message is shown in the following snippet:

```
<script>GET
http://hsbc.com/fundstransfer.do?acct=GeorgeMainwaring&amount=€500
HTTP/1.2</script>
```

Code 7.3: LDAP

Some examples using command-line syntax for **Microsoft Active Directory** services are shown as follows. In the first example, we are searching for all users in the `itadmin` container:

Input:

```
dsquery user "ou=it admin,dc=classroom,dc=local"
```

Result:

```
"CN=Mark Birch,OU=IT Admin,DC=classroom,DC=local"
```

In the second example, we are creating a new user account in the `users` container:

Input:

```
dsadd user "cn=sqlsystem,cn=users,dc=classroom,dc=local" -pwd
Pa$$w0rd1
```

Result:

```
dsadd succeeded:cn=sqlsystem,cn=users,dc=classroom,dc=local
```

Code 7.4: Standard Query language

During a logon through a web application, we can use a valid user account and password, which will result in the following SQL string:

```
SELECT id FROM users WHERE username = 'jack' AND password = 'patch'
```

Then, using that command logic, we could submit the following command:

```
SELECT * FROM users WHERE username = 'user1' AND password =
'mypass1' OR 1=1
```

In this example the `AND` condition is evaluated before the `OR` operator, making the `WHERE` clause `true`. If the application does not perform the appropriate string checks, then the application will select the first record in the user's table as the command logic will make the statement true (`1=1` is always true). This would result in an authentication bypass exploit. *Figure 7.11* shows how this could be input into a login screen:

Figure 7.11 – SQL injection attempt

This type of exploit allows the attacker to access the first account in the table of users. *Figure 7.12* shows a successful login attempt:

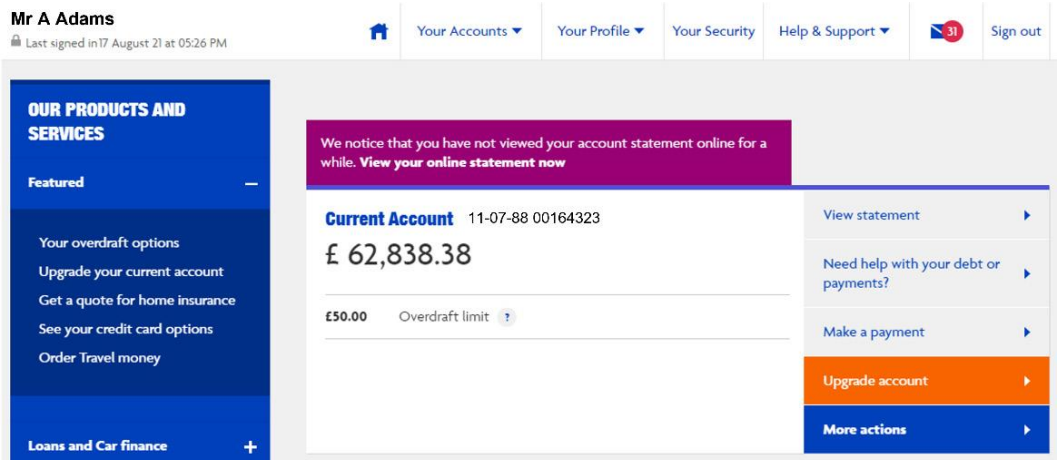


Figure 7.12 – SQL injection login

Now, the hacker can attempt to manipulate account details.

Code 7.5: Switch spoofing

The attacker will connect a device to a switch port that is set up to auto-negotiate as a trunk port. This is targeting the **Dynamic Trunking Protocol** (**DTP**) feature, and if the switch is not secured, then the attacker can forward all VLAN traffic to their device. It is important to disable this configuration as a default option. To remediate this vulnerability, we would set all ports as access-only ports, and for the ports that are used for trunking, we would use the following command:

```
switch(config-if)# switchport nonegotiate
```

Code 7.6

The following example would run a backup job at midnight every Sunday:

```
* 0 * * 0 /bin/sh backup.sh
```

Links

It is useful to refer to industry best practices when considering application vulnerabilities and the **Open Web Application Security Project** (**OWASP**) is a recommended resource:

https://owasp.org/www-project-top-ten/

For more details on Broken authentication, see https://tinyurl.com/OWASPA2

For more information on Insecure References, see https://tinyurl.com/OWASPA5.

For more details on Information disclosure, see https://tinyurl.com/OWASPA3

NIST published a whitepaper with guidance for implementing this framework (https://tinyurl.com/nistSSDF

For more details on Microsoft SDL framework, use the following link:

https://tinyurl.com/MicrosoftSDLFramework

See the following link for more information: https://tinyurl.com/MITRECWE-676

These document many examples of unsafe functions and ways to mitigate their use: https://cheatsheetseries.owasp.org/index.html

In April 2021, **Vodafone** was targeted, and attackers were able to hijack 30,000 IP prefixes, causing massive problems for Google, Microsoft, and **Cloudflare**. For more information on this attack, see the following link: https://tinyurl.com/BGPattack

Shodan (https://www.shodan.io/).

See the **Center for Internet Security** (**CIS**) *benchmarks* for hardening guides: https://workbench.cisecurity.org/benchmarks

There is an interesting **graphical user interface** (**GUI**) utility, allowing for the creation of `crontab` lines, at the following link: https://crontab-generator.org/

Microsoft provides comprehensive help and documentation for PowerShell and this can be found at the following link: https://docs.microsoft.com/en-us/powershell/

For additional information on python, including downloads and help, see the following link: https://www.python.org/

Questions

Here are a few questions to test your understanding of the chapter:

1. Attackers find a vulnerability on a website that allows them to select items from a shopping basket. When the authorize payment button is selected, there is a 500 ms delay. The

attackers run a script that takes 200 ms and allows the final payment to be altered. What is the vulnerability that has been targeted?

A. Buffer overflow

B. Integer overflow

C. Broken authentication

D. Race condition

2. Attackers find a vulnerability on a website that allows them to select items from a shopping basket. There is a running total value for the basket. When items are added beyond a total of $9,999, the total displays a value starting from $0.00. What is the vulnerability that has been targeted?

A. Buffer overflow

B. Integer overflow

C. Broken authentication

D. Weak ciphers

3. What allows attackers to sniff traffic on a network and capture cookies sent over HTTP?

A. Improper headers

B. Poor exception handling

C. Certificate errors

D. Race condition

4. What allows developers to maintain an inventory of all code libraries and licenses used in their applications?

A. Weak cryptography implementations

B. Weak ciphers

C. Weak cipher suite implementations

D. Software composition analysis

5. Developers are reviewing legacy applications written in the C programming language. This is due to a number of recent buffer overflow attacks against the application. They have replaced instances of `gets()` with `fgets()` and `strcpy()` with `strcpy_s()`. What has prompted this activity?

A. Use of unsafe functions

B. Third-party libraries

C. Dependencies

D. Regression

6. What is it called when developers no longer release security patches for their software applications?

   A. End-of-support/end-of-life

   B. Regression issues

   C. Dependencies

   D. Bankruptcy

7. What is an example of code that is not developed by a development team but is incorporated into many software builds?

   A. Use of unsafe functions

   B. Third-party libraries

   C. Dependencies

   D. Regression

8. What is it called when developers rely on a cloud provider API for full functionality of their software applications?

   A. Use of unsafe functions

   B. Third-party libraries

   C. Dependencies

   D. Regression

9. When a software component has previously worked well but now proves to be slow or unresponsive, what is it known as?

   A. Unsafe functions

   B. Unsafe third-party libraries

   C. Software dependencies

   D. Software regression bug

10. When considering input validation for your web application, where should the validation take place?

    A. Client-side

    B. Flash

C. Server-side

D. ActiveX

11. What is runtime or interpreted code that can provide media-rich web content within a web browser?

    A. REST

    B. Browser extensions

    C. ActiveX

    D. HTML5

12. What is runtime or interpreted code that can provide partial page updates (therefore saving bandwidth) when repositioning a map on screen?

    A. AJAX

    B. SOAP

    C. Flash

    D. ActiveX

13. Security professionals have found **IOCs** while reviewing **Security Incident and Event Management** (**SIEM**) logs. The following commands were found from the application server logs:

```
../../../../../etc/password
```

What type of activity did they see?

    A. Directory traversal

    B. XSS

    C. CSRF

    D. SQL injection

14. Security professionals have found IOCs while reviewing SIEM logs. The following commands were found in the application server logs:

```
GET
http://acmebank.com/transferfunds.do?acct=bobjones&amount=$400
HTTP/1.1
```

What type of activity did they see?

    A. Injection

    B. XML

C. LDAP

D. XSRF

15. While reviewing web application firewall logs, security professionals have found IOCs. The following commands were found in the logs:

```
SELECT * FROM users WHERE username = ''OR 1=1 –' AND password
= 'mypass1'
```

What type of activity did they see?

A. Injection

B. XML

C. LDAP

D. SQL

16. While executing malware in an isolated environment, malware has been found on previously unaffected systems. What is the likely cause?

A. Sandbox escape

B. VM hopping

C. VM escape

D. Sandbox detonation

17. Internet traffic has been rerouted causing outages for many large internet providers. Attackers have used default accounts to configure ISP routers. What technology or vector of attack has been used?

A. BGP

B. VLAN hopping

C. LDAP

D. DDoS

18. What type of attack will most likely be effective when untrained users are targeted?

A. Social engineering

B. VLAN hopping

C. Hunts

D. DDoS

19. Security researchers need to understand APT bad actors by observing their tools, tactics, and procedures. What would be the best tool for this?

    A. Honeynet

    B. Honeypot

    C. Decoy files

    D. Antivirus

20. Security researchers place a `password.txt` file in an unsecured location on a publicly accessible server. They are going to map all the IP addresses that attempt to access the file. What is the best description for the `password.txt` file?

    A. Honeynet

    B. Honeypot

    C. Decoy files

    D. Logic bomb

21. Microsoft security researchers need to understand APT bad actors by observing their tools, tactics, and procedures. They gather massive amounts of raw security data every day from customer endpoints. What would be the best approach to identify IOCs?

    A. Processing pipelines

    B. Indexing and search

    C. Log collection and curation

    D. Database activity monitoring

22. What allows an organization to deploy server operating systems that must be replaced when there is an updated version?

    A. Immutable systems

    B. Hardening

    C. Sandbox detonation

    D. License technologies

23. What is it when my organization only allows a core set of applications to be supported on end user devices?

    A. Application whitelisting

    B. Application hardening

C. Application blacklisting

D. Atomic execution

24. What is it when my application will process a transaction in an isolated space, allowing rollback if the write cannot be performed?

A. Application whitelisting

B. Application hardening

C. TOCTOU

D. Atomic execution

25. Linux systems need to run a scheduled backup at midnight every day. What would allow administrators to automate the process?

A. Cron

B. Bash

C. PowerShell

D. Python

26. Linux system administrators need to execute common shell commands. What should they use?

A. Cron

B. Bash

C. PowerShell

D. Python

27. Microsoft administrators need to run powerful command-line utilities and create scripts to automate everyday system tasks. Scripts will also be created using `.PS1` extensions. What will they use?

A. Cron

B. Bash

C. PowerShell

D. Python

28. Acme Corporation needs to support a common programming language that will function across different vendor operating systems. What should they choose?

A. Cron

B. Bash

C. PowerShell

D. Python

Answers

1. D
2. B
3. A
4. D
5. A
6. A
7. B
8. C
9. D
10. C
11. D
12. A
13. A
14. C
15. D
16. A
17. A
18. A
19. A
20. C
21. A
22. A
23. A

24. D

25. A

26. B

27. C

28. D

Chapter 8

Figures

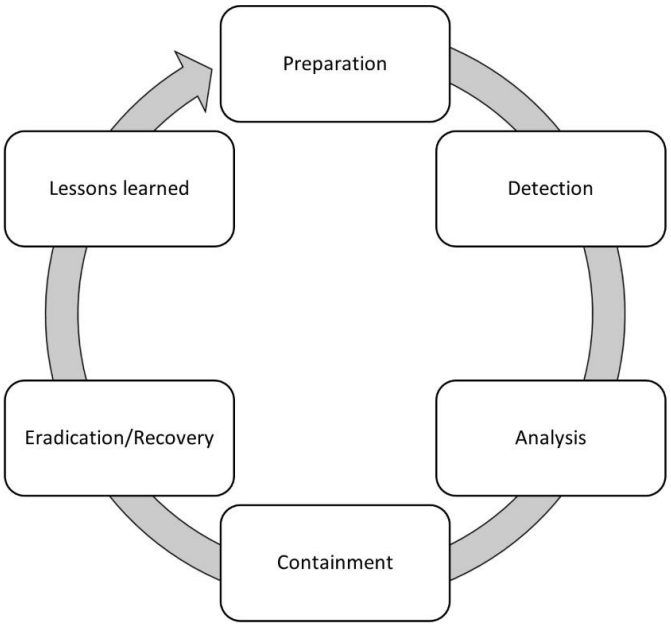


Figure 8.1 – Incident response process

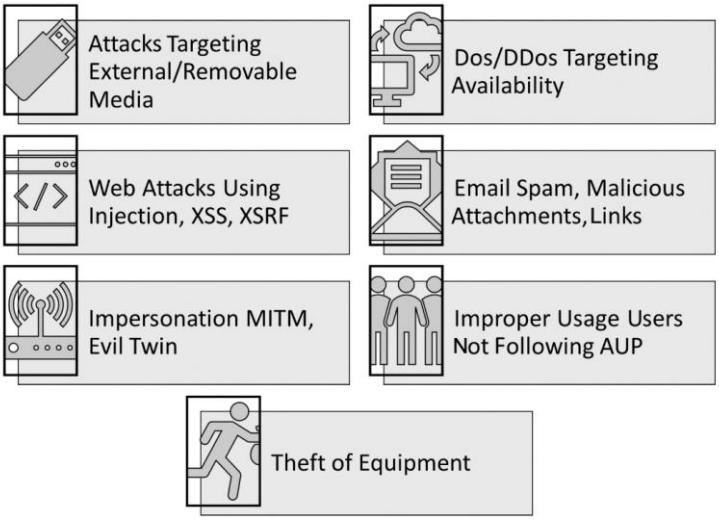


Figure 8.2 – Common attack vectors

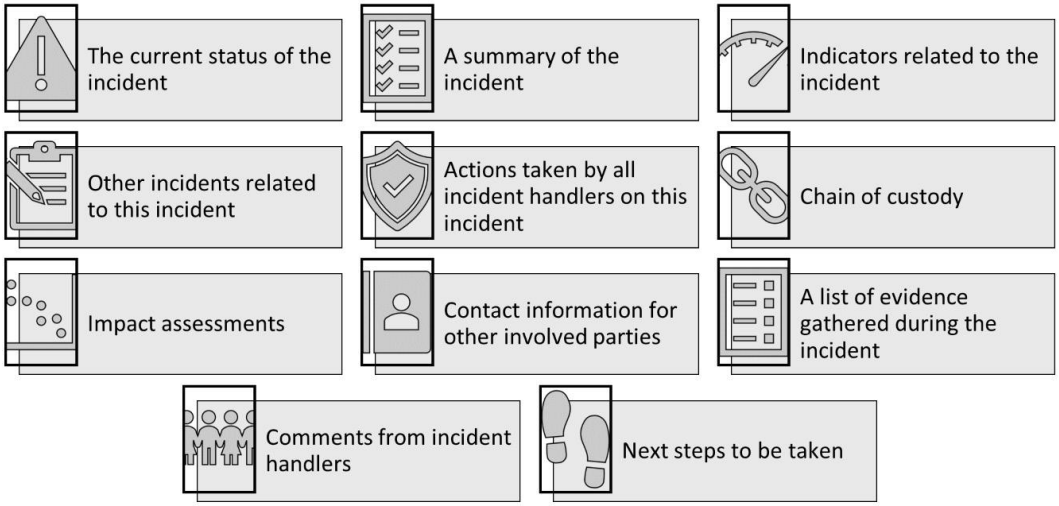


Figure 8.3 – Incident documentation

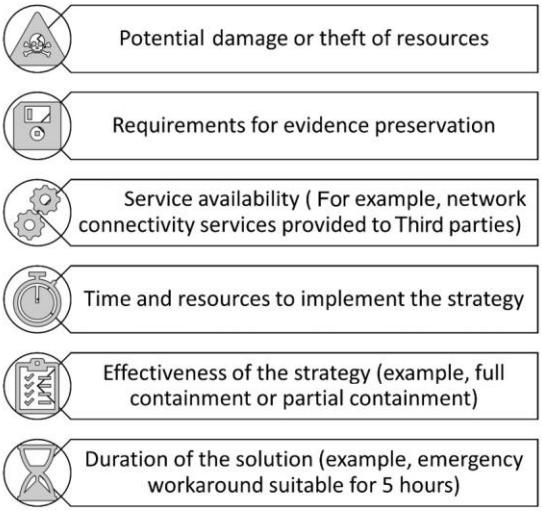


Figure 8.4 – Containment strategy

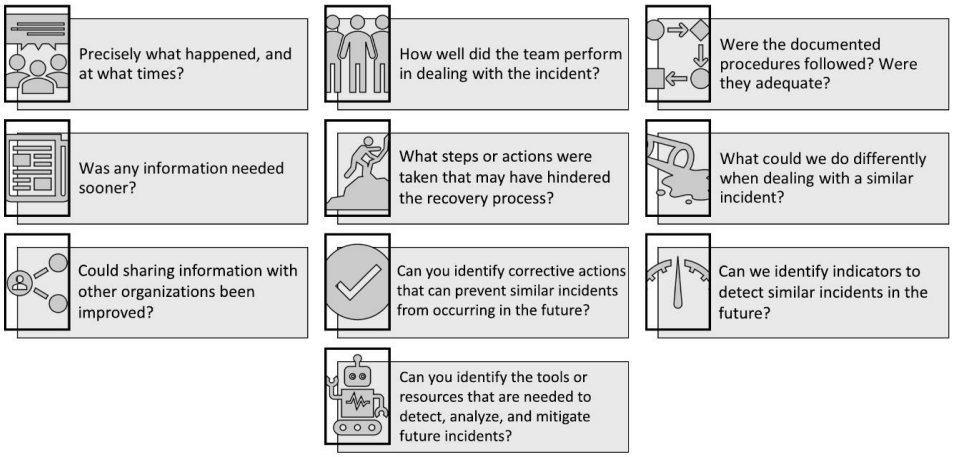


Figure 8.5 – Lessons learned

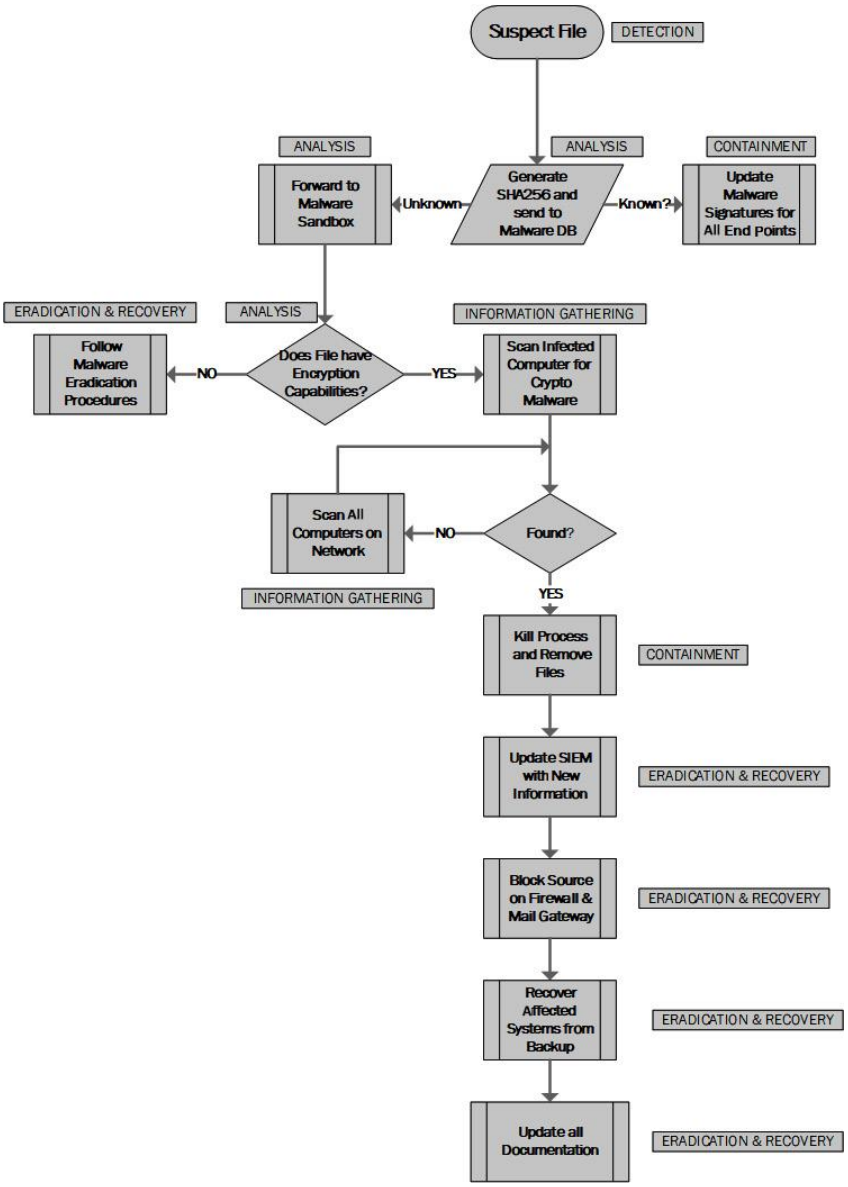


Figure 8.6 – Playbook for a malware incident

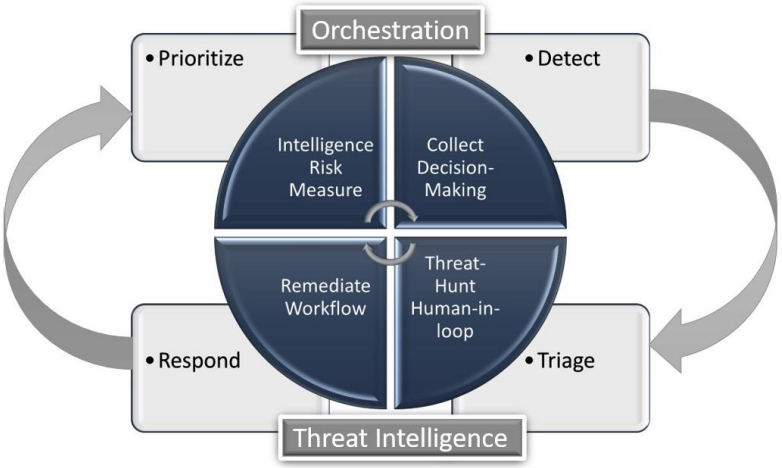


Figure 8.7 – SOAR workflow

Figure 8.8 – Communication plan

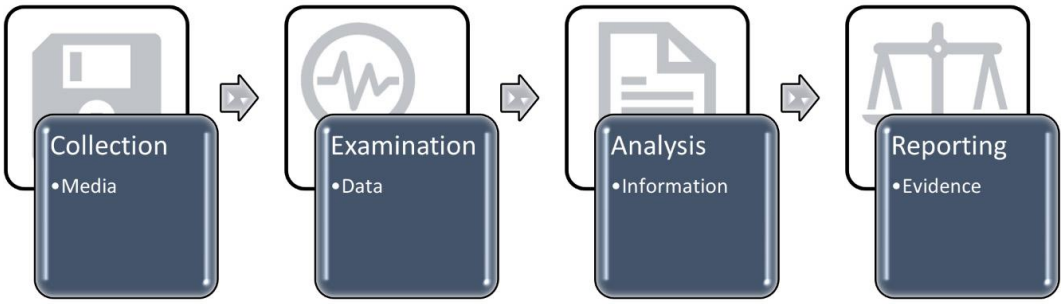


Figure 8.9 – Forensic process

EVIDENCE CHAIN OF CUSTODY FORM Acme Corp			
Case Name:		Reason Evidence Obtained:	
Case Number:			
Item No.	Evidence Type	Model No.	Serial No.
Content Owner		Description	
Forensic Investigator	Creation	Hash Value	Date/Time

CHAIN OF CUSTODY			
Date/Time	Released By:	Received By	Reason for Change

Figure 8.10 – Chain of custody form

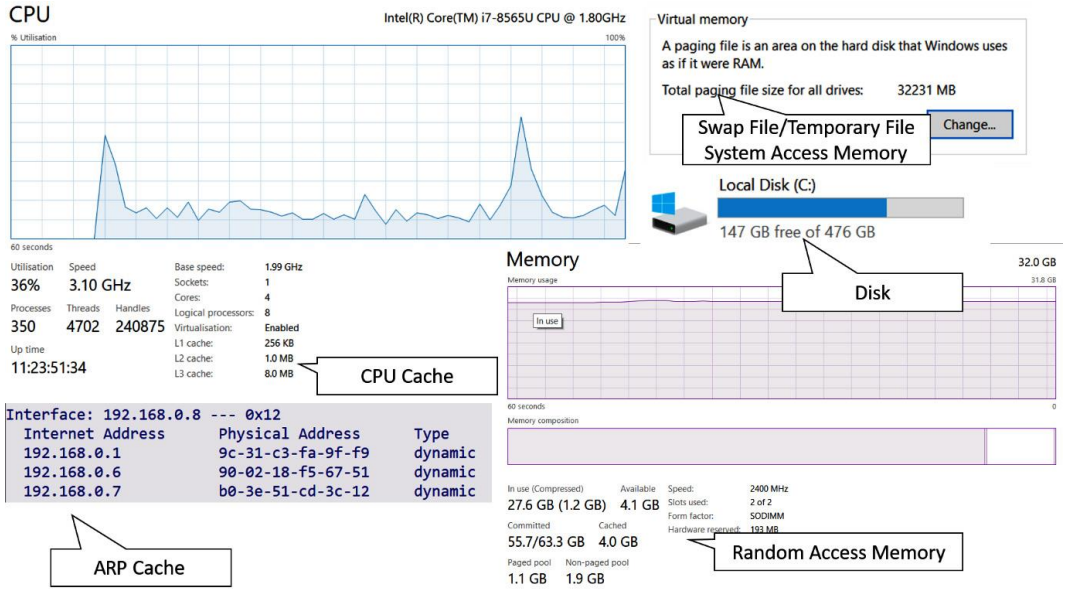


Figure 8.11 – Evidence locations

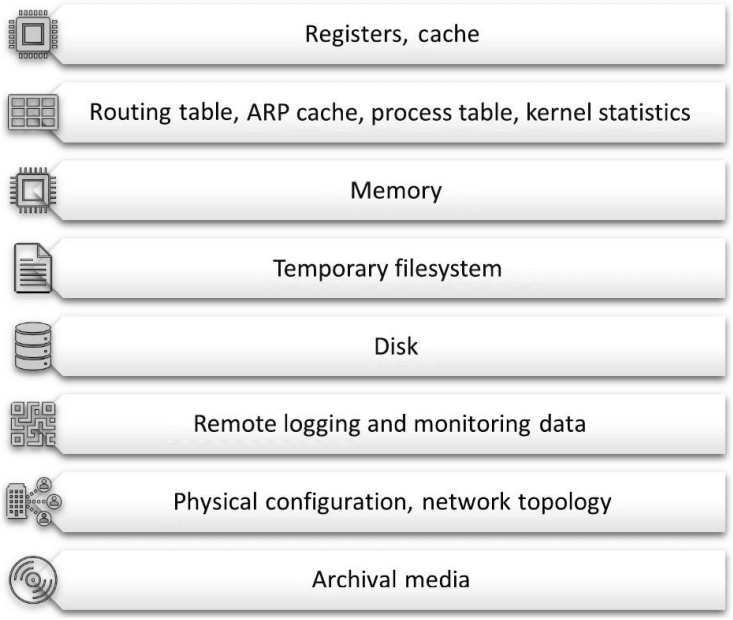


Figure 8.12 – Order of volatility

```
└─# foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
```

Figure 8.13 – The foremost command

```
└─# strings -h
Usage: strings [option(s)] [file(s)]
 Display printable strings in [file(s)] (stdin by default)
 The options are:
  -a - --all                Scan the entire file, not just the data section [default]
  -d --data                 Only scan the data sections in the file
  -f --print-file-name      Print the name of the file before each string
  -n --bytes=[number]       Locate & print any NUL-terminated sequence of at
  -<number>                   least [number] characters (default 4).
  -t --radix={o,d,x}        Print the location of the string in base 8, 10 or 16
  -w --include-all-whitespace Include all whitespace as valid string characters
  -o                        An alias for --radix=o
  -T --target=<BFDNAME>     Specify the binary file format
  -e --encoding={s,S,b,l,B,L} Select character size and endianness:
                            s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit
  -s --output-separator=<string> String used to separate strings in output.
  @<file>                   Read options from <file>
  -h --help                 Display this information
  -v -V --version           Print the program's version number
strings: supported targets: elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 pei-i386 pei-x86-64 elf64-l1om
 elf64-k1om elf64-little elf64-big elf32-little elf32-big pe-x86-64 pe-bigobj-x86-64 pe-i386 srec symbolsre
c verilog tekhex binary ihex plugin
Report bugs to <http://www.sourceware.org/bugzilla/>
```

Figure 8.14 – The strings command

```
└─$ binwalk x86_64-linux-gnu-c++filt

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             ELF, 64-bit LSB shared object, AMD x86-64, version 1 (SYSV)
106640        0x1A090         Copyright string: "Copyright (C) 2020 Free Software Foundation, Inc."
127280        0x1F130         Unix path: /usr/lib/debug/.dwz/x86_64-linux-gnu/binutils-x86-64-linux-gnu.debug
```

Figure 8.15 – Binwalk

```
└─$ strace hostname
execve("/usr/bin/hostname", ["hostname"], 0x7fffd46d3210 /* 23 vars */) = 0
brk(NULL)                               = 0x7fffba4f8000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=42342, ...}) = 0
mmap(NULL, 42342, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f51f94ad000
close(3)                                = 0
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0@n\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1839792, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f51f9470000
mmap(NULL, 1852680, PROT_READ, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f51f92a0000
mprotect(0x7f51f92c5000, 1662976, PROT_NONE) = 0
mmap(0x7f51f92c5000, 1355776, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x25000) = 0x7f51f92c5000
mmap(0x7f51f9410000, 303104, PROT_READ, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x170000) = 0x7f51f9410000
mmap(0x7f51f945b000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1ba000) = 0x7f51f945b000
mmap(0x7f51f9461000, 13576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f51f9461000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0x7f51f9471580) = 0
mprotect(0x7f51f945b000, 12288, PROT_READ) = 0
mprotect(0x7f51f94bd000, 4096, PROT_READ) = 0
mprotect(0x7f51f94aa000, 4096, PROT_READ) = 0
munmap(0x7f51f94ad000, 42342)           = 0
brk(NULL)                               = 0x7fffba4f8000
brk(0x7fffba519000)                     = 0x7fffba519000
uname({sysname="Linux", nodename="dell7580", ...}) = 0
fstat(1, {st_mode=S_IFCHR|0660, st_rdev=makedev(0x4, 0x1), ...}) = 0
ioctl(1, TCGETS, {B38400 opost isig icanon echo ...}) = 0
write(1, "dell7580\n", 9dell7580
)               = 9
exit_group(0)                           = ?
+++ exited with 0 +++
```

Figure 8.16 – The strace command

```
ldd ssh
    linux-vdso.so.1 (0x00007fffe6585000)
    libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f2ebc4b0000)
    libcrypto.so.1.1 => /lib/x86_64-linux-gnu/libcrypto.so.1.1 (0x00007f2ebc1b0000)
    libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f2ebc1a0000)
    libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f2ebc180000)
    libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007f2ebc160000)
    libgssapi_krb5.so.2 => /lib/x86_64-linux-gnu/libgssapi_krb5.so.2 (0x00007f2ebc110000)
    libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f2ebbf30000)
    libpcre2-8.so.0 => /lib/x86_64-linux-gnu/libpcre2-8.so.0 (0x00007f2ebbea0000)
    /lib64/ld-linux-x86-64.so.2 (0x00007f2ebc5bb000)
    libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f2ebbe7e000)
    libkrb5.so.3 => /lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007f2ebbd90000)
    libk5crypto.so.3 => /lib/x86_64-linux-gnu/libk5crypto.so.3 (0x00007f2ebbd60000)
    libcom_err.so.2 => /lib/x86_64-linux-gnu/libcom_err.so.2 (0x00007f2ebbe70000)
    libkrb5support.so.0 => /lib/x86_64-linux-gnu/libkrb5support.so.0 (0x00007f2ebbd40000)
    libkeyutils.so.1 => /lib/x86_64-linux-gnu/libkeyutils.so.1 (0x00007f2ebbd30000)
```

Figure 8.17 – The ldd command

```
└─# file mydoc.pdf
mydoc.pdf: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, in
terpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=5917ff8fa041d4cb54c7846799e32a9e4191
75e2, for GNU/Linux 3.2.0, stripped
```

Figure 8.18 – The file command

```
ExifTool Version Number         : 12.16
File Name                       : nasa.jpg
Directory                       : .
File Size                       : 78 KiB
File Modification Date/Time     : 2021:07:07 17:04:33+01:00
File Access Date/Time           : 2021:07:07 17:04:33+01:00
File Inode Change Date/Time     : 2021:07:07 17:04:33+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Image Description               : Photo Date: 2020-01-10Location: Teague AuditoriumSubject: Graduation ceremony of the 2017
 class of Astronaut Candidates.Photographer: James Blair
Software                        : Picasa
Artist                          : JAMES BLAIR
Copyright                       : NASA
XMP Toolkit                     : XMP Core 5.5.0
Description                     : Photo Date: 2020-01-10Location: Teague AuditoriumSubject: Graduation ceremony of the 2017
 class of Astronaut Candidates.Photographer: James Blair
Rights                          : NASA
Creator                         : JAMES BLAIR, James Blair - NASA - JSC
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
```

Figure 8.19 – ExifTool metadata

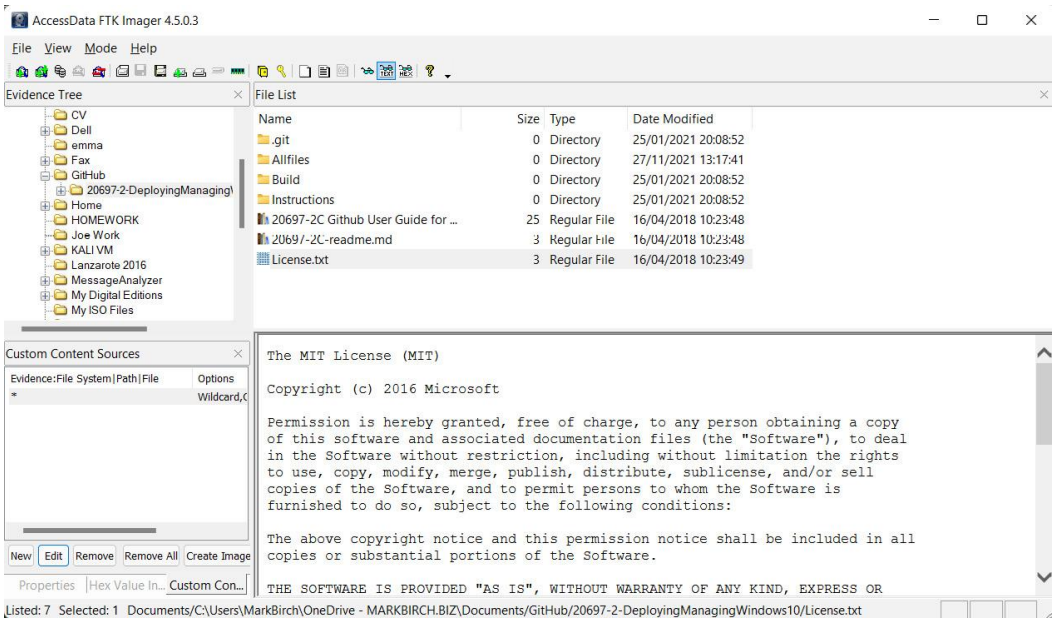


Figure 8.20 – FTK Imager

```
[SupportAssistAgent.exe]
 TCP    192.168.8.113:1040     51.140.84.251:https    CLOSE_WAIT
[SupportAssistAgent.exe]
 TCP    192.168.8.113:1044     40.78.128.150:https    ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1045     a-0001:https           ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1046     204.79.197.222:https   ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1047     13.107.18.254:https    ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1048     131.253.33.254:https   ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1049     13.107.138.9:https     ESTABLISHED
[WINWORD.EXE]
 TCP    192.168.8.113:1050     52.97.212.66:https     ESTABLISHED
[SearchApp.exe]
 TCP    192.168.8.113:1055     52.97.208.2:https      ESTABLISHED
[WINWORD.EXE]
 TCP    192.168.8.113:1070     52.97.133.162:https    ESTABLISHED
[OUTLOOK.EXE]
 TCP    192.168.8.113:1072     52.109.8.21:https      ESTABLISHED
[OfficeClickToRun.exe]
 TCP    192.168.8.113:1073     40.97.164.146:https    CLOSE_WAIT
[dirmngr.exe]
 TCP    192.168.8.113:1074     52.98.145.98:https     ESTABLISHED
[OUTLOOK.EXE]
 TCP    192.168.8.113:1075     40.97.164.146:https    CLOSE_WAIT
[dirmngr.exe]
 TCP    192.168.8.113:1076     87.237.18.210:http     TIME_WAIT
 TCP    192.168.8.113:1077     87.237.18.210:http     TIME_WAIT
 TCP    192.168.8.113:1078     52.97.133.226:https    ESTABLISHED
```

