

Figure 2.1: The control plane dictates how users and devices are authorized to access network resources

Chapter 3: *Explain the importance of change management processes and the impact to security*

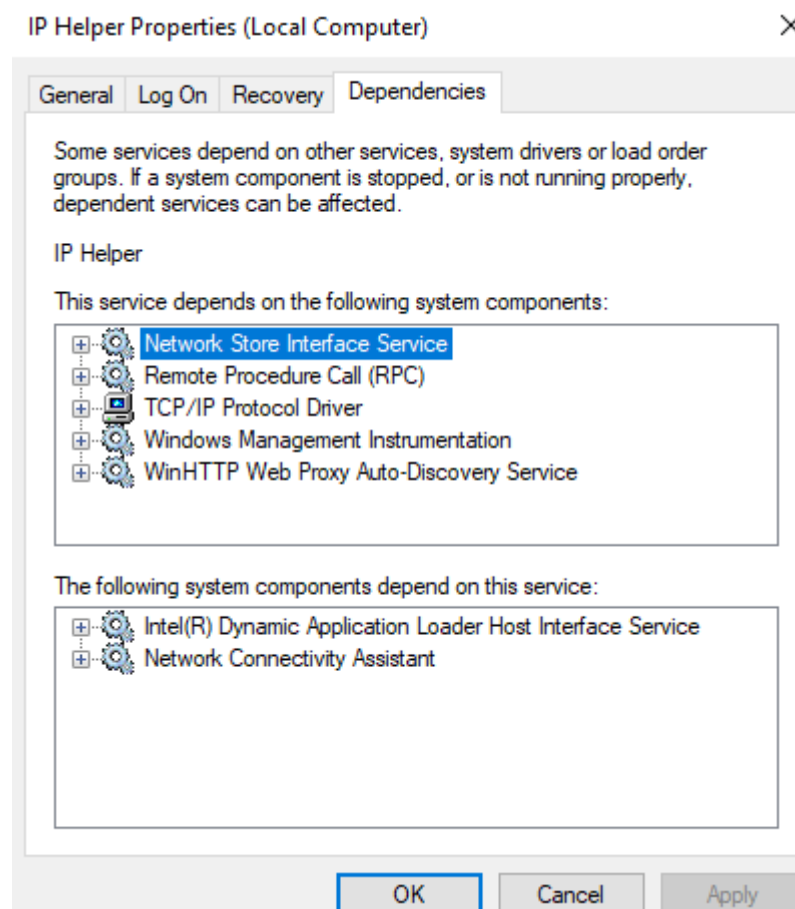


Figure 3.1: The IP Helper properties on a local computer

Chapter 10: *Compare and contrast security implications of different architecture models*

