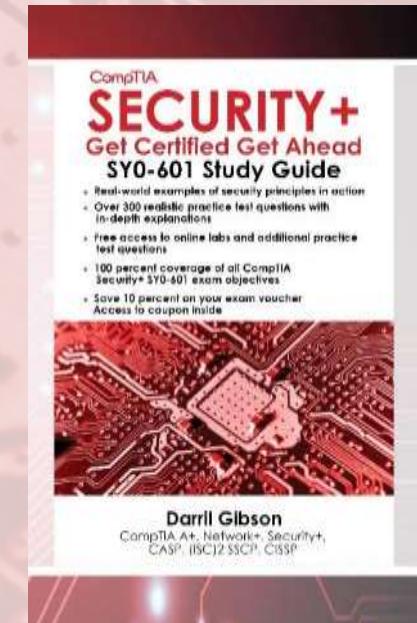


CompTIA Security+

Get Certified Get Ahead

By Darril Gibson

Introduction

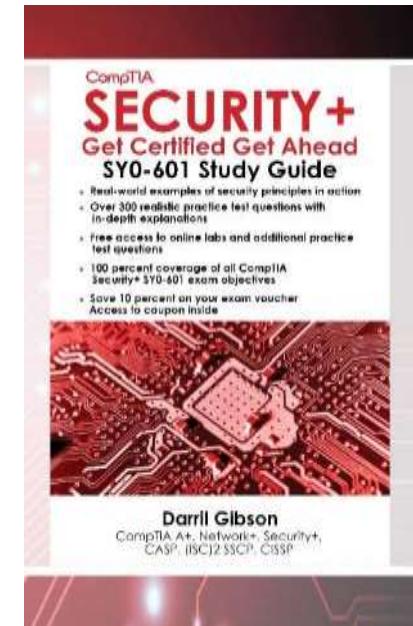


Course Materials

- CompTIA Security+:
Get Certified Get Ahead

SY0-601
Study Guide

By Darril Gibson



Course Outline

- Ch 1: Mastering Security Basics
- Ch 2: Exploring Control Types and Methods
- Ch 3: Exploring Network Technologies and Tools
- Ch 4: Securing Your Network
- Ch 5: Securing Hosts and Data
- Ch 6: Comparing Threats, Vulnerabilities, and Common Attacks

Course Outline (Cont)

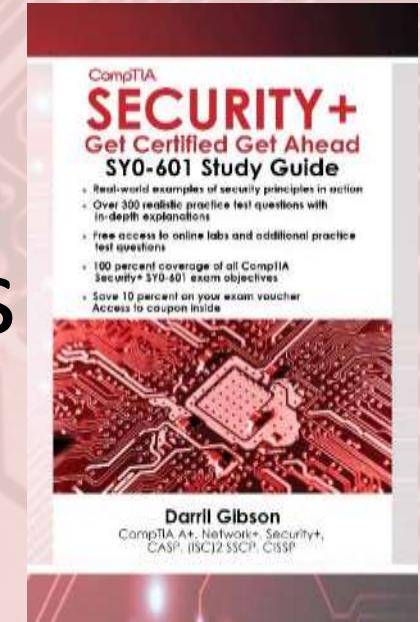
- Ch 7: Protecting Against Advanced Attacks
- Ch 8: Using Risk Management Tools
- Ch 9: Implementing Controls to Protect Assets
- Ch 10: Understanding Cryptography
- Ch 11: Implementing Policies to Mitigate Risks

Chapter 1

Mastering Security Basics

CompTIA Security+
Get Certified Get Ahead

By Darril Gibson

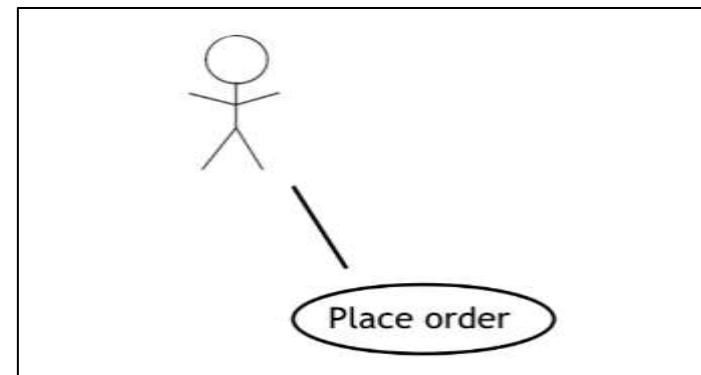


Introduction

- Understanding Core Security Goals
- Introducing Basic Risk Concepts
- Understanding Security Controls
- Using Command-Line Tools
- Understanding Logs

Understanding Core Security Goals

- Use Case
 - Describes a goal an organization wants to achieve
 - Elements
 - Actors
 - Precondition
 - Trigger
 - Postcondition
 - Normal flow
 - Alternate flow



Understanding Core Security Goals

- Confidentiality

- Encryption
- Access controls
 - Identification
 - Authentication
 - Authorization



Understanding Core Security Goals

- Availability
 - Redundancy & Fault tolerance
 - Scalability and Elasticity
- Patching
- Resiliency



Introducing Basic Risk Concepts

- Threats
 - Vulnerabilities
 - Any weakness
 - Risk is
 - The likelihood that a threat will exploit a vulnerability
 - Risk mitigation
 - Reduces the chances that a threat will exploit a vulnerability by implementing controls
-
- ```
graph TD; Threat[Threat] --> Exploits[Exploits]; Exploits --> Vulnerability[Vulnerability]; Vulnerability --> Loss[Resulting in Loss]
```
- The diagram consists of four red rounded rectangular boxes with white text. A red arrow points from the word 'Threat' to a red starburst icon labeled 'Exploits'. Another red arrow points from 'Exploits' to the word 'Vulnerability'. A final red arrow points from 'Vulnerability' to the text 'Resulting in Loss'.

# Understanding Security Controls

---

- Overview
  - Managerial controls are primarily administrative in function
  - Operational controls help ensure that the day-to-day operations of an organization comply with the security policy
  - Technical controls use technology

# Understanding Security Controls

---

- Managerial Controls
  - Risk assessments
  - Vulnerability assessments
- Operational Controls
  - Awareness and training
  - Configuration management
  - Media protection
  - Physical and environmental protection

# Understanding Security Controls

- Technical Controls
  - Encryption
  - Antivirus software
  - IDSs and IPSs
  - Firewalls
  - Least Privilege



# Control Types

---

- Preventative Controls
  - Hardening
  - Training
  - Security guards
  - Change management
  - Account disablement policy
  - Intrusion prevention system (IPS)



# Control Types

- Detective Controls
  - Log monitoring
  - SIEM systems
  - System audit
  - Video surveillance
  - Motion detection
  - Intrusion detection system (IDS)



# Control Types

---

- Corrective and Recovery Controls
  - Backups and system recovery
  - Incident handling processes
- Physical Controls
- Compensating Controls
- Response Controls

# Control Goals

---

- Deterrent
  - Attempt to discourage individuals from causing an incident
  - Cable locks, hardware locks
- Compare to prevention
  - Deterrent encourages people to *decide* not to take an undesirable action
  - Prevention stops them from taking an undesirable action
  - Security guard can be both