Figure 8.21 – netstat output

```
-$ ps -A
  PID TTY          TIME CMD
    1 ?        00:02:10 systemd
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00 rcu_gp
    4 ?        00:00:00 rcu_par_gp
    6 ?        00:00:00 kworker/0:0H-kblockd
    9 ?        00:00:00 mm_percpu_wq
   10 ?        00:00:55 ksoftirqd/0
   11 ?        00:00:45 rcu_sched
   12 ?        00:00:11 migration/0
   13 ?        00:00:00 cpuhp/0
   15 ?        00:00:00 kdevtmpfs
   16 ?        00:00:00 netns
   17 ?        00:00:00 rcu_tasks_rude_
   18 ?        00:00:00 kauditd
   19 ?        00:00:01 khungtaskd
   20 ?        00:00:00 oom_reaper
   21 ?        00:00:00 writeback
   22 ?        00:01:12 kcompactd0
   23 ?        00:00:00 ksmd
   24 ?        00:00:11 khugepaged
```

Figure 8.22 – The ps command

```
└─$ vmstat 5
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0  32924 158228 567508 1705680    0    0     1    12    0    4  1  1 99  0  0
 0  0  32924 157976 567508 1705680    0    0     0     3    0  157  2  3 95  0  0
 0  0  32924 157976 567508 1705680    0    0     0     0    0  273  3  6 91  0  0
 0  0  32924 158228 567508 1705680    0    0     0     0    0  105  2  2 96  0  0
 0  0  32924 158228 567508 1705680    0    0     0     0    0  123  1  3 96  0  0
 0  0  32924 158228 567508 1705680    0    0     0     0    0  117  1  3 96  0  0
 0  0  32924 157220 567508 1705680    0    0     0    17    0  163  2  2 96  0  0
 0  0  32924 157220 567512 1705680    0    0     0    14    0  138  1  4 95  0  0
 0  0  32924 157220 567512 1705680    0    0     0     0    0  109  1  4 95  0  0
 0  0  32924 156716 567512 1705680    0    0     0     0    0   96  1  2 97  0  0
 0  0  32924 156716 567512 1705680    0    0     0     7    0  129  2  3 95  0  0
 0  0  32924 156716 567512 1705680    0    0     0     0    0  105  1  3 96  0  0
 0  0  32924 156716 567512 1705680    0    0     0     0    0   78  1  1 98  0  0
 0  0  32924 156716 567516 1705680    0    0     0    14    0  154  2  3 95  0  0
 0  0  32924 156716 567516 1705680    0    0     0     0    0  107  1  4 95  0  0
 0  0  32924 156716 567516 1705680    0    0     0     0    0   84  1  2 97  0  0
```

Figure 8.23 – The vmstat command

```
COMMAND     PID USER   FD      TYPE     DEVICE  SIZE/OFF      NODE NAME
systemd    1011 mark  cwd       DIR        8,2      4096         2 /
systemd    1011 mark  rtd       DIR        8,2      4096         2 /
systemd    1011 mark  txt       REG        8,2   1669568   2101277 /usr/lib/systemd/systemd
systemd    1011 mark  mem       REG        8,2   1321344   2097650 /usr/lib/x86_64-linux-gnu/libm-2.31.so
systemd    1011 mark  mem       REG        8,2    153808   2100470 /usr/lib/x86_64-linux-gnu/libudev.so.1.6.18
systemd    1011 mark  mem       REG        8,2   1574952   2100478 /usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0
systemd    1011 mark  mem       REG        8,2    149576   2097437 /usr/lib/x86_64-linux-gnu/libgpg-error.so.0.29.0
systemd    1011 mark  mem       REG        8,2     71896   2101097 /usr/lib/x86_64-linux-gnu/libjson-c.so.5.1.0
systemd    1011 mark  mem       REG        8,2     34904   2101096 /usr/lib/x86_64-linux-gnu/libargon2.so.1
systemd    1011 mark  mem       REG        8,2    438568   2099513 /usr/lib/x86_64-linux-gnu/libdevmapper.so.1.02.1
systemd    1011 mark  mem       REG        8,2     30776   2100498 /usr/lib/x86_64-linux-gnu/libuuid.so.1.3.0
systemd    1011 mark  mem       REG        8,2   3044192   2097655 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
systemd    1011 mark  mem       REG        8,2     26976   2097229 /usr/lib/x86_64-linux-gnu/libcap-ng.so.0.0.0
systemd    1011 mark  mem       REG        8,2    584360   2099174 /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0.9.0
systemd    1011 mark  mem       REG        8,2    149608   2099628 /usr/lib/x86_64-linux-gnu/libpthread-2.31.so
systemd    1011 mark  mem       REG        8,2     18688   2097649 /usr/lib/x86_64-linux-gnu/libdl-2.31.so
systemd    1011 mark  mem       REG        8,2    162496   2097199 /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
systemd    1011 mark  mem       REG        8,2    845744   2100462 /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.5
systemd    1011 mark  mem       REG        8,2    133464   2097977 /usr/lib/x86_64-linux-gnu/liblz4.so.1.9.2
systemd    1011 mark  mem       REG        8,2     35280   2101102 /usr/lib/x86_64-linux-gnu/libip4tc.so.2.0.0
systemd    1011 mark  mem       REG        8,2    128944   2098073 /usr/lib/x86_64-linux-gnu/libidn2.so.0.3.7
systemd    1011 mark  mem       REG        8,2   1168056   2097453 /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.6
```

Figure 8.24 – The isof command

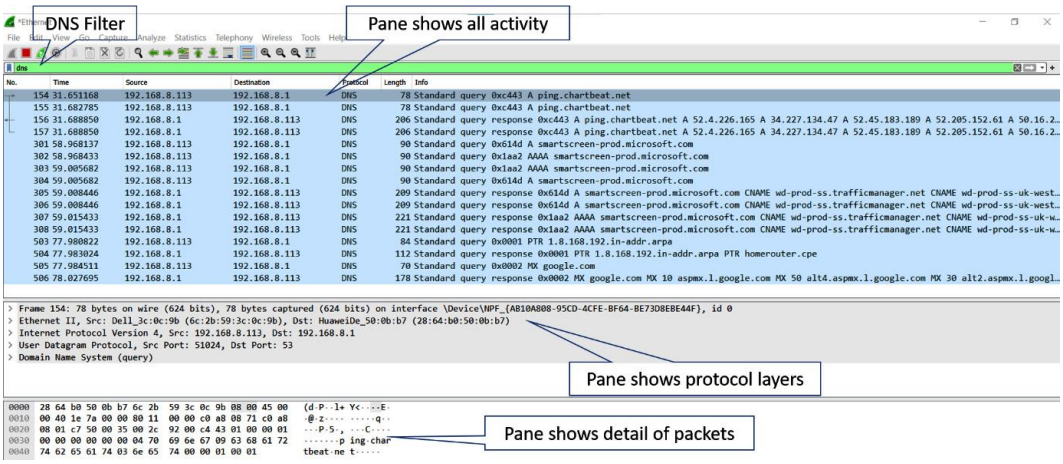


Figure 8.27 – Wireshark

Code

Code 8.1: Here is an example of using the `foremost` command:

```
foremost -t pdf,png -v -i /dev/sda
```

Code 8.2: In this example, we are searching within a binary file, where we need to see if there are any embedded `copyright` strings:

```
strings python3 | grep copyright
```

We are using the `strings` command to search for all the strings within `python3` and piping the output to the `grep` command, to only display strings containing `copyright` characters.

Code 8.3: In the following example, we are reading all the fields contained within the `ssh` executable program file:

```
readelf -a ssh
```

Code 8.4: The following command is used to extract metadata from an image that's been downloaded from a website:

```
exiftool nasa.jpg
```

Code 8.5: In the following example, a `sha256` is being calculated for the Linux `grep` command:

```
sha256sum grep

605aaf67445e899a9a59c66446fa0bb15fb11f2901ea33386b3325596b3c8 423
grep
```

Code 8.6: Netcat

To set up a listening port on the system under investigation, we can type the following command:

```
nc -l -p 12345
```

To connect from the forensics workstation, we can use the following command:

```
nc 10.10.0.3 12345
```

(see code 8.6 for reference). This will allow us to run commands on the system under investigation to reflect all the outputs on the forensics workstation.

To transfer a file for investigation, we can use the following commands. On the system under investigation, we will wait for 180 seconds on `port 12345` to transfer `vreport.htm`:

```
nc -w 180 -p 12345 -l < vreport.htm
```

To transfer the report file to the forensics workstation, we can use the following command:

```
nc 10.10.0.51 12345 > vreport.htm
```

We now have a copy of the report on the forensics workstation (the report is a vulnerability scan that was performed with a different tool).

tcpdump can be used to capture real-time network traffic and also to open captured traffic using common capture formats, such as **pcap**. `tcpdump` is included by default on most Linux distributions. It is the Linux version of Wireshark.

To capture all the traffic on the `eth0` network interface, we can use the following command:

```
tcpdump -I eth0
```

The following screenshot shows the traffic that was captured on `eth0`:

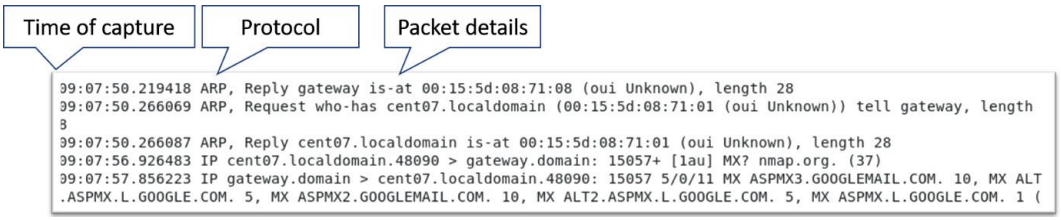


Figure 8.25 – The tcpdump capture

The preceding screenshot shows the command line's `tcpdump` output, which can also be saved for later analysis.

Conntrack is used by security professionals to view the details of the **IPTABLES** (firewall) state tables. It is a very powerful command-line tool, but in this instance, it will be of interest to see extra details about the firewall's state table. It allows for detailed tracking of firewall connections. To see a list of all the current connections and their state, we can use the following command:

```
conntrack -L
```

The output can be seen in the following screenshot:

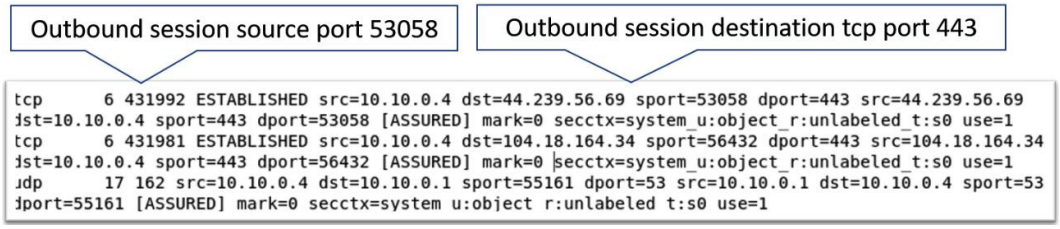


Figure 8.26 – Conntrack output

The preceding screenshot shows the detailed output from the firewall state table, including all current connections. The fine detail for this tool is beyond the scope for CompTIA CAS students, though more details can be found at https://conntrack-tools.netfilter.org/manual.html.

Links

There is comprehensive guidance available within the **NIST SP800-61** documentation on this, which is available at https://tinyurl.com/NIST80061R2

For organizations in the United Kingdom, there are very useful resources available from the **National Cyber Security Centre** (**NCSC**); see the following URL: https://tinyurl.com/ncscirt.

More information can be found at http://capec.mitre.org/data/index.html

More information on Nist SP 800-86 be found here: https://tinyurl.com/nistsp80086.

For further examples and comprehensive documentation, go to https://www.wireshark.org/docs/.

Questions

Answer the following questions to test your knowledge of this chapter:

1. During a security incident, a team member was able to refer to known documentation and databases of attack vectors to aid the response. What is this an example of?

    A. Event classification

    B. A false positive

    C. A false negative

    D. A true positive

2. During a security incident, a team member responded to a SIEM alert and successfully stopped an attempted data exfiltration. What can be said about the SIEM alert?

    A. It's a false positive.

    B. It's a false negative.

    C. It's a true positive.

    D. It's a true negative.

3. During a security incident, a senior team leader coordinated with members already dealing with a breach. They were told to concentrate their efforts on a new threat. What process led to the team leader's actions?

    A. Preparation

    B. Analysis

    C. Triage event

    D. Pre-escalation tasks

4. A CSIRT team needs to be identified, including leadership with a clear reporting and escalation process. At what stage of the incident response process should this be done?

    A. Preparation

    B. Detection

C. Analysis

D. Containment

5. During a security incident, a team member responded to a SIEM alert stating that multiple workstations on a network segment have been infected with crypto-malware. what part of the incident response process should be followed?

   A. Preparation

   B. Detection

   C. Analysis

   D. Containment

6. After a security incident, workstations that were previously infected with crypto-malware were placed in quarantine, wiped, and successfully scanned with an updated antivirus. what part of the incident response process should be followed?

   A. Analysis

   B. Containment

   C. Recovery

   D. Lessons learned

7. During a security incident, multiple systems were impacted by a DDoS attack. To mitigate the effect of the attack, a CSIRT team member follows procedures to trigger a BGP route update. This deflects the attack and the systems remain operational. What documentation did the CSIRT team member refer to?

   A. Communication plan

   B. Runbooks

   C. Configuration guides

   D. Vendor documentation

8. Critical infrastructure has been targeted by attackers who demand large payments in bitcoin to reveal the technology and keys needed to access the encrypted data. To avoid paying the ransom, analysts have been tasked to crack the cipher. What technique will they use?

   A. Ransomware

   B. Data exfiltration

   C. Cryptanalysis

   D. Steganalysis

9. During a security incident, multiple systems were impacted by a DDoS attack. A security professional working in the SOC can view the events on a reporting dashboard and call up automated scripts to mitigate the attack. What system was used to respond to the attack?

    A. Containment

    B. SOAR

    C. Communication plan

    D. Configuration guides

10. A technician who is part of the IRT is called to take a forensic copy of a hard drive on the CEO's laptop. He takes notes of the step-by-step process and stores the evidence in a locked cabinet in the CISO's office. What will make this evidence inadmissible?

    A. Evidence collection

    B. Lack of chain of custody

    C. Missing order of volatility

    D. Missing memory snapshots

11. A forensic investigator is called to capture all the possible evidence from a compromised laptop. To save battery life, the system is put into sleep mode. What important forensic process has been overlooked?

    A. Cloning

    B. Evidence preservation

    C. Secure storage

    D. Backups

12. A forensic investigator is called to capture all possible evidence from a compromised computer that has been switched off. They gain access to the hard drive and connect a write blocker, before recording the current hash value of the hard drive image. What important forensic process has been followed?

    A. Integrity preservation

    B. Hashing

    C. Cryptanalysis

    D. Steganalysis

13. Law enforcement needs to retrieve graphics image files that have been deleted or hidden in unallocated space on a hacker's hard drive. What tools should they use when analyzing the captured forensic image?

A. File carving tools

B. `objdump`

C. `strace`

D. `netstat`

14. FBI forensics experts are investigating a new variant of APT that has replaced Linux operating system files on government computers. What tools should they use to understand the behavior and logic of these files?

A. Runbooks

B. Binary analysis tools

C. Imaging tools

D. `vmstat`

15. A forensic investigator suspects stolen data is hidden within JPEG images on a suspect's computer. After capturing a forensic image, what techniques should they use when analyzing the JPEG image files?

A. Integrity preservation

B. Hashing

C. Cryptanalysis

D. Steganalysis

16. Attackers have managed to install additional services on a company's DMZ network. Security personnel need to identify all the systems in the DMZ and all the services that are currently running. What command-line tool best gathers this information?

A. `Nmap`

B. `Aircrack-ng`

C. Volatility

D. The Sleuth Kit

17. A forensic investigator is called to capture all possible evidence from a compromised computer that has been switched off. They gain access to the hard drive and connect a write blocker. What tool should be used to create a bit-by-bit forensic copy?

A. `dd`

B. Hashing utilities

C. `sha256sum`

D. `ssdeep`

18. To stop a running process on a Red Hat Linux server, an investigator needs to see all the currently running processes and their current process IDs. What command-line tool will allow the investigator to view this information?

    A. `netstat -a`

    B. `ps -A`

    C. `tcpdump -i`

    D. `sha1sum <filename>`

19. While analyzing a running Red Hat Linux server, an investigator needs to show the number of available computing resources and currently used resources. The requirements are for the running processor, memory, and swap space on the disk. What tool should be used?

    A. `vmstat`

    B. `ldd`

    C. `lsof`

    D. `tcpdump`

20. During a live investigation on a Fedora Linux server, a forensic analyst needs to view a listing of all opened files, the process that was used to open them, and the user account associated with the open files. What would be the best command-line tool to use?

    A. `vmstat`

    B. `ldd`

    C. `lsof`

    D. `tcpdump`

21. While analyzing a running Red Hat Linux server, an investigator needs to run commands on the system under investigation to reflect all the outputs on the forensics workstation. The analyst also needs to transfer a file for investigation using minimum interactions. What command-line tool should be used?

    A. `netcat`

    B. `tcpdump`

    C. `conntrack`

    D. Wireshark

22. Security professionals need to assess the security of wireless networks. A tool needs to be identified that allows wireless traffic to be monitored, and the WEP and WPA security to be attacked (via packet injection) and cracked. What would be the best command-line tool to use here?

    A. `netcat`

    B. `tcpdump`

    C. `Aircrack-ng`

    D. Wireshark

23. A forensic investigator needs to search through a network capture saved as a `pcap` file. They are looking for evidence of data exfiltration from a suspect host computer. To minimize disruption, they need to identify a command-line tool that will provide this functionality. What should they choose?

    A. `netcat`

    B. `tcpdump`

    C. `Aircrack-ng`

    D. Wireshark

24. A forensic investigator is performing analysis on syslog files. They are looking for evidence of unusual activity based upon reports from **User Behavior Analytics** (**UBA**). Several packets show signs of unusual activity. Which of the following requires further investigation?

    A. `nc -w 180 -p 12345 -l < shadow.txt`

    B. `tcpdump -I eth0`

    C. `conntrack -L`

    D. `Exiftool nasa.jpg`

25. Recent activity has led to an investigation being launched against a recent hire in the research team. Intellectual property has been identified as part of code now being sold by a competitor. UBA has identified a significant amount of JPEG image uploads to a social networking site. The payloads are now being analyzed by forensics. What techniques will allow them to search for evidence in the JPEG files?

    A. The Steganalysis tool

    B. The Cryptanalysis tool

    C. The Binary Analysis tool

    D. The Memory Analysis tool

Answers

The following are the answers to this chapter's questions:

1. A
2. C
3. C
4. A
5. D
6. C
7. B
8. C
9. B
10. B
11. B
12. A
13. A
14. B
15. D
16. A
17. A
18. B
19. A
20. C
21. A
22. C
23. B
24. A
25. A

Chapter 9

Figure

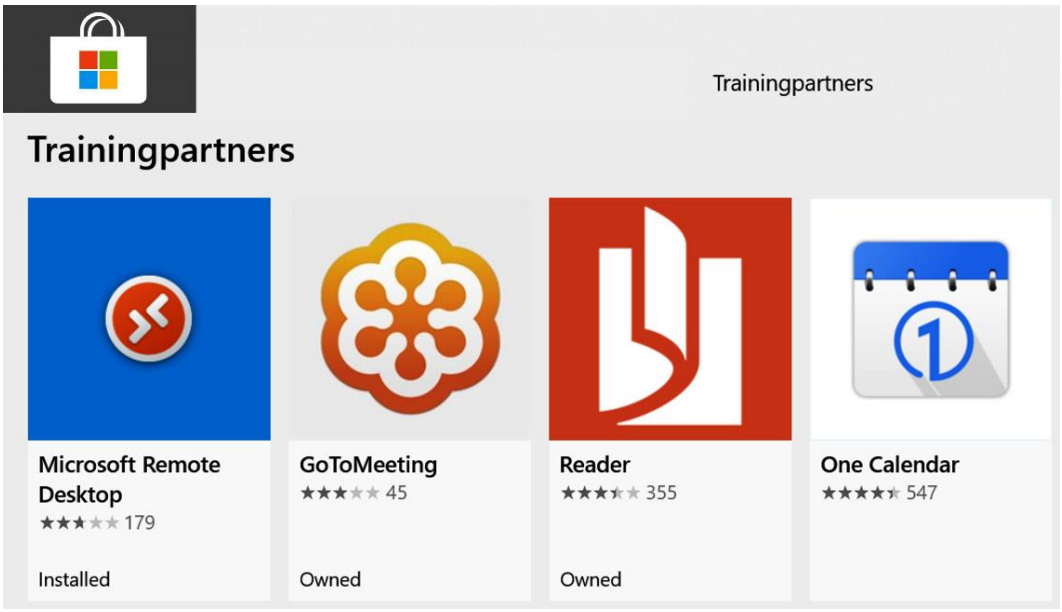


Figure 9.1 – A restricted Microsoft Store application

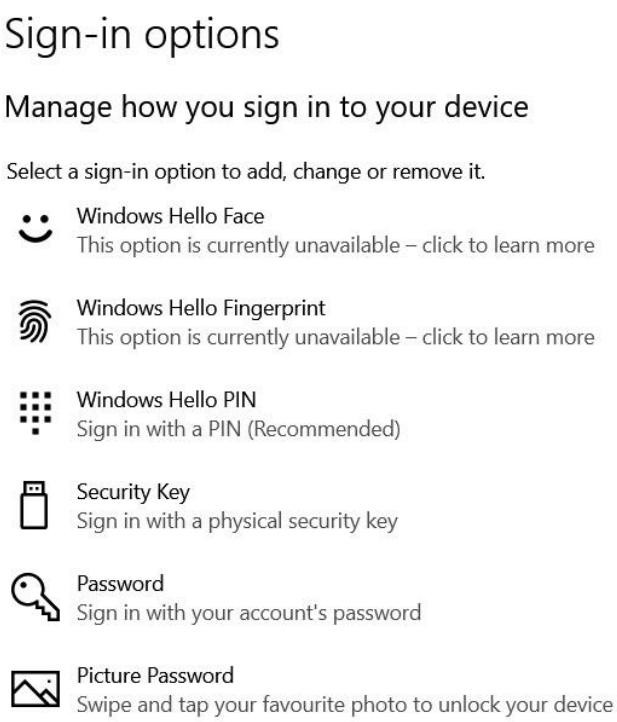


Figure 9.2 – MFA authentication methods on Windows

Figure 9.3 – Remote wipe options

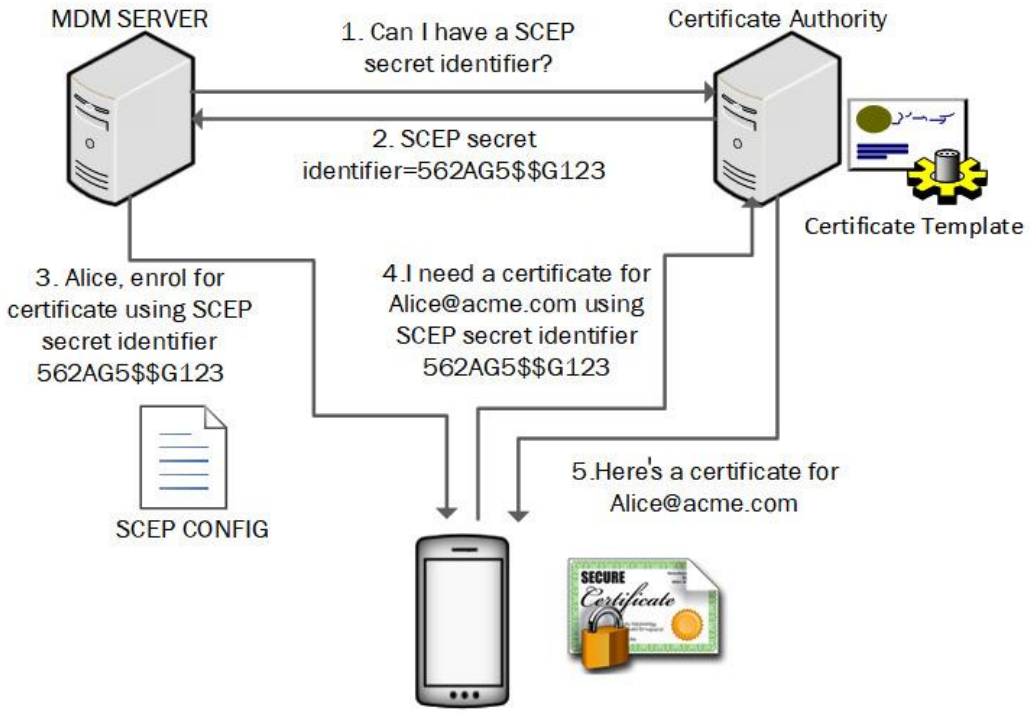


Figure 9.4 – The SCEP enrolment process

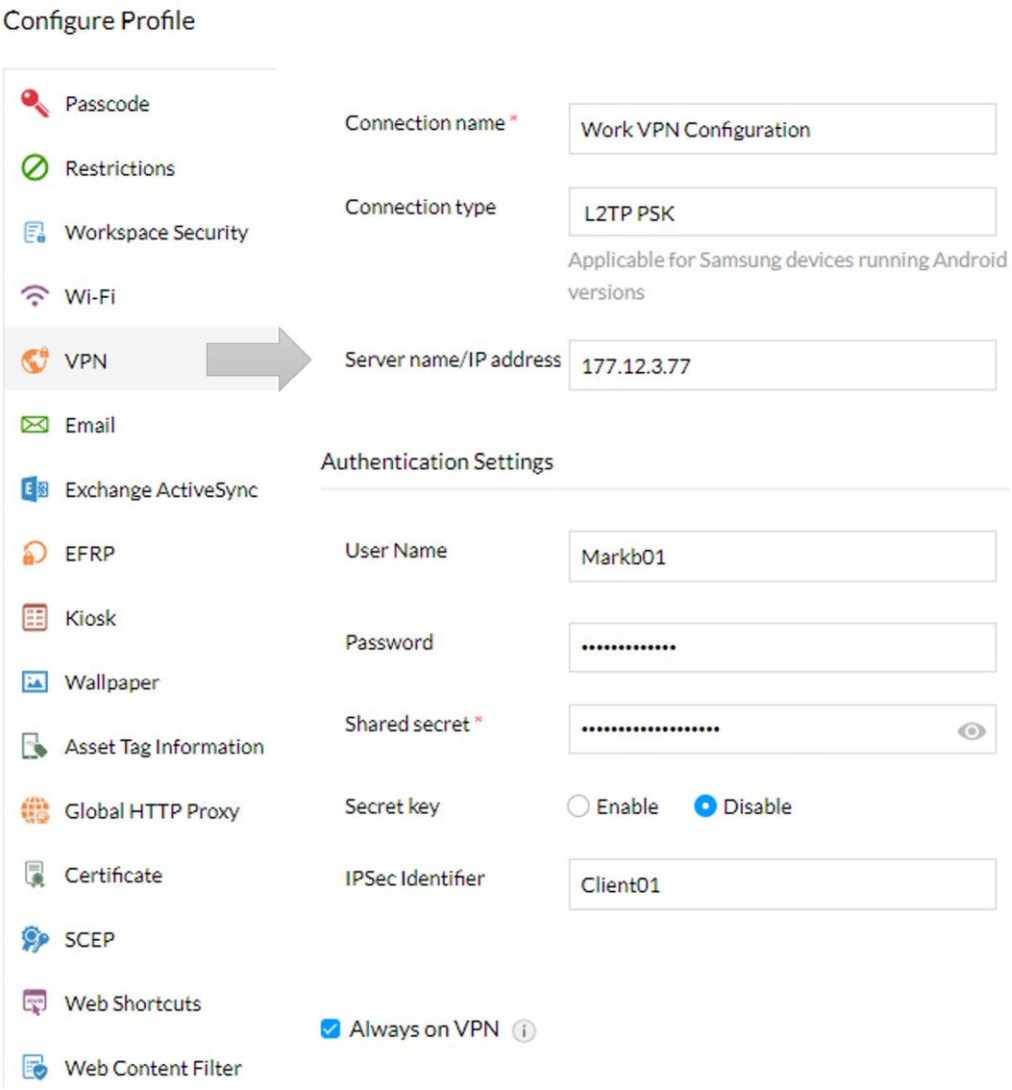


Figure 9.5 – An example VPN device configuration profile

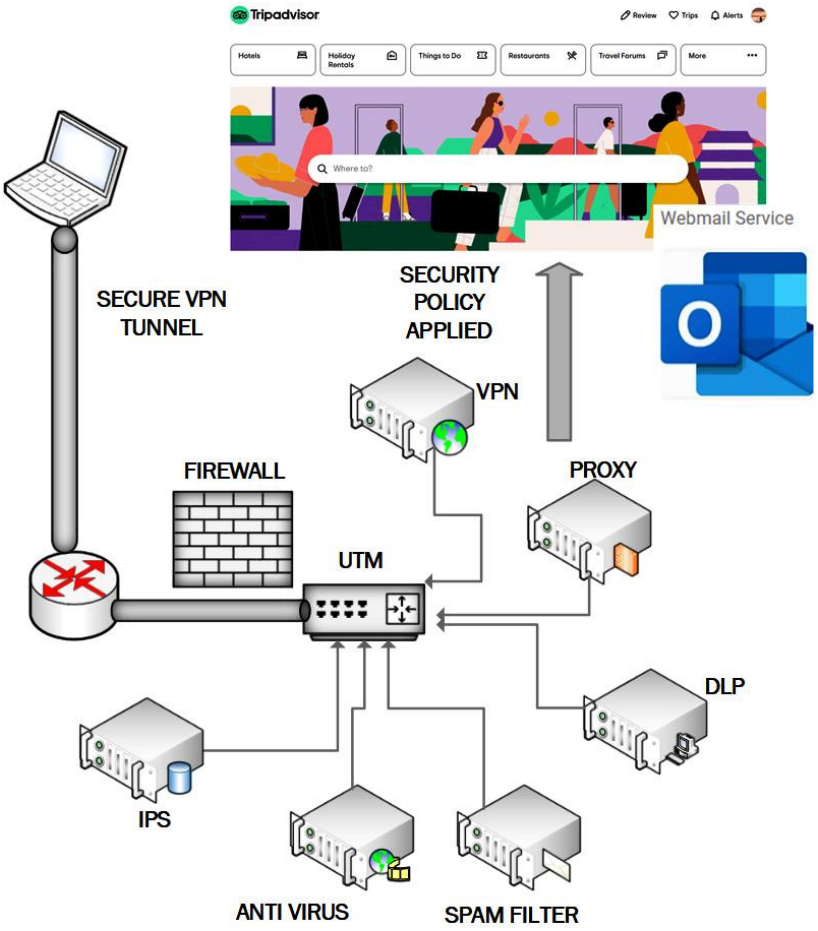


Figure 9.6 – A VPN client connecting through a full tunnel configuration

Figure 9.7 – The Strava mapping feature

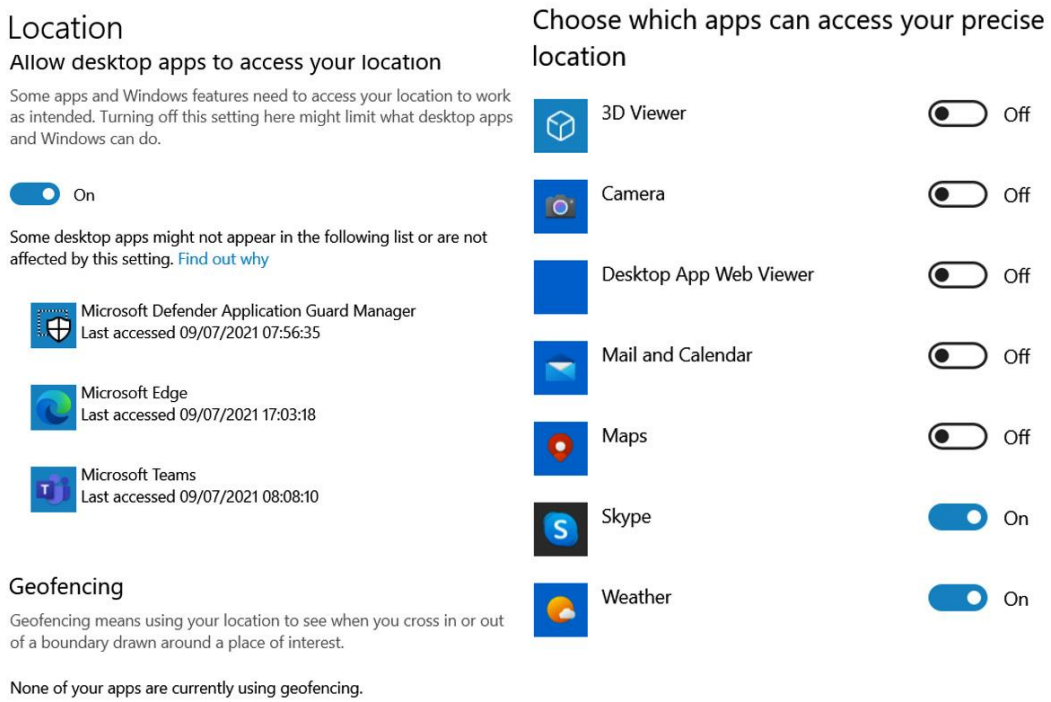


Figure 9.8 – The Microsoft location services privacy settings

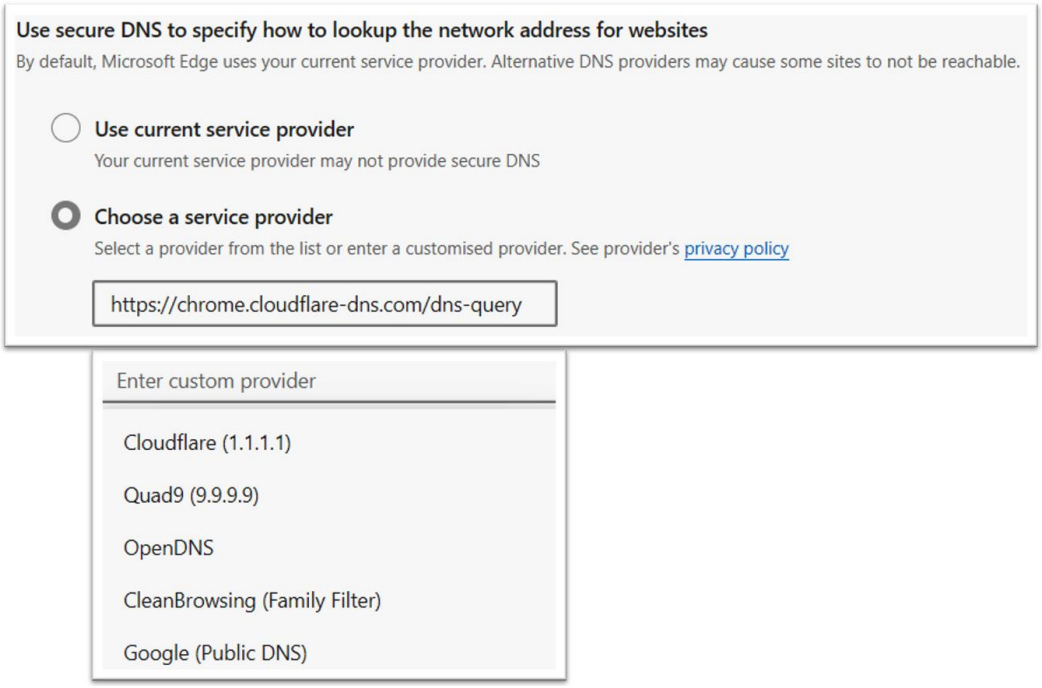


Figure 9.9 – The Microsoft Edge browser DoH settings

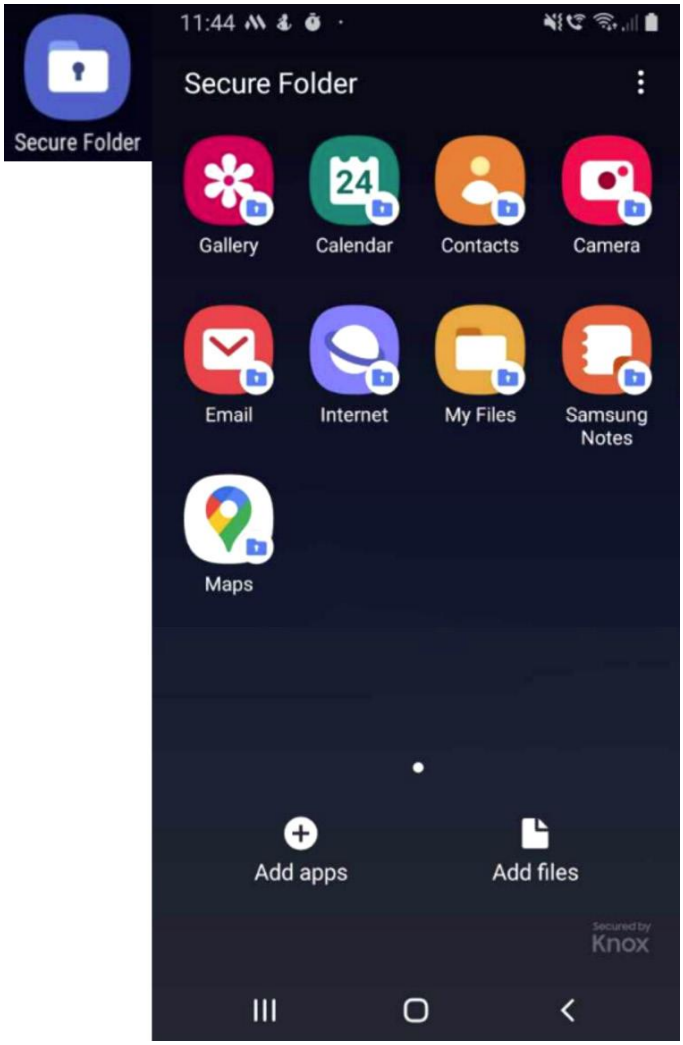


Figure 9.10 – Samsung Secure Folder

Administrator		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
RedisService	RedisService	Redis Server Service