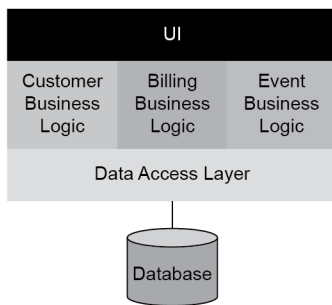


Figure 10.1: Different microservices from one UI accessing one database

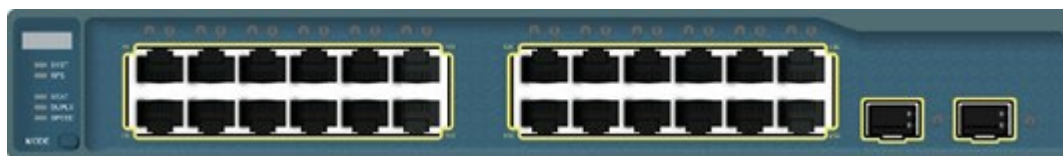


Figure 10.2: Switch the inputs and outputs of a switch in a LAN

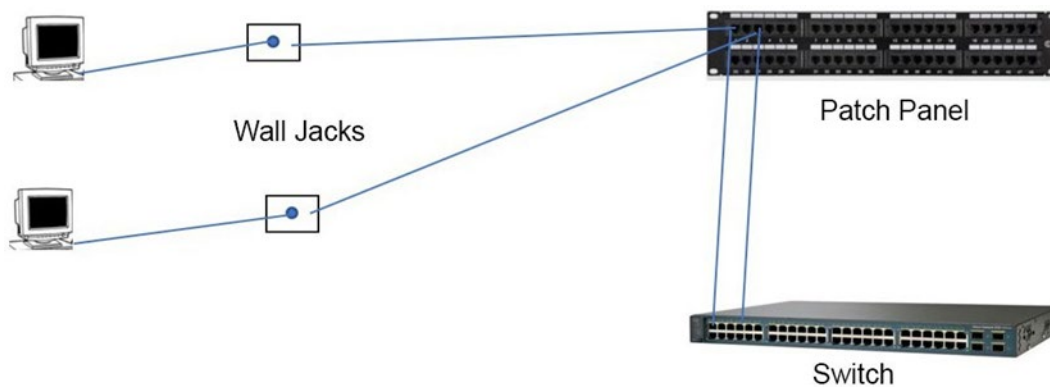


Figure 10.3: Network layout

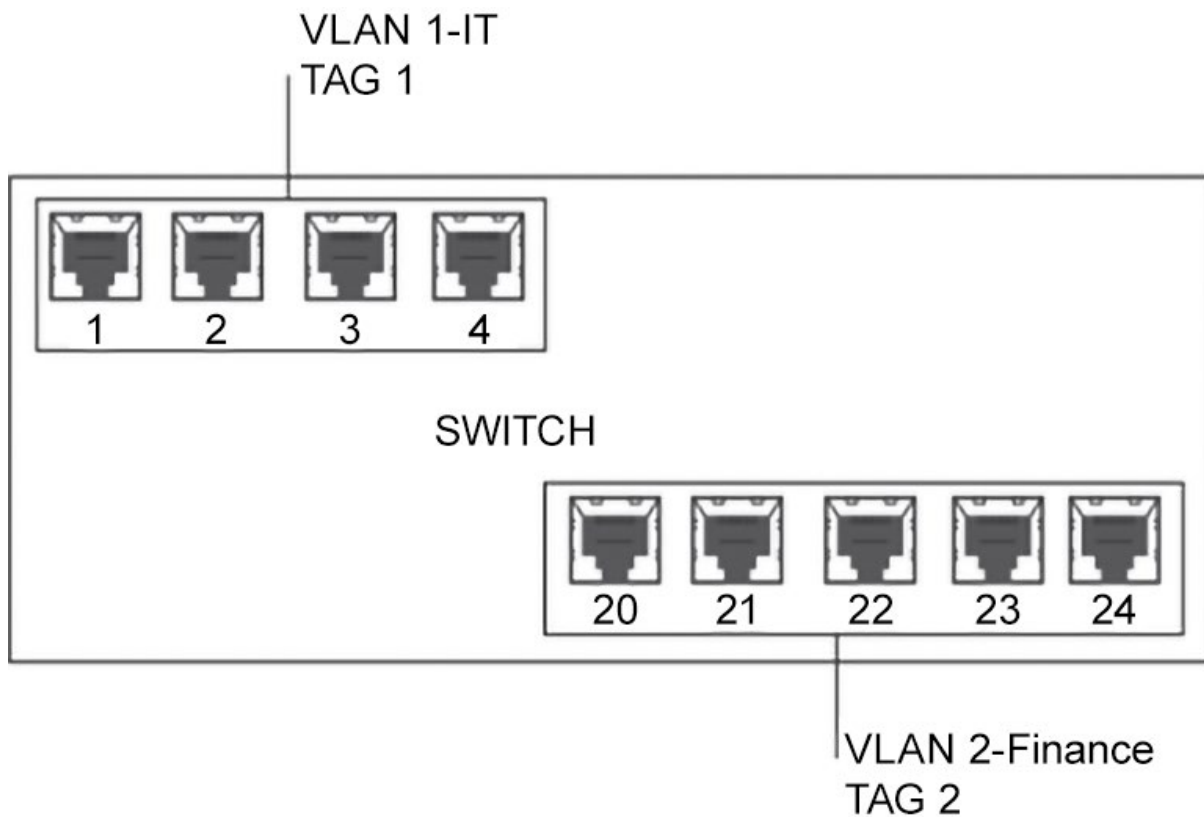


Figure 10.4: Two VLAN switches

Containers

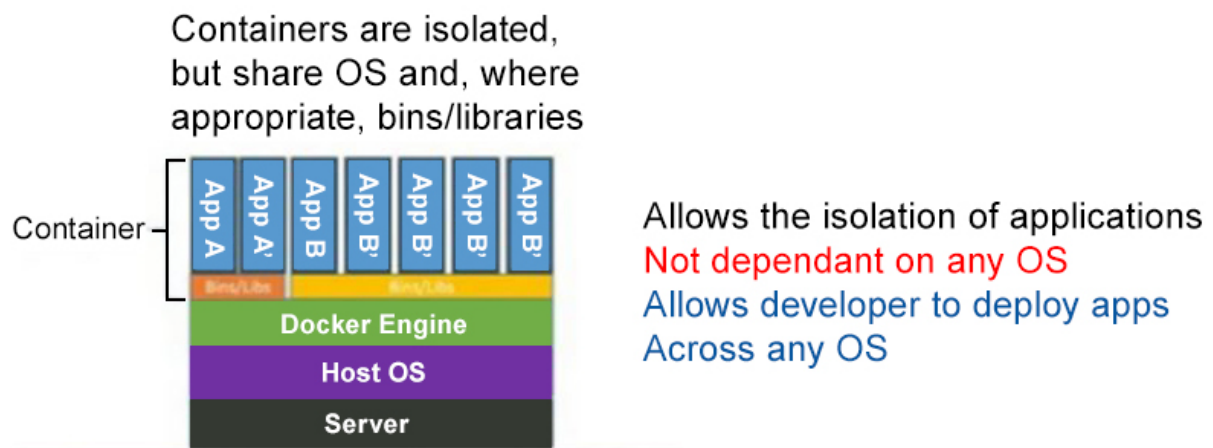


Figure 10.5: A typical container setup

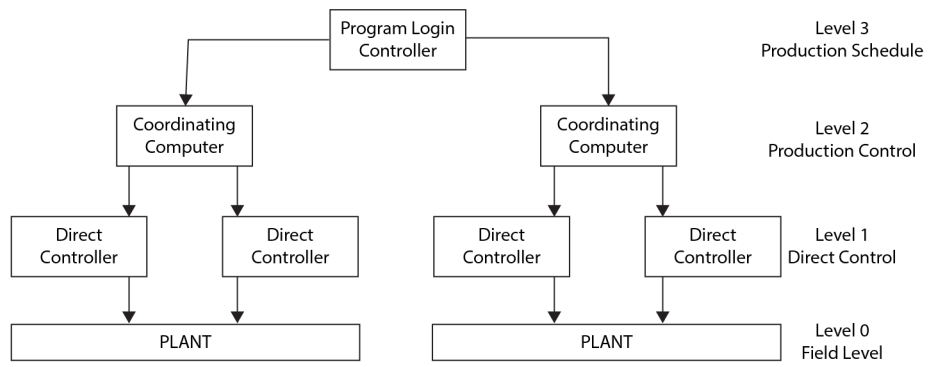


Figure 10.6: SCADA systems

Chapter 12: Compare and contrast concepts and strategies to protect data

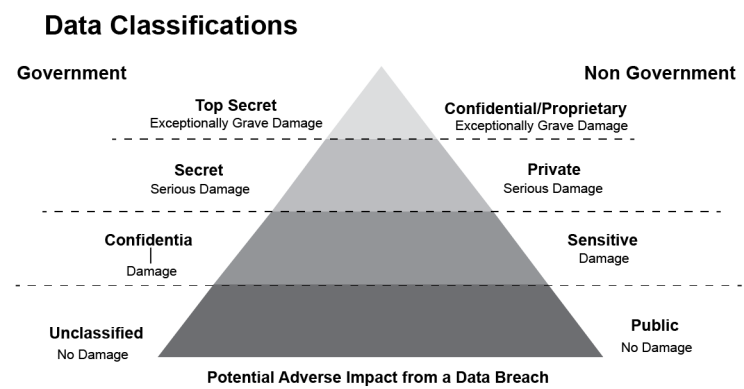


Figure 12.1: Governmental versus non-governmental data

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT 13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ROT 13	A	B	C	D	E	F	G	H	I	J	K	L	M

Table 12.2: ROT13 logical operation key

Chapter 13: *Explain the importance of resilience and recovery in security architecture*