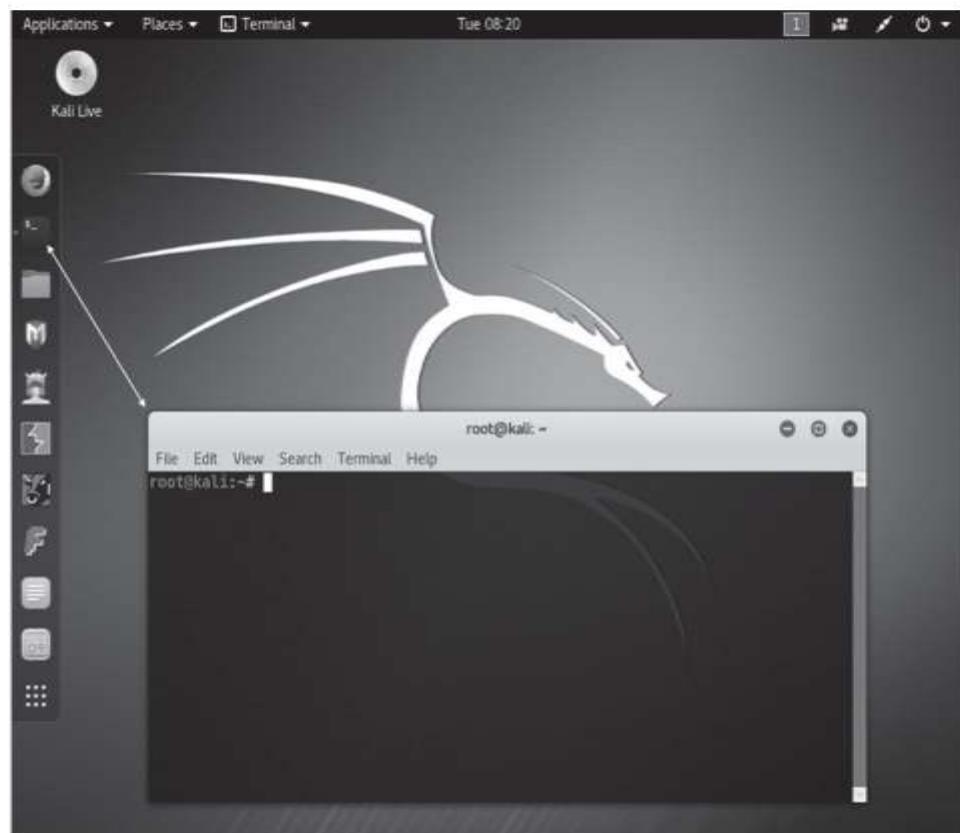
# Using Command-Line Tools

- Windows
  - Launch Command Prompt
  - Launch Command Prompt (Admin)



# Using Command-Line Tools

- Linux
  - Launch terminal in Kali



# Commands

---

- Ping
  - Basic command to test connectivity
    - ping 192.168.1.1
  - Firewalls and ICMP
  - Checking DNS name resolution

# Commands

---

- hping
- Ipconfig (Windows)
- ifconfig (Linux)
- Netstat
- Tracert and traceroute
- Pathping
- Arp

# Commands

---

- Linux and LAMP
  - cat
  - grep
  - head
  - tail
  - logger
  - journalctl
  - chmod

# Understanding Logs

---

- Windows Logs
  - Security log
  - System
  - Application log
- Network Logs
  - Security log



# Understanding Logs

---

- Centralized Logging Methods
- SIEM Systems
  - Syslog
    - Syslog-ng and Rsyslog
    - NXLog

# Linux Logs

---

- var/log/syslog
- var/log/messages
- var/log/boot.log
- var/log/auth.log
- var/log/faillog
- var/log/kern.log
- var/log/httpd/
  - Apache directory

# Appendix A Command Line Basics

---

- Free with the study guide online extras
  - Understanding Switches and Getting Help
  - Understanding Case
  - Understanding Linux Permissions
    - Read (R) Write (W) Execute (X)
- rwx rw- r- -
- drwx r- - - -

# Converting Linux Permissions to Numbers

---

- Octal 0 = Binary 0 0 0
- Octal 1 = Binary 0 0 1
- Octal 2 = Binary 0 1 0
- Octal 3 = Binary 0 1 1
- Octal 4 = Binary 1 0 0
- Octal 5 = Binary 1 0 1
- Octal 6 = Binary 1 1 0
- Octal 7 = Binary 1 1 1
- Octal 0 = Binary 0 0 0
  - No permissions (- - -)
- Octal 4 = Binary 1 0 0
  - Read (r - -)
- Octal 5 = Binary 1 0 1
  - Read and Execute (r - x)
- Octal 6 = Binary 1 1 0
  - Read and Write (r w -)
- Octal 7 = Binary 1 1 1
  - Read, Write, and Execute (r w x)

# Appendix B Logs

---

- Free with the study guide online extras
- Reading Logs
  - When it happened
  - Where it happened
  - What happened
  - Who did it
- Applying critical thinking skills

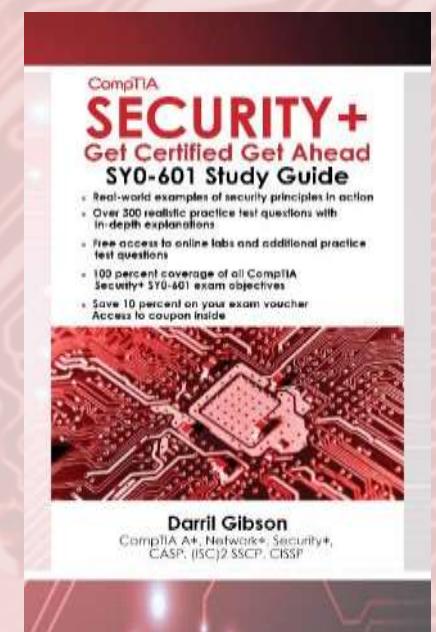
# Chapter 1 Summary

---

- Understanding Core Security Goals
- Introducing Basic Risk Concepts
- Understanding Security Controls
- Using Command-Line Tools
- Understanding Logs
- Check out the free online labs

# Chapter 2

## Understanding Identity and Access Management



## CompTIA Security+

### Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Exploring Authentication Management
- Managing Accounts
- Comparing Authentication Services
- Comparing Access Control Schemes

# Exploring Authentication Concepts

---

- Identification
  - User professes an identity
- Authentication
  - User proves identity
- Authorization
  - Access to resources granted based on proven identity

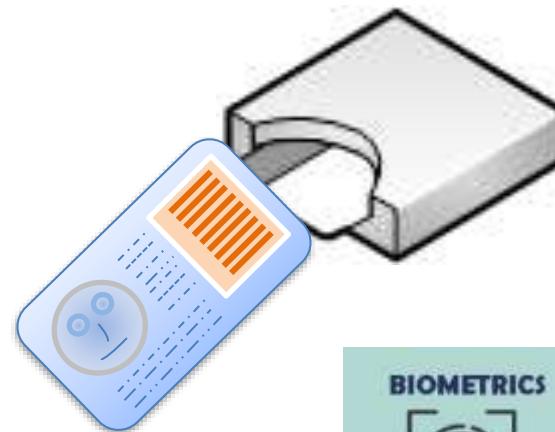
# Exploring Authentication Concepts

---

- AAA (authentication, authorization, and accounting)
- Accounting
- Audit trail

# Factors of Authentication

- Something you know
  - Such as username and password
- Something you have
  - Such as a smart card
- Something you are
  - Such as a fingerprint or other biometric identification