Figure 9.11 – Disabled default Windows accounts

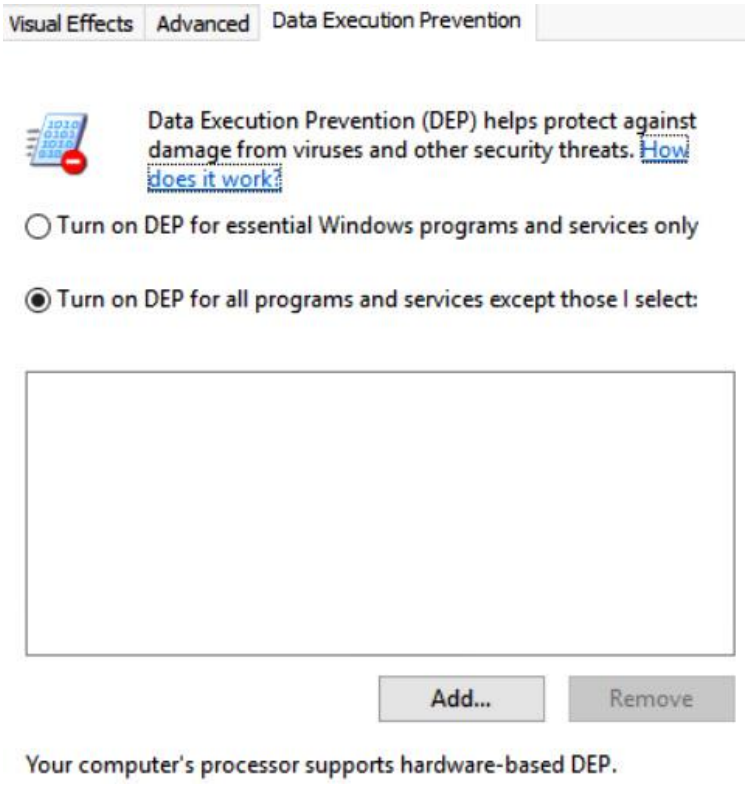


Figure 9.12 – The Microsoft DEP feature

```
[root@cent07 ~]# useradd henry -s /bin/rbash
[root@cent07 ~]# passwd henry
```

Figure 9.13 – Implementing a restricted shell

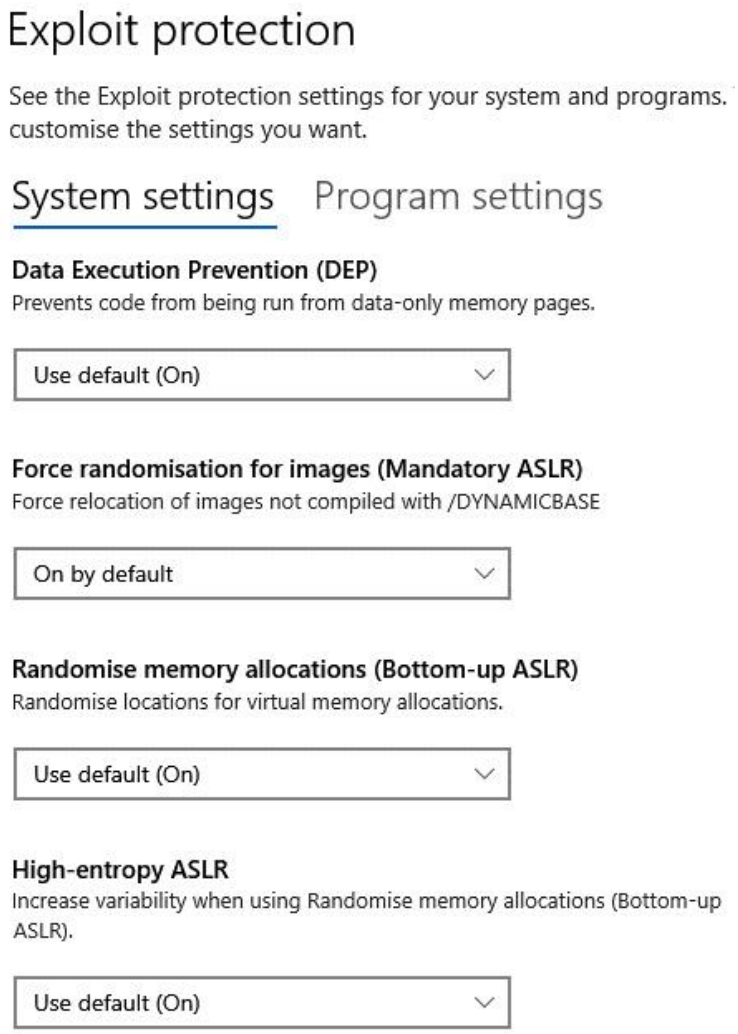


Figure 9.14 – Microsoft Windows ASLR settings

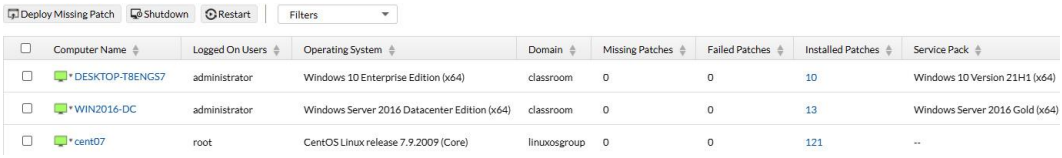


Figure 9.15 – ManageEngine Patch Manager Plus

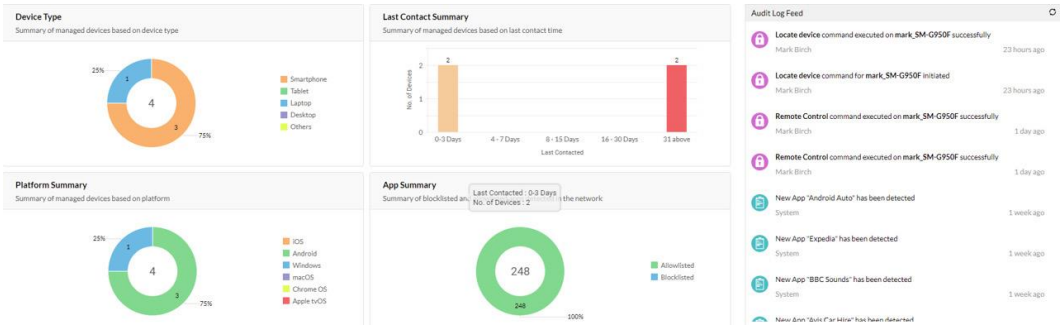


Figure 9.16 – Endpoint device monitoring

```
httpd_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_connect_ftp --> off
httpd_can_connect_ldap --> off
httpd_can_connect_mythtv --> off
httpd_can_connect_zabbix --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_memcache --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> off
httpd_dbus_sssd --> off
httpd_dontaudit_search_dirs --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> off
httpd_execmem --> off
httpd_graceful_shutdown --> on
httpd_manage_ipa --> off
httpd_mod_auth_ntlm_winbind --> off
httpd_mod_auth_pam --> off
httpd_read_user_content --> off
httpd_run_ipa --> off
httpd_run_preupgrade --> off
httpd_run_stickshift --> off
httpd_serve_cobbler_files --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_sys_script_anon_write --> off
```

Figure 9.17 – SELinux enforcable settings

PCT Number	Allocation
0	BIOS
1	BIOS configuration
2	Option ROMs
3	Option ROM configuration
4	MBR (master boot record)
5	MBR configuration

Figure 9.18 – PCR values

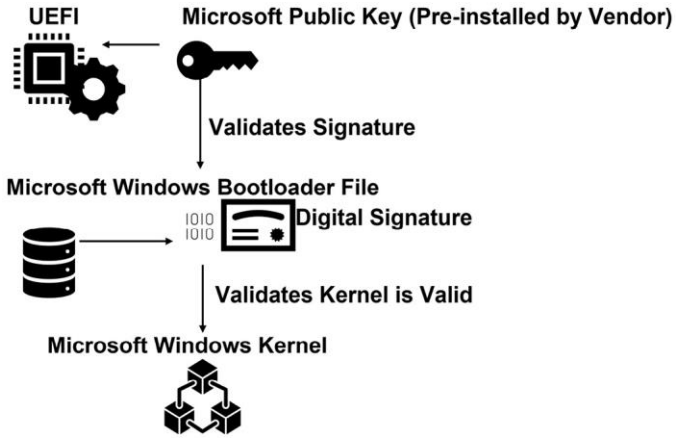


Figure 9.19 – The Microsoft Windows Secure Boot components

Figure 9.20 – The Windows UEFI menu

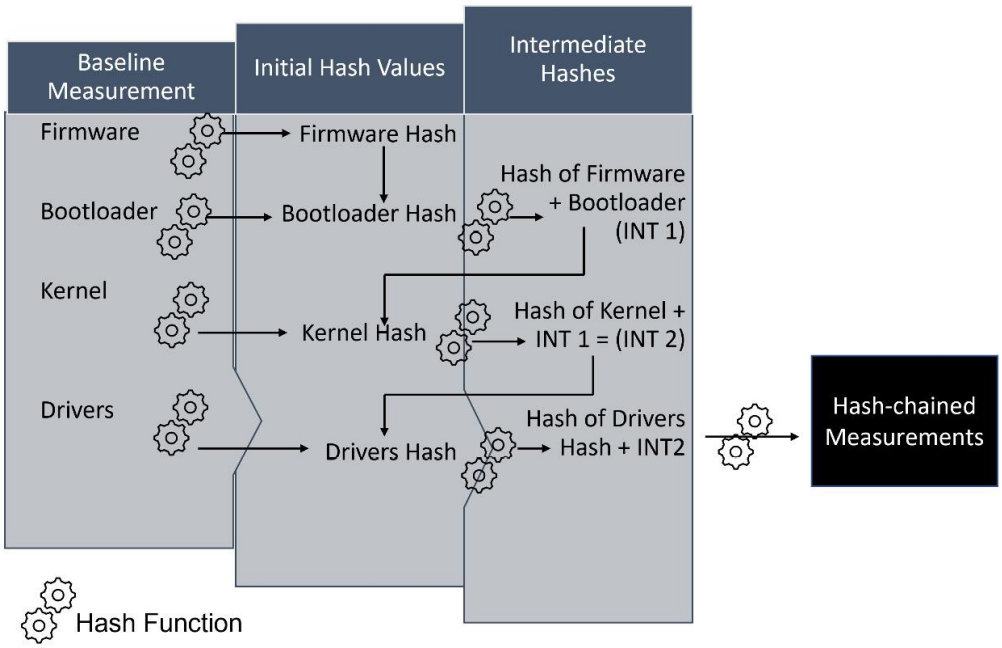
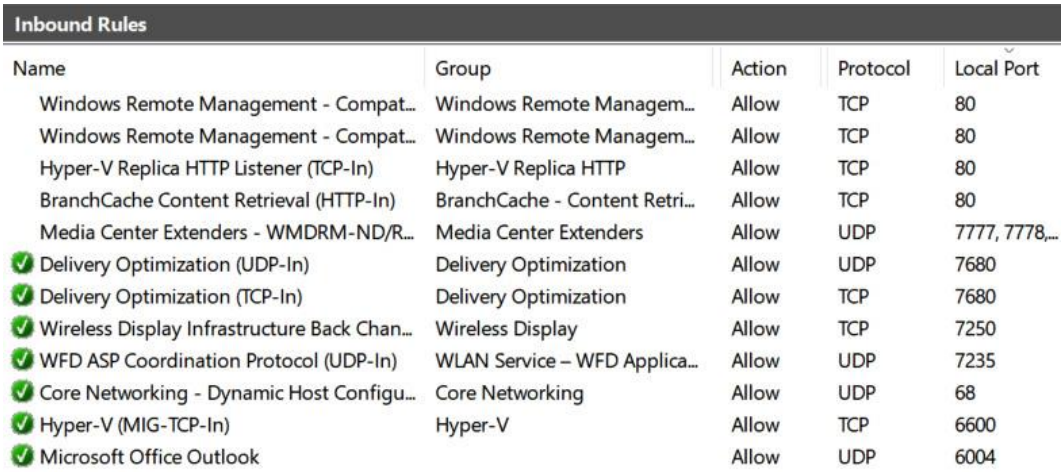


Figure 9.21 – The Measured Boot process



Inbound Rules

Name	Group	Action	Protocol	Local Port
Windows Remote Management - Compat...	Windows Remote Managem...	Allow	TCP	80
Windows Remote Management - Compat...	Windows Remote Managem...	Allow	TCP	80
Hyper-V Replica HTTP Listener (TCP-In)	Hyper-V Replica HTTP	Allow	TCP	80
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retri...	Allow	TCP	80
Media Center Extenders - WMDRM-ND/R...	Media Center Extenders	Allow	UDP	7777, 7778,...
Delivery Optimization (UDP-In)	Delivery Optimization	Allow	UDP	7680
Delivery Optimization (TCP-In)	Delivery Optimization	Allow	TCP	7680
Wireless Display Infrastructure Back Chan...	Wireless Display	Allow	TCP	7250
WFD ASP Coordination Protocol (UDP-In)	WLAN Service – WFD Applica...	Allow	UDP	7235
Core Networking - Dynamic Host Configu...	Core Networking	Allow	UDP	68
Hyper-V (MIG-TCP-In)	Hyper-V	Allow	TCP	6600
Microsoft Office Outlook		Allow	UDP	6004

Figure 9.22 – Windows Defender Firewall

```
└─$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.0.0/8           anywhere
DROP       all  --  192.168.0.0/24       anywhere
DROP       all  --  172.0.0.0/16         anywhere
```

Figure 9.23 – Some iptables firewall rules

Code

Code 9.1: The following command drops all packets from the `10.10.0.0/24` source network:

```
iptables -A INPUT -I eth0 -s 10.10.0.0/24 -j DROP.
```

Links

For more information on Adups, see the report at https://tinyurl.com/adupshack.

For more details on eFuse, see the following URL: https://tinyurl.com/samsungefuse

For more details on the ManageEngine product see the following URL: https://tinyurl.com/MEpatchmanager.

Please see the following URLs for more details on **CrowdStrike** and **Microsoft Defender for Endpoint**:

- https://tinyurl.com/crowdstrikeEDR
- https://tinyurl.com/defenderEDR

Questions

1. Some executives from an organization attend an industry conference. Using mobile devices and wireless headsets, they are able to stay in touch with colleagues back at the workplace. What may present a security concern in this situation?

   A. Tethering

   B. WPA3

   C. Device certificates

   D. Bluetooth

2. Some marketing executives from an organization attend an international trade exhibition and must connect to the company email by using their mobile devices during the event. The CISO is concerned this may represent a risk. What would best mitigate this risk?

   A. NFC

   B. A split-tunnel VPN

   C. Geofencing

   D. Always-on VPN settings

3. What function should be disabled to ensure scientists cannot use their mobile devices to bridge the corporation's network with a cellular operator's network?

   A. Tethering

   B. WPA3

   C. Device certificates

   D. Bluetooth

4. What should be implemented to ensure only company-approved applications can be installed on company devices?

   A. Containerization

   B. Token-based access

   C. A patch repository

   D. Whitelisting

5. A user calls the service desk because her Samsung smartphone is prompting her to install updates that the vendor says will offer more functionality and security. What is this an example of?

A. MFA requirements

B. Token-based access

C. A patch repository

D. Firmware over-the-air

6. An employee's company mobile device is reported as stolen 24 hours after the event. Sensitive data has been posted online by hackers. What would have mitigated this risk if the report had been made earlier?

A. MFA requirements

B. A remote wipe

C. A patch repository

D. Firmware over-the-air

7. What type of setting will ensure mobile devices will only be able to access Wi-Fi when they connect securely to the company WLAN?

A. WPA3 SAE

B. Device certificates

C. Device profiles

D. Bluetooth

8. An employee has noticed several suspicious payments made from a company debit card via Google Pay on their company smartphone. They recently attended a busy trade conference. What technology was likely used to make the payments?

A. NFC

B. Peripherals

C. Geofencing

D. VPN settings

9. How can we prevent certain mobile applications from being accessible when employees take COPE devices out of the warehouse?

A. NFC

B. MFA

C. Geofencing

D. VPN settings

10. The service desk receives a call from a senior manager. She is concerned that spyware may be installed on her smartphone. Recent news, traffic, and weather updates have been targeted specifically for her location. What is the most likely reason for this activity?

    A. Airplane mode

    B. Location services

    C. NFC

    D. Geofencing

11. A user is concerned that DNS lookups may be logged by government agencies. The user would like to protect their privacy. What would be the best method to protect privacy during name resolution?

    A. Geofencing

    B. VPN settings

    C. DNS over HTTPS (DoH)

    D. Containerization

12. A nation-state sends a security team to scope out a military site in California in the United States. They use mobile devices to gather images, map the locations of communications equipment, and record detailed information about troop movements. What are they performing?

    A. Geotagging

    B. Geofencing

    C. Physical reconnaissance

    D. Personal data theft

13. A personal device has many applications installed that are not available through the Apple App Store. The device subsequently fails compliance checks. What has likely made the device fail to be compliant with the security policies?

    A. Jailbreaking

    B. Sideloading

    C. Containerization

    D. An unauthorized application store

14. A senior employee has followed a QC link and installed a mobile application used to order food and beverages at a local restaurant. The application is not available on the Google Play Store. **Acceptable Use Policy** (**AUP**) states that applications can only be downloaded from

the official vendor store. What best describes what has allowed this application to be installed?

A. Supply chain issues

B. Sideloading

C. Containerization

D. An unauthorized application store

15. Developers need to test mobile applications on a variety of hardware before making them available on official application stores. How can they install the applications locally on mobile devices?

A. Update the supply chain.

B. Use sideloading.

C. Use containerization.

D. Use an unauthorized application store.

16. A sales director would like to allow sales employees to use their personal devices for accessing company applications and data as part of an effort to reduce business costs. What would be the best control to mitigate the risk of employees co-mingling personal and company data?

A. Geotagging

B. Geofencing

C. Containerization

D. Remote wipes

17. When on a business trip, a CEO was detained for several hours at border control. When he was eventually reunited with his mobile phone, it had physical evidence of tampering. He powered on the device and input the correct pin, but found that all of the company applications and data were inaccessible. What has led to this situation?

A. Geofencing

B. Containerization

C. Remote wipes

D. An eFuse

18. A user has been able to run an unmanaged Linux operating system alongside a managed Windows 10 build on a company laptop. What actions would allow security professionals to prevent this issue from re-occurring?

A. Removing end-of-support devices

B. Using local drive encryption

C. Disabling CPU virtualization support

D. Enforcing secure encrypted enclaves and SME

19. Security administrators have deployed SELinux in enforcing mode. All unnecessary services have been removed. In a further attempt to enforce security, a number of commands – including `vmstat` and `grep` – have been blocked from some user accounts. What best describes this action?

A. Whitelisting

B. Shell restrictions

C. ASLR

D. Memory encryption

20. The CISO is meeting with software engineers to better understand some of the challenges that they face. He is asking if there are any settings that can be incorporated into build images that will help to prevent attacks against the system memory. What two features should be chosen?

A. ASLR

B. Patching

C. Firmware

D. NX/XN

21. What is deployed to mitigate the risk of privilege elevation and the misuse of applications on Android mobile devices?

A. SELinux

B. TPM technology

C. SEAndroid

D. Attestation services

22. What built-in module stores PCR values and enforces integrity on a hardware platform?

A. The TPM module

B. Secure Boot mode

C. UEFI

D. The BIOS

23. What would be the best choice of technical control to block a fast-spreading worm that targets a well-known **NetBIOS** port?

    A. UEBA

    B. A host-based firewall

    C. A HIDS

    D. Redundant hardware

24. A reporting tool has alerted the administrator that Joe Smith, who is leaving the company in 4 weeks, has uploaded a large number of PDF documents to his personal cloud storage. What has likely triggered this event?

    A. UEBA

    B. A host-based firewall

    C. EDR software

    D. Self-healing hardware

25. A system administrator needs to ensure the root account cannot be used to gain access to user data on a Linux **Network File System** (**NFS**) server. What actions would allow security professionals to prevent this issue from occurring?

    A. Ensuring passwords are stored in a shadow file

    B. Running SELinux in enforcing mode

    C. Disabling CPU virtualization support

    D. Enforcing secure encrypted enclaves and SME

Answers

1. D
2. D
3. A
4. D
5. D
6. B
7. C

8. A
9. C
10. B
11. C
12. C
13. A
14. D
15. B
16. C
17. D
18. C
19. B
20. A and D
21. C
22. A
23. B
24. A
25. B

Chapter 10

Figures

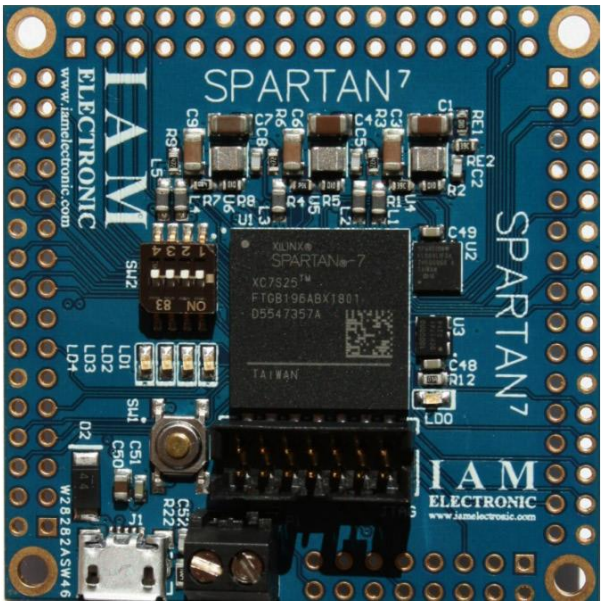


Figure 10.1 – FPGA integrated system board

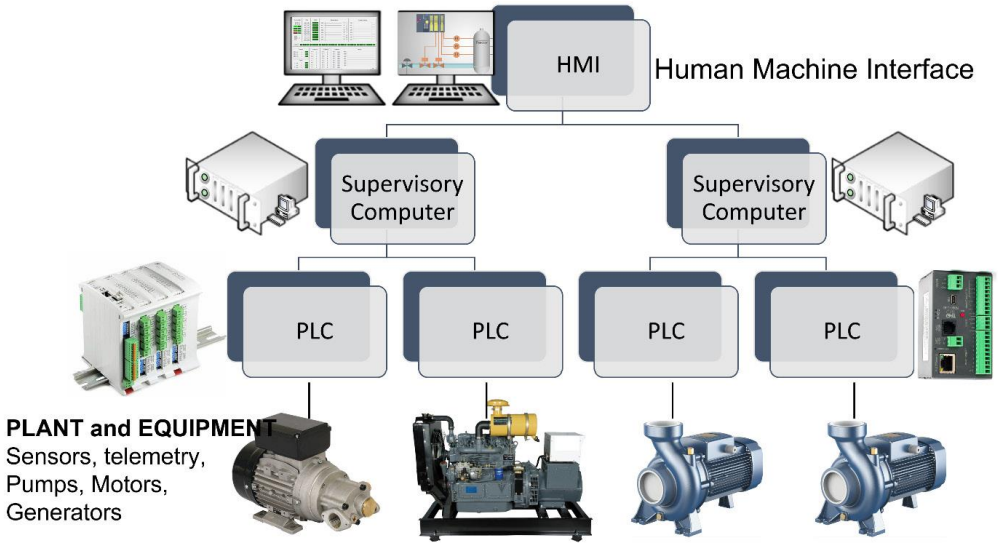


Figure 10.2 – SCADA system

Figure 10.3 – Siemens PLC models

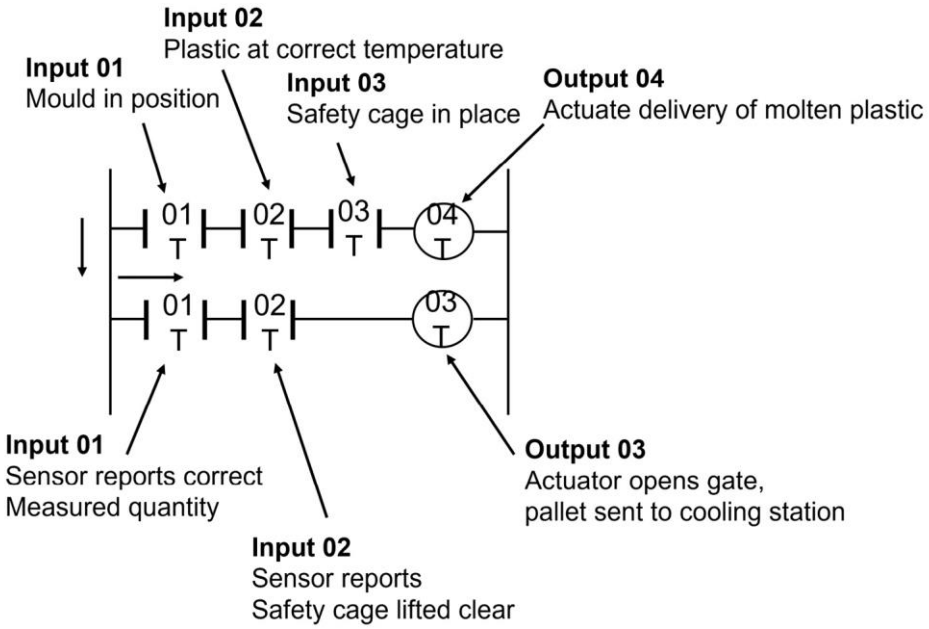


Figure 10.4 – Ladder logic processing

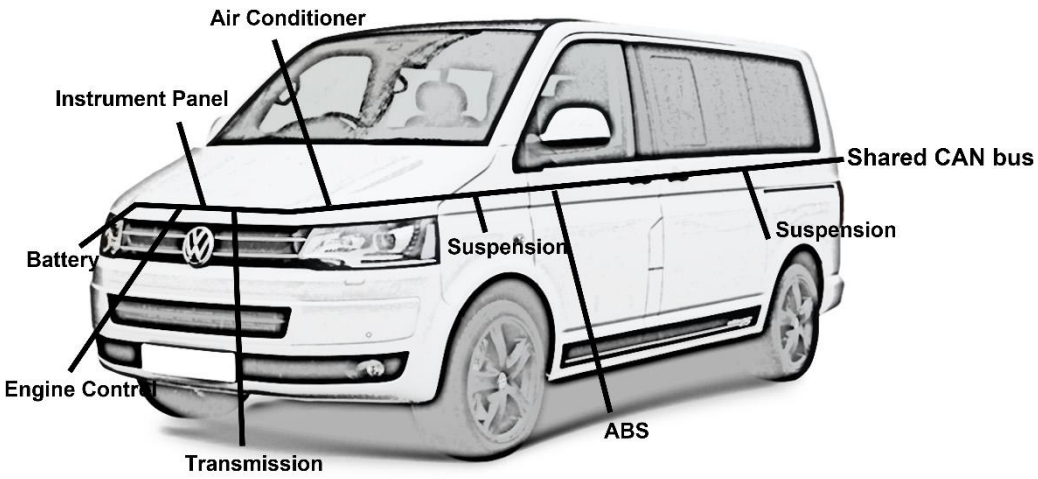


Figure 10.5 – CAN bus architecture

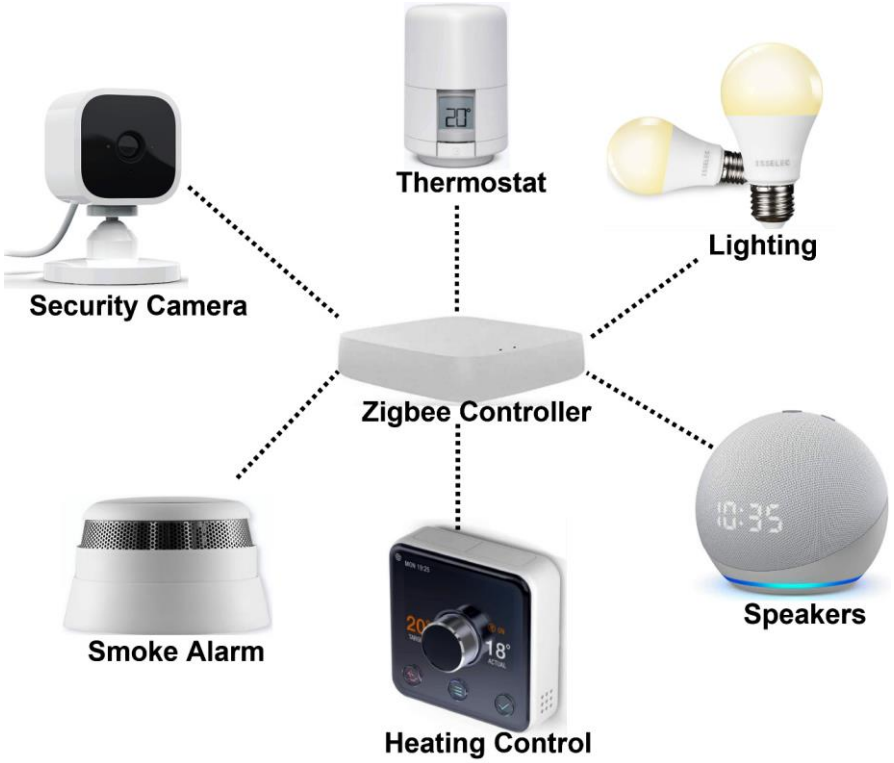


Figure 10.6 – Zigbee network

Device Profiles	Pneumatic Valve	Semi-Conductor	AC Drive	Sensor	
	Object Library Communications, Applications, Time Synchronization				CIP Layers
	Data Management Services Explicit and I/O Messages				
	Connection Management and Routing				
OSI Layers	TCP/UDP IP	CompoNet Network and Transport	ControlNet Network and Transport	DeviceNet Network and Transport	
	IEEE 802.3	CompoNet Time Slot	ControlNet CTDMA	CAN CSMA/NBA	
	Ethernet Physical Layer	CompoNet Physical Layer	ControlNet Physical Layer	DeviceNet Physical Layer	

Figure 10.7 – CIP communication model

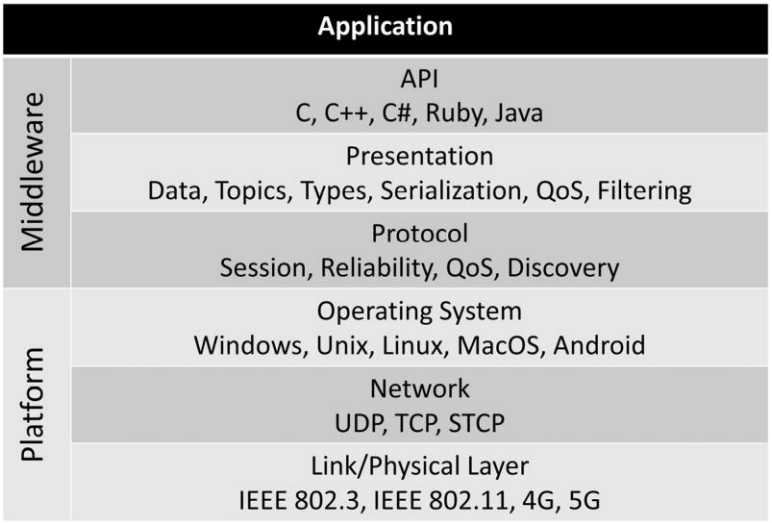


Figure 10.8 – DDS layers

Links

For details on ONR, see the following link: https://tinyurl.com/ONRnuclearfines

To read more about the work of NERC and CIP, you can access the following link: https://tinyurl.com/nercstandards.

For more information on ladder logic, see the following link: https://tinyurl.com/ladderlogicplc.

See the following URL for current known vulnerabilities concerning the Modbus protocol. https://tinyurl.com/modbus-cves.

For more information regarding DDS-Security please see the following URL: https://tinyurl.com/dds-security.