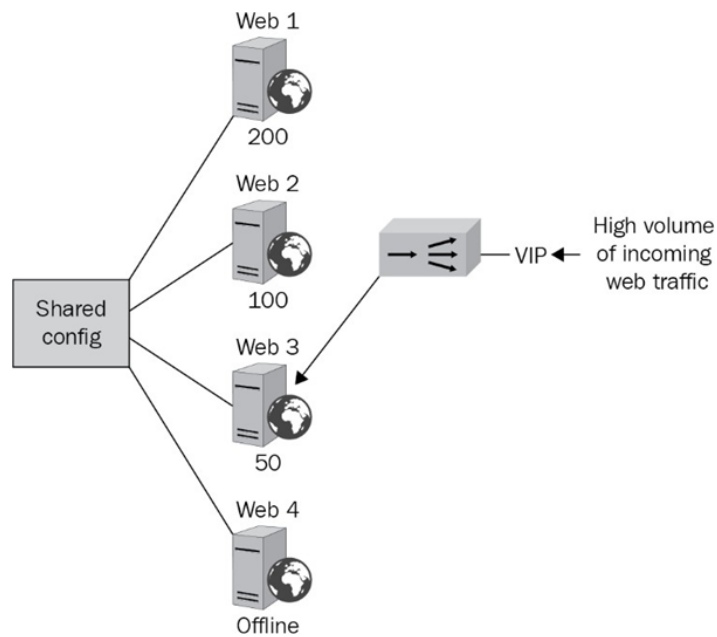


Figure 13.1: Load balancer layout

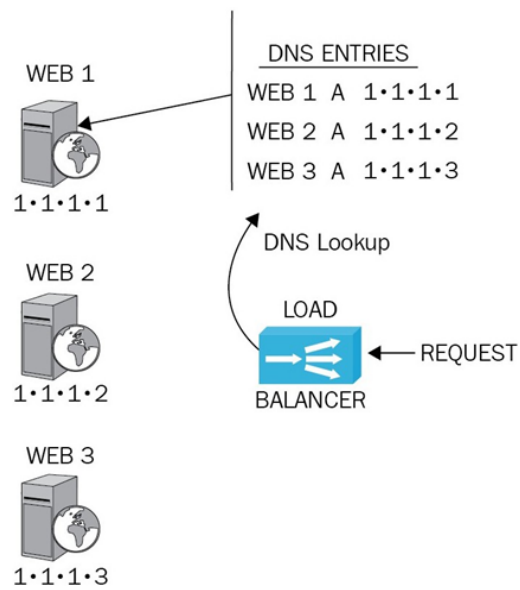


Figure 13.2: DNS round robin

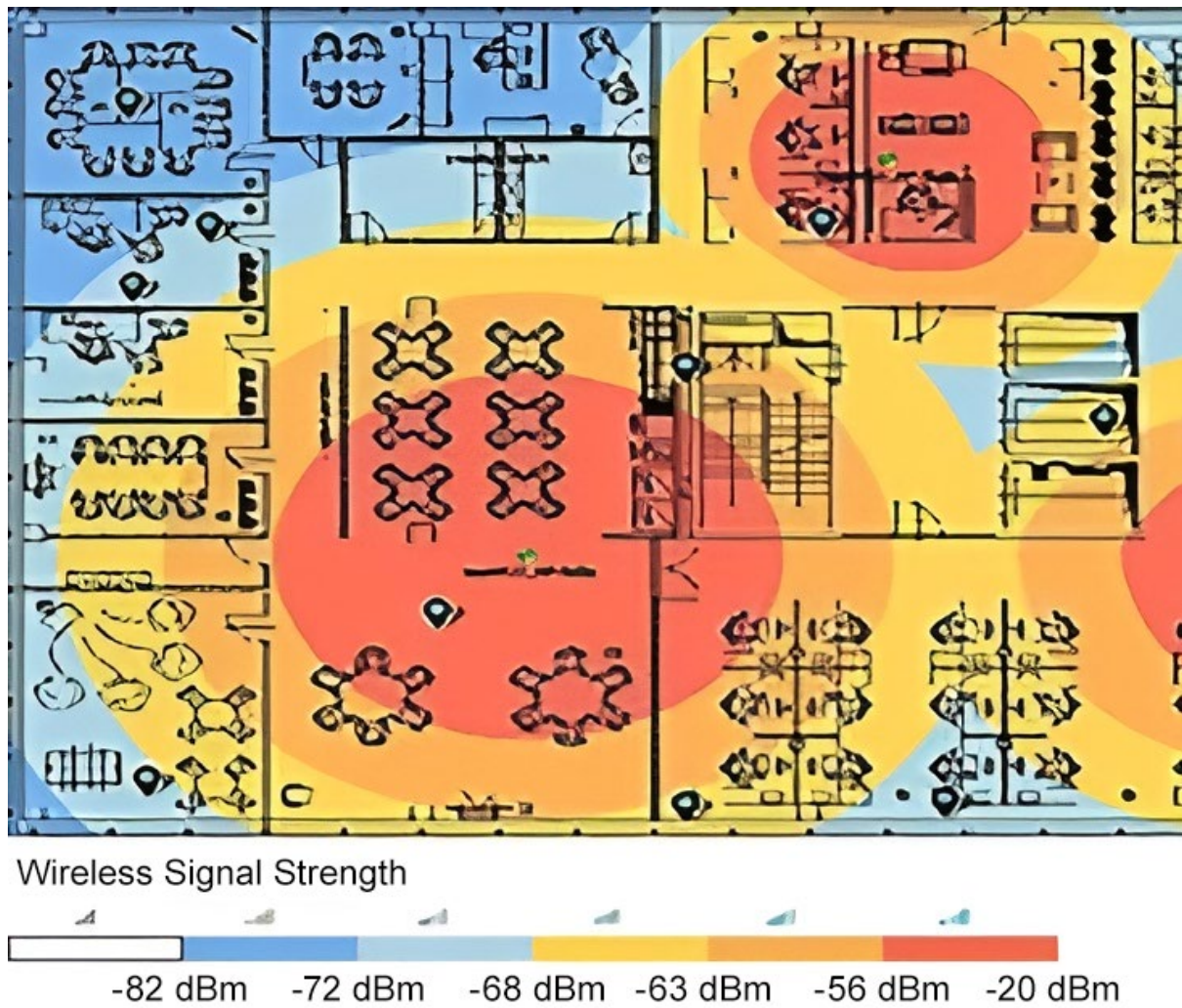



Figure 14.1: Example heat map of wireless networks

Chapter 16: Explain various activities associated with vulnerability management



[CVE List](#) [CNAs](#) [WGs](#)

Search CVE ListDownloadsData FeedsUpd

TOTAL CVE Records: 2150

NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](#)

NOTICE: Legacy CVE List download formats will be phased out. New CVE List download format is available.

HOME > CVE > SEARCH RESULTS

Search Results

There are 2506 CVE Records that match your search.