# Something You Know

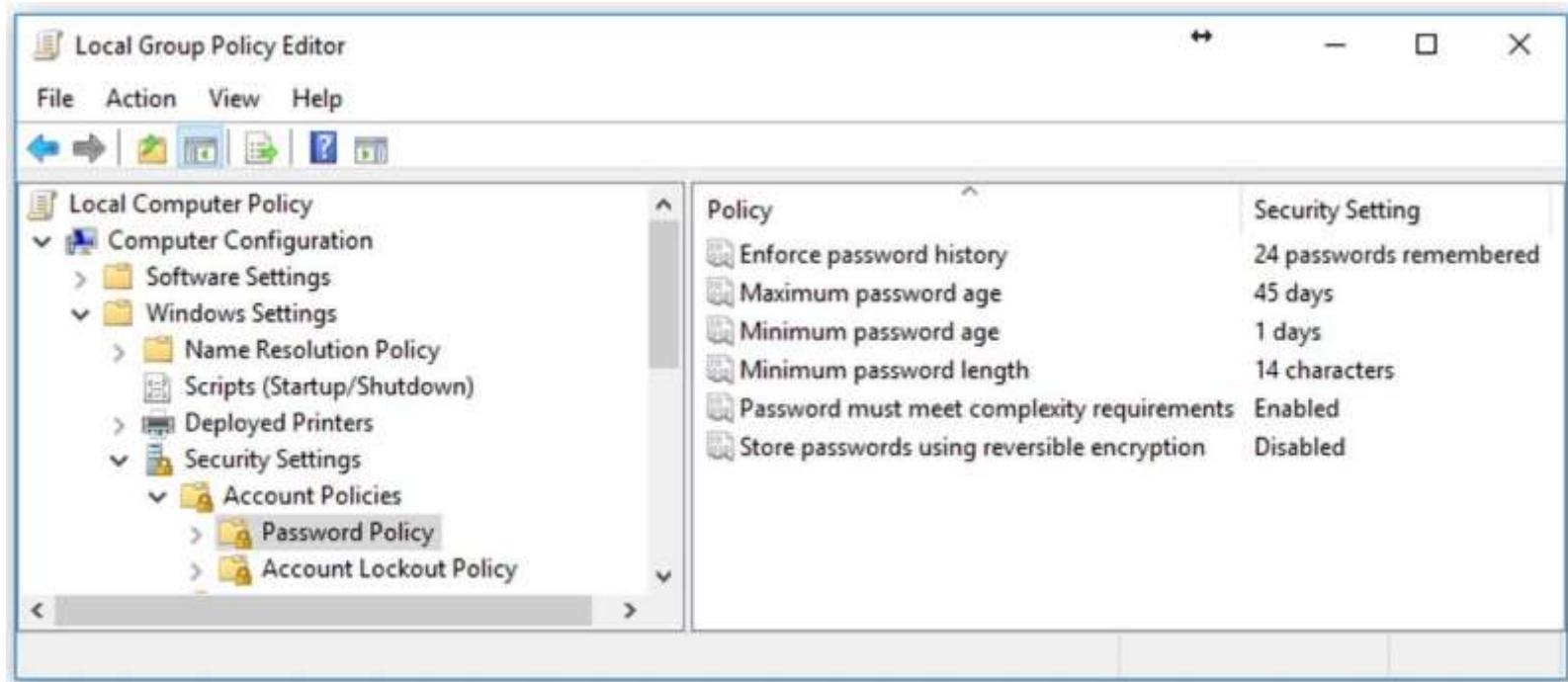
---

- Password complexity
  - Uppercase, lowercase, numbers, special characters
- Password expiration
  - Forces users to change password
- Password vaults
- Password history and password reuse
  - Prevents users from reusing same password



# Something You Know

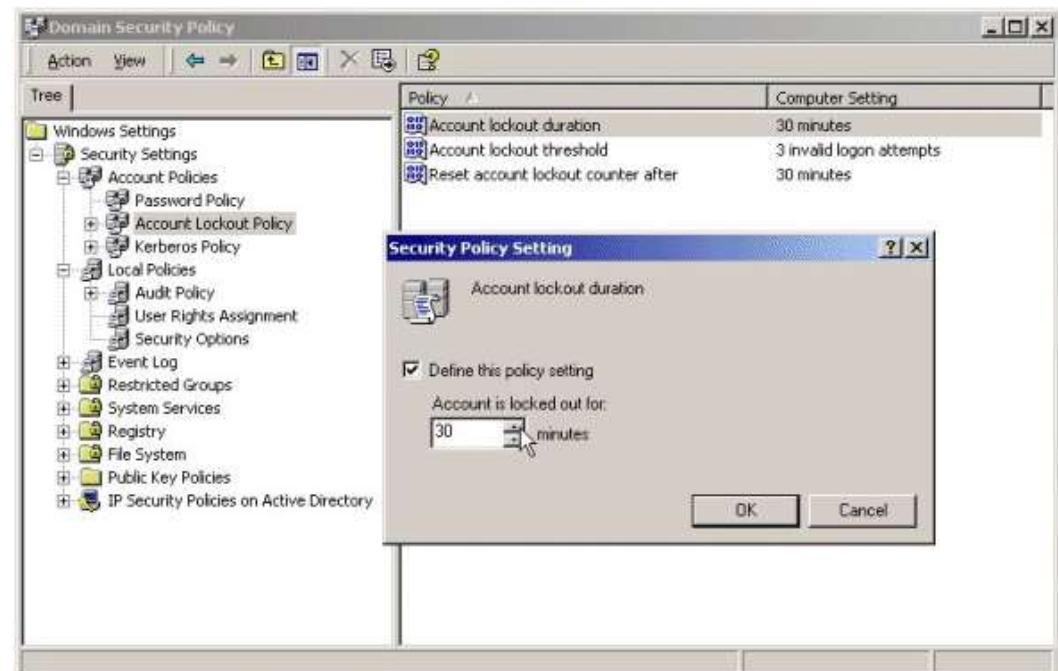
- Password policy settings



# Something You Know

- Account lockout policies

- Account lockout threshold
- Account lockout duration



# Something You Know

---

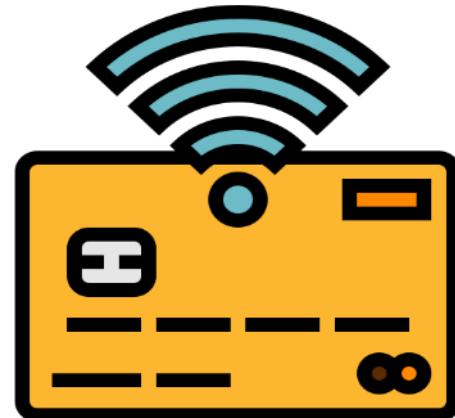
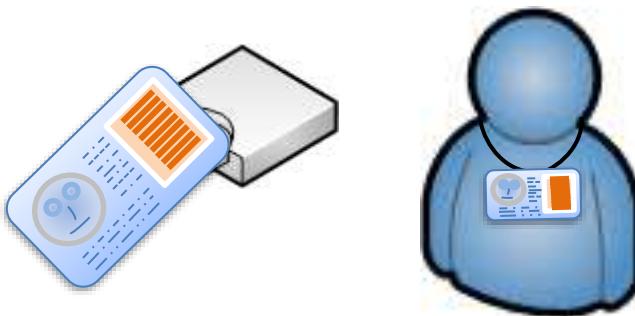
- Password keys
- Knowledge-Based Authentication
- Implementing Account Lockout Policies
- Changing Default Passwords
- Training Users About Password Behaviors



# Something You Have

---

- Smart cards
  - CACs and PIVs (US government)



- Tokens or Key fobs



# Something You Have

- HOTP and TOTP used in hardware tokens
- HOTP
  - HMAC-based One-Time Password
- TOTP
  - Time-based One-Time Password
  - Expire after 30 seconds



# Something You Have

---

- Authentication applications
- Two-Step Verification
  - Sent via SMS, a phone call, a push notification



# Something You Are

---

- Biometrics Methods
  - Fingerprint, thumbprint, or handprints
  - Retinal scanners (scans the retina of one or both eyes)
  - Iris scanners (scans the iris of one or both eyes)



# Something You Are

---

- Biometrics Methods
  - Vein matching
  - Voice recognition
  - Facial recognition
  - Gait analysis



# Biometrics

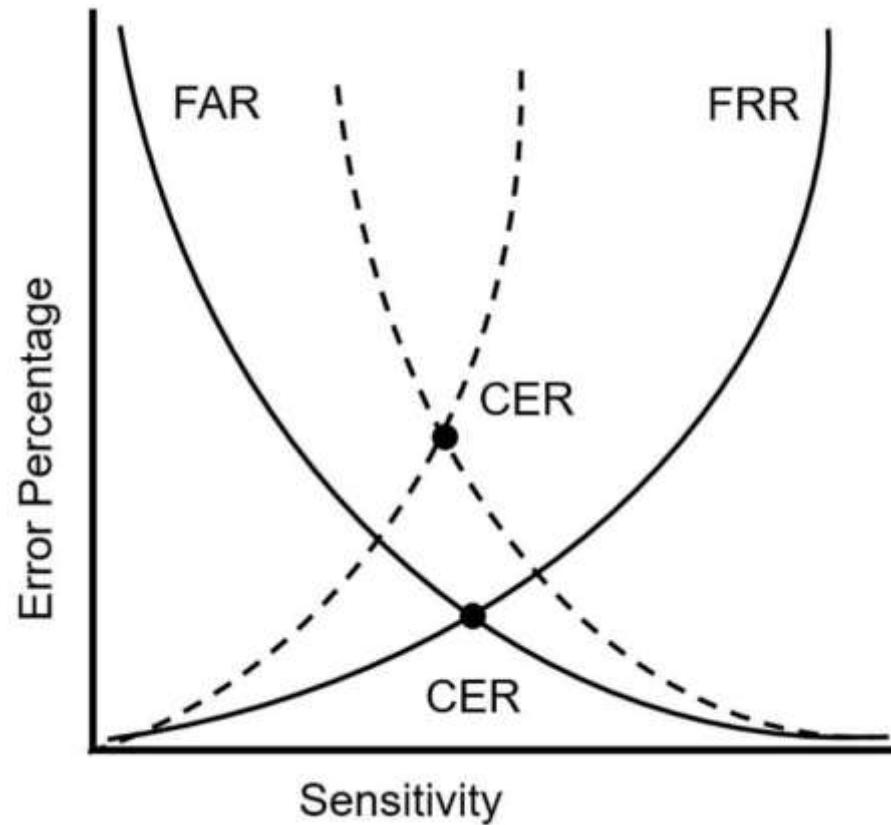
---

- False acceptance
- False rejection
- True acceptance
- True rejection

|                 | Biometric System<br>Not Accurate | Biometric System<br>Accurate |
|-----------------|----------------------------------|------------------------------|
| Registered User | <b>False Acceptance</b>          | True Acceptance              |
| Unknown User    | <b>False Rejection</b>           | True Rejection               |