Questions

1. Which regulated business sector is intended to benefit citizens and generate no commercial profit?

   A. Energy

   B. Manufacturing

   C. Healthcare

   D. Public services

2. Which regulated business sector would typically involve the processing and storage of PHI?

   A. Energy

   B. Manufacturing

   C. Healthcare

D. Public utilities

3. Which regulated business sector may be targeted by competitors who want to steal a company's IP?

   A. Energy

   B. Manufacturing

   C. Healthcare

   D. Public utilities

4. What type of network would likely include legacy vulnerable components?

   A. SCADA

   B. Zigbee

   C. IoT

   D. LAN

5. What risk mitigation would be used when supporting SCADA and business networks for an energy provider?

   A. Segment vulnerable systems

   B. Virtual LANs (VLANs)

   C. Deploy to the DMZ

   D. Upgrade all systems

6. What is a type of processor chip that performs a dedicated task and may be used for bitcoin mining?

   A. IoT

   B. SoC

   C. ASIC

   D. FPGA

7. What is a specialist hardened computer that will control actuators, valves, and pumps in an industrial environment?

   A. Desktop computer

   B. PLC

   C. Mainframe computer

D. Sensor

8. What is a type of processor chip that can be reprogrammed in the field?

   A. IoT

   B. SoC

   C. ASIC

   D. FPGA

9. This term covers many technologies including home automation, building control systems, and many other areas where automation of hardware is required.

   A. IoT

   B. SoC

   C. ASIC

   D. FPGA

10. What is the database logging system known as that will collect data from process controls such as sensors, instrumentation, and other types of controls?

    A. Historian

    B. Ladder logic

    C. SIS

    D. HVAC

11. This is a simple programming language based upon relay-based logic, used originally in electromechanical relays.

    A. Historian

    B. Ladder logic

    C. Zigbee

    D. Modbus

12. What is the de facto standard message transport protocol used in industrial environments that offers no security against tampering with message integrity and is therefore vulnerable to MITM attacks?

    A. CAN

    B. Modbus

    C. DNP3

D. Zigbee

13. What is the networking middleware known as a pub-sub model that is aimed at publishing messages to subscribers?

    A. CAN

    B. DDS

    C. DNP3

    D. Zigbee

14. Which wireless protocol intended primarily for home automation allows communication with low-power devices over distances varying between 10 and 100 meters?

    A. CAN

    B. CIP

    C. DNP3

    D. Zigbee

15. What is a protocol used for the transmission of messages on industrial networks? There are four types of networks offering different transport and network models, including 802.3 Ethernet.

    A. CAN

    B. CIP

    C. DNP3

    D. Zigbee

Answers

1. D
2. C
3. B
4. A
5. A
6. C
7. B
8. D

9. A
10. A
11. B
12. B
13. B
14. D
15. B

Chapter 11

Figures

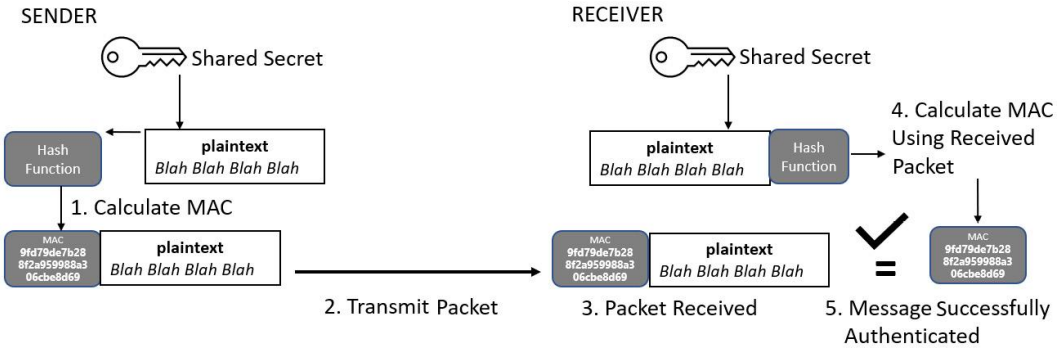


Figure 11.1 – HMAC

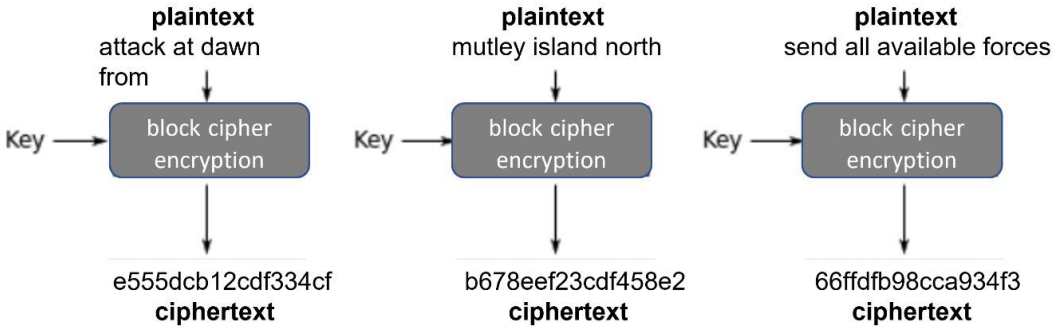


Figure 11.2 – ECB mode

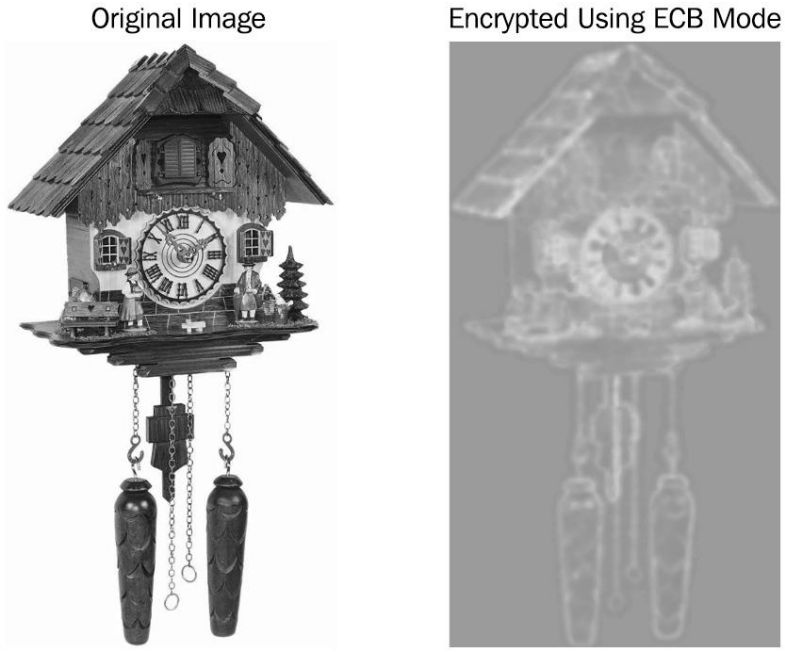


Figure 11.3 – ECB cipher weakness

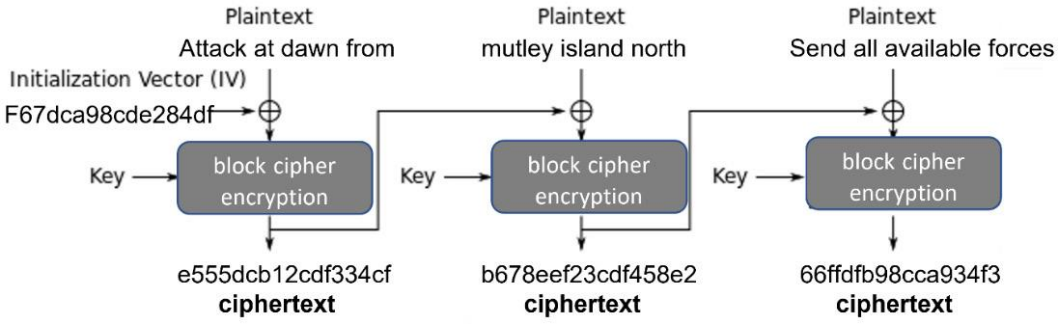


Figure 11.4 – CBC mode

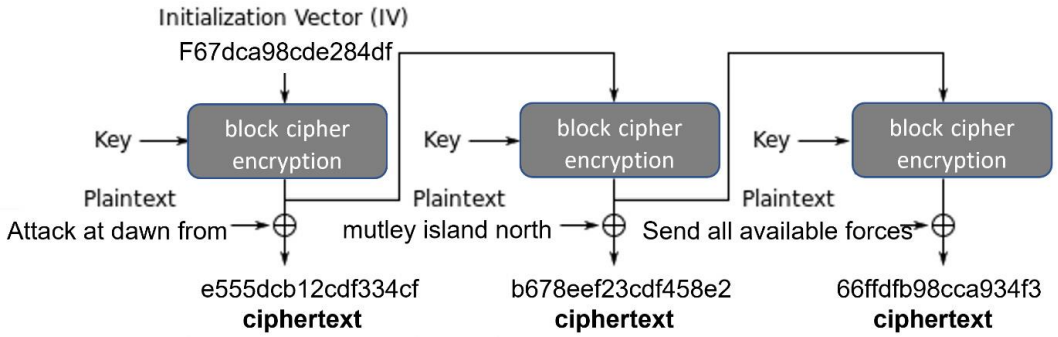


Figure 11.5 – OFB mode

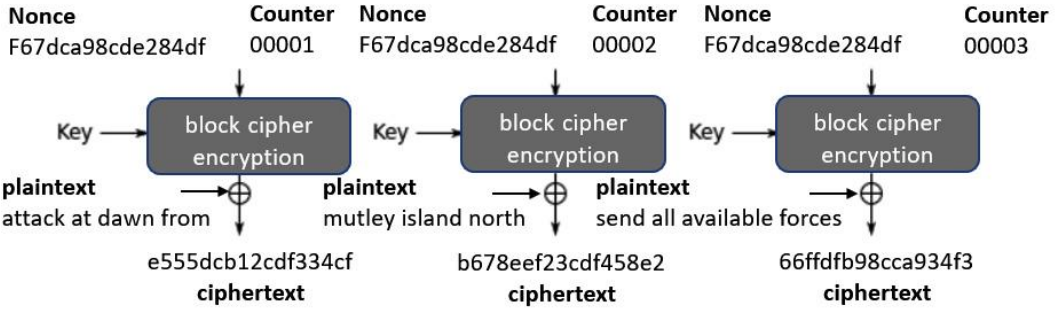


Figure 11.6 – CTR mode

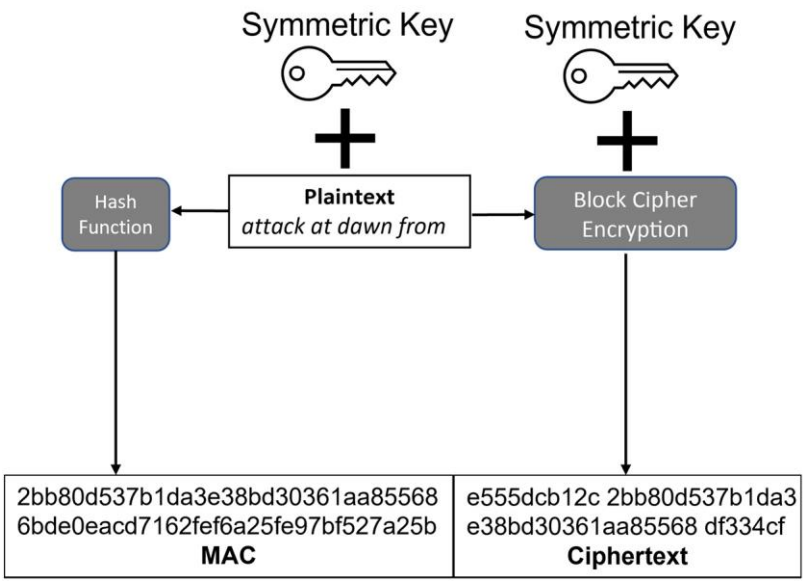


Figure 11.7 – GCM using AEAD

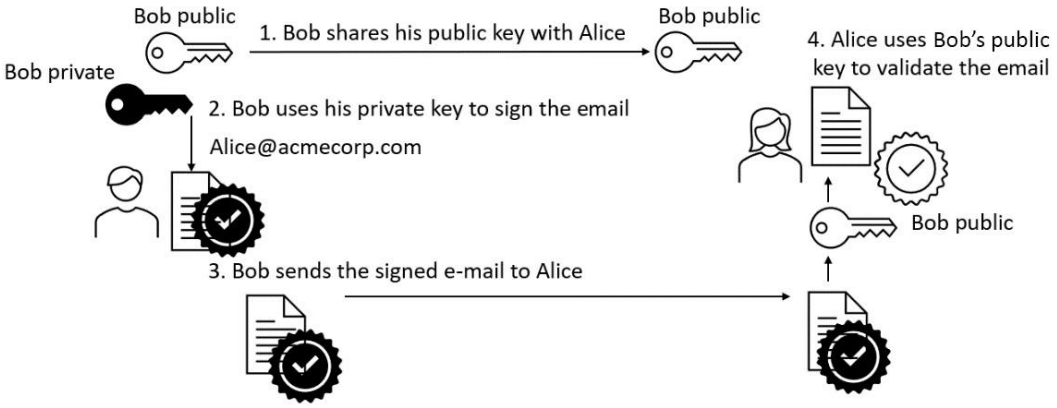


Figure 11.8 – Digital signature algorithm (DSA)

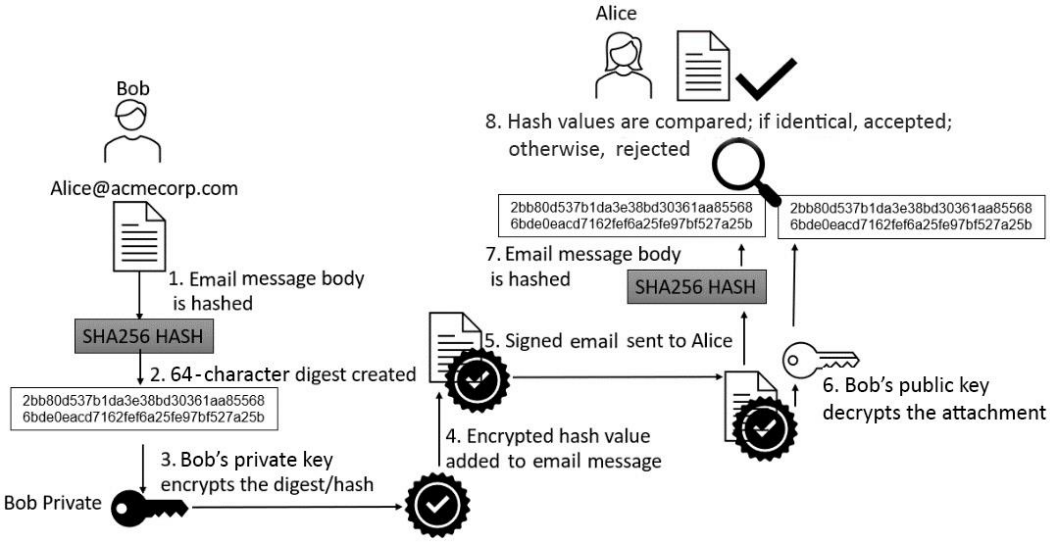


Figure 11.9 – Detailed signing process

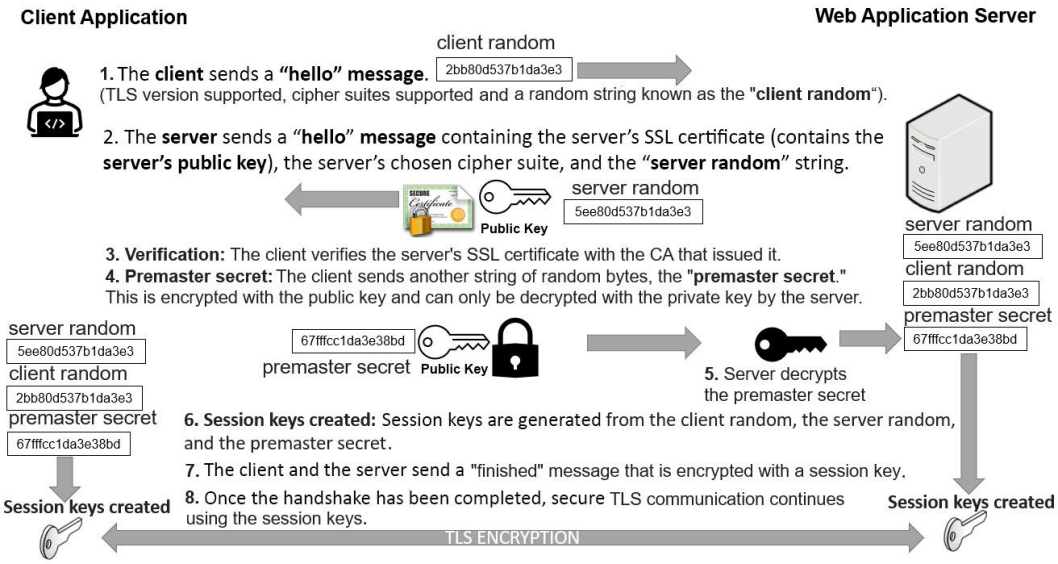


Figure 11.10 – SSL/TLS session handshake

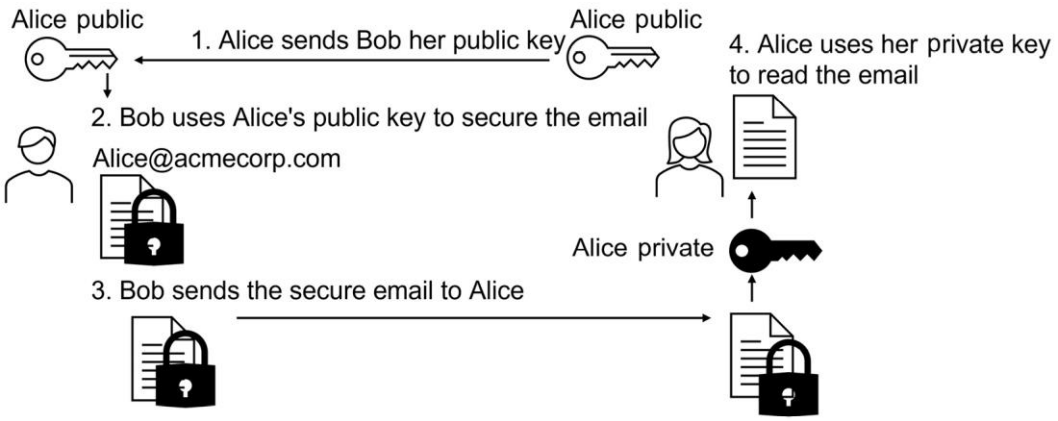


Figure 11.11 – S/MIME

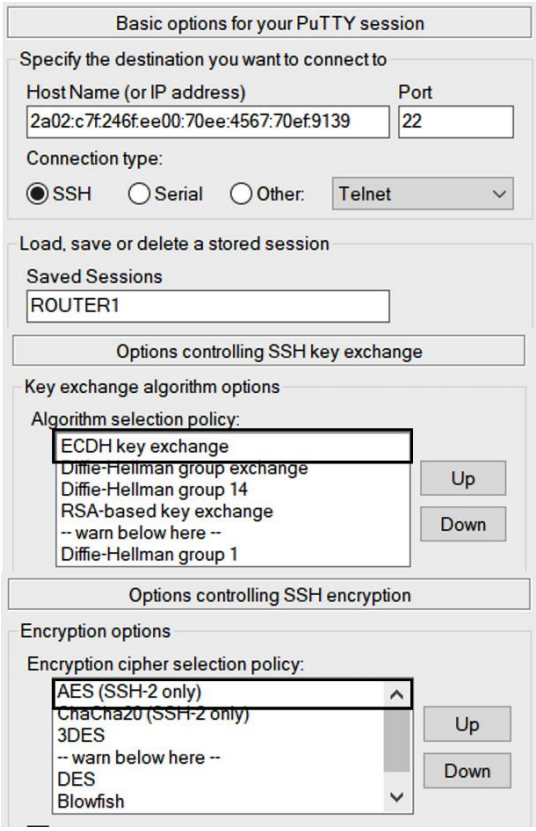


Figure 11.12 – PuTTY SSH configuration

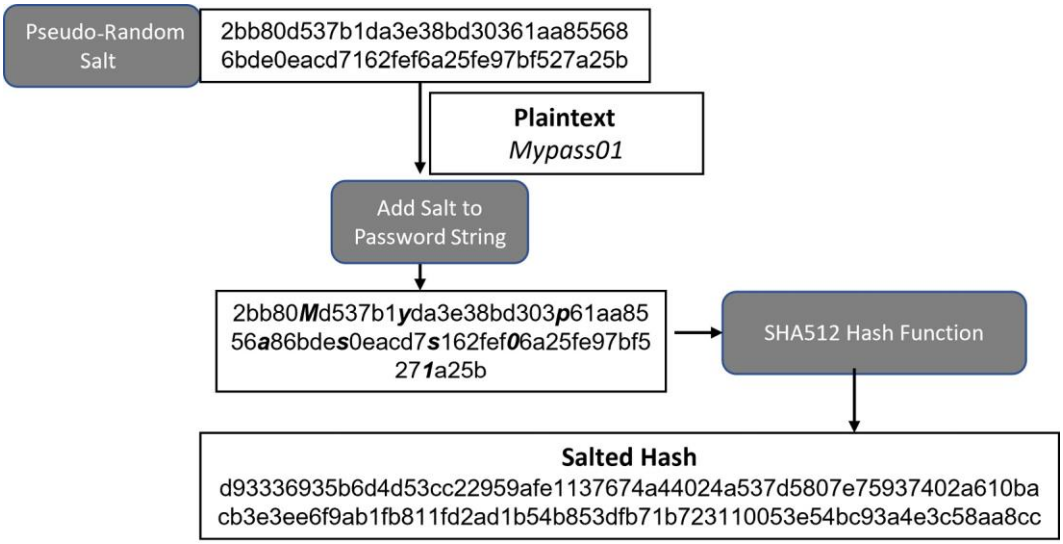


Figure 11.13 – Password salting

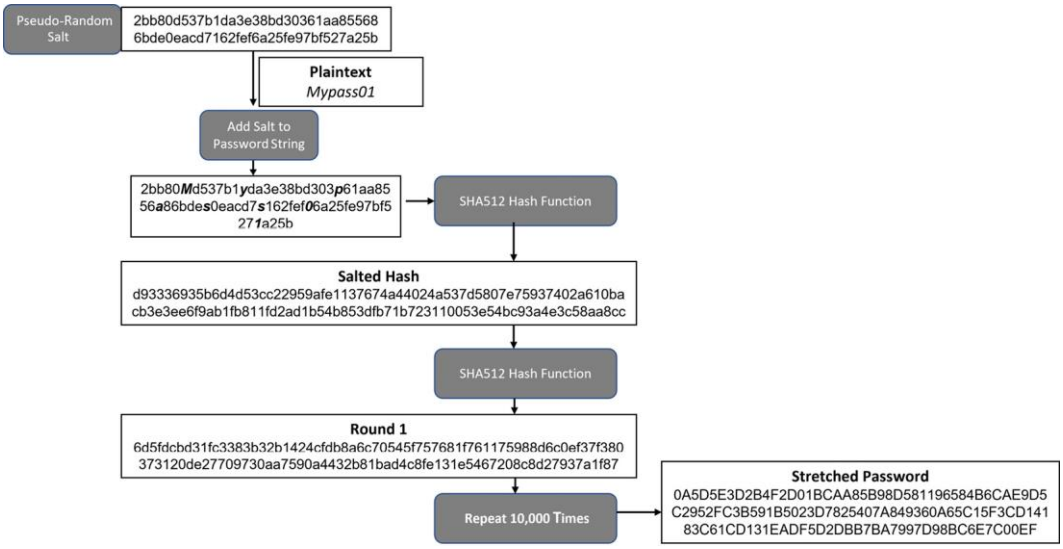


Figure 11.14 – PBKDF2 key stretching

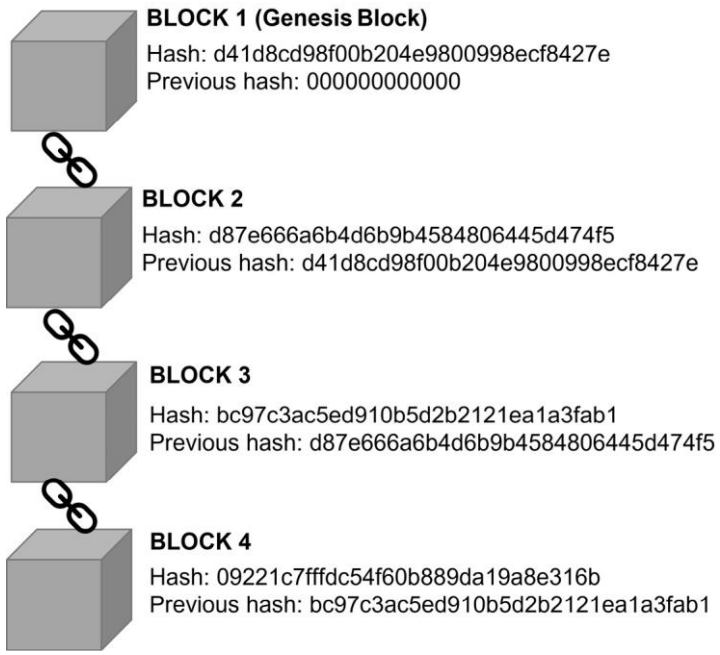


Figure 11.15 – Blockchain

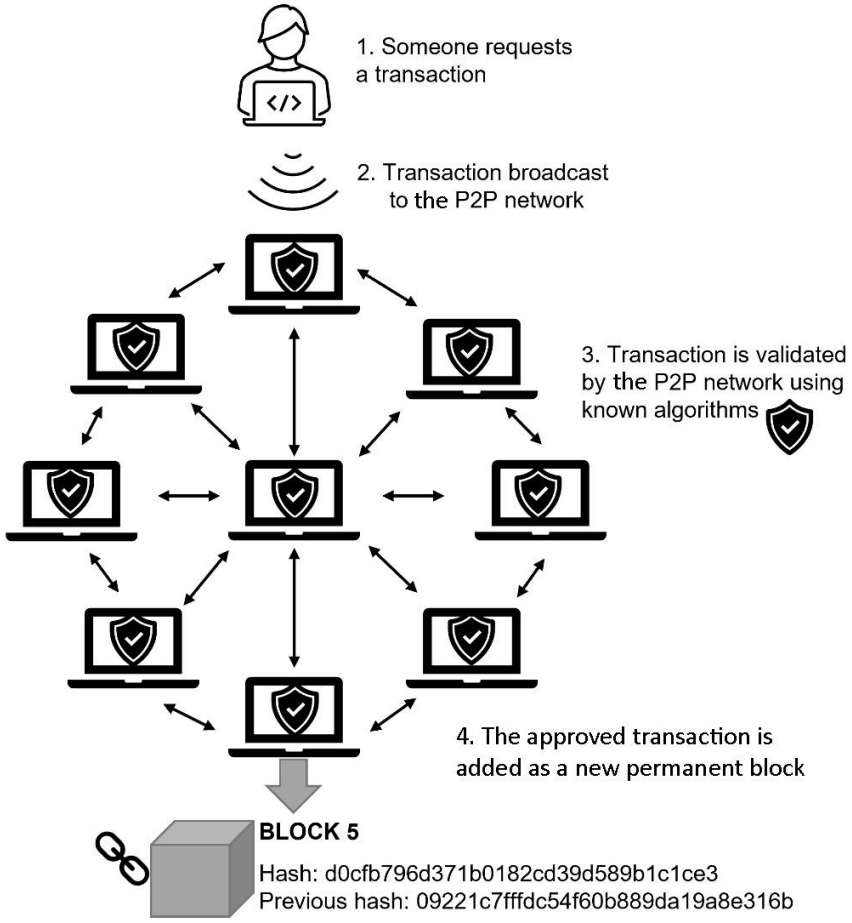


Figure 11.16 – Transaction approved by the P2P network

Code

Code11.1: Secure Hashing Algorithm (SHA)

In the following command, we have used a Linux Bash shell command to generate a hash to verify whether the bootstrap log has been tampered with:

```
sha256sum bootstrap.log
```

The output of this command is as follows:

```
1709de6f628968c14d3eed2f306bef4f39e4ab036e51386a59a487ec0
e4213fe bootstrap.log
```

Windows comes with a Command Prompt utility called `CERTUTIL -HASHFILE <Filename>`.

We can use this command to capture a hash value for the Windows operating system's kernel file:

```
certutil -hashfile ntoskrnl.exe sha256
```

The output of this command is as follows:

```
SHA256 hash of ntoskrnl.exe:
4ffa3d9c8a12bf45c4de8540f42d460bc2f55320e63caac4fdfabb
b384720b40
```

Windows PowerShell can also be used to generate hash values. The format is `Get-Filehash <Filename> -Algorithm <hashtype>`:

```
Get-FileHash ntoskrnl.exe -Algorithm SHA256
```

The output of this command is as follows:

```
Algorithm       Hash


---------       ---
-
SHA256          4FFA3D9C8A12BF45C4DE8540F42D460BC2F55320E6
3CAAC4FDFABBB384720B40
```

To address both integrity and authentication for a packet, we can use hash functions and a shared secret.

Links

For more information on NIST SP 800-38E, please see https://tinyurl.com/nist800-38e

Check out the following URL for more information on CNSA: https://tinyurl.com/nsa-cnsa-standards.

For examples of quantum computing and the threats to cryptography, go to https://tinyurl.com/quantumthreats

To read more about the heist on the Emirates based bank, go to https://tinyurl.com/deepfakeheist.

The following URL provides an interesting news article on deep fakes: https://tinyurl.com/deepfakereport

Questions

Answer the following questions to test your knowledge of this chapter:

1. Recent log analysis has revealed that archived documents have been tampered with, even though the hash-matching database shows that the values have not changed. What could have caused this?

   A. A weak symmetric cipher

   B. Hash collision

   C. An asymmetric algorithm with a small key size

   D. A poor choice of block cipher

2. Recent log analysis has revealed that archived documents have been tampered with. To mitigate this vulnerability, which of the following should *not* be used?

   A. RACE-320

   B. MD5

   C. SHA-384

   D. SHA3-256

3. Developers are creating a **File Integrity Monitoring** (**FIM**) solution to market to government agencies. What would be a good choice, considering FIPS compliance?

   A. RACE-256

   B. MD5

   C. SHA-512

   D. ECC

4. Google engineers are configuring security for a new regional data center. They are looking to implement SSL/TLS for customer-facing application servers. What would be a good choice, considering the need for speed and security?

   A. ChaCha256 and Poly1305

   B. 3DES and CBC

   C. AES256 and CBC

D. Salsa256 and CBC

5. What is used to authenticate packets that are sent over a secure SSL/TLS connection?

   A. SHA

   B. HMAC

   C. MD

   D. Key exchange

6. Hackers can gain access to encrypted data transmissions. Log analysis shows that some application servers have different blockchain cipher configurations. Which log entries would cause the most concern?

   A. GCM

   B. ECB

   C. CBC

   D. CTR

7. When you're choosing a symmetric algorithm for real-time media streaming applications, what would be the best choice?

   A. 3DES

   B. AES

   C. ChaCha

   D. RC4

8. A government department is configuring a VPN connection. They are looking for a highly secure key exchange protocol due to the threats that are being posed by nation state threat actors. What would be a good choice?

   A. AES

   B. ECDHE p521

   C. ChaCha-256

   D. SHA-512

9. What type of key agreement would *most* likely be used on IPSec tunnels?

   A. Diffie-Hellman

   B. DSA

   C. RSA

D. Salsa

10. What is a good choice regarding a signing algorithm that will work well on low-powered mobile devices?

    A. DSA

    B. RSA

    C. ECDSA

    D. HMAC

11. What is the first step in the handshake for a secure web session that's using SSL/TLS?

    A. Server hello

    B. Session key created

    C. Client hello

    D. Pre-master secret

12. A government agency needs to ensure that email messages are secure from mailbox to mailbox. It cannot be guaranteed that all SMTP connections are secure. What is the *best* choice?

    A. SSL/TLS

    B. S/MIME

    C. IPSec

    D. SSH

13. An engineer sees the following output while connecting to a router:

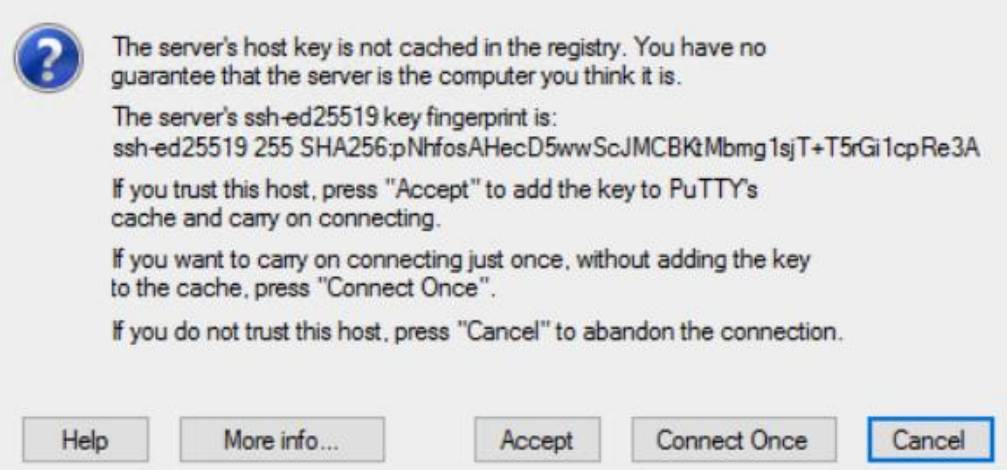


Figure 11.17 – SSH warning

The engineer logged onto the device using SSH the same day earlier. What is the most likely cause of this message?

A. Weak ciphers

B. Key rotation

C. Incorrect password

D. Incompatible cipher suite

14. While setting up a commercial customer-facing web application server, what would be a good choice regarding a key exchange that will support forward secrecy?

A. DH

B. RSA

C. ChaCha

D. ECDHE

15. What term is used to describe the message integrity that's provided by protocols such as Poly1305 and GCM?

A. Non-repudiation

B. Authenticated encryption with associated data

C. Perfect forward secrecy

D. Collision resistance

16. What would be used to provide non-repudiation when you're sending a business associate an email message?

A. TLS/SSL

B. AES-256

C. S/MIME

D. IPSec

17. A developer is protecting the password field when they're storing customer profiles in a database. What would be a good choice for protecting this data from offline attacks? Choose two.

A. PBKDF2

B. AES

C. bcrypt

D. ChaCha

18. What do Alice and Bob need to exchange before they send signed email messages to each other?

    A. Private keys

    B. Cipher suite

    C. Public keys

    D. Pre-shared keys

19. What will be used when Alice needs to sign an important business document to her colleague, Bob?

    A. Alice's public key

    B. Alice's private key

    C. Bobs public key

    D. Bobs private key

20. What encryption protocol will be used to encrypt emails while in transit, across untrusted networks, when the client has no encryption keys?