Name	Description
CVE-2023-5752	When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the setup script (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This is a separate vulnerability.
CVE-2023-5557	A flaw was found in the tracker-miners package. A weakness in the sandbox allows a maliciously-crafted file to escape the sandbox and access the host file system.
CVE-2023-4990	Directory traversal vulnerability in MCL-Net versions prior to 4.6 Update Package (P01) may allow attackers to read arbitrary files on the system.
CVE-2023-4918	A flaw was found in the Keycloak package, more specifically org.keycloak.userprofile. When a user registers, their attributes are added as regular user attributes. All users and clients with proper rights and roles are able to read users' attributes, potentially exposing sensitive information and jeopardizing their environment.

Figure 16.1: The CVE list—package vulnerabilities

Chapter 17: *Explain security alerting and monitoring concepts and tools*

03/02/2023 23:52:06	Succeed	Move	File	
	C:\WINDOWS\System32\drivers\Synth3dVsp.sys			Operation aborted - not in setup
03/02/2023 23:52:06	Succeed	Move	File	
	C:\WINDOWS\System32\drivers\pcip.sys			Operation aborted - not in setup
03/02/2023 23:52:06	Succeed	Move	File	
	C:\WINDOWS\System32\drivers\vpcivsp.sys			Operation aborted - not in setup
03/02/2023 23:52:06	Succeed	Move	File	
	C:\WINDOWS\System32\drivers\storvsp.sys			Operation aborted - not in setup

Figure 17.1: Log file

```
^(?;4[0-9]{12}(?:[0-9]{3}?|[25][1-7][0-9]{14}|6(?:011)5[0-9]
[0-9])[0-9]{12}|3[47][0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}
|(?:2131|1800|35\d{3}\d{11}))$
```

Figure 17.2: A regex string for capturing credit card data

Chapter 18: Given a scenario, modify enterprise capabilities to enhance security

Firewall or Router - ACL		
Allow	TCP Port 80	HTTP
Allow	TCP Port 443	HTTPS
Allow	TCP Port 53	DNS
Allow	UDP Port 53	DNS
Last Rule	Deny All	