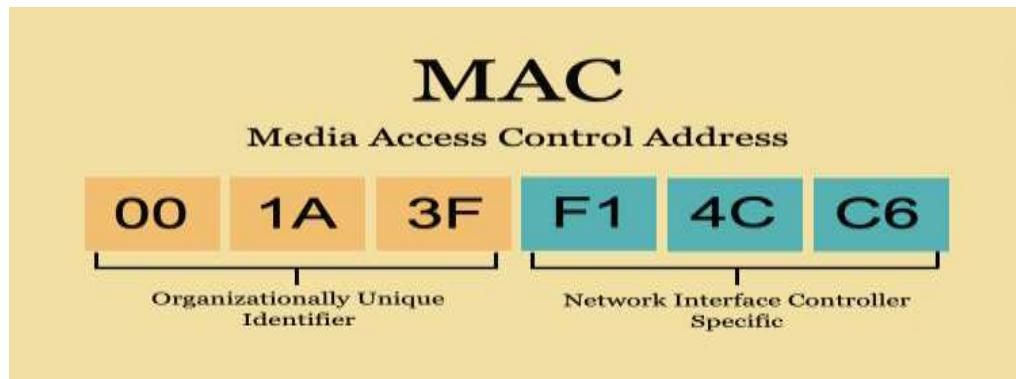
# Biometrics

- Crossover error rate
  - False acceptance rate
  - False rejection rate
  - Lower CER indicates better accuracy



# Somewhere You are

- Often uses geolocation
  - IP address
  - MAC address



# Authentication Attributes

---

- Something You Exhibit
- Someone You Know



# Two-factor/Multifactor Authentication

---

- Multifactor authentication
  - Combines authentication from two or more factors
- Examples:
  - PIN and CAC
  - PIV and password
  - Fingerprint and smart card

# Managing Accounts

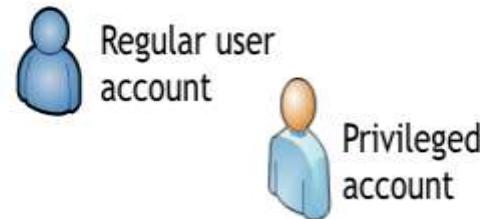
---

- Credential Policies and Account Types
  - Personnel or end-user accounts
  - Administrator and root accounts
  - Service accounts
  - Device accounts
  - Third-party accounts
  - Guest accounts
  - Shared and generic

# Managing Accounts

---

- Privileged Access Management
- Using Two Accounts
- Prohibiting Shared and Generic Accounts



# Managing Accounts

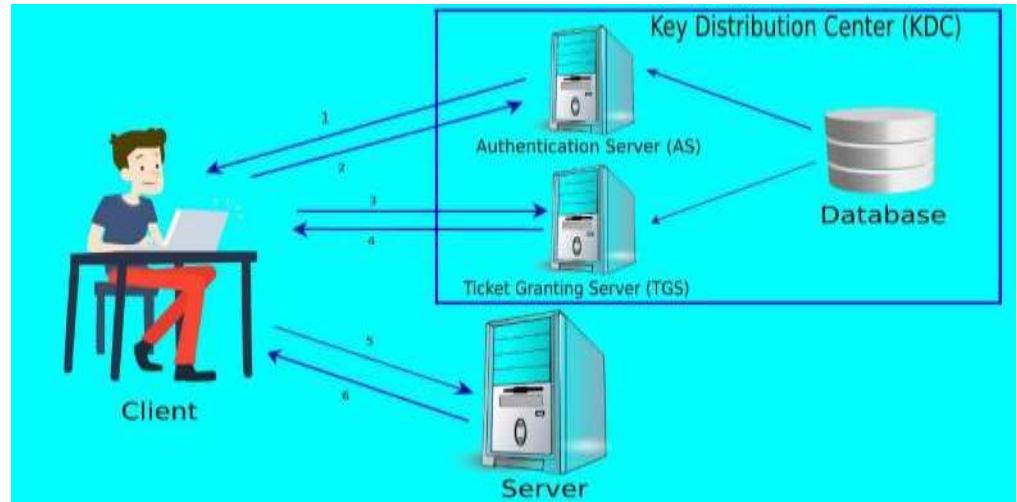
---

- Disablement Policies
  - Terminated employee
  - Leave of absence
  - Delete account
- Time-Based Logins
- Account Audits



# Comparing Authentication Services

- Single Sign-On
- Kerberos
- SSO and a Federation



# Comparing Authentication Services

---

- SAML
  - Principle
  - Identify provider
  - Service provider
  - Can also be used for authorization
- SAML and Authorization
- OAuth
- OpenID and OpenID Connect

# Comparing Access Control Models

---

- Role-Based Access Control
  - Uses roles (often implemented as groups)
  - Grant access by placing users into roles based on their assigned jobs, functions, or tasks
  - Often use a matrix

| Role             | Server Privileges | Project Privileges                                                                                                                    |
|------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Administrators   | All               | All                                                                                                                                   |
| Executives       | None              | All                                                                                                                                   |
| Project Managers | None              | All on assigned projects<br>No access on unassigned projects                                                                          |
| Team Members     | None              | Access for assigned tasks<br>Limited views within scope of their assigned tasks<br>No views outside the scope of their assigned tasks |

# Role-Based Access Control

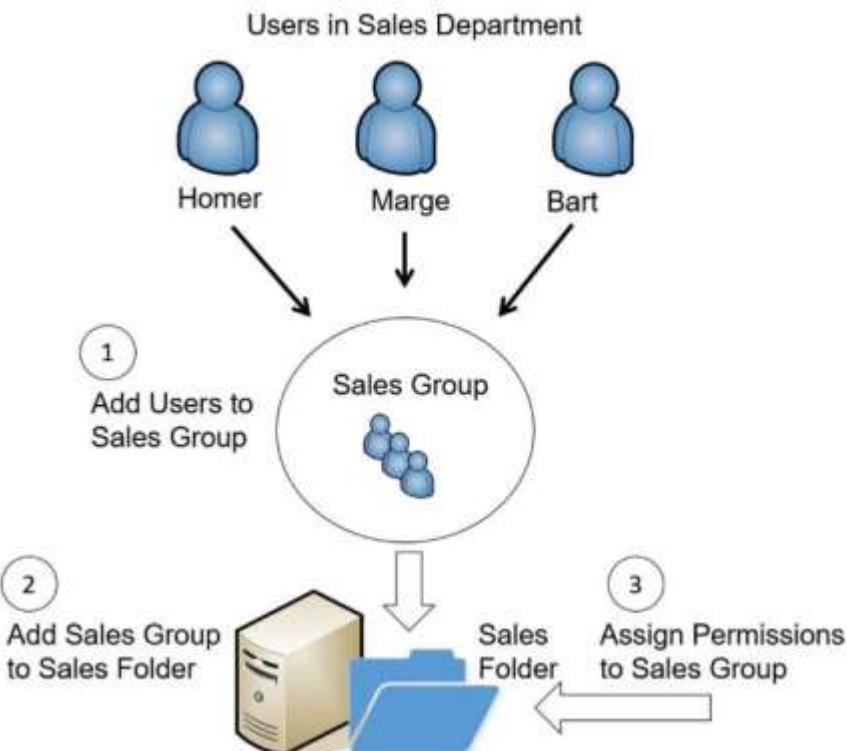
---

- Roles Based on Jobs and Functions
  - Administrators
  - Executives
  - Project Managers
  - Team Members
- Can be
  - Hierarchy-based
  - Job-, task-, or function-based



# Group-Based Privileges

1. Create a Sales group and add each of the user accounts to the Sales group
2. Add the Sales group to the Sales folder
3. Assign appropriate permissions to the Sales group for the Sales folder



# Rule-Based Access Control

---

- Rule-Based Access Control
  - Based on a set of approved instructions, such as an access control list
  - Can use triggers to respond to an event