    A. SSL/TLS

    B. IPSecC

    C. SSH

    D. S/MIME

Answers

1. B
2. B
3. C
4. A
5. B
6. B
7. C
8. B

9. A
10. C
11. C
12. B
13. B
14. D
15. B
16. C
17. A and C
18. C
19. B
20. A

Chapter 12

Figures

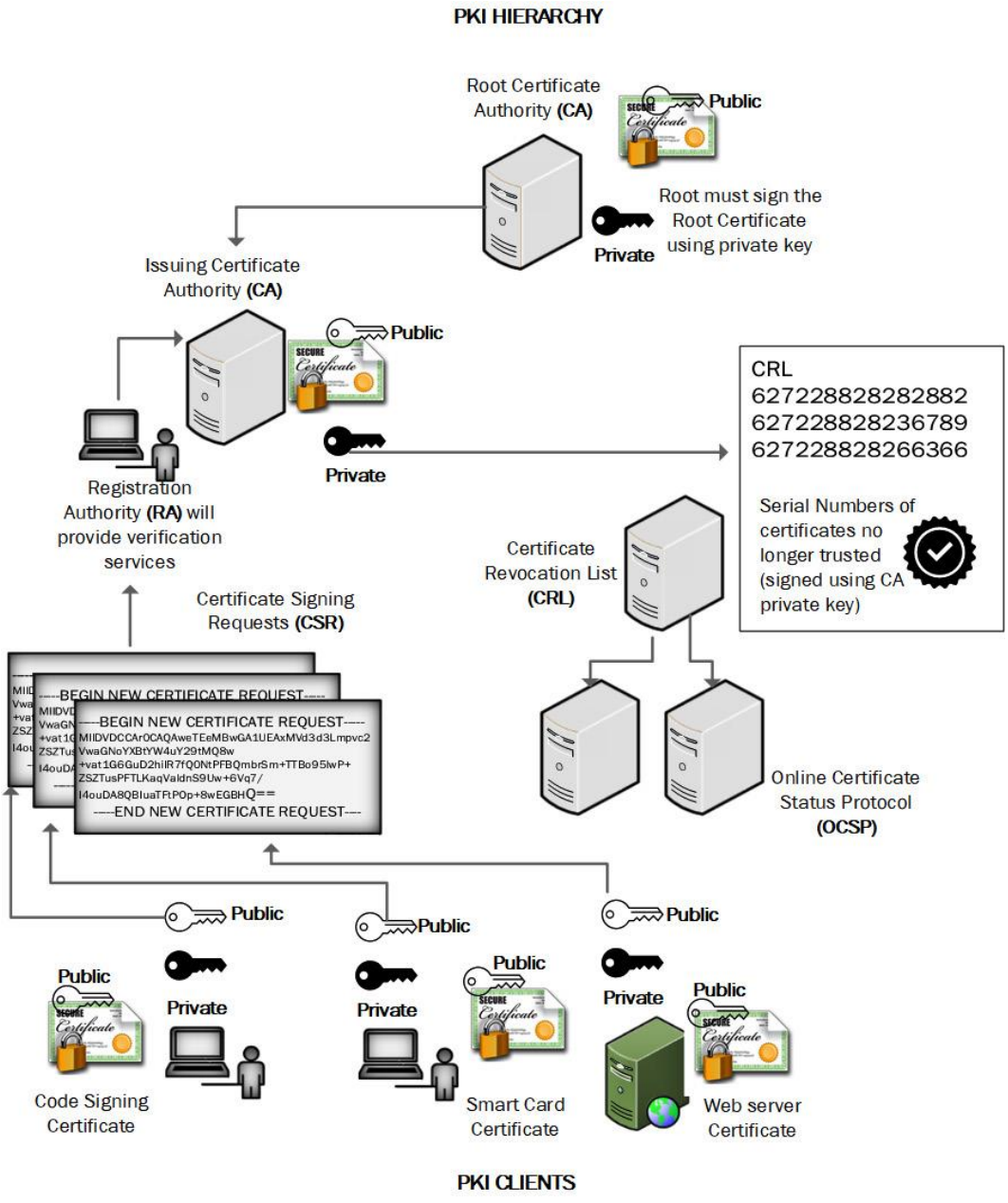


Figure 12.1 – Common components of PKI

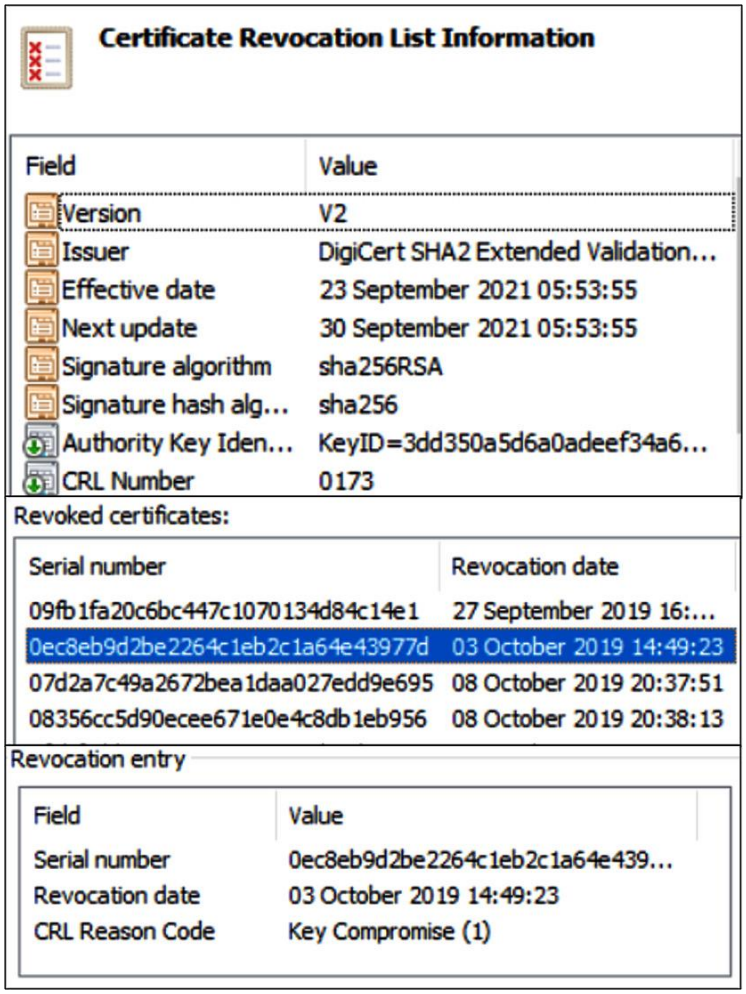


Figure 12.2 – CRL

Figure 12.3 – Wildcard certificate

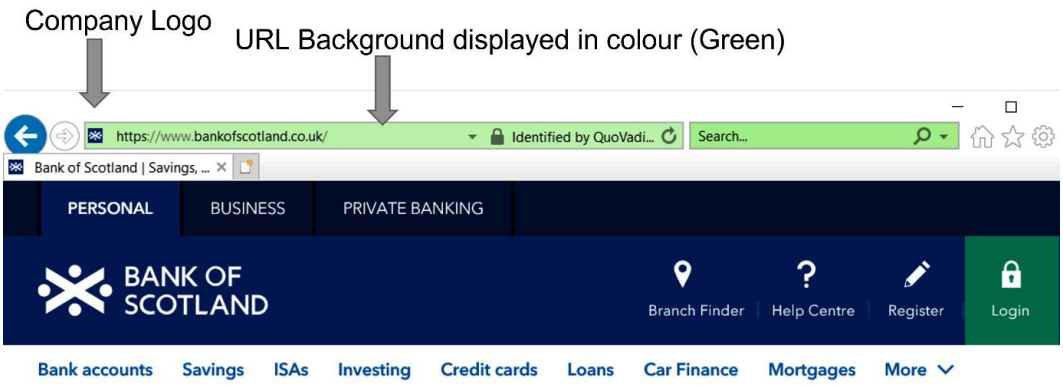


Figure 12.4 – Extended validation certificate

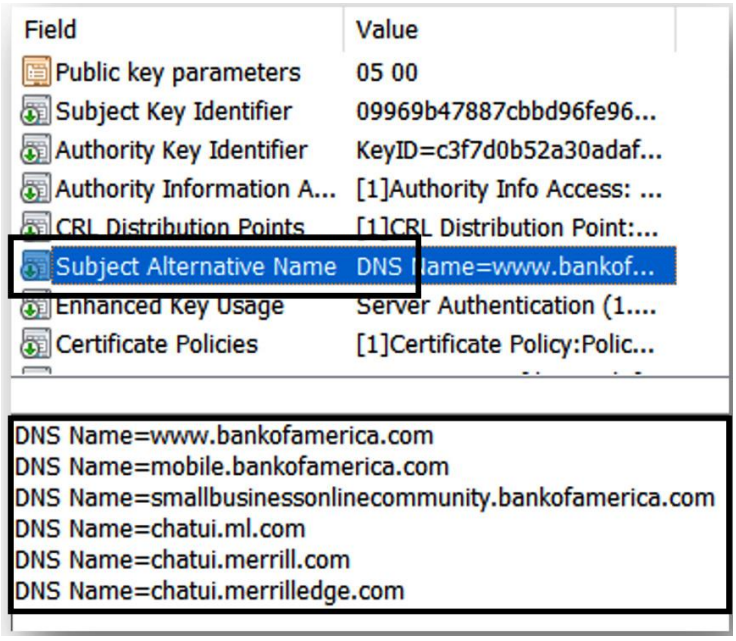


Figure 12.5 – SAN

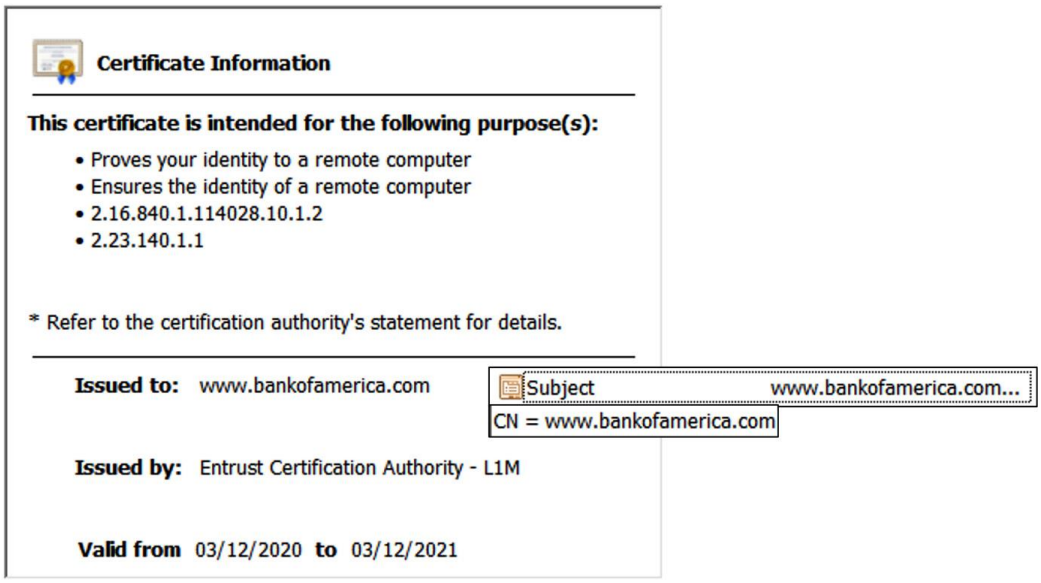


Figure 12.6 – CN extension

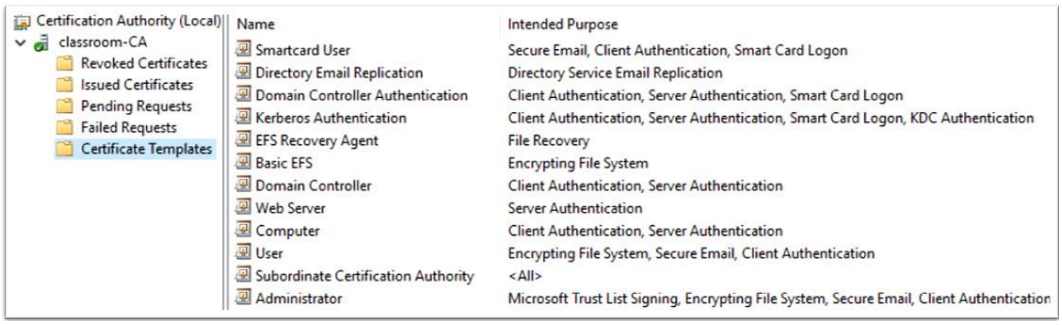


Figure 12.7 – Microsoft CA templates

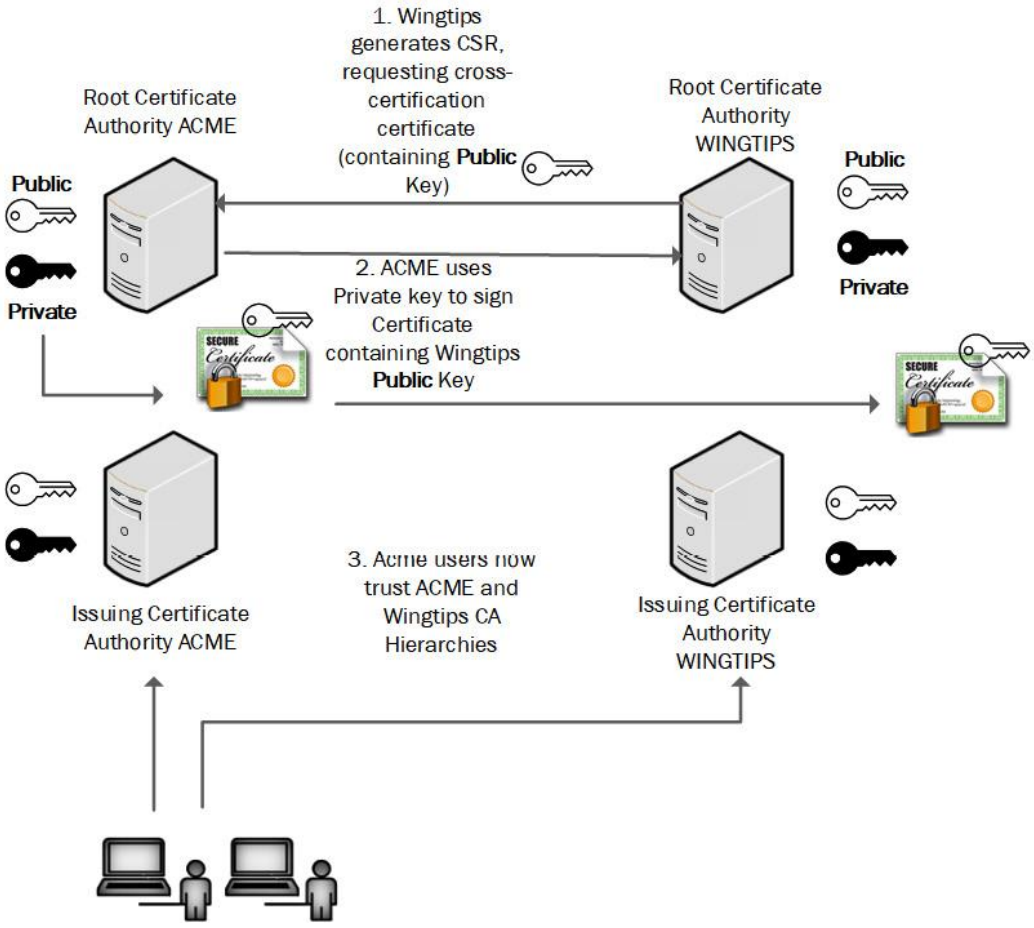


Figure 12.8 – Cross-certification certificate generation

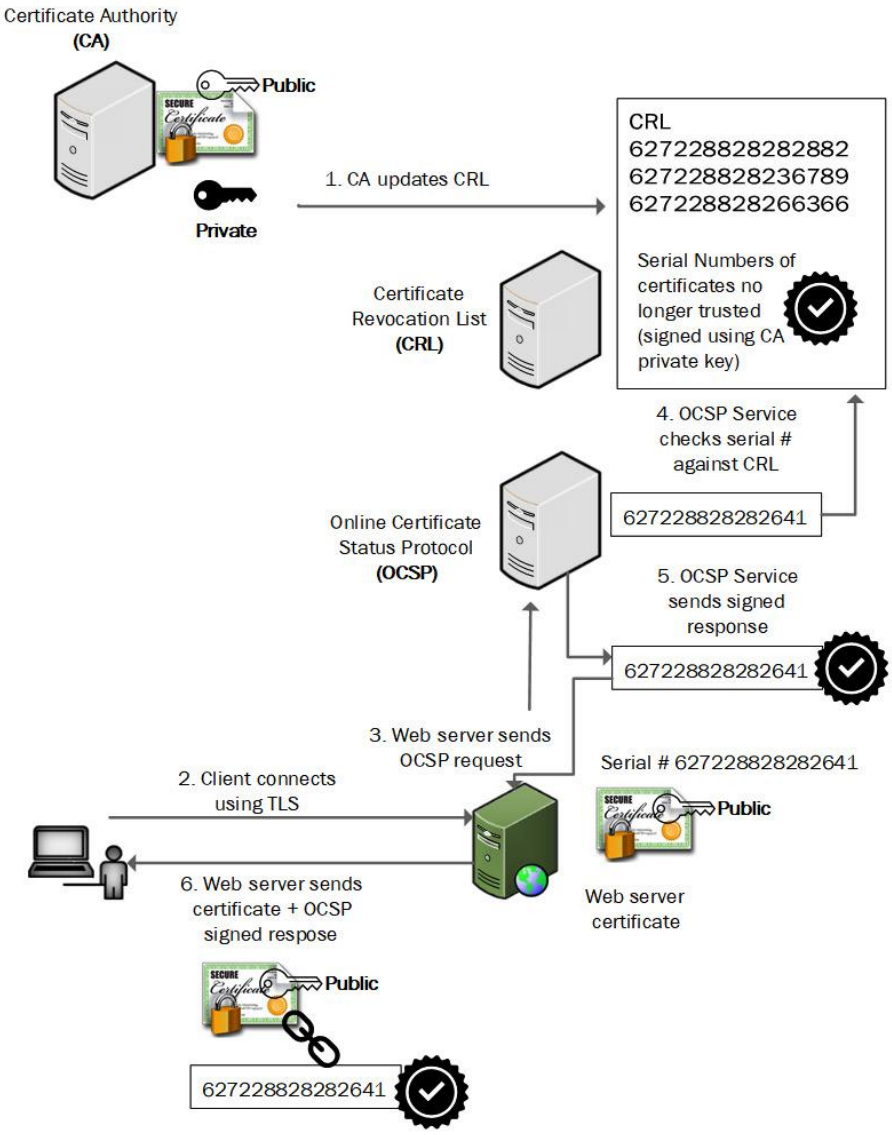


Figure 12.9 – Certificate stapling

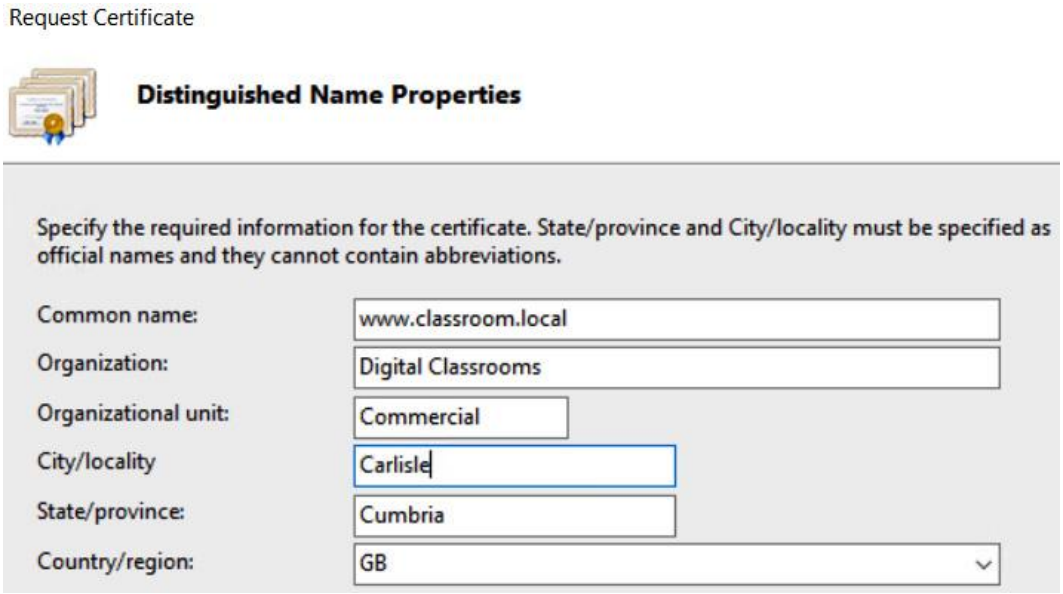


Figure 12.10 – CSR template

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEhDCCA2wCAQAwgYIxCzAJBgNVBAYTAkdCMRAwDgYDVQQIDAdDdW1icmlhMREw
DwYDVQQHDAhDYXJsaXNsZTEbMBkGA1UECgwSRGlnaXRhbCBDbGFzc3Jvb21zMRMw
EQYDVQQLDApDb21tZXJjaWFsMRwwGgYDVQQDDBN3d3cuY2xhc3Nyb29tLmxvY2Fs
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7GdXkpYp8ofm85OFzywB
mqqJDM6v+GqIZ4YCZ+xUgC17Tseqi7upg877S6h0fggHTfXA7OkN6Nelt2p1sIr5
0r4L2ssfX0/1SQZ3pagwPAow1/sFBtW8LQEh4R1lmlt88TjS6oHKb/ia/v2B3uTA
1W8z9S2xyu9fWp5b94wARU+2Ge5dTJzPj6iqTyV/kihftJtDwVRnfZLg4f257In/
+Rq12dJe+T/2Yv8q/XfVEnDls7M6HuOBbyKFSPXBipOW7xS6vvm9G6miUpTaG31A
rrBfHu4dDjtAsXu/tGQwAhTaVQFg7uoSrvCAcnVftfyCXAAnaQrnZ9qc08lo+pxg
zQIDAQABoIIBujAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTQzOTMuMjBUBgkrBgEE
AYI3FRQxRzBFAgEFDBpXSU4yMDE2LURDLmNsYXNzcm9vbS5sb2NhbAwXY2xhc3Ny
b29tXGFkbWluaXN0cmF0b3IMC0luZXRNZ3IuZXhlMHIGCisGAQQBgjcNAgIxZDBi
AgEBHloATQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUA
bAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHID
AQAwgc8GCSqGSIb3DQEJDjGBwTCBvjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAww
CgYIKwYBBQUHAwEweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYI
KoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUD
BAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQU
M2RG7j2BOT7X/wH0dX+UF0oI164wDQYJKoZIhvcNAQEFBQADggEBAGvl3PV6v7C+
wIM0I6u7kJVNFzXWFGOIytTw3aAWIjJKRzwmjZNlaejDtvz89rNHQS/3ETmDN439
7/MPnfqYLLe4CWDdgJiQrOllUN3DWw9JTbHUVjHxR4eKtHNAYy42xTnAitdenv06
WpxNwxLdny1QWPOBWiqgItkjzrqldfrCl1J2+eQ5Q3hFoXh8j4KmqftrZlJt2kx7
XMWRE5Fow9YyVgexOZzxAaeqVkJ9oMMftDvHHbrsdJC0NWLsa1Rz9WNoSFg6PhTy
xTYoP/HGS7ZXJfwSeUBC4rWdZWdKfbd9lwmXreQSgqDt3tJ5KIybtCMDl6RVLhJa
zg4HofIxWcA=
-----END NEW CERTIFICATE REQUEST-----
```

Figure 12.11 – CSR Base64 encoding

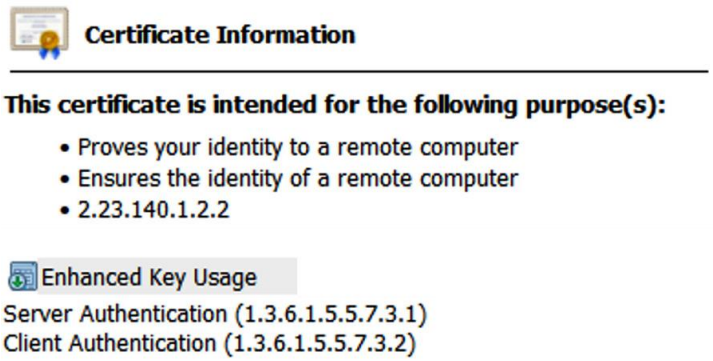


Figure 12.12 – Enhanced Key Usage extension

Links

This guidance is documented in *NIST Special Publication (SP) 800-57 Part 1 Revision 5*, found at the following link: https://tinyurl.com/800-57REV5.

Questions

1. ACME needs to request a new website certificate. Where will they send the request (in the first instance)?

   A. Root CA

B. Subordinate/intermediate CA

C. RA

D. CRL

2. Software engineers are developing a new **customer relationship management** (**CRM**) tool. They need to ensure customers will be able to verify the code is trustworthy. What type of certificate will they request?

   A. Client authentication

   B. Server authentication

   C. Digital signatures

   D. Code signing

3. Web developers have created a new customer portal for online banking. They need to ensure their corporate customers are satisfied with the security provisions when connecting to the portal. Which certificate type should they request for the portal?

   A. Wildcard certificate

   B. Extended validation

   C. Multi-domain

   D. General-purpose

4. A large e-commerce provider needs to minimize administration by allocating a single certificate to multiple sites. The sites will be country-specific, with different domain names. What would be the best choice of certificate to deliver this requirement?

   A. Wildcard certificate

   B. Extended validation

   C. General-purpose

   D. SAN

5. A multinational airline has a customer-booking portal. They need to minimize administration by allocating a single certificate to multiple sites. The sites will provide support for booking, queries, and check-in. The company-registered domain name (`WingTip.com`) will be used in each case. What would be the best choice of certificate to deliver this requirement?

   A. Wildcard certificate

   B. Extended validation

   C. General-purpose

D. SAN

6. Wingtip Aerospace needs to ensure that certificates can be trusted by government agencies as part of an ongoing collaboration project. What allows the Wingtip Aerospace certificates to be trusted by government employees?

   A. Cross-certification

   B. Chaining

   C. Wildcard certificate

   D. Extended validation

7. Which key is embedded in an X.509.v3 digital certificate?

   A. Public

   B. Private

   C. Digital signature

   D. Symmetric

8. A **chief information security officer** (**CISO**) for a large financial company is concerned that criminals may create certificates with the same CN as the company, leading to fraudulent activity. What would best protect against this threat?

   A. Wildcard certificate

   B. Extended validation

   C. Certificate pinning

   D. Certificate stapling

9. A large online retailer would like the customer web browsing experience to be low latency, with a speedy secure handshake and verification of the website certificate. What would best meet this requirement?

   A. Extended validation

   B. Certificate pinning

   C. Certificate stapling

   D. CSR

10. A user discovers that a colleague has accessed their secure password key and may have made a copy of the private key (stored on the device). What action should security professionals take to mitigate the threat of a key compromise?

    A. Publish the public key on the CRL

B. Delete the public and private keys

C. Interview the work colleague

D. Implement disciplinary proceedings against the colleague

11. Which HTTP extension will ensure that all connections to the bank's e-commerce site will always also be encrypted using the assigned X.509 certificate?

A. HTTP X-Frame headers

B. HTTP Strict Transport Security (HSTS)

C. HTTP Secure (HTTPS) Secure Sockets Layer (SSL) 3.0 Cipher Block Chaining (CBC)

D. Extended validation

12. When a public key is bundled within the UEFI firmware on a new Windows laptop, what is this termed as?

A. Exposed private keys

B. Crypto shredding

C. Improper key handling

D. Embedded keys

13. A cybercriminal has stolen the smartphone of the **chief executive officer** (**CEO**) from ACME bank. They have attempted to guess the **personal identification number** (**PIN**) code several times, eventually locking the device. After mounting the storage in a lab environment, it is not possible to access the stored data. What has likely prevented a data breach?

A. Embedded keys

B. Exposed private keys

C. Crypto shredding

D. Improper key handling

14. Several employees are required to bring their laptops into the office in order to obtain new encryption keys, due to a suspected breach within the department. What is taking place?

A. Rekeying

B. Crypto shredding

C. Certificate pinning

D. Cryptographic obfuscation

15. When an engineer connects to a switch using a **Secure Shell** (**SSH**) connection, there is a request to download and trust a new public key certificate. There was no such request when connecting from the same computer the previous day. What is the likely cause of this request?

    A. Compromised keys

    B. Exposed private keys

    C. Extended validation

    D. Key rotation

Answers

1. C
2. D
3. B
4. D
5. A
6. A
7. A
8. C
9. C
10. A
11. B
12. D
13. C
14. A
15. D

Chapter 13

Figures

Figure 13.1 – Risk management steps

Asset Customer Marketing Database			
Threat	Likelihood	Impact	Risk
Data Breach	6	9	54
Ransomware	8	9	72
Corruption	2	5	10

Figure 13.2 – Qualitative risk assessment matrix

POWERPLANT SCADA SYSTEM			
Data	Confidentiality	Integrity	Availability
Admin Information	LOW	LOW	LOW
Telemetry Data	MED	HIGH	MED
Scada Alerts	LOW	HIGH	HIGH
Aggregate score	MED	HIGH	HIGH

Figure 13.3 – CIA aggregate scoring

Production Plant Value $10,000,000				
Threat	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Annual Rate of Occurrence (ARO)	Annual Loss Expectancy (ALE)
Flood	20%	$2,000,000	2%	$40,000

Figure 13.4 – Quantitative risk assessment

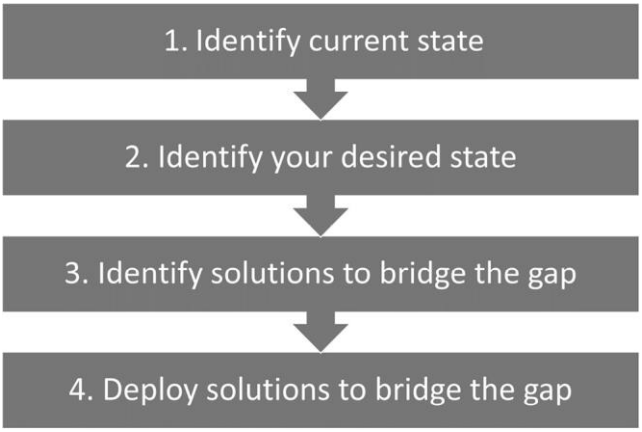


Figure 13.5 – Gap analysis

ROI = (reduction in risk – cost of control) = $

Figure 13.6 – ROI calculation

$$\frac{\text{ROI = (reduction in risk – cost of control)}}{\text{cost of control}} \text{ X 100 = \%}$$

Figure 13.7 – ROI calculation displays a percentage value

Figure 13.8 – Risk response types

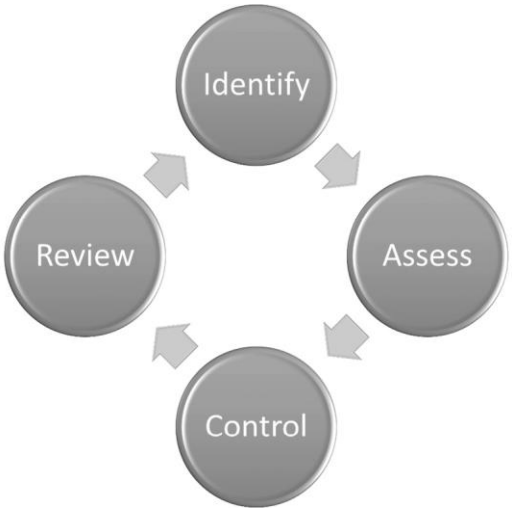


Figure 13.9 – Risk management life cycle

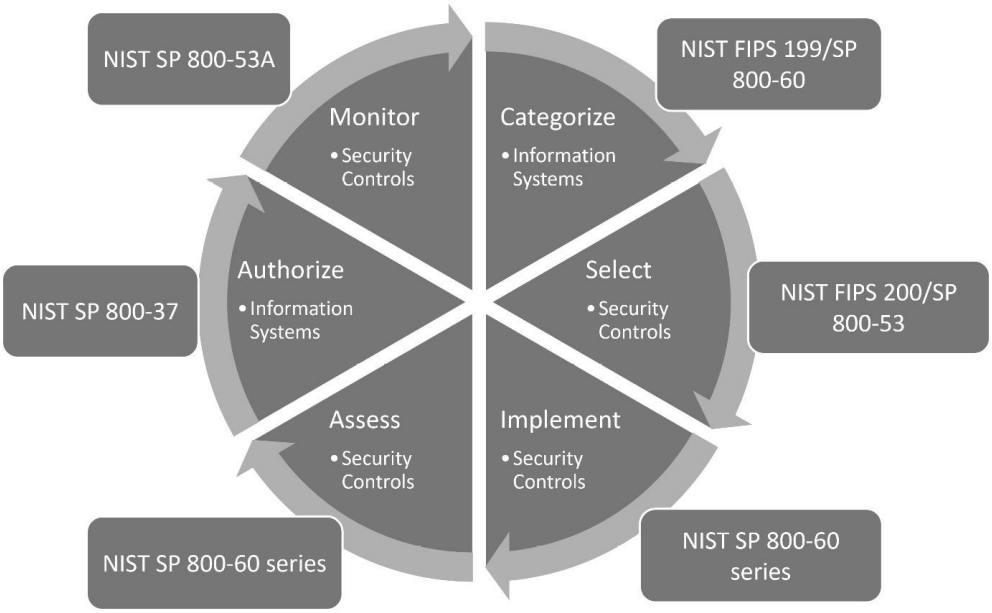


Figure 13.10 – DoD RMF

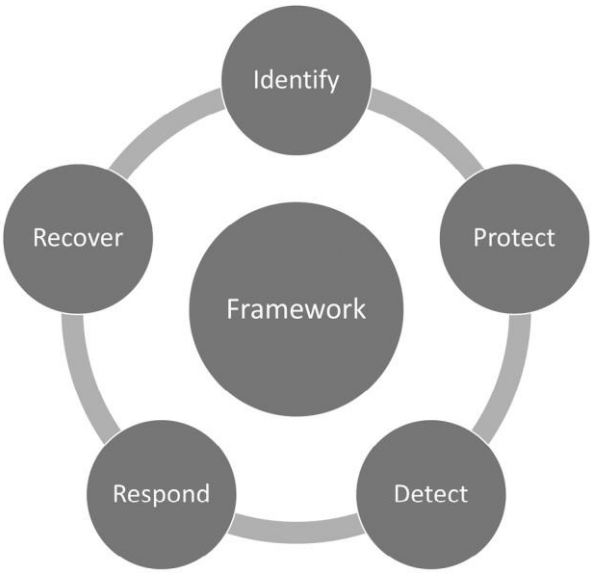


Figure 13.11 – Risk management life cycle

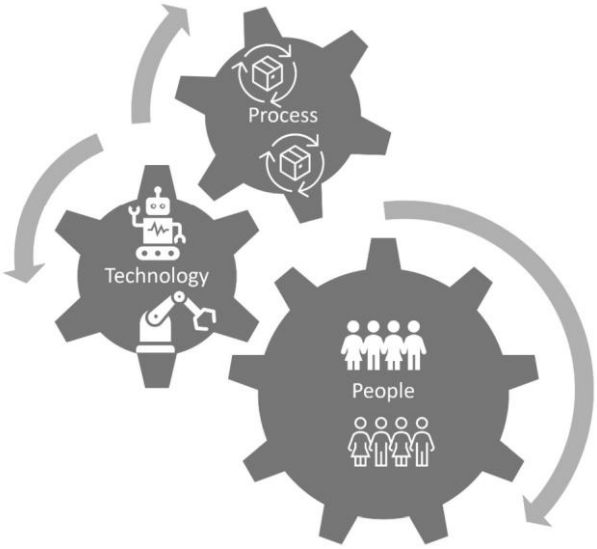


Figure 13.12 – Risk control relationship

Risk ref No.	Division	Department	Activity	Risk	Control Rating	Risk Level
1.0	IT	IT Helpdesk	User technical support	Understaffed dept cannot respond to user requests	Medium	Low
2.0	Sales	Online Sales	Process customer card payments	Inadequate security for payment card details, not PCI DSS compliant	Weak	High
3.0	HR	HR Staff	Health & Safety	Failure to comply with government safe working practices	Weak	High
4.0	Finance	Payroll	Salary payments	Incorrect employee payslips due to lack of training	Weak	Med

Figure 13.13 – Sample risk register

Links

The exact details for this framework can be seen in *DoDI 8510.01*, available at the following link: https://tinyurl.com/DoDRMF

To understand in more detail how an enterprise can implement this framework, see the downloadable document at https://tinyurl.com/NISTCyberSecFramework

More information on FEDRAMP can be found at the following link: https://www.fedramp.gov/.

More information can be found at the following links:

- https://tinyurl.com/cloudCSA
- https://tinyurl.com/cloudccmatrix

More information on ISO/IEC 27002:2013 can be found at the following link: https://tinyurl.com/27000iso.

Questions

Answer the following questions to test your knowledge of this chapter:

1. What type of risk assessment would use likelihood and impact to produce a numerical risk rating?
    A. Qualitative assessment
    B. Gap assessment
    C. Quantitative risk assessment
    D. Impact assessment
2. What type of risk assessment would use metrics including asset value, monetary loss during an event, and a value that could be expected to be lost during the course of a year?
    A. Qualitative assessment
    B. Gap assessment
    C. Quantitative risk assessment
    D. Impact assessment
3. What is the metric that is used to calculate the loss during a single event?
    A. Efficiency factor (EF)
    B. ALE
    C. SLE

D. ARO

4. If my database is worth $100,000 and a competitor steals 10% of the records during a breach of the network and this happens twice in a year, what is the SLE?

   A. $100,000

   B. $1,000

   C. $20,000

   D. $10,000

5. If my database is worth $100,000 and a competitor steals 10% of the records during a breach of the network and this happens twice in a year, what is the ALE?

   A. $200,000

   B. $1,000

   C. $20,000

   D. $10,000

6. A company currently loses $20,000 each year due to IP breaches. A **managed security service provider** (**MSSP**) guarantees to provide 100% protection for the database over a 5-year contract at an annual cost of $15,000 per annum. What is the ROI in $?

   A. $75,000

   B. $25,000

   C. $125,000

   D. $2,500

7. If my risk management team need to understand where the business may be lacking security controls, what should they perform?

   A. Qualitative assessment

   B. Gap assessment

   C. Quantitative risk assessment

   D. Impact assessment

8. What type of risk response would purchasing cyber liability insurance be classed as?

   A. Transfer

   B. Accept

   C. Avoid

D. Mitigate

9. What would be considered both a deterrent and useful security practice to ensure employees' job performance can be audited when they are not present?

   A. Job rotation

   B. Mandatory vacation

   C. Least privilege

   D. Auditing

10. What is the term for risk that is present within an industry, prior to any controls?

    A. Remaining

    B. Residual

    C. Inherent

    D. Acceptance

11. What is the term for risk that remains within an industry, after the deployment of security controls?

    A. Remaining

    B. Residual

    C. Inherent

    D. Acceptance

12. What is the metric that an organization can use to measure the amount of time that was taken to restore services?

    A. MTTR

    B. MTBF

    C. ALE

    D. ARO

13. What is the metric that an organization can use to measure the reliability of a service?

    A. MTTR

    B. MTBF

    C. ALE

    D. ARO

14. What type of risk response may be considered by a financial start-up company with a high-risk appetite if the potential rewards are significant and the risk is minimal?

    A. Transfer

    B. Accept

    C. Avoid

    D. Reject

15. What is a good practice when assigning users privileges to reduce the risk of overprivileged accounts?

    A. SoD

    B. Job rotation

    C. Mandatory vacation

    D. Least privilege

16. What is an organizational policy that would make it less likely that a user will insert a **Universal Serial Bus** (**USB**) storage device that they received at an exposition?

    A. Training and awareness

    B. Auditing

    C. DLP controls

    D. AUP

17. What will an enterprise use to track activities that may lead to enterprise risk?

    A. Key risk indicators

    B. Risk appetite

    C. Risk tolerance

    D. Trade-off analysis

18. What is the term that is used to describe the situation where a vendor has proprietary technology that makes it difficult for a customer to switch vendor?

    A. Vendor risk

    B. Vendor lock-in

    C. Third-party liability

    D. Vendor management plan

19. If a customer is concerned that a third-party development team may go bust during an engagement, what can they use to ensure they will have access to the source code?
    A. Change management
    B. Staff turnover
    C. Peer code review
    D. Source code escrow
20. What is the metric that an organization should use to calculate the total loss during a year?
    A. MTTR
    B. MTBF
    C. ALE
    D. ARO

Answers

1. A
2. C
3. C
4. D
5. C
6. B
7. B
8. A
9. B
10. C
11. B
12. A
13. B
14. B
15. D
16. A

17. A

18. B

19. D

20. D

Chapter 14

Figures

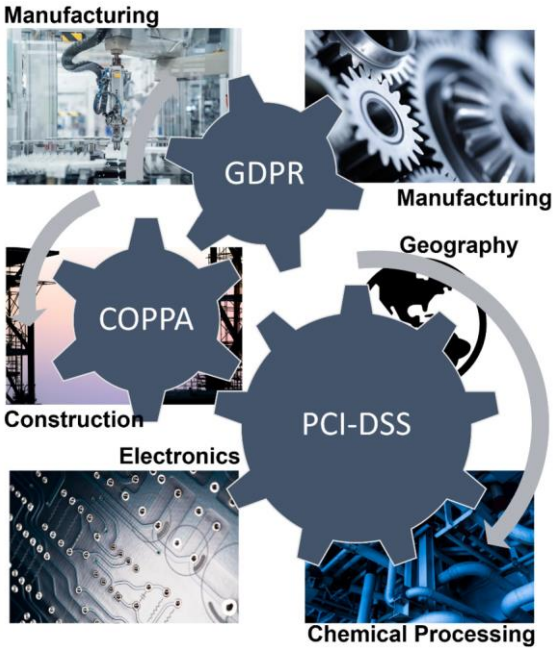


Figure 14.1 – Integrating diverse industries

Data Classification	Description
Public data	This data can be freely used, reused, and redistributed without repercussions. Examples include press releases and marketing bulletins.
Internal-only data	Data that is accessible to internal company employees who are assigned access. Examples include business plans and internal e-mail.
Confidential data	Data that requires specific authorization and/or clearance. Examples include cardholder data and social security numbers.
Restricted data	Loss would result in a significant business impact. Examples include research data and intellectual property.

Figure 14.2 – Data classification

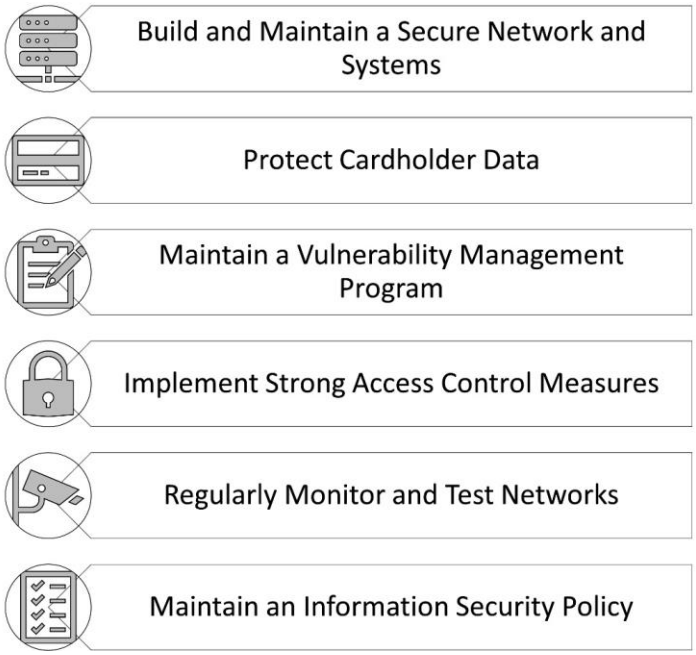


Figure 14.3 – PCI DSS requirements

Role	Description
Data Controller	The data controller is the business or organization that is accountable for GDPR compliance.
Data Processor	The processor can be the business or a third party. An example is the payroll service.
Data Protection Officer (DPO)	A DPO is responsible for overseeing the data protection approach, strategy, and its implementation. The DPO is responsible for GDPR compliance.
Supervisory Authority	A public authority in an EU country responsible for monitoring compliance with GDPR. In the U.S., it is **the Federal Trade Commission**.

Figure 14.4 – GDPR roles

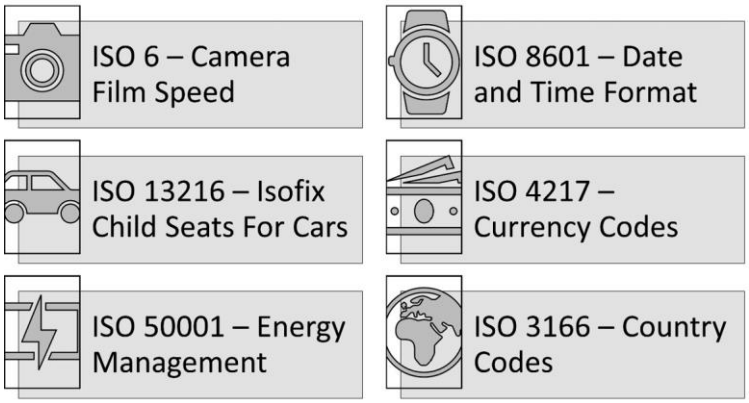


Figure 14.5 – ISO standards examples

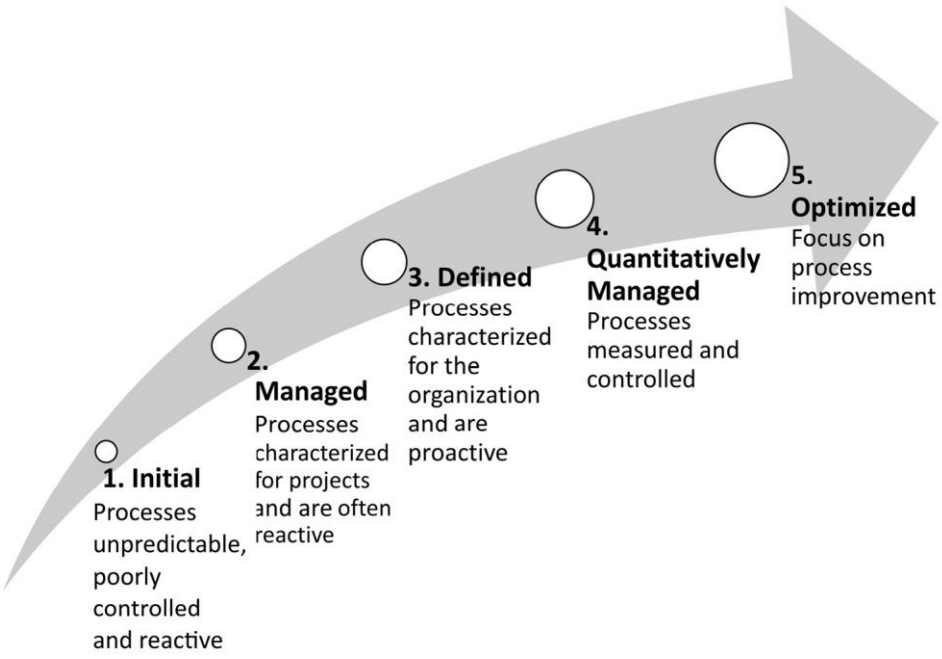


Figure 14.6 – CMMI maturity levels

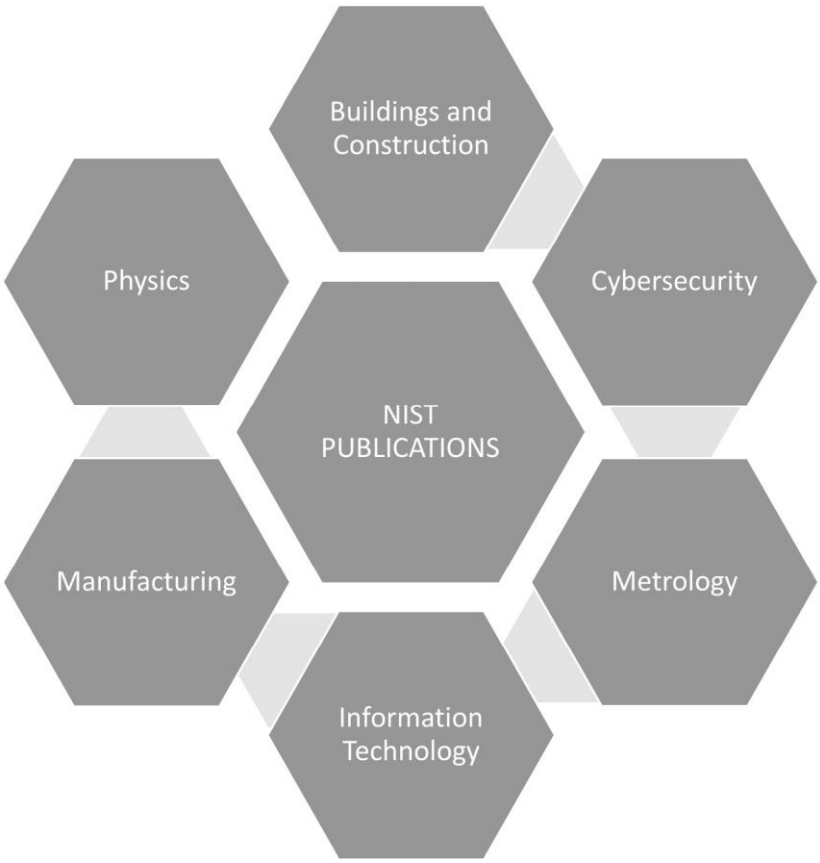


Figure 14.7 – NIST supported industries

CCRA recognition for components up to EAL 2 and ALC_FLR only

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Samsung Electronics Co Ltd

for

Samsung Galaxy Devices on Android 10 - Fall

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2020-10-15

Validation Report Number: CCEVS-VR-VID11109-2020

CCTL: Gossamer Security Solutions

Assurance Level: PP Compliant

Protection Profile Identifier:
PP-Module for VPN Client Version 2.1
Protection Profile for Mobile Device Fundamentals Version 3.1
Extended Package for Wireless LAN Client Version 1.0

Original Signed By

Director, Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership

Figure 14.8 – CC Certificate of compliance

Certified Products	Examples
Access Control Devices and Systems	NetIQ Access Manager, Hewlett Packard Storage Manager Software
Boundary Protection Devices and Systems	WatchGuard NGFW, SonicWall Firewall
Data Protection	Samsung Knox File Encryption, McAfee Data Loss Prevention (DLP)
Databases	Microsoft SQL Server 2019, IBM DB2
Detection Devices and Systems	Tripwire Enterprise, Trend Micro Deep Security
ICs, Smart Cards, and Smart Card-Related Devices and Systems	Samsung Microcontroller for Smart Card, NXP Secure Smart Card Controller
Key Management Systems	Fortix Security Suite, Verizon UniCERT
Mobility	MobileIron, BlackBerry Unified Endpoint Management (UEM), VMware Workspace ONE
Multi-Function Devices	HP Digital Sender, Xerox PrimeLink Copier/Printer
Network and Network-Related Devices and Systems	Cisco ASA 9.12, Dell EMC Networking SmartFabric (Storage Area Network)
Operating Systems	Red Hat Enterprise, macOS Catalina, Microsoft Windows 10
Products for Digital Signatures	Thales Luna K7 Cryptographic Module, DocuSign Signature Appliance
Trusted Computing	TPM Firmware

Figure 14.9 – CC categories and examples

CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01	Establish, document, approve, communicate, apply, evaluate, and maintain, audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	
A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk-Based Planning Assessment	
A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	Audit and Assurance
A&A-05	Define and implement an audit management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and a review of past reports and supporting evidence.	Audit Management Process	
A&A-06	Establish, document, approve, communicate, apply, evaluate, and maintain, a risk-based corrective action plan to remediate audit findings, and review and report remediation status to relevant stakeholders.	Remediation	

Figure 14.10 – CSA STAR Level 1 compliance

Links

You can get more information about the PCI DSS requirements by visiting the following link: https://www.pcisecuritystandards.org.

For more information about the ISO, you can visit the following link: https://www.iso.org/home.html

Visit the following link for more details on the NIST SP800 series: https://tinyurl.com/nist800series.

More information about the FTC and COPPA can be found by visiting the following link: https://tinyurl.com/copparegs.

To view a comprehensive list of certified products, please visit the following link: https://www.commoncriteriaportal.org/products/.

For more details on personal certification, visit the following link: https://ccsk.cloudsecurityalliance.org/en.