FTP Traffic

Implicit Deny: With no allow rule granting permission, final rule applies

Figure 18.1: Implicit deny

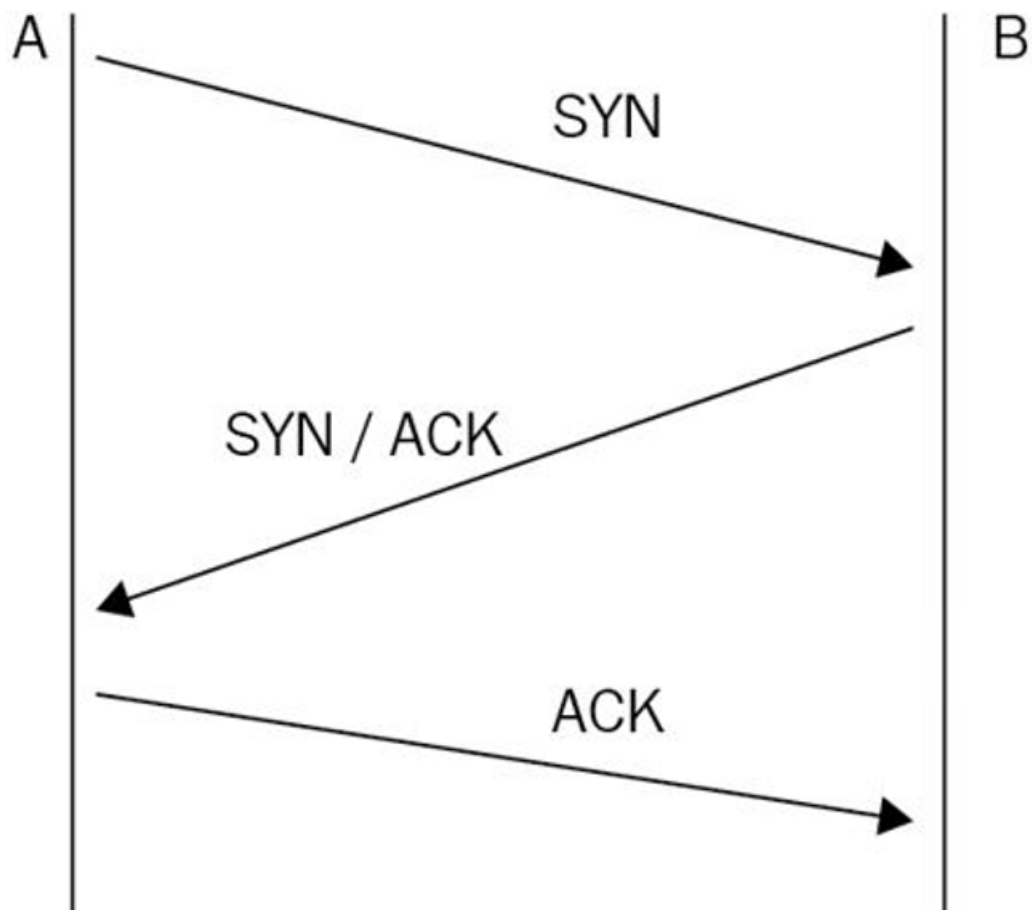


Figure 18.2: The TCP/IP three-way handshake

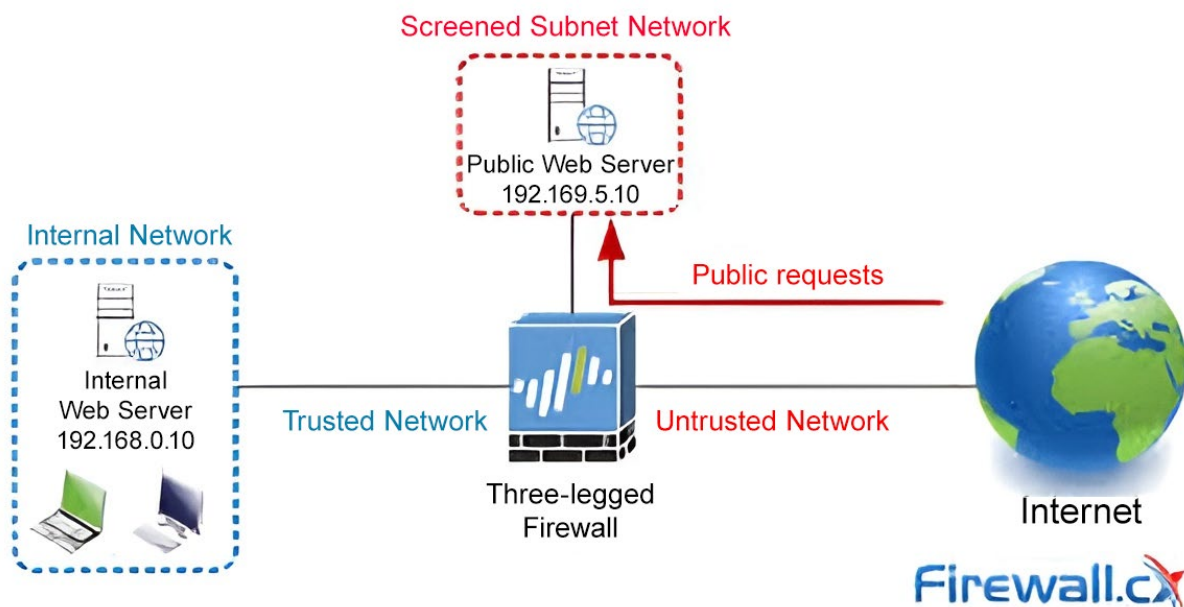


Figure 18.3: A three-legged/triple-horned firewall

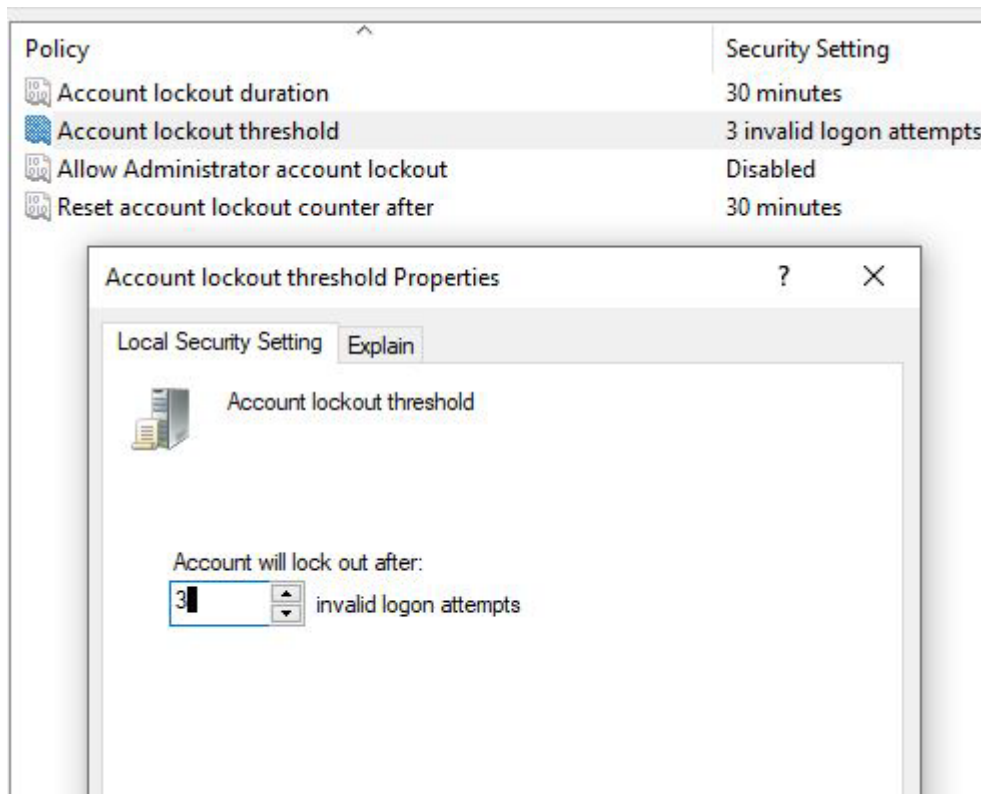


Figure 18.4: Account lockout policy

```
C:\WINDOWS\system32>sfc/scannow
```

Beginning system scan. This process will take some time.

Beginning verification phase of system scan.

Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them. For online repairs, details are included in the CBS log file located at windir\Log\CBS\CBS.log. For example C:\Windows\Log\CBS\CBS.log. For offline repairs, details are included in the log file provided by the /OFFLOGFILE flag.

Figure 18.5: Output of the file integrity monitor

Chapter 19: *Given a scenario, implement and maintain identity and access management*