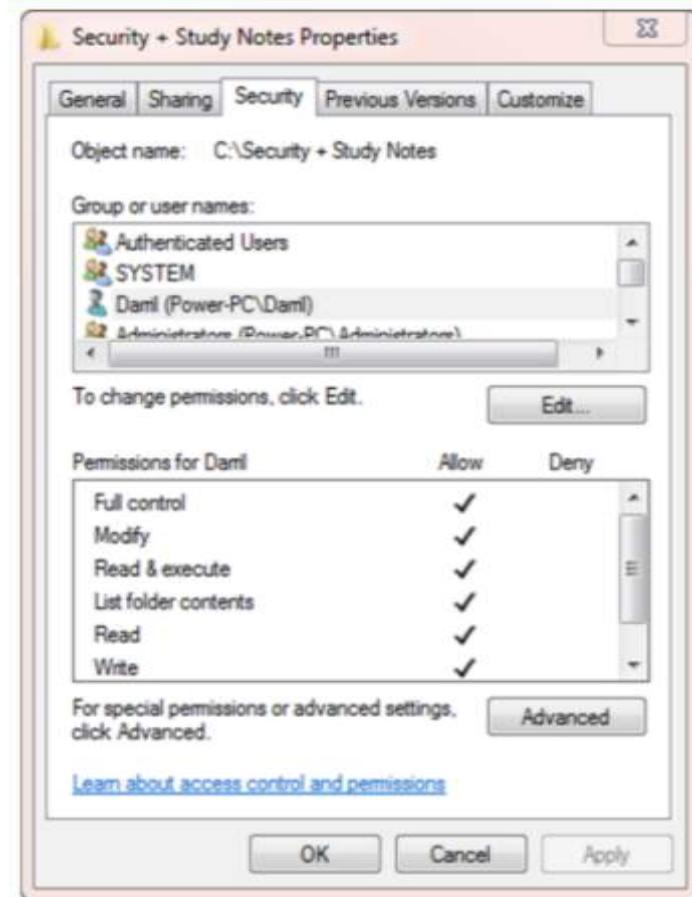
# Discretionary Access Control

---

- Resources identified as objects
  - Files, folders, shares
- Specifies that every object has an owner
- Owner has full, explicit control of the object
- Beware of Trojans
  - Dual accounts for administrators

# Discretionary Access Control

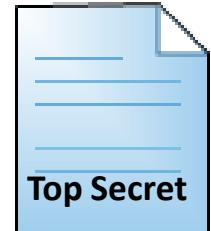
- Filesystem Permissions
  - Write
  - Read
  - Read & execute
  - Modify
  - Full control
- SIDs and DACLs



# Mandatory Access Control

---

- Uses labels to determine access
  - Subjects and objects are assigned labels
  - Permissions granted when the labels match
- 
- SELinux (Security-Enhanced Linux)
    - Uses MAC model
    - Helps prevent malicious or suspicious code from executing



# Mandatory Access Control

- Lattice

|                     |                 |               |
|---------------------|-----------------|---------------|
| Nuclear Power Plant | 007             | Happy Sumo    |
| Research            | Three-Eyed Fish | Legal Issues  |
| Payroll             | Budget          | Safety Issues |
| Training            | Job Openings    | Holidays      |

← Top Secret Level

← Secret Level

← Confidential Level

← For Official Use Level

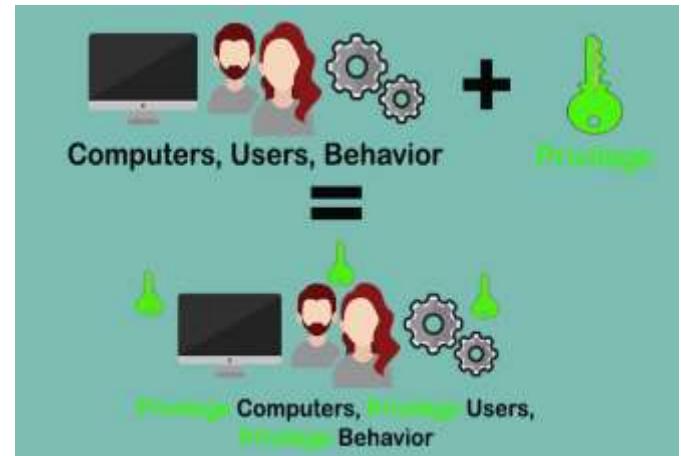
# Attribute-Based Access Control

---

- Commonly used in SDNs
- Evaluates attributes and grants permissions based on attributes
- Often implemented with plain language policy statements
- Policy statements typically include four elements
  - Subject
  - Object
  - Environment
  - Action

# Conditional Access

- User or group membership
- IP location
- Device



# Chapter 2 Summary

---

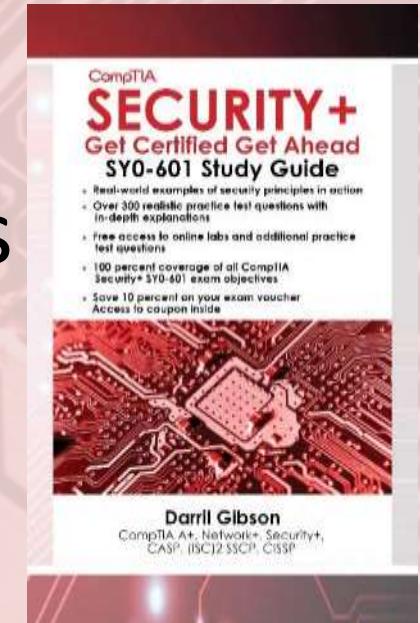
- Exploring Authentication Management
- Managing Accounts
- Comparing Authentication Services
- Comparing Access Control Schemes
- Check out the free online labs

# Chapter 3

## Exploring Network Technologies and Tools

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Reviewing Basic Networking Concepts
- Basic Networking Protocols
- Understanding Basic Network Devices
- Implementing Network Designs
- Summarizing Routing and Switching Use Cases

# Attack Introduction

---

- Sniffing attack
- DoS and DDoS
- Poisoning attack

# Basic Networking Protocols

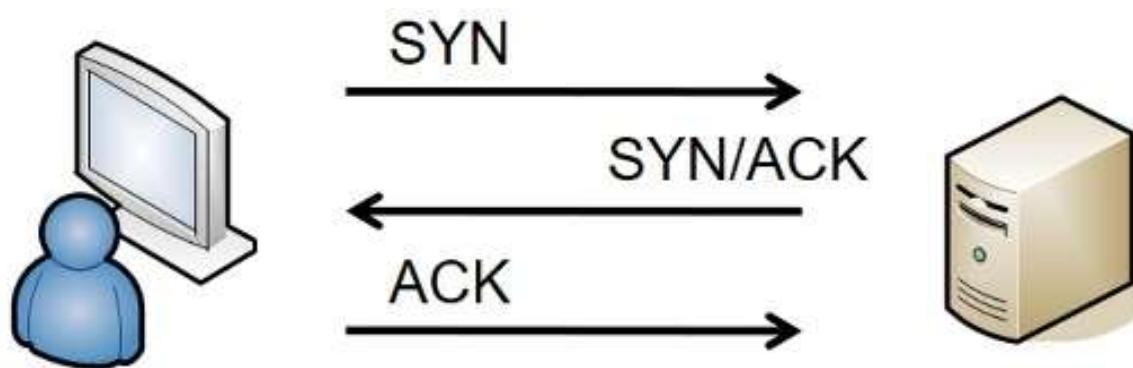
- Basic Connectivity Protocols

- TCP

- Guaranteed delivery
    - Three-way handshake

- UDP

- Best effort



# Basic Networking Protocols

---

- Reviewing Basic Connectivity Protocols
  - IPv4 and IPv6
  - ICMP
    - Commonly blocked at firewalls
    - If ping fails, ICMP may be blocked
  - ARP
    - Resolves MAC addresses for IPv4



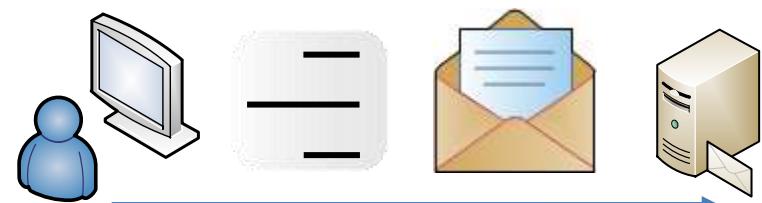
# Protocols and Use Cases

---

- Transport voice and video over network
  - RTP & SRTP
- Transfer files over a network
  - FTP
  - TFTP
  - SSH
  - SSL
  - TLS
  - IPsec
  - SFTP
  - FTPS