For up-to-date lists of export controls concerning organizations within the US, visit the following URL: https://www.trade.gov/us-export-controls.

For export controls concerning the United Kingdom, visit the following link: https://www.gov.uk/business-and-industry/export-controls.

For more details on the NSA contractor, refer to the following URL: https://tinyurl.com/nsawhistleblower

For more information regarding GDPR, you can visit the following URL: https://gdpr.eu/

You can visit the following link for more information on **NIST SP800-47**: https://tinyurl.com/nist80047.

More information on the CSA code of conduct can be found at the following link: https://tinyurl.com/csagdprcompliance.

Questions

Here are a few questions to test your understanding of the chapter:

1. What must a government agency consider when planning to store sensitive data with a global **CSP**?

    A. Data sovereignty

    B. Data ownership

    C. Data classification

    D. Data retention

2. Who is accountable for the storage and protection of customer data? They must ensure that they implement controls to meet legal and regulatory requirements.

    A. Data controller

    B. Data protection officer

    C. Data processor

    D. Supervisory authority

3. A CISO is assessing regulatory requirements for hospital employees and patient data (within Europe). What type of information will need to be protected and which regulation will be most important? (Choose two)

   A. GDPR

   B. Financial records

   C. Intellectual property

   D. PII

   E. COPPA

4. A multinational company wants the assurance that data will not be accessible when their contract with a **CSP** expires. What technology may be applicable?

   A. Crypto Erase

   B. Pulping

   C. Shredding

   D. Degaussing

5. A global automobile manufacturer must ensure that its products are compatible with its worldwide customer base. What regulations or standards will be most important?

   A. Export control regulations

   B. General Data Protection Regulation (GDPR)

   C. International Organization for Standardization (ISO)

   D. National Institute of Standards and Technology (NIST)

6. A SaaS provider has several products designed to attract a young audience, while revenue is generated by advertising and subscriptions within the US. What regulations will be the most important for the provider?

   A. Capability Maturity Model Integration (CMMI)

   B. National Institute of Standards and Technology (NIST)

   C. Children's Online Privacy Protection Act (COPPA)

   D. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

7. A SaaS provider has several commercial products to assist with an automobile manufacturer. They must assure potential customers that the cloud provider is secure and trustworthy. What accreditation can the SaaS provider attain to appeal to its customers?

   A. International Organization for Standardization (ISO)

B. Capability Maturity Model Integration (CMMI)

C. National Institute of Standards and Technology (NIST)

D. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

8. A software development company is trying to win a contract for a US. Federal Government agency. They must assure the customer that they have a robust security framework for the delivery of software and services. What is the most relevant?

   A. International Organization for Standardization (ISO)

   B. Capability Maturity Model Integration (CMMI)

   C. National Institute of Standards and Technology (NIST)

   D. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

9. What compliance will be most important to a US-based e-commerce retailer with respect to the storage of cardholder data and electronic transactions?

   A. Payment Card Industry Data Security Standard (PCI DSS)

   B. International Organization for Standardization (ISO)

   C. Interconnection security agreement (ISA)

   D. Non-disclosure agreement (NDA)

10. A smartcard manufacturer needs to sell products to a global market. They need to show compliance using internationally agreed-upon protocols. What would be a useful accreditation or assurance that their products have been evaluated and will meet the security requirements of their customers?

    A. International Organization for Standardization (ISO)

    B. Capability Maturity Model Integration (CMMI)

    C. National Institute of Standards and Technology (NIST)

    D. Common Criteria (CC)

11. What regulatory body is intended to protect the personal data of **EU** citizens?

    A. General Data Protection Regulation (GDPR)

    B. National Institute of Standards and Technology (NIST)

    C. International Organization for Standardization (ISO)

    D. Common Criteria (CC)

12. A US smartcard manufacturer needs to sell its products in a global market. They need to ensure that the technology is not sold to countries or governments hostile to the US. What guidance or regulations should they consult?

    A. Due care

    B. Export controls

    C. Legal holds

    D. E-discovery

13. A government department has data privacy requirements, and they need to have employees and service providers sign this agreement. They should be made aware of the strict terms of this agreement and the penalties that may be forthcoming. What type of agreement will be important?

    A. Service level agreement (SLA)

    B. Master service agreement (MSA)

    C. Non-disclosure agreement (NDA)

    D. Memorandum of understanding (MOU)

14. A large multinational company intends to purchase multiple products on a rolling contract from a **CSP**. They need to document payment terms, dispute resolution, intellectual property ownership, and geographic operational locations within the scope of the contract. What type of contract would be most suitable?

    A. Service level agreement (SLA)

    B. Master service agreement (MSA)

    C. Memorandum of understanding (MOU)

    D. Operational-level agreement (OLA)

15. Wingtips Corporation would like to build resiliency into its network connections. They are working with an **Internet Service Provider** (**ISP**) that proposes a highly available MPLS solution. To ensure the vendor is able to deliver the service with 99.999% uptime, what documentation will be important?

    A. Service level agreement (SLA)

    B. Memorandum of understanding (MOU)

    C. Interconnection security agreement (ISA)

    D. Operational level agreement (OLA)

16. What agreement should be used when business partners need to share data? This agreement may stipulate a timeline for the information exchange to be supported, security requirements, data types that will be exchanged, and the actual sites that will be part of the data interchange.

    A. Service level agreement (SLA)

    B. Master service agreement (MSA)

    C. Memorandum of understanding (MOU)

    D. Interconnection security agreement (ISA)

17. What agreement ensures that the customer data will be protected by the service provider and that agreed-upon steps are in place if data breaches or any adverse action were to occur?

    A. Non-disclosure agreement (NDA)

    B. Memorandum of understanding (MOU)

    C. Interconnection security agreement (ISA)

    D. Operational level agreement (OLA)

    E. Privacy level agreement (PLA)

18. An investigation is to be performed on an employee suspected of stealing company **Intellectual Property** (**IP**). What must be done first to ensure that the data is not deleted?

    A. Due care

    B. Export controls

    C. Legal holds

    D. E-discovery

19. An investigation is to be performed on an employee suspected of stealing company **Intellectual Property** (**IP**). There are over 10 gigabytes of data stored across several information systems. What must be done to ensure that the relevant data is collected?

    A. Due care

    B. Export controls

    C. Legal holds

    D. E-discovery

20. What document may be used when business partners need to document responsibilities? This document will not be written by lawyers and is intended to formalize a verbal agreement or a handshake.

    A. Service level agreement (SLA)

    B. Master service agreement (MSA)

    C. Memorandum of understanding (MOU)

    D. Interconnection security agreement (ISA)

Answers

1. A
2. A
3. A, D
4. A
5. C
6. C
7. D
8. B
9. A
10. D
11. A
12. B
13. C
14. B
15. A
16. D
17. E
18. C
19. D
20. C

Chapter 15

Figure

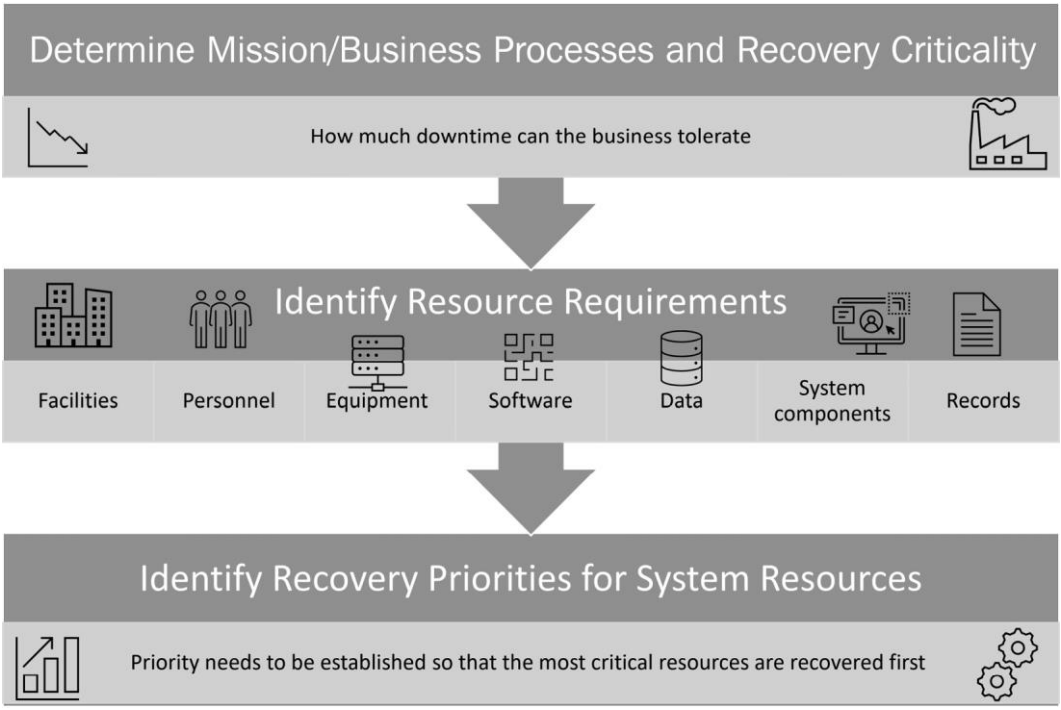


Figure 15.1 – BIA purpose

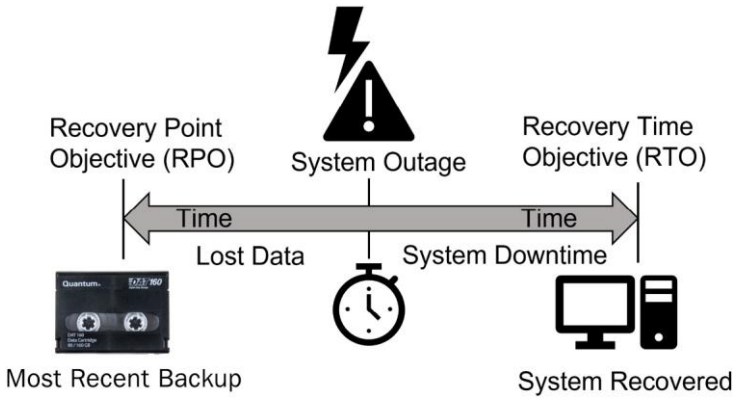


Figure 15.2 – Recovery Point Objective

Mission-Essential Function	MTD	RTO	RPO
Customer booking system	24 hours	4 hours	1 hour
Invoice payment system	96 hours	24 hours	1 hour

Figure 15.3 – Mission-essential functions

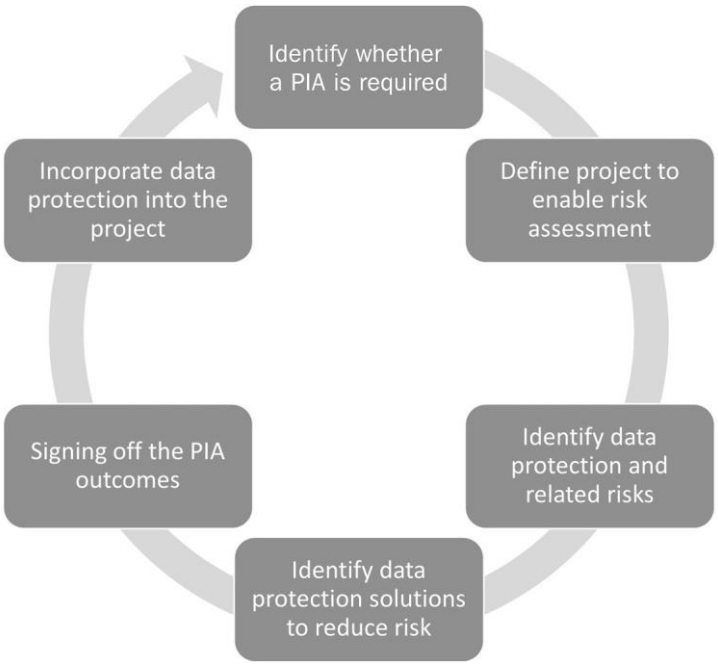


Figure 15.4 – PIA

Figure 15.5 – NIST-recommended contingency plan

Figure 15.6 – Elements of a COOP

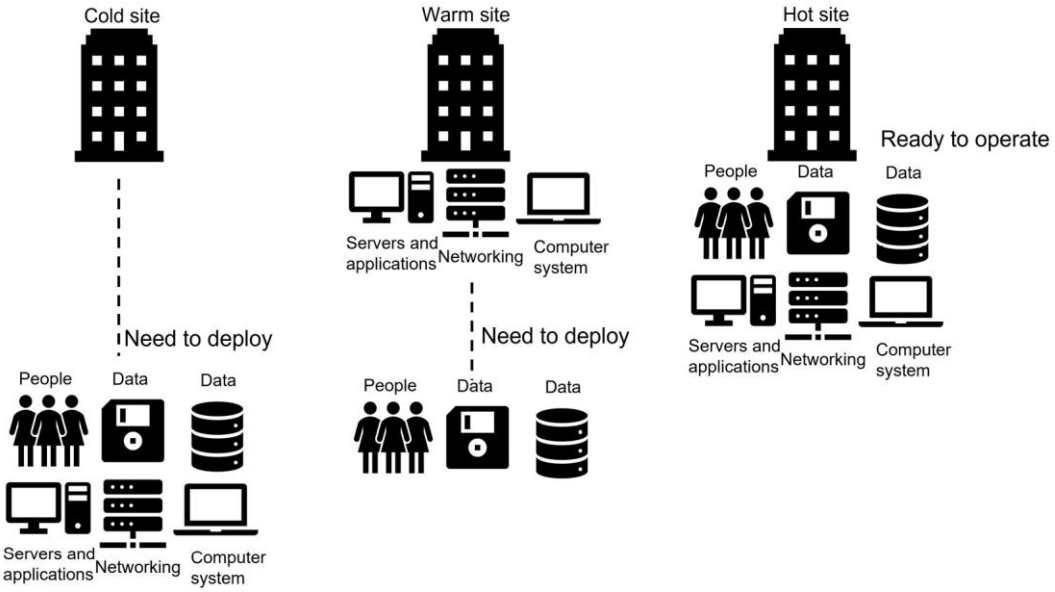


Figure 15.7 – Cold, warm, and hot sites

Figure 15.8 – Mobile data center (© Todd Huffman – Flickr images)

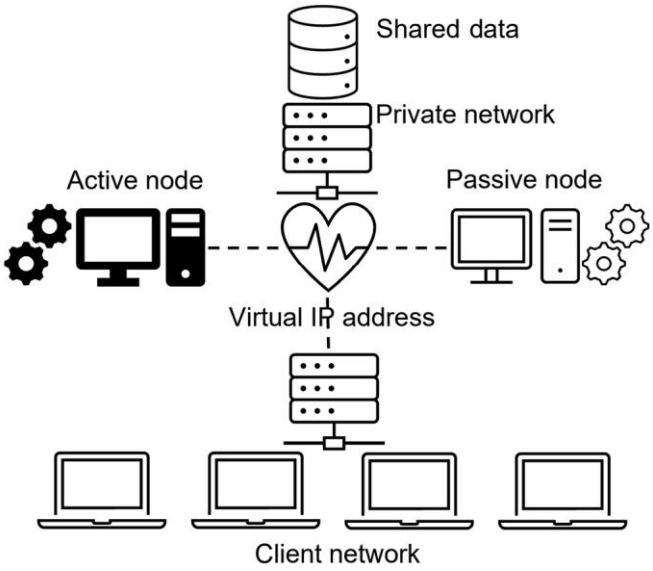


Figure 15.9 – Failover cluster

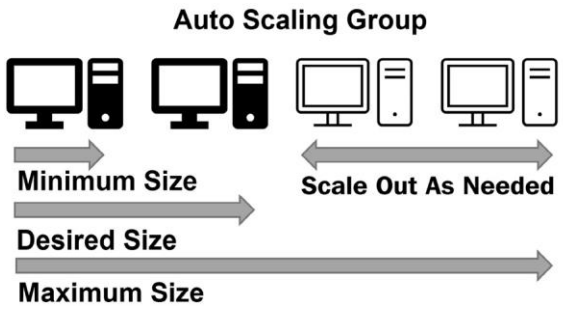


Figure 15.10 – Autoscaling

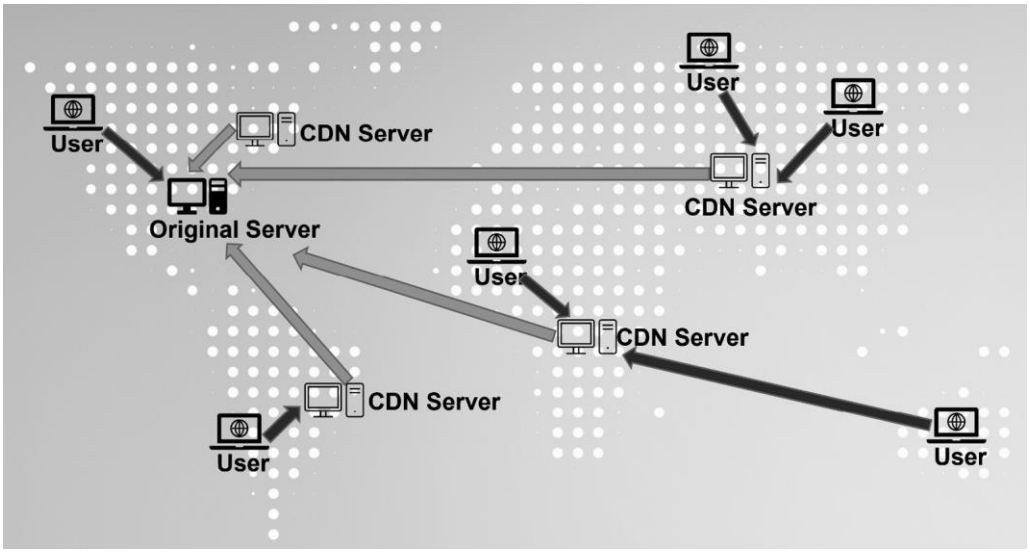


Figure 15.11 – CDN

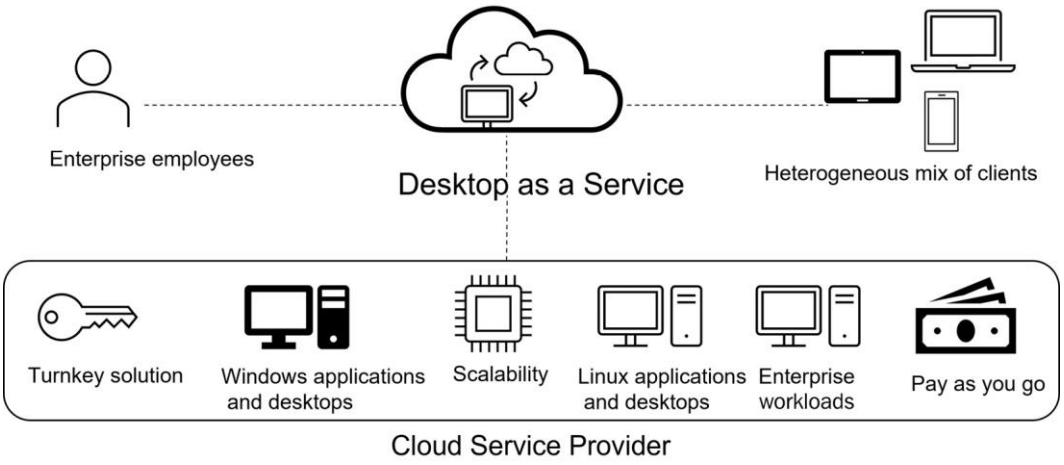


Figure 15.12 – Desktop as a Service

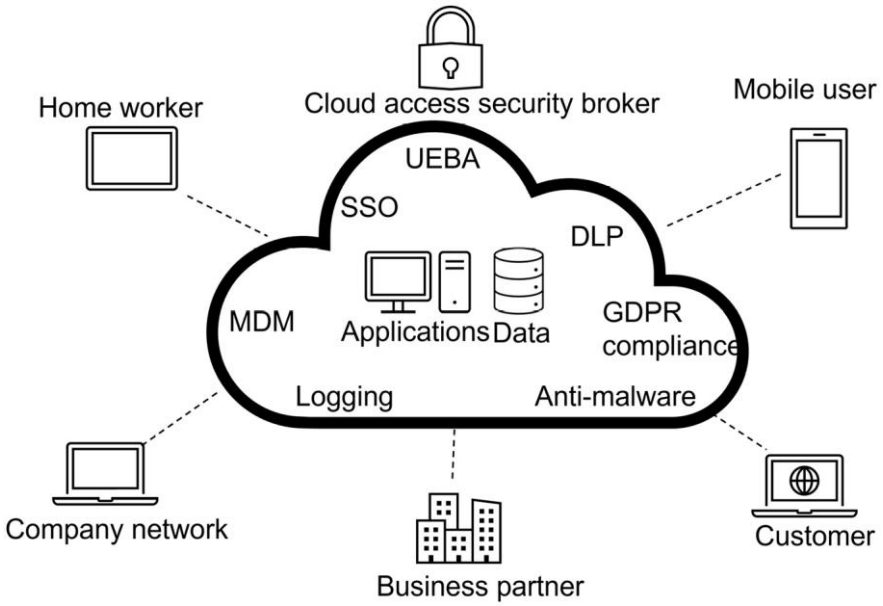


Figure 15.13 – CASB

Links

There is a useful planning document that can be downloaded, for use in this type of assessment, at the following URL: https://tinyurl.com/GDPR-DPIA

plan for the restoration of business functions in the event of serious disruptions.

Organizations that require guidance on the effective creation and management of BCPs should reference **ISO 22301** for an overview of the standard. The following publication may be useful: https://tinyurl.com/isopub22301.

More information on **NIST SP800-34** can be found at this URL: https://tinyurl.com/nistsp80034.

Questions

Here are a few questions to test your understanding of the chapter:

1. What metric is used by planners for a critical resource that would cause severe adverse effects for the enterprise? This metric forms the line in the sand that cannot be crossed.
    A. Recovery point objective
    B. Recovery time objective
    C. Recovery service level
    D. Maximum tolerable downtime
2. What metric is a goal set by the enterprise to ensure a critical service will be operational within a specified timeframe?
    A. Recovery point objective
    B. Recovery time objective
    C. Recovery service level
    D. Mission-essential functions
3. What is a planning objective used when the restoration of a critical service will also require data to be restored?
    A. Recovery point objective
    B. Recovery time objective
    C. Recovery service level
    D. Mission-essential functions
4. What planning objectives ensure that critical services are recovered first, while other functional elements, such as printing customer tickets, are given a lower priority?
    A. Recovery point objective
    B. Recovery time objective
    C. Recovery service level
    D. Mission-essential functions
5. What type of assessment should be performed by an organization that stores, transmits, or processes data that contains private information?
    A. Business impact assessment
    B. Privacy impact assessment

C. RISK assessment

D. Safety assessment

6. An organization has leased office space and suitable facilities for computing equipment. The intention is to relocate personnel and systems and become operational in the event that the main office location is unavailable. What have they used?

   A. A cold site

   B. A warm site

   C. A hot site

   D. A mobile site

7. A planning team has identified a requirement for a site, housing equipment and facilities ready for the business to use. Personnel and data will need to be moved to the site to become operational. What have they identified?

   A. A cold site

   B. A warm site

   C. A hot site

   D. A mobile site

8. An e-commerce site needs a failover location that has all the equipment and data needed for the business to continue operations. The site should allow the organization to switch operations within a short time frame. What should they use?

   A. A cold site

   B. A warm site

   C. A hot site

   D. A mobile site

9. What kind of scalability have we identified when we add additional **Central Processing Units** (**CPUs**), **Random Access Memory** (**RAM**), faster disk **input/output** (**I/O**), and additional network connections?

   A. Vertically scalability

   B. Replication

   C. Performance scalability

   D. Horizontally scalability

10. What type of scalability is achieved by adding more workloads in the form of additional computers or compute nodes? This can work well if the resources can be deployed on demand using autoscaling.

    A. Vertically scalability

    B. Replication

    C. Performance scalability

    D. Horizontally scalability

11. What type of data replication will be needed where there can be no time lag, where the data is written or committed to both systems at the same time (this is the more costly solution)?

    A. Symmetric

    B. Cloud-based

    C. Asymmetric

    D. CDN

12. What is used when the customer works with the **CSP** to define expected day-to-day compute needs? The customer can then choose a plan where spikes in demand result in the automatic provisioning of additional compute resources.

    A. Autoscaling

    B. Caching

    C. Bootstrapping

    D. Clustering

13. Select the cloud service, where the service provider is often referred to as a gatekeeper. This service will protect the enterprise data from inbound threats (into the cloud) and outbound threats such as data exfiltration.

    A. IaaS

    B. CASB

    C. PaaS

    D. SWG

14. What is a cloud platform where the customer only pays for computing time and does not need to worry about maintaining servers or reserving network bandwidth? This type of computing makes better use of cloud resources as the customer only pays for what they use.

    A. Infrastructure computing

B. Cloud access security broker

C. Serverless computing

D. Virtual computing

15. What cloud storage solution is intended to protect data stored with cloud providers? Data blocks are first encrypted using the AES 256-bit symmetric algorithm and the encrypted block is then split and distributed across multiple data stores.

A. Bit splitting

B. Data dispersion

C. Availability

D. Collection

16. What is a cloud storage solution where data blocks are dispersed across multiple storage systems or cloud providers? If one provider is unavailable, then we can still access the data as the algorithm used is similar to RAID5 or RAID6.

A. Bit splitting

B. Data dispersion

C. Availability

D. Collection

17. What is the testing that uses stakeholder involvement to assess the effectiveness of the plan? Scenarios can be discussed and actions that need to be performed can be evaluated. This exercise ensures that the **Disaster Recovery Team** (**DRT**) or **Cyber Security Incident Response Team** (**CSIRT**) do not need to perform exhaustive testing until the plans are *fine-tuned*.

A. Checklist

B. Walk-through

C. Tabletop exercises

D. Full interruption test

18. What is the final stage in the testing of BCP/DRP plans? This can disrupt business operations, so should only be used when all other types of tests have been successfully executed.

A. Checklist

B. Tabletop exercises

C. Full interruption test

D. Parallel test/simulation test

19. What technology is offered by CSPs to allow for the rapid deployment of virtualized infrastructure? It is common to apply the configuration to a compute node or cluster as it boots up from a standard image (such as Linux, Unix, or Windows).

    A. Autoscaling

    B. Distributed allocation

    C. Bootstrapping

    D. Replication

20. What type of network allows for geographically dispersed servers delivering content in the form of web pages, media, and images to worldwide consumers? This network uses caching to ensure that data is available on the edge of the network, where users or customers will benefit from lower latency.

    A. Autoscaling

    B. Distributed network

    C. Content delivery network

    D. Replicated network

Answers

1. D
2. B
3. A
4. C
5. B
6. A
7. B
8. C
9. A
10. D
11. A
12. A

13. B
14. C
15. A
16. B
17. C
18. C
19. C
20. C

Chapter 16: Mock Exam 1

Welcome to the study guide assessment test! These test questions are designed to resemble real-world **CASP 004** exam questions. To make this test as realistic as possible, you should attempt to answer these questions *closed book* and allocate the correct amount of time. You can use some paper or a scratchpad to jot down notes, although this will be different in a real test environment. If you wish to look at the PearsonVue candidate testing rules, check out the following URL: https://home.pearsonvue.com/comptia/onvue.

- End of Study Assessment Test
- Number of Questions: 50
- Passing Score: 83% (Estimated)

Questions

1. Developers are building sensitive references and account details into the application code. Security engineers need to ensure that the organization can secure the **continuous integration/continuous delivery** (**CI/CD**) pipeline. What would be the best choice?

   A. Perform dynamic application security testing.

   B. Use a centralized trusted secrets manager service.

   C. Use interactive application security testing.

   D. Ensure the developers are using version control.

2. What type of assessment should be performed by an organization that stores, transmits, or processes data that contains private information?

   A. Business Impact Assessment

   B. Privacy Impact Assessment

   C. Risk assessment

   D. Safety assessment

3. The ACME corporation has recently run an annual risk assessment as part of its regulatory compliance. The risk management team has identified a high-level risk that could lead to fraudulent activities. The team has recommended that certain privileged tasks must be performed by more than one person for the task to be validated. What is this an example of?

   A. Job rotation

   B. Least privilege

C. Separation of duties

D. Multi-factor authentication

4. Security professionals are analyzing logs that have been collected from MDM software. The following log entries are available:

Device	Date/Time	Location	Event	Description
Android_2975	08NOV21 1720	57°20'22.0"N 5°39'04.0"W	Push	App 1022 install
Android_2975	08NOV21 1830	57°20'22.0"N 5°39'04.0"W	Inventory	App 1022 added
Android_2975	08NOV21 1920	57°20'00.0"N 5°39'08.0"W	Check-in	Normal
Android_2975	08NOV21 1922	28°43'25.0"N 13°50'30.0"W	Check-in	Normal
Android_2975	08NOV21 2041	28°43'25.0"N 13°50'30.0"W	Check-in	Normal
Android_2975	08NOV21 2055	57°20'22.0"N 5°39'04.0"W	Status	Storage 60% usage

Figure 16.1 – MDM audit log

What is the security concern and what response would best mitigate the risks of the mobile device?

A. An application was installed maliciously; change the MDM configuration to remove application ID 1022.

B. Sensitive data exposure; recover the device for analysis and clean up the local storage.

C. Impossible time travel; disable the device's account and carry out further investigation.

D. Anomalous status reporting; initiate a remote wipe of the device.

5. An e-commerce site has recently upgraded its web application servers to use TLS 1.3, though some customers are calling the service desk as they can no longer access the services. After analyzing the logs that had been generated on the client's devices, the following was observed:

```
ERROR_SSL_VERSION_OR_CIPHER_MISMATCH
```

What is the most likely cause of the reported error?

A. Clients are configured to use ECDHE.

B. Clients are configured to use RC4.

C. Clients are configured to use PFS.

D. Clients are configured to use AES-256 GCM.

6. The security professionals are reviewing all the servers in the company and discover that a server is missing crucial patches that would mitigate a recent exploit that could gain root access. Which of the following describes the teams' discovery?

A. A vulnerability

B. A threat

C. A breach

D. A risk

7. ACME bank has a compliance requirement. They require a third-party penetration test of the customer-facing banking application to be conducted annually. What type of penetration testing would ensure the lowest resource usage?

A. Black-box testing

B. Gray-box testing

C. Red-team exercises

D. White-box testing

E. Blue-team exercises

8. Recently, the ACME corporation has merged with a similar-sized organization. The SOC staff now have an increased workload and are failing to respond to all alerts. What is the likely cause of this behavior?

A. False positive

B. Alert fatigue

C. False negative

D. True positive

9. A small regional bank, with no dedicated security team, must deploy security at the edge of the network. They will need a solution that will offer protection from multiple threats that may target the bank's network. What would be the best solution for the bank?

A. Router

B. WAF

C. UTM

D. DLP

10. During baseline security training for new developers, attention must be focused on the use of third-party libraries. What is the most important aspect for a commercial development team that's considering the use of third-party libraries? Choose two.

A. Third-party libraries may have vulnerabilities.

B. Third-party libraries may be incompatible.

C. Third-party libraries may not support DNSSEC.

D. Third-party libraries may have licensing restrictions.

11. A CISO wants to change the culture of the organization to strengthen the company's security posture. The initiative will bring the development and operations teams together when code is released to the production environment. What is the best description of this initiative?

    A. DevOps

    B. A team-building exercise

    C. A tabletop exercise

    D. SecDevOps

12. A development team is working with a customer to develop a mobile application. The customer has already defined all the requirements upfront and wants the application to be developed using very strict timelines. It is not anticipated that any changes will be made to the initial definition. What software development approach would be the most suitable for this engagement?

    A. Agile

    B. Waterfall

    C. Spiral

    D. Build and Fix

13. A CISO for a large multinational bank would like to address security concerns regarding the use and auditing of local administrator credentials on end devices. Currently, users are given local administrator privileges when access is required. This current practice has resulted in undocumented changes, a lack of accountability, and account lockouts. What could be implemented to address these issues?

    A. Use **Privileged Access Management** (**PAM**) to maintain user accounts in the local admin group.

    B. Deploy EDR to remove users from local admins group and enable audit logs.

    C. Use **Privileged Access Management** (**PAM**) to remove user accounts from the local admin group and prompt the user for explicit approval when elevation is required.

    D. Deploy EDR to remove users from the local admins group and enable UEBA.

14. The ACME corporation has been suffering from increasing numbers of service outages on the endpoints due to ever-increasing instances of new malware. The Chief Financial Officer's laptop was impacted while working remotely from a hotel. The objective is to prevent further instances of endpoint disruption. Currently, the company has deployed a web proxy at the edge of the network. What should the company deploy to mitigate these threats?

    A. Replace the current antivirus with an EDR solution.

B. Remove the web proxy and install a UTM appliance.

C. Implement application blacklisting on the endpoints.

D. Add a firewall module to the current antivirus solution.

15. A company has been testing its **Disaster Recovery Plan** (**DRP**) while team members have been assessing challenges that had been encountered while testing in parallel. Computing resources ran out at 65% of the restoration process for critical services. What documentation should be modified to address this issue?

A. Recovery point objective

B. Business Impact Assessment

C. Mission-essential functions

D. Recovery service level

16. A security professional is performing a system penetration test. They successfully gain access to a shell on a Linux host as a standard user and want to elevate their privilege levels. What would be the most effective way to perform privilege escalation?

A. Spawn a shell using sudo and use a text editor to update the sudoer's file.

B. Perform ASIC password cracking on the host.

C. Access the `/etc/passwd` file to extract the usernames.

D. Use the `UNION` operator to extract the database schema.

17. A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After running various diagnostics tools, the analyst determines that the suspect code is performing a lot of **input/output** (**I/O**) on the disk drive. The following screenshot shows the output from one of the diagnostics tools:

```
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 3  0      0 799732   2116 1768564    0    0     2     3   20   41  0  0 99  0  0
 7  0      0 776620   2116 1764604    0    0     0    42   52 2619 53  8 40  0  0
 5  0      0 352824   2116 1805164    0    0     0   791   84 2361 76 11 12  0  0
 0  0      0 173924   2116 1870360    0    0     0   171   84 4231 62 18 20  0  0
11  0    520 160120   2104 1864472    0   90     0   133   84 4227 57 17 26  0  0
 9  0    520 492232   2104 1917992    0    0 27000 32222  117 3616 62 16 22  0  0
 4  0    520 699960   2104 1707728    0    0     0  1795   44 2646 66  8 25  0  0
```

Figure 16.2 – Diagnostic output

Based on this output, which ID should the analyst focus their attention on?

A. ID `99`

B. ID `40`

C. ID `22`

D. ID `12`

18. A CISO needs to ensure there is an effective incident response plan. As part of the plan, a CSIRT team needs to be identified, including leadership with a clear reporting and escalation process. At what part of the incident response process should this be done?

    A. Preparation

    B. Detection

    C. Analysis

    D. Containment

19. The ACME corporation's CSIRT team responded to an incident where several routers failed at the same time. The cause of the failure is unknown, and the routers have been reconfigured and restored to operational condition. The integrity of the router's configuration has also been verified. Which of the following should the team perform to understand the failure and prevent it in the future?

    A. Root cause analysis

    B. Continuity of operations plan

    C. After-action report

    D. Lessons learned

20. Jeff, a developer with the ACME corporation, is concerned about the impact of new malware on an **ARM** CPU. He knows that the malware can insert itself in another process memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

    A. Execute-never (XN)

    B. EDR software

    C. Total memory encryption

    D. Virtual memory encryption

21. Security professionals have detected anomalous activity on the edge network. To investigate the activity further, they intend to examine the contents of the `pcap` file. They are looking for evidence of data exfiltration from a suspect host computer. To minimize disruption, they need to identify a command-line tool that will provide this functionality. What should they use?

    A. `netcat`

    B. `tcpdump`

C. `Aircrack-ng`

D. Wireshark

22. Ann, a security analyst, is investigating anomalous activity within syslog files. She is looking for evidence of unusual activity based on reports from **User Entity Behavior Analytics** (**UEBA**). Several events may be indicators of compromise. Which of the following requires further investigation?

A. `Netstat -bn`

B. `vmstat -a 5`

C. `nc -w 180 -p 12345 -l < shadow.txt`

D. `Exiftool companylogo.jpg`

23. UEBA has generated alerts relating to significant amounts of `PNG` image uploads to a social networking site. The account that has generated the reports is a recent hire in the Research and Development division. A rival manufacturer is selling products that appear to be based on the company's sensitive designs.

    The payloads are now being analyzed by forensics investigators. What tool will allow them to search for evidence in the PNG files?

A. Steganalysis tool

B. Cryptanalysis tool

C. Binary analysis tool

D. Memory analysis tool

24. Marketing executives are attending an international trade exhibition and must connect to their company's email using their mobile devices during the event. The CISO is concerned that this may present a risk. What would best mitigate this risk?

A. Near-field communication (NFC)

B. Split-tunnel VPN

C. Geofencing

D. Always-on VPN settings

25. A company employee has followed a QC link and installed a mobile application that's used to book and schedule activities at a vacation resort. The application is not available on Google Play Store. Company policy states that applications can only be downloaded from the official vendor store or company portal. What best describes what has allowed this app to be installed?

A. Supply chain issues

B. Side loading

C. Containerization

D. Unauthorized application stores

26. A company has deployed a hardened Linux image to mobile devices. The restrictions are as follows:

- All unnecessary services must be removed.
- Only company-deployed apps can be run.
- The runtime code is protected against memory exploits.

The CISO is concerned that an attacker may be able to launch attacks using common utilities and command-line tools. What could be deployed to mitigate the CISO's concerns?

A. Whitelisting

B. Shell restrictions

C. ASLR

D. Memory encryption

27. A regional **Internet Service Provider** (**ISP**) is experiencing outages and poor service levels over some of its copper-based infrastructure. These faults are due to the reliance on legacy hardware and software. Several times during the month, a contracted company must follow a checklist of 12 different commands that must be run in serial to restore performance to an acceptable level. The ISP would like to make this an automated process. Which of the following techniques would be *best* suited for this requirement?

A. Deploy SOAR utilities and runbooks.

B. Replace the associated hardware.

C. Provide the contractors with direct access to syslog data.

D. Switch the copper-based infrastructure to fiber.

28. A security analyst is investigating a possible buffer overflow attack. The attack seems to be attempting to load a program file. Analysis of the live memory reveals that the following string is being run:

```
code.linux_access.prg
```

Which of the following technologies would *best* mitigate the manipulation of memory segments?

A. NX bit

B. ASLR

C. DEP

D. HSM

29. A CISO at a regional power supply company is performing a risk assessment. The CISO must consider what the *most* important security objective is when applying cryptography to control messages. The control messages are critical and enable the operational technology to ensure the generators are outputting the correct electrical power levels. What is the most important consideration here?

    A. Importing the availability of messages

    B. Ensuring the non-repudiation of messages

    C. Enforcing protocol conformance for messages

    D. Ensuring the integrity of messages

30. Alan, a CISO for an online retailer, is performing a quantitative risk assessment. The assessment is based on the public-facing web application server. Current figures show that the application server experiences 80 attempted breaches per day. In the past 4 years, the company's data has been breached two times. Which of the following represents the ARO for successful breaches?

    A. 50

    B. 0.8

    C. 0.5

    D. 29,200

31. Security engineers are assessing the capabilities and vulnerabilities of a widely used mobile operating system. The company intends to deploy a secure image to mobile phones and tablets. The mobile devices mustn't be vulnerable to the risk of privilege elevation and the misuse of applications. What would be the *most* beneficial to the company for addressing these concerns?

    A. Security-Enhanced Linux (SELinux)

    B. Trusted Platform Module (TPM)

    C. Security-Enhanced Android (SEAndroid)

    D. Attestation services

32. Gerry, a CISO for a national healthcare provider, is assessing proposals for network storage solutions. The proposal is for NAS to be deployed to all regional hospitals and clinics. As the data that will be stored will be sensitive and subject to strict regulatory compliance, security

is the most important consideration. The proposal is for appliances running a Linux kernel and providing secure access to authenticated users through NFS. One major concern is ensuring that the root account cannot be used to gain access to user data on the Linux NFS appliances. What would *best* prevent this issue from occurring?

A. Ensure passwords are stored in a shadow file.

B. Run SELinux in enforced mode.

C. Disable **central processing unit** (**CPU**) virtualization support.

D. Enforce secure encrypted enclaves/memory encryption.

33. ACME chemicals is conducting a risk assessment for its legacy operational technology. One of their major concerns is the widespread use of a standard message transport protocol that's used in industrial environments. After performing a vulnerability assessment, several CVEs are discovered with high CVSS values. The findings describe the following vulnerabilities:

- CVE-2018-11452: Denial-of-service of the affected device
- CVE-2018-7842: Elevation of privilege by conducting a brute-force attack on the parameters that were sent to the controller
- CVE-2017-6034: An attacker can replay the `run`, `stop`, `upload`, and `download` commands

Additional CVEs report multiple vulnerabilities, including no security against message integrity being tampered with and being vulnerable to MITM attacks. What is the network/protocol that has most likely been assessed?

A. Ethernet

B. Modbus

C. Distributed Network Protocol 3 (DNP3)

D. Zigbee

34. Mechanical engineers are using a simple programming language based on relay-based logic, as shown in the following diagram:

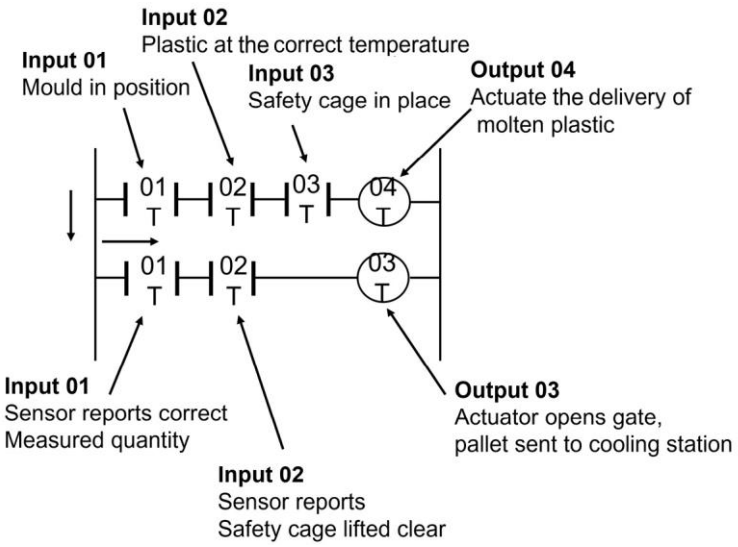


Figure 16.3 – Relay-based logic

What language/protocol are the engineers are using?

A. Historian

B. Ladder logic

C. Zigbee

D. Modbus

35. A small water treatment plant is being controlled by a SCADA system. There are four main treatment tanks, each being serviced by an input pump and an output pump. The design of the plant offers redundancy as the plant can operate without all the tanks being available. The plant is comprised of a standard SCADA mix of operational technology, including PLCs and a supervisory computer.

    What system failure will cause the biggest outage?

    A. Loss of a treatment tank

    B. Loss of supervisory computer

    C. Failure of an input pump

    D. Failure of a PLC

36. A development team is implementing a customer-facing API that uses a database backend. Before the deployment, the team is concerned about attacks, such as XSS, XSRF, and injection attacks. To mitigate these types of attacks, the team needs to identify security controls that could be implemented. Which of the following sources could the team consult to address these security concerns?

    A. SDLC

B. OVAL

C. IEEE

D. OWASP

37. The customers of a large online retailer are reporting high levels of latency when they are searching for products on the e-commerce site. The site consists of an array of load-balanced APIs that do not require authentication. The application servers that host the APIs are showing heavy CPU utilization. WAFs that have been placed in front of the APIs are not generating any alerts.

    Which of the following should a security engineer recommend to *best* remedy these performance issues promptly?

    A. Implement rate limiting on the API.

    B. Implement geo-blocking on the WAF.

    C. Implement OAuth 2.0 on the API.

    D. Implement input validation on the API.

38. ACME bank engineers are configuring security for a new data center. They are looking to implement SSL/TLS for customer-facing application servers. Customers will connect to the bank API through a deployed mobile application. They must now choose a symmetric algorithm that offers the greatest speed and security. Which should they choose?

    A. ChaCha256 + poly1305

    B. 3DES + CBC

    C. AES256 + CBC

    D. Salsa256 + CBC

39. Hackers can gain access to encrypted data transmissions. After performing vulnerability assessments on the application servers, several cipher suites are available for backward compatibility. Which of the following would represent the *greatest* risk?

    A. TLS_RSA_WITH_AES_128_CBC_SHA

    B. TLS_RSA_WITH_RC4_40_MD5

    C. TLS_DHE_RSA_WITH_AES_256_CBC_SHA

    D. TLS_RSA_WITH_3DES_EDE_CBC_SHA

40. A company is deploying an online streaming service for customers. The content needs to be protected; only the paid subscribers should be able to view the streams. The company wants to choose the *best* solution for low latency and security. What would be the best choice?

A. 3DES

B. AES

C. ChaCha

D. RC4

41. A government agency is configuring a VPN connection between Fort Meade and a field office in New York. Of primary importance is having a highly secure key exchange protocol due to the threats posed by nation state threat actors. Which encryption protocol would be a good choice?

A. Advanced Encryption Standard (AES)

B. ECDHE p521

C. ChaCha-256

D. SHA-512

42. Software developers are deploying a new customer-facing CRM tool. The deployment will require the customers to download an application on their system. Customers must be able to verify that the application is trustworthy. What type of certificate will the software developers request to fulfill this requirement?

A. Client authentication

B. Server authentication

C. Digital signatures

D. Code signing

43. A large insurance provider has grown in size and now supports customers in many different countries. Due to this increased footprint, they are looking to minimize administration by allocating a single certificate to multiple sites. The sites will be country-specific, with different domain names. What would be the best choice for delivering this requirement?

A. Wildcard certificate

B. Extended validation

C. General-purpose

D. Subject Alternate Name (SAN)

44. The CISO is delivering a security briefing to senior members of staff. One of the topics of conversation concerns the current e-commerce site. During a Q&A session, the CISO is asked questions about PKI and certificates. A rudimentary question is asked – what key is stored on a certificate? What should the CISO answer?

A. Public key

B. Private key

C. Public and private keys

D. Signing key

45. A large online bank would like to ensure that customers can quickly validate that the bank's certificates are not part of a CRL. What would best meet this requirement?

A. Extended validation

B. Certificate pinning

C. OCSP

D. CRL

46. Website engineers are configuring security extensions to be deployed to all customer-facing web application servers. What HTTP extension will ensure that all the connections to the application servers will also be encrypted using the assigned X.509 certificate?

A. HTTP X-FRAME headers

B. HTTP Strict Transport Security (HSTS)

C. HTTPS SSL 3.0 CBC

D. Extended validation

47. Nation state-sponsored actors have stolen the smartphone of a government official. They have attempted to guess the PIN code several times, eventually locking the device. They are attempting to gain access to the data using forensic tools and techniques but the data cannot be accessed. What has likely prevented a data breach from occurring?

A. Hardware write blocker

B. USB data blocker

C. Crypto shredding

D. Improper key handling

48. A small startup energy company has built up a database of clients. It is estimated that this database is worth $100,000. During a data breach, a cyber-criminal (working for a competitor) steals 10% of the records. The company fails to put adequate controls in place and a second breach occurs within 12 months.

What is the Annual Loss Expectancy (ALE)?

A. $200,000

B. $1,000

C. $20,000

D. $10,000

49. A defense contractor currently loses an estimated $2,000,000 each year due to intellectual property theft. The company has a solid reputation for R&D and manufacturing but has no dedicated security staff. A **Managed Security Service Provider** (**MSSP**) guarantees that they will provide 90% protection for the data over a 5-year contract at an annual cost of $250,000 per annum. What is the ROI in dollars?

    A. $10,000,000

    B. $9,000,000

    C. $750,000

    D. $7,750,000

50. An automobile manufacturer suffers a power outage at one of its foundries. The facility supplies critical components for the company. The COOP designated the foundry as a mission-essential service, and it was agreed that the foundry must be operational within 24 hours. The energy supplier has struggled to repair severe storm-damaged cables. As a result, the facility is without power for 72 hours. What is the metric that describes this 72-hour outage?

    A. Mean time to recovery (MTTR)

    B. Mean time between failure (MTBF)

    C. Recovery Time Objective (RTO)

    D. Annualized rate of occurrence (ARO)

Assessment test answers

1. **B**. Use a centralized trusted secrets manager service. Secrets can include user or auto-generated passwords, APIs, and other application keys/credentials, SSH keys, databases, and other system-to-system passwords. You should use private certificates for secure communication and private encryption keys.

    External reference: https://www.beyondtrust.com/resources/glossary/secrets-management.

    See *Chapter 4*, *Deploying Enterprise Authentication and Authorization Controls*, for more details on secure account management concepts.

2. **B**. Privacy Impact Assessment. A PIA should be undertaken by any organization that stores, transmits, or processes data that contains private information. Data types will vary but can include documents, database records, and media such as CCTV footage and voice recordings. See *Chapter 15*, *Business Continuity and Disaster Recovery Concepts*.

3. **C**. Separation of duties. When an employee has privileges that enable them to make high-level decisions without needing the consent of another employee, then we are missing essential checks and balances. Consider a **Chief Financial Officer** (**CFO**), who approves new suppliers, approves the suppliers' invoices for services, and signs their paychecks. This example would allow for fraudulent activities and would be mitigated by establishing accounts receivable and accounts payable business functions. See *Chapter 13*, *Applying Appropriate Risk Strategies*.

4. **C**. Impossible time travel. Disable the device's account and carry out further investigations.

   See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls* (covers location services and **user and entity behavior analytics** (**UEBA**)).

5. **B**. Clients are configured to use RC4. RC4 is considered weak encryption and would not be supported while using TLS 1.3. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

6. **A**. A vulnerability. When a system is missing patches, it is vulnerable to attacks. During a risk assessment, we need to assess vulnerabilities and potential threats that could target the vulnerability. See *Chapter 6*, *Vulnerability Assessment and Penetration Testing Methods and Tools*.

7. **A**. Black-box testing will take the least amount of time but may not discover all vulnerabilities. See *Chapter 6*, *Vulnerability Assessment and Penetration Testing Methods and Tools*.

8. **B**. Alert fatigue. This is when the staff are overwhelmed with too many alerts. See *Chapter 1*, *Designing a Secure Network Architecture*.

9. **C**. **Unified Threat Management** (**UTM**). This can combine multiple security functions into a single appliance. See *Chapter 1*, *Designing a Secure Network Architecture*.

10. **A** and **D**. Third-party libraries may have vulnerabilities and Third-party libraries may have licensing restrictions. See *Chapter 2*, *Integrating Software Applications into the Enterprise*.

11. **D**. SecDevOps. The development team and operations teams work together to ensure code is delivered error-free. See *Chapter 2*, *Integrating Software Applications into the Enterprise*.

12. **B**. The waterfall methodology means that we must have defined all the requirements at the start of the process and that no changes will be made during the development cycle. See *Chapter 2*, *Integrating Software Applications into the Enterprise*.

13. **C**. Use **Privileged Access Management** (**PAM**) to remove user accounts from the local admin group and prompt the user for explicit approval when elevation is required. This solution allows accounts to elevate their privileges and that these actions will be audited. See *Chapter 4*, *Deploying Enterprise Authentication and Authorization Controls*.

14. **A**. Replace the current antivirus with an EDR solution. The end devices must be protected when they are not on the company network. The other solutions will not adequately fulfill the requirements. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

15. **D**. Recovery Service Level. See *Chapter 15*, *Business Continuity and Disaster Recovery Concepts*.

16. **C**. Access the `/etc/passwd` file to extract the usernames. As the account is a standard user, they will not have the right to edit configuration files (sudoers), so the best option is to access the `passwd` file (you do not need any privileges to do this). See *Chapter 7*, *Risk Mitigation Controls*.

17. **C**. ID22 shows a high amount of disk I/O using the `vmstat` command. See *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

18. **A**. Preparation. For details on creating an incident response plan, see *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

19. **A**. Root cause analysis. This would be performed as a result of lessons learned/AAR. See *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

20. **A**. **Execute-never** (**XN**). CPU chips support memory protection within the hardware. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

21. **B**. `tcpdump`. This is a command-line protocol analyzer that's capable of capturing traffic and can be used to analyze previous captures. pcap is a standard packet capture file format. See *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

22. **C**. `nc -w 180 -p 12345 -l < shadow.txt`. Netcat can be used to run remote commands on a target system, allowing for files to be transferred. See *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

23. **A**. Steganalysis tool. This tool would search for data hidden within the graphics file. See *Chapter 8*, *Implementing Incident Response and Forensics Procedures*.

24. **D**. Always-on VPN settings. They will always have an encrypted connection that's routed through the company network. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

25. **D**. Unauthorized application stores. See *Chapter 9, Enterprise Mobility and Endpoint Security Controls*.

26. **B**. Shell restrictions. The current settings mitigate the main threats but do not prevent built-in commands from being run. See *Chapter 9, Enterprise Mobility and Endpoint Security Controls*.

27. **A**. Deploy SOAR utilities and runbooks. This will automate this repetitive process and take some of the workload off the technicians. See *Chapter 8, Implementing Incident Response and Forensics Procedures*.

28. **B**. ASLR. This mitigation is built into the operating system and is considered a better option (NX+DEP is hardware-based and less effective).

29. **D**. Ensuring the integrity of messages. Control messages will not normally be confidential but must be tamper-proof. This is the best solution. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

30. **C**. 0.5. The ARO over 4 years is 0.5 as there were only two successful breaches. See *Chapter 13, Applying Appropriate Risk Strategies*.

31. **C**. **Security-Enhanced Android** (**SEAndroid**). This is SELinux for mobile devices. See *Chapter 9, Enterprise Mobility and Endpoint Security Controls*.

32. **B**. Run SELinux in enforced mode. This will enforce **Mandatory Access Control** (**MAC**). See *Chapter 9, Enterprise Mobility and Endpoint Security Controls*.

33. **B**. Modbus. This is a well-used control protocol that's used within industrial controlled environments. It is vulnerable to many different threats. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

34. **B**. Ladder logic. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

35. **B**. Loss of a supervisory computer. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*. This can also be seen in the following diagram:

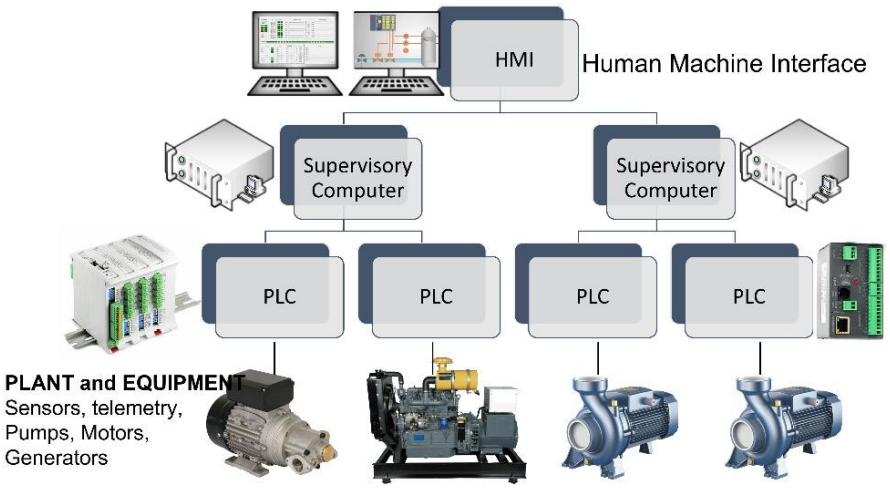


Figure 16.4 – The hierarchy of and dependencies within a SCADA system

36. **D**. OWASP. This will be the best source of reference when securing web applications.

37. **A**. Implement rate limiting on the API. This will allow for the number of connections that are forwarded to the web servers to be *throttled*.

38. **A**. ChaCha256 + poly1305. This offers a major performance advantage over existing technologies. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

39. **B**. TLS_RSA_WITH_RC4_40_MD5. RC4 (symmetric encryption) should not be used and will cause systems to be out of compliance. MD5 (hashing algorithm) is also weak and should not be used. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

40. **C**. ChaCha. This is a stream cipher and will offer very good performance for streaming media. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

41. **B**. ECDHE p521. This is currently the strongest form of key exchange. The other answers refer to symmetric encryption or hashing. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

42. **D**. Code signing. The application code needs to be digitally signed. See *Chapter 12*, *Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

43. **D**. **Subject Alternate Name** (**SAN**). This will allow a single certificate to be issued for multiple sites. A wildcard would not be suitable as the domain names will be different. See *Chapter 12*, *Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

44. **A**. Public key. A digital certificate validates the public key. Private keys are not shared but can be stored in escrow if a copy needs to be made. See *Chapter 12*, *Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

45. **C**. OCSP. This allows a quick response to be provided when a CRL check is required. See *Chapter 12, Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

46. **B**. **HTTP Strict Transport Security** (**HSTS**). This will ensure that all the connections are forced to use HTTPS/TLS. See *Chapter 2, Integrating Software Applications into the Enterprise*.

47. **C**. Crypto shredding. The symmetric key that was used to encrypt the data is destroyed, making data recovery ineffective. See *Chapter 12, Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

48. **C**. $20,000.

    Asset Value (**AV**) = 100,000

    Exposure Factor (**EF**) = 10%

    Single Loss Expectancy (**SLE**) = 10,000

    Annual Rate of Occurrence (**ARO**) = 2

    Annual Loss Expectancy (**ALO**) = 20,000 (SLE x ARO)

    See *Chapter 13, Applying Appropriate Risk Strategies*.

49. **D**. $7,750,000. ROI= (9,000,000 Reduction in risk – 750,000 cost of control). The contract is for 5 years, so the potential loss would be 10,000,000. As we mitigate 90% of the loss, we have saved 9,000,000 but must pay 5 x 250,000 = 1,250,000. See *Chapter 13, Applying Appropriate Risk Strategies*.

50. **A**. **Mean time to recovery** (**MTTR**). See *Chapter 13, Applying Appropriate Risk Strategies*.

Hopefully, you have enjoyed testing yourself via a typical mix of CASP questions. For more exam resources, please visit https://www.casp.training.

Chapter 17: Mock Exam 2

Welcome to the study guide assessment test! These test questions are designed to resemble real-world **CASP 004** exam questions. To make the test as realistic as possible, you should attempt these questions *closed book* and allocate the appropriate amount of time. You can use some notepaper or a scratchpad to jot down notes, although this will be different in a real test environment. To find the PearsonVue candidate testing rules, check out https://home.pearsonvue.com/comptia/onvue.

End of Study Assessment Test

Number of Questions: 50

Passing Score: 83% (Estimated)

Questions

1. A company works with a **cloud service provider** (**CSP**) that provides *bleeding-edge* technology to perform data analytics and deep learning techniques on the company's data. As the technology becomes more widespread, it appears that a rival CSP can offer the same solutions for a 50% cost saving. However, it seems that the database format and rule sets that have been created can't be transferred to the rival CSP. What term would best describe this situation?

   A. Vendor risk

   B. Vendor lock-in

   C. Third-party liability

   D. Vendor management plan

2. A major retailer works with a small, highly regarded, third-party development team. They intend to invest significant resources into a new customer-facing set of APIs. The retailer is concerned about the financial stability of the development company and worries that they may need to start the development project from scratch if the developers go bust. What could be used to allay the fears of the retailer?

   A. Change management

   B. Staff turnover

   C. Peer code review

   D. Source code escrow

3. Andy is the CSO within a department of the *United Kingdom's* **HM Revenue and Customs** *(***HMRC***)*. All new systems that will require government funding must be assessed concerning cost savings by working with a CSP. Andy is overseeing a proposed new system that will

reduce the workload of the Inland Revenue HMRC employees. What must a government agency consider when planning to store sensitive data with a global CSP?

A. Data sovereignty

B. Data ownership

C. Data classifications

D. Data retention

4. A Privacy Impact Assessment is being conducted on behalf of a private healthcare provider. A consultant is assessing regulatory requirements for the hospital's employee and patient data (within Europe). The data that is currently being held includes the following:

- Patient's address
- Patient's bank account details
- Patient's medical history
- Patient's X-ray records
- Employee bank account details

What type of information will need to be protected and which regulations are the most important? (Choose *two*)

A. COPPA

B. **Personally identifiable information** (**PII**)

C. Financial records

D. Intellectual property

E. GDPR

5. A regional bank intends to work with a CSP to harness some of the benefits associated with cloud computing. The bank wants the assurance that data will not be accessible when their contract with a CSP expires. What technology would be most applicable?

A. Crypto erase

B. Pulping

C. Shredding

D. Degaussing

6. A company manufactures medical devices, including instruments and scanners. The company intends to sell and market its devices to a global customer base. The company

must ensure its products are compatible with its worldwide customer base. What regulations or standards will be the *most* important?

A. Export Control Regulations

B. **General Data Protection Regulation** (**GDPR**)

C. **International Organization for Standardization** (**ISO**)

D. **National Institute of Standards and Technology** (**NIST**)

7. A startup software development company is trying to win a US Federal Government contract to provision an **Enterprise Resource Planning** (**ERP**) application. They must assure the customer that they have a robust security framework for delivering software and services. What is the most relevant accreditation?

A. Open Web Application Security Project (OWASP)

B. Capability Maturity Model Integration (CMMI)

C. National Institute of Standards and Technology (NIST)

D. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

8. A large US-based retailer is transitioning toward an online selling platform. While customer details and payment card details will be stored in-house, a CSP will be used to host the e-commerce site, including the online shop. What compliance will be most important to the retailer concerning storing cardholder data and electronic transactions?

A. Payment Card Industry Data Security Standard (PCI DSS)

B. General Data Protection Regulation (GDPR)

C. Interconnection security agreement (ISA)

D. Non-disclosure agreement (NDA)

9. Eva is the CISO for a global stocks and shares trading site. She is performing a risk assessment that focuses on customer data being stored and transmitted. Customers are mainly based in North America with a small percentage based globally, including Europe. When it comes to considering regulatory and legal requirements, which of the following will be the most important?

A. General Data Protection Regulation (GDPR)

B. Payment Card Industry Data Security Standard (PCI DSS)

C. International Organization for Standardization (ISO)

D. Federal Information Security Management Act (FISMA)

10. A US smartcard manufacturer needs to sell its products in a global market. They need to ensure that the technology is not sold to countries or governments that are hostile to the US. What guidance or regulations should they consult?

    A. Due care

    B. Export controls

    C. Legal holds

    D. E-discovery

11. A government department has data privacy requirements and they need to have employees and service providers sign this agreement. They should be made aware of the strict terms of this agreement and the penalties that may be forthcoming if these requirements/standards are not met. What type of agreement will be important?

    A. Service-level agreement (SLA)

    B. Master service agreement (MSA)

    C. Non-disclosure agreement (NDA)

    D. Memorandum of understanding (MOU)

12. A large multinational company intends to purchase multiple products on a rolling contract from a CSP. They need to document, payment terms, dispute resolution, intellectual property ownership, and geographic operational locations within the scope of the contract. What type of contract would be the most suitable?

    A. Service-level agreement (SLA)

    B. Master service agreement (MSA)

    C. Memorandum of understanding (MOU)

    D. Operational-level agreement (OLA)

13. A global pharmaceutical company would like to build resiliency into its network connections. They are working with an ISP, who proposes a highly available MPLS solution. To ensure the vendor can deliver the service at 99.999% uptime, what documentation will be important?

    A. Service-level agreement (SLA)

    B. Memorandum of understanding (MOU)

    C. Interconnection security agreement (ISA)

    D. Operational-level agreement (OLA)

14. A software development company and a mobile phone manufacturer have entered a business partnership. The business partners need to share data during a series of upcoming

projects. This agreement will stipulate a timeline for the information exchange to be supported, security requirements, data types that will be exchanged, and the actual sites that will be part of the data interchange. What documentation best details these requirements?

A. SLA

B. MSA

C. MOU

D. ISA

15. A regional healthcare provider needs to address ever-escalating costs. They propose to host some of the information systems with a CSP. The healthcare provider needs assurances that any sensitive data will be protected by the service provider, and that agreed-upon steps are in place if data breaches or any adverse action were to occur. What document would address these requirements?

    A. Non-disclosure agreement (NDA)

    B. Memorandum of understanding (MOU)

    C. Interconnection security agreement (ISA)

    D. Operational-level agreement (OLA)

    E. Privacy-level agreement (PLA)

16. A government agency begins an investigation on an employee suspected of stealing company **intellectual property** (**IP**). What must be done first to ensure the data is not deleted?

    A. Due care

    B. Export controls

    C. Legal holds

    D. E-discovery

17. A company has several internal business units. The business units are semi-autonomous but need to support each other for the business to be efficient. To ensure the business units can work together, it is important to document responsibilities for each business unit. This document will not be written by lawyers and is intended to formalize previous verbal agreements. What documentation would best suit this requirement?

    A. Service-level agreement (SLA)

    B. Master service agreement (MSA)

C. Memorandum of understanding (MOU)

D. Interconnection security agreement (ISA)

18. An aerospace sub-contractor supplies parts to a major commercial aircraft manufacturer. The SLAs are very strict, with financial penalties for transgressions. Mission-critical processes must be identified within the subcontractor's plant to avoid any lengthy production delays. What metric can be used by the company to ensure a critical service will be operational within the specified timeframe?

A. Recovery point objective

B. Recovery time objective

C. Recovery service level

D. Mission essential functions

19. A public transportation provider has recently completed a BIA and has determined that the **Continuity of Operations Plan** (**COOP**) will require an alternative site to be available in the event of a major incident at the main operational site. The planning team has identified a requirement for a site, housing equipment, and facilities ready for the business to use. Personnel and data will need to be moved to the site to become operational. What have they identified?

A. Cold site

B. Warm site

C. Hot site

D. Mobile site

20. A CISO for a cellular telephony provider is working with a **Cloud Service Provider** (**CSP**) to define expected day-to-day computing needs. The company wants to be able to choose a plan where spikes in demand result in additional compute resources being automatically provisioned. What technology would *best* meet this requirement?

A. Autoscaling

B. Caching

C. Bootstrapping

D. Clustering

21. A company wants to be more flexible concerning employee work/life balance. To allow for this cultural change, remote access and working from home will become widespread. Senior management has concerns about data security, as most of the company information systems are now cloud-based. The concerns that were discussed include the following:

- Data loss prevention
- Control over native features of cloud services, such as collaboration and sharing
- **User and entity behavior analytics** (**UEBA**)
- Configuration auditing
- Malware detection
- Data encryption and key management
- Context-based access control

As employees will not be connected to the company network, various management concerns must be addressed. What solution would *best* address these concerns?

A. NGFW

B. CASB

C. DLP

D. SWG

22. What form of testing uses stakeholder involvement to assess the effectiveness of the plan? Scenarios can be discussed and actions that need to be performed can be evaluated. This exercise ensures the **Disaster Recovery Team** (**DRT**) or **Cyber Security Incident Response Team** (**CSIRT**) do not need to perform exhaustive testing until the plans are *fine-tuned*.

A. Checklist

B. Walk-through

C. Tabletop exercises

D. Full interruption test

23. A cloud customer needs workloads to be rapidly deployed to support a large and diverse customer base. One important requirement is to allow virtualized infrastructure to be deployed, where configuration is applied to a compute node or cluster as it boots up from a standard image (such as Linux, Unix, or Windows). What technology would *best* suit this requirement?

A. Autoscaling

B. Distributed allocation

C. Bootstrapping

D. Replication

24. A news delivery platform provider needs to deliver content in the form of web pages, media, and images to worldwide consumers. The requirement is for geographically dispersed servers using caching to ensure that data is available on the edge of the network, where users or customers will benefit from lower latency. What technology would best suit this requirement?

    A. Autoscaling

    B. Distributed network

    C. Content delivery network

    D. Replicated network

25. A medical instrument manufacturer is currently experiencing problems in the production plant. The company is using a mix of **Industrial Control Systems** (**ICS**) on a common network backbone to operate the plant. Some of the manufacturing processes are time-critical and occasionally, bottlenecks occur at peak times during the day. To ensure that the time-critical processes are not impacted by bottlenecks, what technology would most likely mitigate these problems?

    A. Safety Instrumented System (SIS)

    B. Data Distribution Service (DDS)

    C. Operational Technology (OT)

    D. Controller Area Network (CAN)

26. A utility company is following industry guidelines to harden its server systems. One of the first steps that the guidelines suggest is to identify all the available and unneeded services. What tool would *best* suit this requirement?

    A. Binary analysis tools

    B. Port scanner

    C. HTTP interceptor

    D. Protocol analyzer

27. A well-known developer's content sharing portal has been targeted by a DDoS attack. Although it's the web application servers that are being targeted, the effect of all the traffic flooding the network has made all the services unavailable. Security experts are looking to implement protection methods and implement blackhole routing for the web application servers. What has this mitigation achieved?

    A. Traffic is inspected for malicious payloads

    B. Traffic intended for the systems is dropped

C. Traffic to the systems is inspected before it reaches the destination

D. Rules restrict the amount of traffic throughput

28. Security analysts are responding to SIEM alerts that are showing a high number of IOC events. The analysts have a reason to suspect that there may be APT activity in the network. Which of the following threat management frameworks should the team implement to better understand the TTPs of the potential threat actor?

A. NIST SP 800-53

B. MITRE ATT&CK

C. The Cyber Kill Chain

D. The Diamond Model of Intrusion Analysis

29. National Dynamics, an aerospace company, is looking to strengthen its cybersecurity posture by focusing on its network defenses. The company is concerned about the availability of the company's services to its B2B partners. Many manufacturing processes use JIT techniques to optimize production and false positives mustn't drop legitimate traffic. Which of the following would satisfy this requirement?

A. NIDS

B. NIPS

C. WAF

D. Reverse proxy

30. A small law firm is looking to reduce its operating costs. Currently, vendors are proposing solutions where the CSP will host and manage the company's website and services. Due to legal and regulatory requirements, the company requires that all the available resources in the proposal must be dedicated. Due to cost constraints, the company does not want to fund a private cloud. Given the company requirements, which of the following is the *best* solution for this company?

A. Community cloud service model

B. Multi-tenancy SaaS

C. Single-tenancy SaaS

D. An on-premises cloud service model

31. A company that uses **Active Directory Services** (**ADS**) is migrating services from LDAP to secure LDAP (LDAPS). During the pilot phase, the server team has been troubleshooting connectivity issues from several different client systems. Initially, the clients would not connect as the LDAP server had been assigned a wildcard certificate,

`*.classroom.local`. To fix these problems, the team replaced the wildcard certificate with a specific named certificate, `win2016-dc.classroom.local`. Further problems are causing the connections to fail. The following screenshot shows the output from a troubleshooting session:

```
[root@cent07 ~]# openssl s_client -host win2016-dc.classroom.local -port 636
CONNECTED(00000003)
Server certificate
-----BEGIN CERTIFICATE-----
MIIFTzCCBDegAwIBAgITHwAAAAQ0pZcvscL82QAAAAAABDANBgkqhkiG9w0BAQsF
ADBJMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFgljbGFz
c3Jvb20xFTATBgNVBAMTDGNsYXNzcm9vbS1DOTAeFw0vMTA3MiEwNTOwNDVaFw0v
u2THpmYtUB038Qd3+Ob/nXCUseV+YPoNtnu1n9TpemdpTc0qzw/cP37TVrQnKwy5
6v0b0TMjabbB0i+35CocagPMnaEZQuPN0T/nyI4ttdQgBsAc8Kg4HB3p9MtEN2mG
haDcOg+WfXrc5erGr/NSKPaNzEDPjGSnKDWTyZJuBR3nmrauogJjranrDHNY8nJx
8SJSP2CnF9sJtzIn+lNDcIwDrg==
-----END CERTIFICATE-----
subject=/CN=WIN2016-DC.classroom.local
issuer=/DC=local/DC=classroom/CN=classroom-CA
```

Figure 17.1 – LDAPS client troubleshooting session

Which of the following *best* explains why the LDAPS service failed initially and still fails client connection attempts? (Select *two*)

A. The clients do not support the LDAP protocol by default.

B. The LDAPS service has not been started, so the connections will fail.

C. `Classroom.local` is under a DDoS attack and cannot respond to OCSP requests.

D. The clients may not trust the issuing `CA-classroom.classroom.local` by default.

E. LDAPS should be running on UDP rather than TCP.

F. The company is using the wrong port. It should be using port 389 for LDAPS.

G. LDAPS does not support wildcard certificates.

32. A sales team relies on a CRM application to generate leads and maintain customer engagement. The tool is considered a mission-essential function to the company. During a business impact assessment, the risk management team indicated that data, when restored, cannot be older than 2 hours before a system failure. What planning objective should be used when the restoration will also require data to be restored?

A. Recovery point objective

B. Recovery time objective

C. Recovery service level

D. Mission-essential functions

33. A large defense contractor has recently received a security advisory documenting the activities of highly skilled nation-state threat actors. The company's hunt team believes they have identified activity consistent with the advisory. Which of the following techniques would be *best* for the hunt team to use to entice the adversary to generate malicious activity?

    A. Perform audits on all firewall logs.

    B. Implement a bug bounty program.

    C. Increase security using isolation and segmentation schemes.

    D. Deploy decoy files on the host's systems on the same network segment.

34. A new online retailer must ensure that all the new web servers are secured in advance of a PCI DSS security audit. PCI DSS requirements are strict and define acceptable cipher suites. Deprecated cipher suites should not be used as they offer weak encryption and are vulnerable to on-path attacks. In preparation for the audit, a security professional should disable which of the following cipher suites?

    A. `TLS_RSA_WITH_AES_128_CCM_8_SHA256`

    B. `TLS_RSA_WITH_RC4_128_SHA`

    C. `TLS_RSA_WITH_AES_128_CBC_SHA256`

    D. `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`

35. A distribution company is attempting to harden its security posture regarding mobile devices. To secure the dedicated Android devices that are used in the warehouse, the company has developed SELinux policies. Security engineers have compiled and implemented the policy. Before deploying the Android devices to the warehouse staff, which mode should the devices be configured for?

    A. Disabled

    B. Permissive

    C. Enforcing

    D. Preventing

36. A software development company is concerned as it has discovered that company intellectual property is circulating on social media. The CISO wants to implement a solution that will allow the company to determine the source of these leaks. Which of the following should be implemented to identify the internal source for any future exposures?

    A. Digital rights management

    B. Hashing

C. Watermarking

D. Identity proofing

37. A company has recently undertaken a project to move several services into the cloud. A cloud service provider now hosts the following services:

- Corporate intranet site
- Online storage application
- Email and collaboration suite

The company must ensure that the data is protected from common threats, including malware infections, exfiltration of PII and healthcare data.

To be more proactive, an additional requirement is that SOC staff must receive alerts when there are any large transfers of corporate data from the company's hosted storage. Which of the following would best address the company's cyber-security requirements?

A. NIDS

B. CASB

C. DLP agent

D. Containers

E. Vulnerability scanner

38. A CISO is reviewing the current security of an electricity supply company. The company has many operational sites and must connect the sites securely to the company headquarters, which is where the company's data center is located. The technology that's supported within these sites includes industrial control systems and PLCs. The technology is legacy and uses the Modbus protocol across the networks. A VPN solution is being proposed to securely connect all the sites to the company's data center.

The CISO is concerned that a recent security advisory, concerning certain asymmetric algorithms, may impact the company's operations. Which of the following will be most likely impacted by weak asymmetric encryption?

A. Modbus

B. VPN links

C. Industrial control systems

D. Datacenter equipment

39. Security administrators have run a scan on a network segment to detect vulnerabilities. They are trying to discover any protocols that may be running on host computers that may expose user passwords or sensitive data. The following screenshot shows the output from the scan:

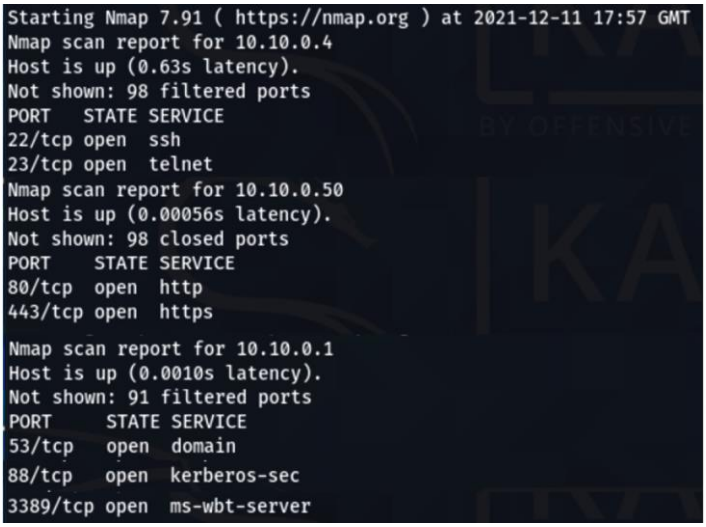


Figure 17.2 – Security scan output

To secure the network segment, additional rules must be enabled on the network firewall. Which rules should be added to meet this security requirement? Choose *two*.

A. `SRC Any DST 10.10.0.1 PORT 53 PROT TCP ACTION Deny`

B. `SRC Any DST 10.10.0.4 PORT 23 PROT TCP ACTION Deny`

C. `SRC Any DST 10.10.0.4 PORT 22 PROT TCP ACTION Deny`

D. `SRC Any DST 10.10.0.50 PORT 80 PROT TCP ACTION Deny`

E. `SRC Any DST 10.10.0.1 PORT 88 PROT TCP ACTION Deny`

F. `SRC Any DST 10.10.0.50 PORT 443 PROT TCP ACTION Deny`

40. A systems administrator has deployed all updated patches for Windows-based machines. However, the users on the network are experiencing exploits from various threat actors, which the patches should have corrected. Which of the following is the *most* likely scenario here?

A. The machines were infected with malware.

B. The users did not reboot their computers after the patches were deployed.

C. The systems administrator used invalid credentials to deploy the patches.

D. The patches were deployed on non-Windows-based machines.

41. A penetration tester is trying to gain access to a remote system. The tester can see the secure login page and knows one user account and email address but has not discovered a

password yet. Which of the following would be the *easiest* method of obtaining a password for the known account?

A. Man-in-the-middle

B. Reverse engineering

C. Social engineering

D. Hash cracking

42. An external hacker has managed to exploit an unpatched vulnerability in a web application server. They were able to use the web application service account to download malicious software. The attacker tried (unsuccessfully) to gain root privileges to install the software and was subsequently discovered. The server admin team rebuilt and patched the server. Which of the following should the team perform to prevent a similar attack in the future?

A. Remove the application service account

B. Air gap the web application server

C. Configure SELinux and set it to enforcing mode

D. Schedule regular restarts of the service to terminate sessions

E. Use Nmap to perform regular uncredentialed vulnerability scans

43. A manufacturing company is deploying IoT locks, sensors, and cameras, which operate wirelessly. The devices will be used to allow physical access by locking and unlocking doors and other access points. Recent CVEs have been listed against the devices, for which the vendor has yet to provide firmware updates. Which of the following would *best* mitigate this risk?

A. Connect the IoT devices directly to ethernet switches and create a segmented VLAN.

B. Require sensors to digitally sign all transmitted control messages.

C. Add all the IoT devices to an isolated wireless network and use WPA2 and EAP-TLS.

D. Implement a wireless intrusion detection system.

44. A forensics investigator is following up on an incident where suspicious images have been stored on an employee's computer. The computer is currently powered off in the employee's workspace. Which of the following tools is *best* suited to retrieving full or partial image files from the storage device, which have been deleted so that the attacker evades detection?

A. `memdump`

B. `foremost`

C. `dd`

D. `nc`

45. An aerospace company is adding promotional material to a public-facing web application server. The server will host a website containing many images, highlighting a production plant and test facilities. The CISO is concerned that the images may contain geographic coordinates in the metadata, and some of the physical locations need to remain secret. What tool can be used to ensure that the images will not contain sensitive data within the metadata?

A. grep

B. ExifTool

C. Tcpdump

D. Wireshark

46. A critical service on a production system keeps crashing at random times. The systems administrator suspects that the code has not been adequately tested and may contain a bug. When the service crashes, a memory dump is created in the `/var/log` directory. Which of the following tools can the systems administrator use to reproduce these symptoms?

A. DAST

B. Vulnerability scanner

C. Core dump analyzer

D. Hex dump

47. Ontario Outdoors Inc is expecting major disruptions due to a winter weather warning. The CISO has been reviewing company policies to ensure adequate provisions are in place to deal with these environmental impacts and finds that some are missing or incomplete. The CISO must ensure that a document is immediately drafted to move various personnel and equipment to other locations to avoid downtime in operations. What is this an example of?

A. A disaster recovery plan

B. An incident response plan

C. A business continuity plan

D. A risk avoidance plan

48. Acme corporation operates a nuclear power station and relies on a legacy ICS to perform equipment monitoring functions. Regulatory compliance requires that this monitoring is mandatory. Penalties for non-compliance could be costly. The ICS has known vulnerabilities but cannot be updated or replaced. The company has been refused cyber-liability insurance.

Which of the following would be the *best* option to manage this risk in the company's production environment?

A. Avoid the risk by removing the ICS from production

B. Transfer the risk associated with the ICS vulnerabilities

C. Mitigate the risk by restricting access to the ICS

D. Accept the risk and upgrade the ICS when possible

49. Following a security incident, forensics has handed over a database server to the server admin team to begin the recovery phase. The team is looking to deploy an automated build by running a script. When accessing the Bash shell, they observe the following command as the most recent entry in the server's shell history:

```
dd if=dev/sda of=dev/sdb
```

Which of the following *most* likely occurred?

A. Forensics have used binary analysis tools to search the metadata.

B. The drive was cloned for forensic analysis.

C. The hard drive was formatted after the incident.

D. There is evidence that the forensics team may have missed.

50. A software engineer is looking to implement secure code while the code is still in the development environment. The goal is to deploy code that meets stability and security assurance goals. Which of the following code analyzers will produce the desired results?

A. SAST

B. DAST

C. Fuzzer

D. Peer code review

Answers

1. **B**. Vendor lock-in. This makes it difficult to switch providers as the technology is often proprietary. See *Chapter 13*, *Applying Appropriate Risk Strategies*.

2. **D**. Source code escrow. External developers represent third-party risk. This can be mitigated by storing the code with an escrow service. This protects the IP of the developers but also protects the customer. See *Chapter 13*, *Applying Appropriate Risk Strategies*.

3. **A**. Data sovereignty. The type of data that's stored by a government department would typically have strict regulatory controls. A global CSP may store the data offshore. *See Chapter 13, Applying Appropriate Risk Strategies*.

4. **B** and **E**. This type of data would be labeled as PII and GDPR regulatory controls would be important as the patients and employees may be EU citizens. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

5. **A**. Crypto erase. The customer will not have physical access to the data, so they will not be able to ensure other methods of destruction can be implemented. Crypto Erase will render the data unrecoverable. See *Chapter 13, Applying Appropriate Risk Strategies*.

6. **C**. **International Organization for Standardization** (**ISO**). This will ensure that the products will be suitable across international boundaries. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

7. **B**. **Capability Maturity Model Integration** (**CMMI**). This accreditation is required to tender for US government software contracts. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

8. **A**. **Payment Card Industry Data Security Standard** (**PCI DSS**). Storage and processing of customer card details will be subject to PCI DSS compliance. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

9. **A**. **General Data Protection Regulation** (**GDPR**). As this is not government or payment card data, then the focus will be on customers based in the EU. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

10. **B**. Export controls. This is important when you're exporting technology. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

11. **C**. **Non-disclosure agreement** (**NDA**). This is legally enforceable and protects intellectual property. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

12. **B**. **Master service agreement** (**MSA**). This is useful when it is necessary to set baseline terms for future services. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

13. **A**. **Service-level agreement** (**SLA**). This will allow the customer and the service provider to agree upon delivered services and the metrics that will be used to measure performance. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

14. **D**. **Interconnection security agreement** (**ISA**). This is important for documenting the details when a connection is made between two or more parties. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

15. **E**. **Privacy-level agreement** (**PLA**). This is very important when you're looking to assure customers who must adhere to strict regulatory compliance. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

16. **C**. Legal holds. This ensures that the data will be retained for any legal process. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

17. **C**. **Memorandum of understanding** (**MOU**). This is not a legal document but it can be very useful when there needs to be co-operation between two or more parties. See *Chapter 14, Compliance Frameworks, Legal Considerations, and Their Organizational Impact*.

18. **B**. Recovery time objective. A recovery time objective is a planning objective that is set by stakeholders within the business. It may be cost-driven and requires careful consideration. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

19. **B**. Warm site. A warm site will not be as costly as a hot site but will not be operational until data is restored and staff are available to operate the site. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

20. **A**. Autoscaling. This allows the company to access additional computing power using automation. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

21. **B**. CASB. The company data must be protected in the cloud. Not all users will originate from a company network, so NGFW and SWG will not work. DLP does not address all the requirements. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

22. **C**. Tabletop exercises. Stakeholders will discuss how they will act when dealing with a presented scenario. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

23. **C**. Bootstrapping. This allows the automated deployment of customized workloads from a standard base image. PowerShell **Desired State Configuration** (**DSC**) is an example of this technology. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

24. **C**. Content Delivery Network. This allows the timely delivery of time-sensitive services and reduces latency. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

25. **B**. **Data Distribution Service** (**DDS**). DDS has built-in provisions for **Quality of Service** (**QoS**). See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

26. **B**. Port Scanner. Nmap is a good choice for the following:

```
Scanning www.comptia.org (52.165.16.154) [1000 ports]

Discovered open port 443/tcp on 52.165.16.154

Discovered open port 80/tcp on 52.165.16.154
```

`Completed SYN Stealth Scan at 15:36, 9.18s elapsed (1000 total ports)`

See *Chapter 5*, *Threat and Vulnerability Management*.

27. **B**. Traffic intended for the systems is dropped. A good example of this technique is **Remote Triggered Black Hole** (**RTBH**) routing. See *Chapter 1*, *Designing a Secure Network Architecture*.

28. **B**. MITRE ATT&CK. MITRE receives government funding to carry out research and is well known for its published attack frameworks and tactics. The matrices are created to understand the tactics and techniques that attackers will use against operating systems, cloud network mobility, and industrial control systems. See *Chapter 5*, *Threat and Vulnerability Management*.

29. **A**. NIDS. Such systems protect an organization from inbound threats across the network. The technology is primarily passive, generating alerts that must be actioned by SOC staff. See *Chapter 1*, *Designing a Secure Network Architecture*.

30. **C**. Single-tenancy SaaS. As the CSP will be hosting and managing the company services, then the service that the customer is paying for will be **Software as a Service** (**SaaS**) to isolate the workloads. They can pay a premium to have a single tenancy. See *Chapter 3*, *Enterprise Data Security, Including Secure Cloud and Virtualization Solutions*.

31. **D** and **G**. The clients may not trust the issuing `CA-classroom.classroom.local` by default. LDAPS does not support wildcard certificates.

    The first issue that the server team solved was the problem that LDAPS does not support wildcard certificates. The second problem is most likely that the **certificate authority** (**CA**) is not trusted. If this is an internal CA, then the root CA certificate will need to be installed in the trusted enterprise store of all client computers. See *Chapter 12*, *Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs*.

32. **A**. Recovery point objective. When data must be available to service a mission-critical service, then the recovery point objective metric must be used. See *Chapter 15*, *Business Continuity and Disaster Recovery Concepts*.

33. **D**. Deploy decoy files on hosts systems on the same network segment. If an APT has access to the network, then a decoy file will be a good test to observe any malicious activity. See *Chapter 7*, *Risk Mitigation Controls*.

34. **B**. `TLS_RSA_WITH_RC4_128_SHA`. RC4 is weak encryption and will not be used in any regulated industries. See *Chapter 11*, *Implementing Cryptographic Protocols and Algorithms*.

35. **C**. Enforcing. To run an SElinux policy and make **Mandatory Access Control** (**MAC**) effective, the systems must be *powered* up in enforced mode. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

36. **C**. Watermarking. If an organization wants to detect theft or exfiltration of sensitive data, then documents can be checked out from an information system, but an automatic watermark will be applied to the document using the identity of the user who checked out the document. See *Chapter 3*, *Enterprise Data Security, Including Secure Cloud and Virtualization Solutions*.

37. **B**. CASB. A CASB is often referred to as a gatekeeper that protects the enterprise data from inbound threats into the cloud and outbound threats such as data exfiltration. Another benefit of CASB is to ensure regulatory compliance, by labeling and monitoring the use of the data, to ensure compliance. See *Chapter 15*, *Business Continuity and Disaster Recovery Concepts*.

38. **B**. VPN links. A VPN allows traffic to be secured when it's passing through untrusted networks. If the external traffic uses weak encryption, then it could be accessed by an adversary. See *Chapter 1*, *Designing a Secure Network Architecture*.

39. **B** and **D**.

    ```
    SRC Any DST 10.10.0.4 PORT 23 PROT TCP ACTION Deny

    SRC Any DST 10.10.0.50 PORT 80 PROT TCP ACTION Deny
    ```

    Port `23` supports the telnet protocol; this allows unsecured traffic to be sent when you're configuring equipment across a network. Port `80` allows for unsecured web traffic. Port `53` is for DNS traffic; this does not transmit passwords or sensitive data. Port `88` is Kerberos; this encrypts the transmission of user login traffic. Port `22` is SSH, encrypting traffic is used to access a console session on another host system. See *Chapter 1*, *Designing a Secure Network Architecture*, for more information on firewall rules.

40. **B**. The users did not reboot the computer after the patches were deployed. Certain patches may not be effective until the operating system is rebooted. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

41. **C**. Social engineering. Once an attacker has access to credentials, the most likely exploit to reveal a password is social engineering. See *Chapter 6*, *Vulnerability Assessment and Penetration Testing Methods and Tools*.

42. **C**. Configure SELinux and set it to enforcing mode. SELinux enforces mandatory access control, allowing for strict enforceable policies to be deployed. This would further restrict a compromised account from accessing other resources on the system. See *Chapter 9*, *Enterprise Mobility and Endpoint Security Controls*.

43. **C**. Add all the IoT devices to an isolated wireless network and use WPA2 and EAP-TLS. As all the devices connect wirelessly, they must be connected to a wireless segment. It is important to separate the network as there are vulnerable systems. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

44. **B**. Foremost. This is a forensics tool that can search for complete or partial files that have been deleted or hidden in some way. See *Chapter 8, Implementing Incident Response and Forensics Procedures*.

45. **B**. ExifTool. The following screenshot shows the partial output from ExifTool:

```
ExifTool Version Number         : 12.36
File Name                       : image1.jpg
Directory                       : .
File Size                       : 6.9 MiB
File Modification Date/Time     : 2021:05:02 09:07:40+01:00
File Access Date/Time           : 2021:12:12 16:47:16+00:00
File Inode Change Date/Time     : 2021:12:12 16:47:23+00:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
GPS Altitude                    : 297 m Above Sea Level
GPS Date/Time                   : 2021:01:06 15:07:31Z
GPS Latitude                    : 56 deg 34' 14.00" N
GPS Longitude                   : 3 deg 36' 39.00" W
Circle Of Confusion             : 0.005 mm
Field Of View                   : 69.4 deg
Focal Length                    : 4.2 mm (35 mm equivalent: 26.0 mm)
GPS Position                    : 56 deg 34' 14.00" N, 3 deg 36' 39.00" W
Hyperfocal Distance             : 2.14 m
Light Value                     : 8.8
```

Figure 17.3 – The GPS data from an image file

Using ExifTool allows an analyst to determine the location the image was taken from.

46. **A**. DAST. DAST tools allow a tester to recreate the error. See *Chapter 2, Integrating Software Applications into the Enterprise*.

47. **C**. A business continuity plan. A business continuity plan allows the organization to identify potential problems and have alternative plans of action. See *Chapter 15, Business Continuity and Disaster Recovery Concepts*.

48. **C**. Mitigate the risk by restricting access to the ICS. The only available course of action is to segment the network that contains the legacy equipment. This is a common approach when it comes to dealing with operational technology. See *Chapter 10, Security Considerations Impacting Specific Sectors and Operational Technologies*.

49. **B**. The drive was cloned for forensic analysis. See *Chapter 8, Implementing Incident Response and Forensics Procedures*.

50. **A**. SAST. The code is still in the development environment, so SAST will be the most appropriate option here. See *Chapter 2, Integrating Software Applications into the Enterprise*.

Hopefully, you enjoyed testing yourself with a typical mix of CASP questions. For more exam resources and extra content please visit https://www.casp.training.