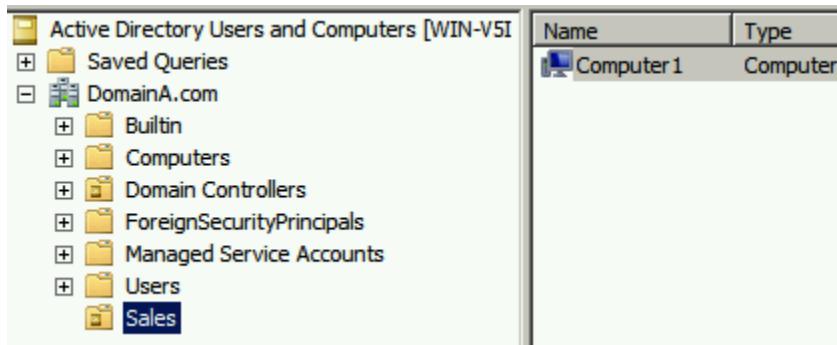


Figure 19.1: Active Directory

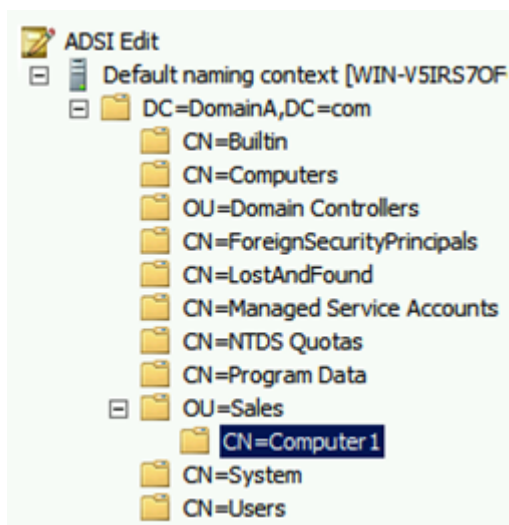


Figure 19.2: ADSI Edit

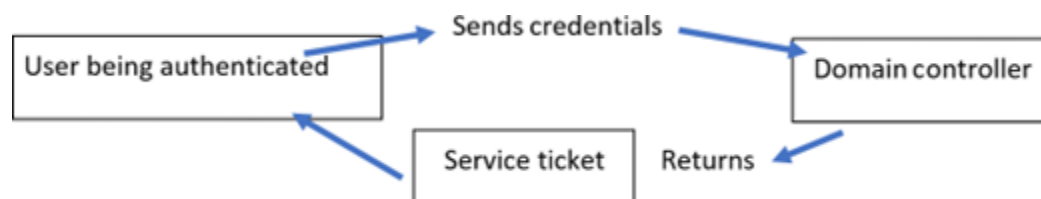


Figure 19.3: TGT

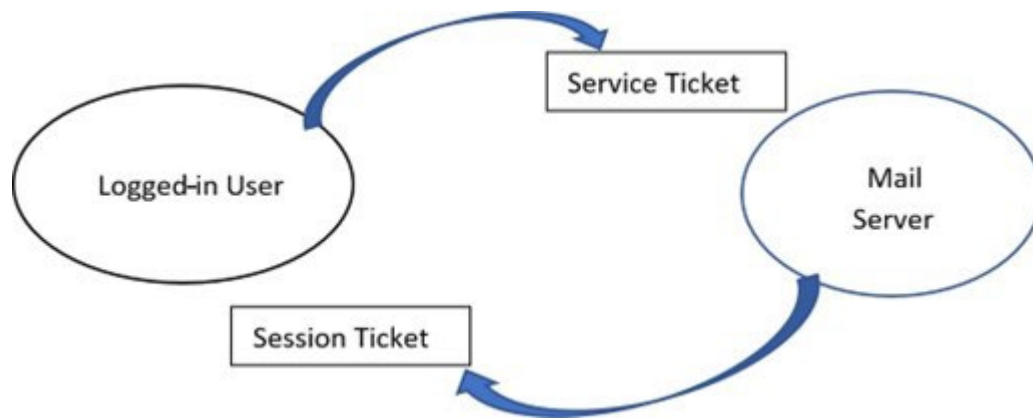


Figure 19.4: Mutual authentication



Figure 19.5: Group-based access

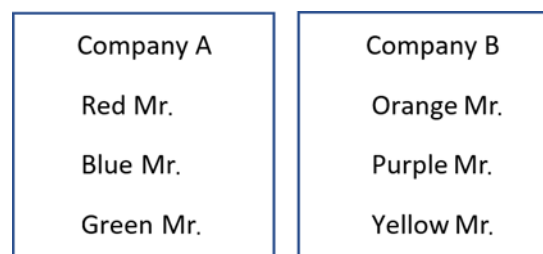


Figure 19.6: Directory services listing for a joint ventures

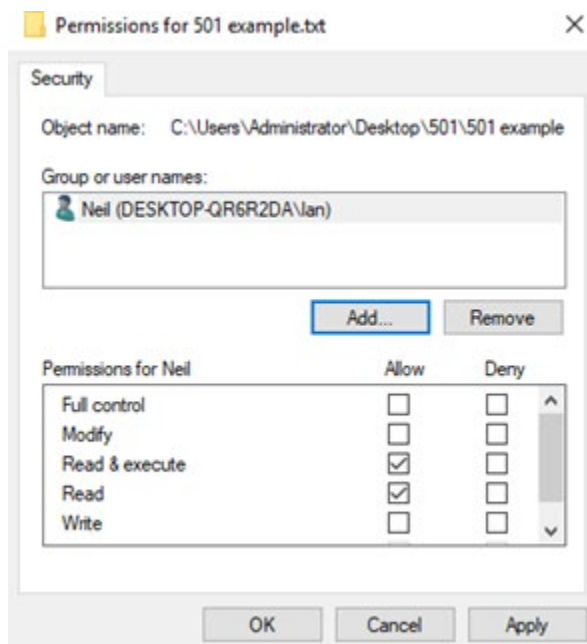


Figure 19.7: Discretionary Access Control

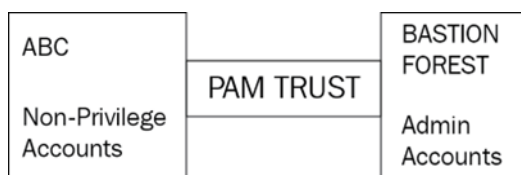


Figure 19.8: PAM

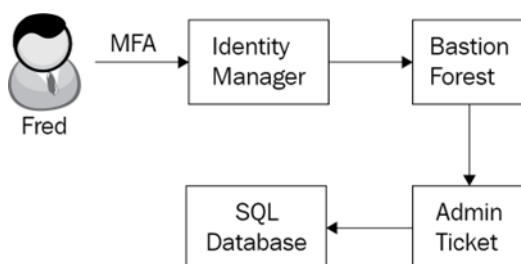


Figure 19.9: Secure access workflow for database administration

Chapter 21: *Explain appropriate incident response activities*

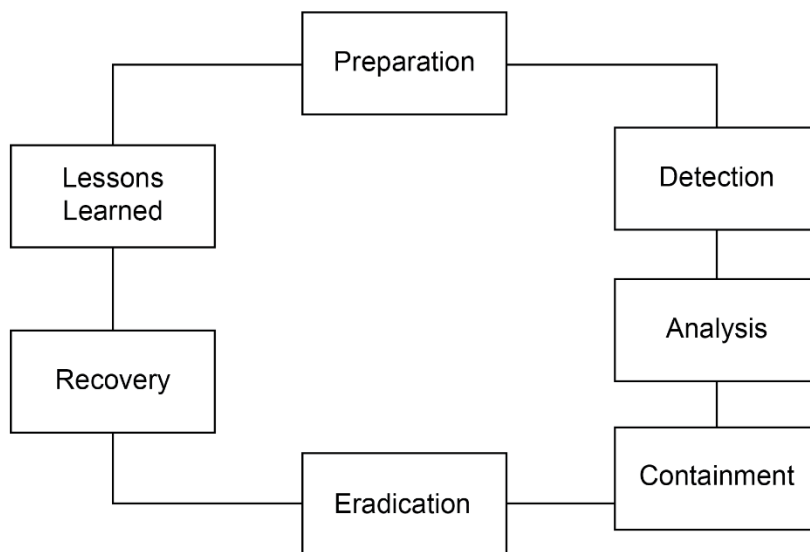


Figure 21.1: Incident response process

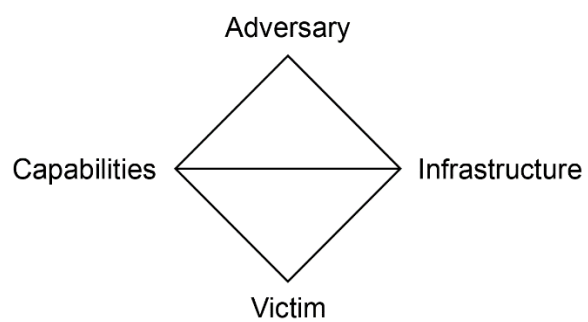