# Protocols and Use Cases

- Email and web usage
  - SMTP
  - POP3 & Secure POP
  - IMAP4 and Secure IMAP
  - HTTP
  - HTTPS



# Protocols and Use Cases

---

- Directory services
  - LDAP – 389
    - Port 636 when encrypted with SSL or TLS
  - Kerberos – Port 88
- Remote access
  - SSH
  - Netcat
  - RDP

# Protocols and Use Cases

---

- OpenSSH
- Time synchronization
  - NTP
  - SNTP

# Appx C Ports

| Protocol                    | Port    | Protocol           | Port    |
|-----------------------------|---------|--------------------|---------|
| SMTP                        | TCP 25  | SMTP TLS/SSL       | TCP 587 |
| IMAP4                       | TCP 143 | Secure IMAP4       | TCP 993 |
| POP3                        | TCP 110 | Secure POP         | TCP 995 |
| SSH                         | TCP 22  | TLS                | TCP 443 |
| FTP data port (active mode) | TCP 21  | SFTP (uses SSH)    | TCP 22  |
| FTP (PASV) control          | TCP 21  | FTPS (uses TLS)    | TCP 989 |
| FTP control                 | TCP 20  | FTPS (uses TLS)    | TCP 990 |
| TFTP                        | UDP 69  | SCP (uses SSH)     | TCP 22  |
| HTTP                        | TCP 80  | HTTPS (uses TLS)   | TCP 443 |
| DNS name queries            | UDP 53  | DNS zone transfers | TCP 53  |

# Appx C Ports

| Protocol                  | Port          | Protocol                      | Port         |
|---------------------------|---------------|-------------------------------|--------------|
| NetBIOS (TCP rarely used) | TCP/UDP 137   | LDAP                          | TCP 389      |
| NetBIOS                   | UDP 138       | LDAPS                         | TCP 636      |
| NetBIOS                   | TCP 139       | Telnet (Not Recommended)      | TCP 23       |
| L2TP                      | UDP 1701      | IPsec (for VPN with IKE)      | UDP 500      |
| PPTP                      | TCP 1723      | Remote Desktop Protocol (RDP) | TCP/UDP 3389 |
| SNMP                      | UDP 161       | SNMP trap                     | UDP 162      |
| SIP                       | TCP 5060/5061 | SMB                           | TCP 445      |
| DHCP (client to server)   | UDP 67/68     | DHCP (server to client)       | UDP 68       |
| RADIUS                    | UDP 1812/1813 | RADIUS with EAP               | TCP 1812     |
| TACACS+                   | TCP 49        | Kerberos                      | TCP/UDP 88   |

# Network Address Allocation

---

- IPv4 – 32 bits (192.168.1.5 )
- Private IP Addresses
  - **10.x.y.z.**  
10.0.0.0 through 10.255.255.255
  - **172.16.y.z–172.31.y.z.**  
172.16.0.0 through 172.31.255.255
  - **192.168.y.z.**  
192.168.0.0 through 192.168.255.255

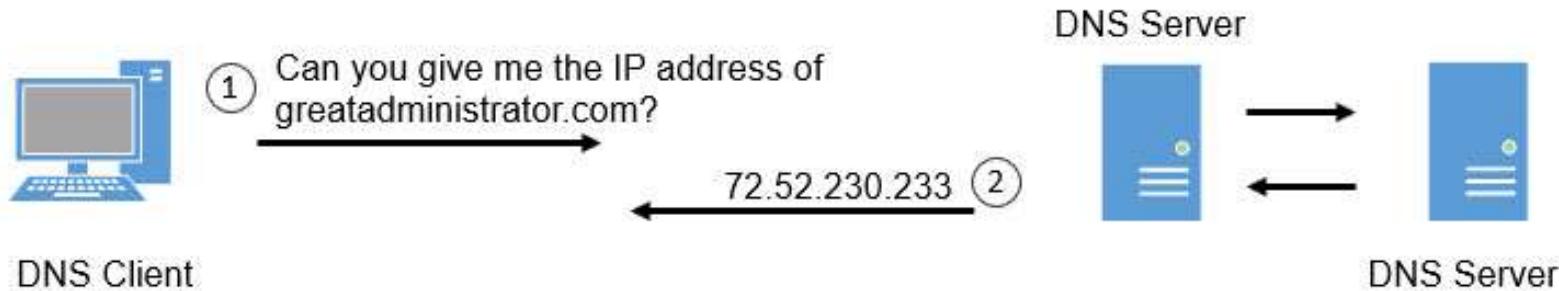
# Network Address Allocation

---

- IPv6 – 128 bits
  - fe80:0000:0000:0000:02d4:3ff7:003f:de62
- DHCP Snooping
  - DHCP Discover
  - DHCP Offer
  - DHCP Request
  - DHCP Acknowledge

# Understanding DNS

- Domain Name Resolution Use Case



## Records

- A - IPv4 Host
- AAAA - IPv6 Host
- PTR - Pointer
- MX - Mail server
- CNAME – Alias
- SOA - TTL

# Understanding DNS

---

- Queries to DNS server use UDP port 53
- Zone transfers between servers use TCP port 53
- DNSSEC
  - DNS poisoning

# Protocols and Use Cases

---

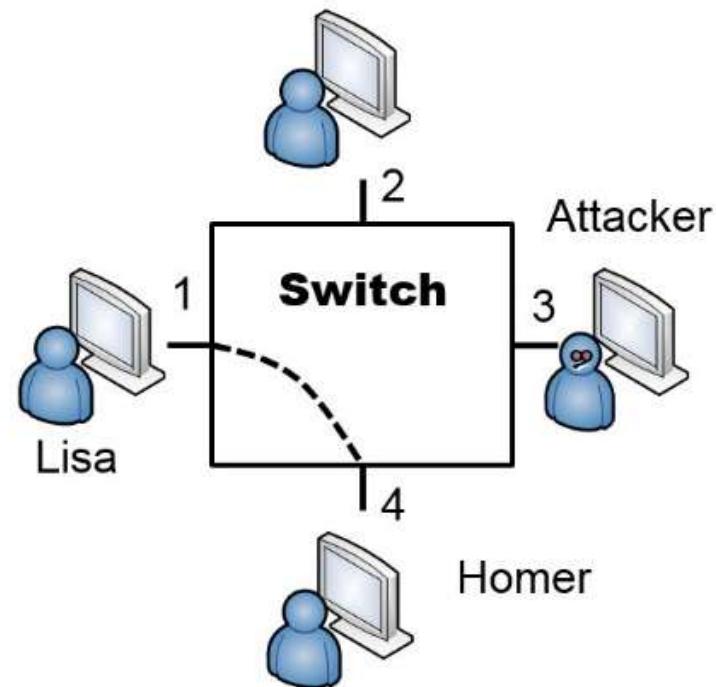
- Commands
  - Nslookup
  - Dig
- Subscription services
- Quality of Service



# Understanding Basic Network Devices

---

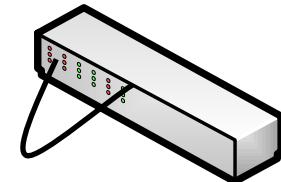
- Unicast – one-to-one traffic
- Broadcast – One-to-all traffic
- Switch learns
  - Security benefit
  - Port security
  - Physical security



# Switches

---

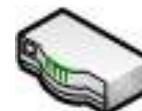
- Port security
  - Disable unused ports
  - MAC address filtering
- Broadcast Storm and Loop Prevention
  - Caused if two ports connected together
  - STP and RSTP protect against switching loops
- Bridge Protocol Data Unit Guard



# Routers

---

- Route traffic between networks
- Do not pass broadcasts



- Routers and ACLs
  - Filter based on
    - IP addresses and networks
    - Ports
    - Protocol numbers



# Routers

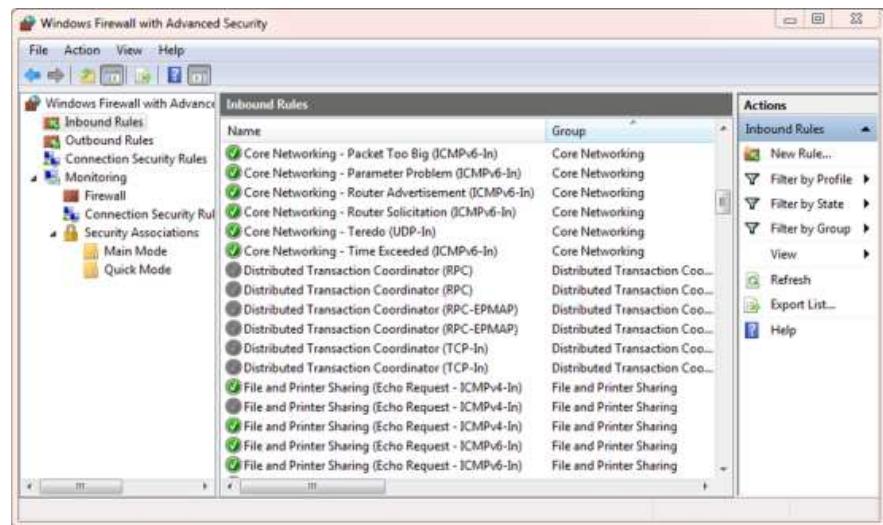
---

- Implicit deny
  - Last rule in ACL
- Command
  - route command

# Firewalls



- Host-based
- Software versus hardware firewalls
- Next-generation firewall



# Identifying OSI Relevance

- Next-generation firewalls
  - All 7 layers up to Application layer

| Layer Number | Layer Name   | Devices                                                                                                                 | Protocols                                                                                   |
|--------------|--------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1            | Physical     | Cables, hubs                                                                                                            | Ethernet, cabling protocols                                                                 |
| 2            | Data Link    | Switches                                                                                                                | MAC, ARP, VLANs                                                                             |
| 3            | Network      | Router, layer 3 switch                                                                                                  | IPv4, IPv6, IPsec, ICMP                                                                     |
| 4            | Transport    |                                                                                                                         | TCP, UDP                                                                                    |
| 5            | Session      |                                                                                                                         |                                                                                             |
| 6            | Presentation |                                                                                                                         |                                                                                             |
| 7            | Application  | Proxy servers, web application firewalls, next-generation firewalls, UTM security appliances, and web security gateways | DNS, FTP, FTPS, SFTP, TFTP, HTTP, HTTPS, IMAP4, LDAP, POP3, SFTP, SMTP, SNMP, SSH, and TFTP |

# Firewalls

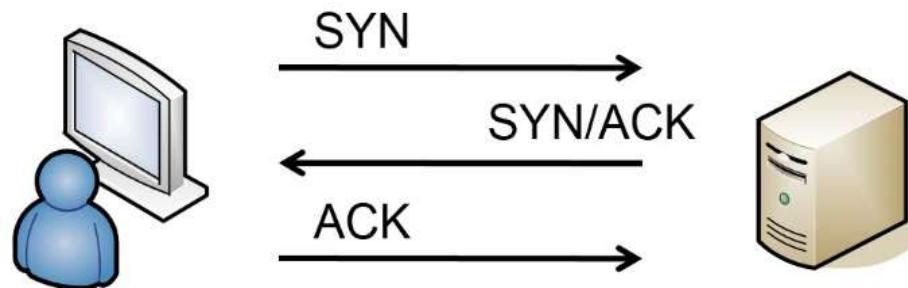


- Stateless
  - Permission (deny, allow)
  - Protocol (TCP, UDP, Any)
  - Source (IP address or IP block)
    - IP address example: 192.168.1.20/32
    - IP block example: 192.168.1.0/24
  - Destination (IP address or IP block)
  - Port or protocol (80 for HTTP, 25 for SMTP)
  - Ends with deny any any (or something similar)

# Firewalls



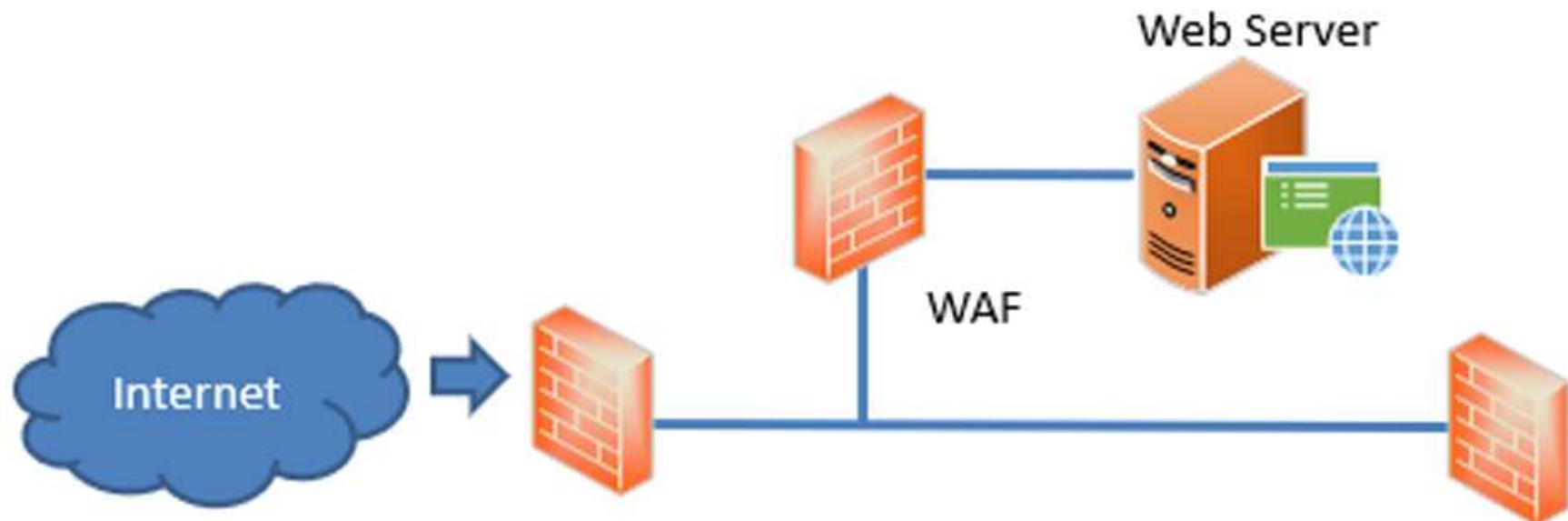
- Stateful
  - Makes decisions based on context, or state, of traffic
  - Can ensure TCP traffic is part of an established TCP session
    - If not, traffic is blocked