Figure 21.2: Diamond model of intrusion analysis

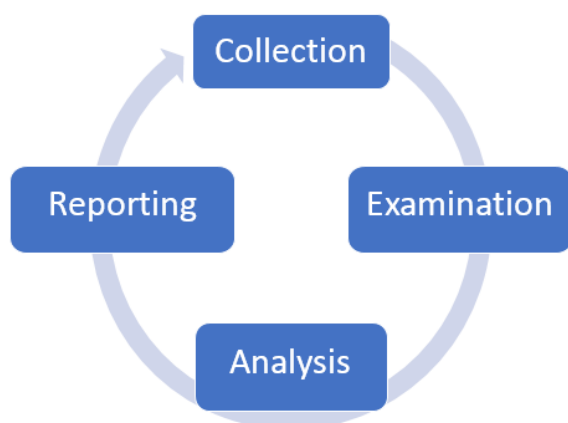


Figure 21.3: Forensics process

Chapter 23: *Summarize elements of effective security governance*

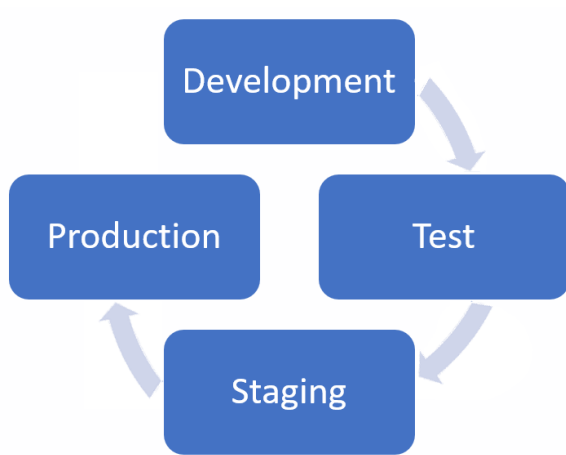


Figure 23.1: Software Development Life Cycle (SDLC)s

Chapter 24: *Explain elements of the risk management process*

I	Very High	7	10	20	25
M	High	7	7	15	20
P	Medium	4	5	7	15
A	Low	4	1	1	3
C		Low	Medium	High	Very High
T		LIKELIHOOD			

Figure 24.1: Risk matrix

Chapter 28: *Given a scenario, implement security awareness practices*

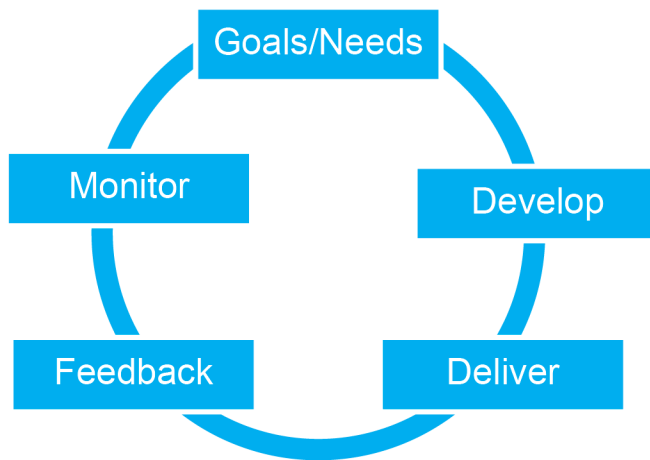


Figure 28.1: A security awareness practices framework

Chapter 29: Accessing the online practice resources

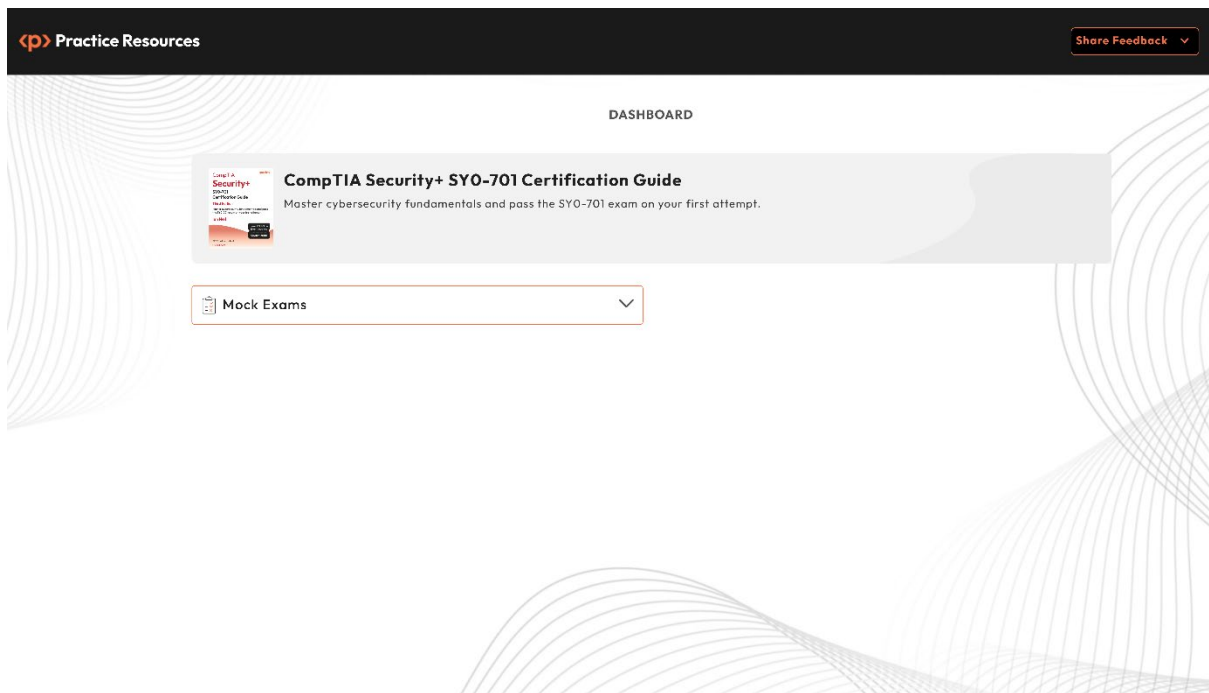


Figure 29.1: Online practice resources on a desktop device



Figure 29.2: QR code for the page that lets you unlock this book's free online content.

UNLOCK YOUR PRACTICE RESOURCES

With your copy of **CompTIA Security+ SY0-701 Certification Guide** you get access to online practice resources. Enter the sign-up code that came with your book to instantly unlock access.

CompTIA

Security+

SY0-701

Certification Guide

Third Edition

Master cybersecurity fundamentals and pass the SY0-701 exam on your first attempt

Ian Neil

Save 10% off on Exam voucher! Coupon inside!

FREE online content HDQKJ23456

Book

ISBN: 9781835461532

Ian Neil • Jan 2024

Do you have an account?

☐ Yes, I have an existing account

☐ No, I have don't have an account

PROCEED

Figure 29.3: Unlock page for the online practice resources

UNLOCK YOUR PRACTICE RESOURCES

With your copy of **CompTIA Security+ SY0-701 Certification Guide** you get access to online practice resources. Enter the sign-up code that came with your book to instantly unlock access.

CompTIA

Security+

SY0-701

Certification Guide

Third Edition

Master cybersecurity fundamentals and pass the SY0-701 exam on your first attempt

Ian Neil

Save 10% off on Exam voucher! Coupon inside!

FREE online content HDQKJ23456

Book

ISBN: 9781835461532

Ian Neil • Jan 2024

Enter Your Purchase Details

Enter Unique Code*

[Where To Find the Code?](#)

☐ Email me when new practice questions or features are added to the practice resources platform. Also, recommend me books related this one.

REQUEST ACCESS

Figure 29.4: Enter your unique sign-up code to unlock the resources

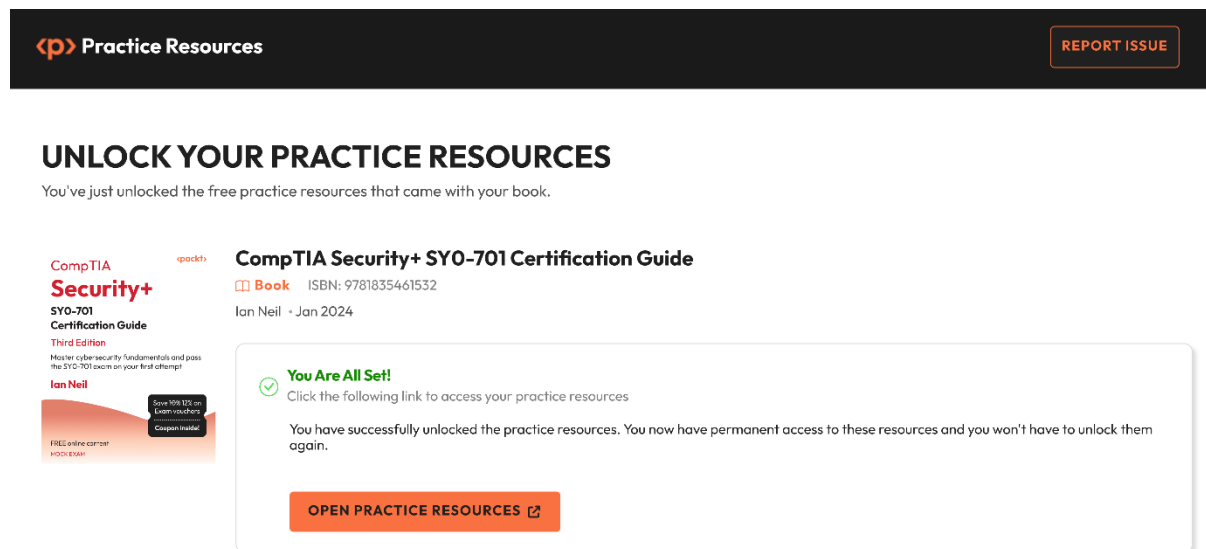


Figure 29.5: Page that shows up after a successful unlock

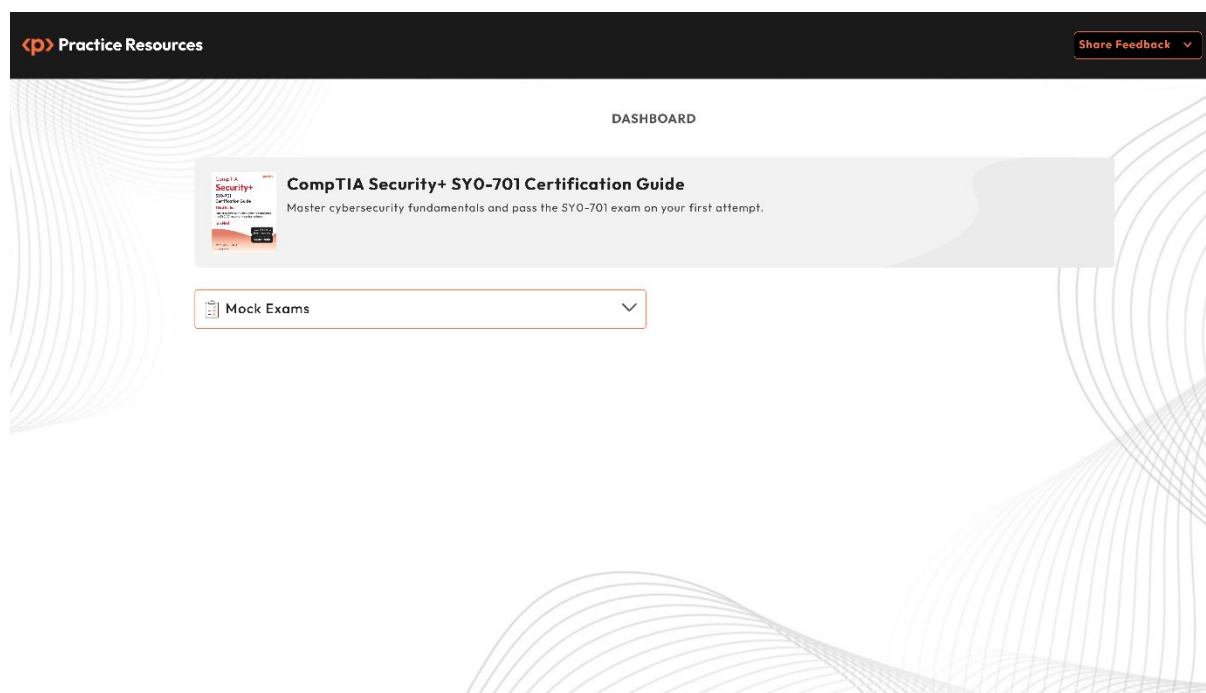


Figure 29.6: Dashboard page for CompTIA practice resources



Figure 29.7: QR code to bookmark practice resources website