# Firewalls



- Web application firewall (WAF)
  - Protects a web application or web server



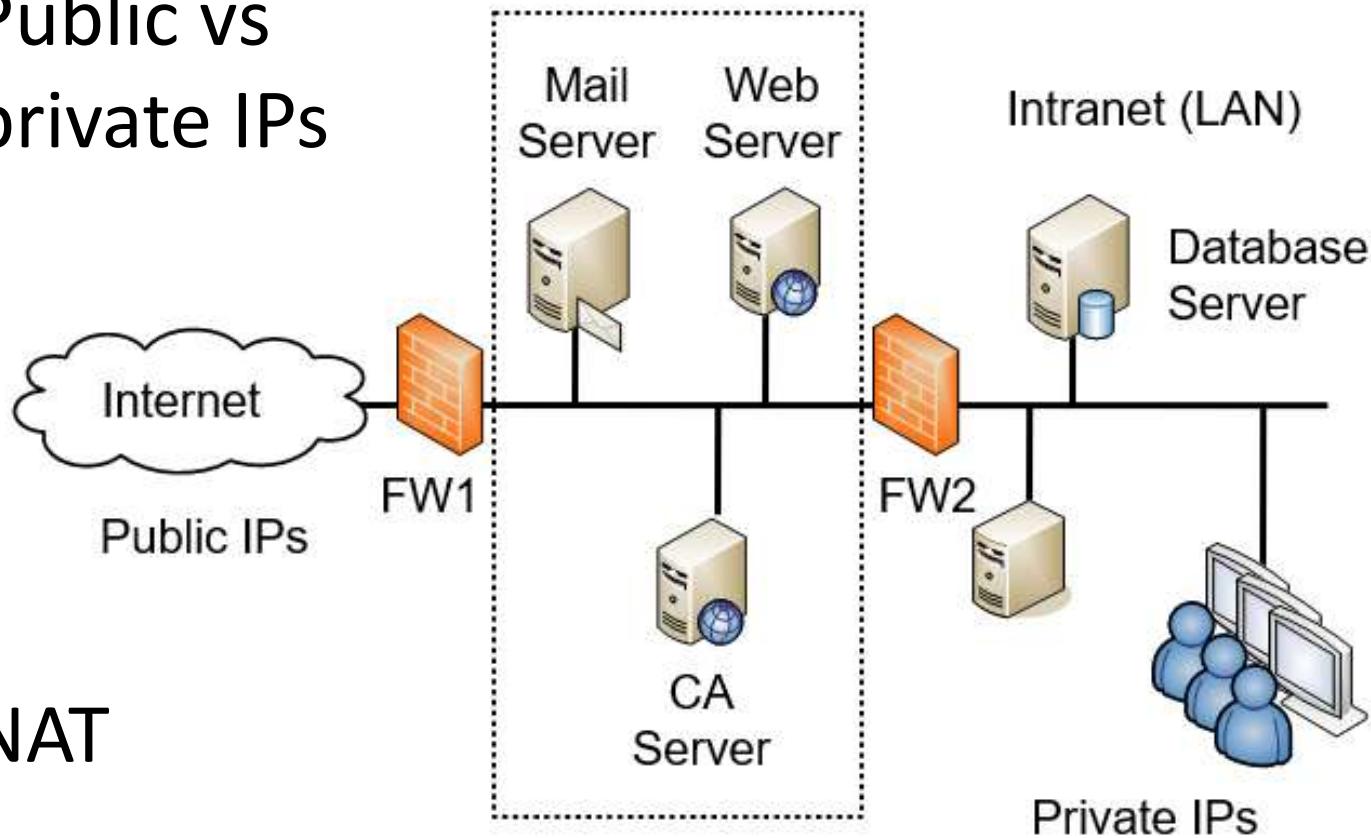
# Network Designs

---

- Intranet
  - Internal network
- Extranet
  - Part of a network that can be accessed by authorized entities from outside of the network
- Screened subnet
  - Previously called demilitarized zone

# Screened Subnet

- Public vs private IPs



- NAT

# Screened Subnet

---

- Network Address Translation (NAT)
  - Static NAT
  - Dynamic NAT
- Physical isolation and air gaps
- Logical separation and segmentation
  - Typically done with routers and firewalls

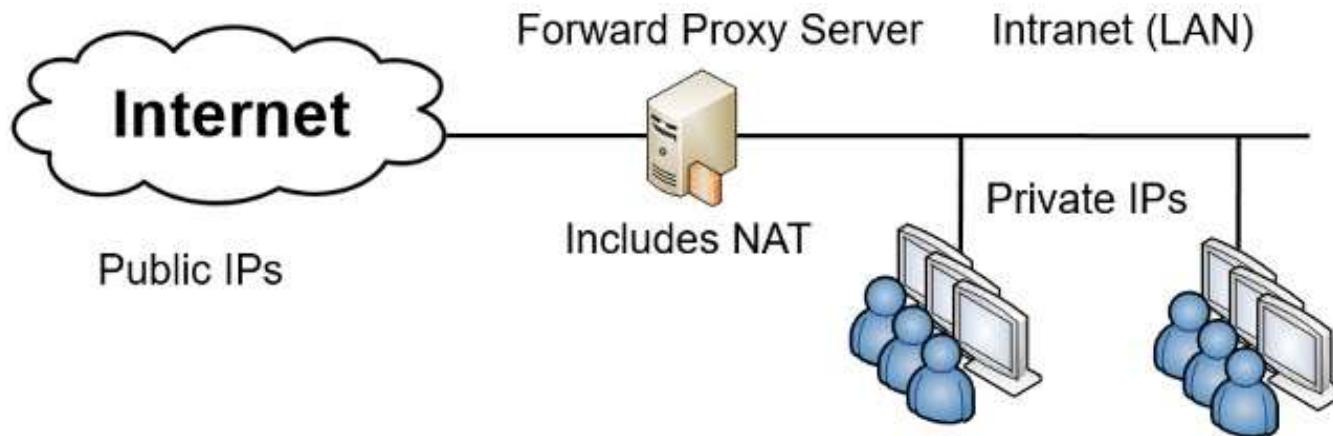
# Screened Subnet

---

- VLAN (created with a switch)
  - Logically group computers
  - Logically separate/segment computers
- East-West Traffic
- Zero Trust

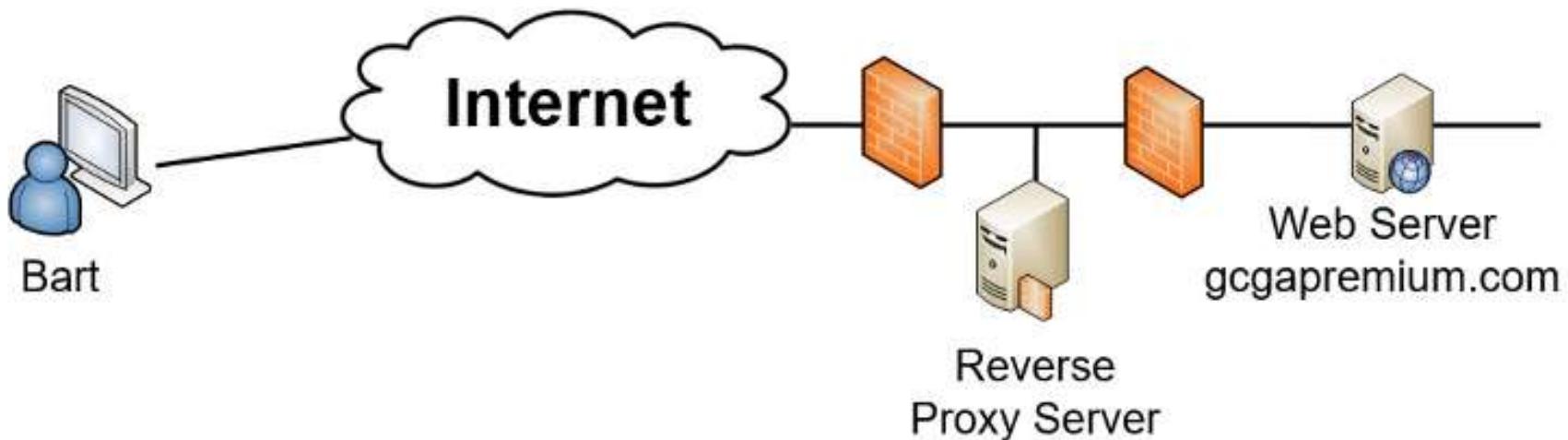
# Proxies (Proxy Servers)

- Caching content for performance
- Using URL filters to restrict access
- Transparent proxy vs nontransparent proxy



# Proxies (Proxy Servers)

- Reverse proxy



- Application proxy

# Unified Threat Management

---

- Combines multiple security controls
- Reduces administrative workload
- Web security gateways
- UTM security appliances
  - Firewall, antivirus protection, anti-spam protection, URL filtering, and content filtering.
  - DDoS mitigator

# Network Designs

---

- Jump server
  - Sometimes called a jump box
  - A hardened server used to access and manage devices in another network
  - Can use to access server in screened subnet via jump box in internal network
  - Common to use passwordless SSH login
- IPv6

# Summarizing Use Cases

---

- Switches
  - Prevent switching loops
    - STP or RSTP on switches.
  - Prevent BPDU attacks
  - Prevent unauthorized users from connecting to unused ports
    - Port security methods
  - Provide increased segmentation of user computers
    - VLANs

# Chapter 3 Summary

---

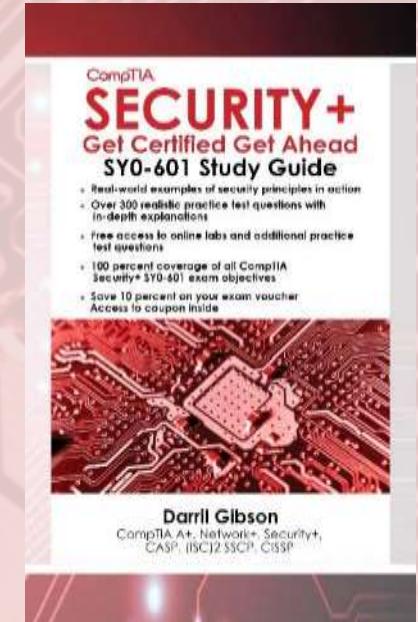
- Reviewing Basic Networking Concepts
- Basic Networking Protocols
- Understanding Basic Network Devices
- Implementing Network Designs
- Summarizing Routing and Switching Use Cases
- Check out the free online labs

# Chapter 4

# Securing Your Network

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Exploring Advanced Security Devices
- Securing Wireless Networks
- Understanding Wireless Attacks
- Using VPNs for Remote Access

# Understanding IDSs and IPSs

---

- Intrusion Detection System (IDS)
  - Detective control
  - Attempts to detect attacks after they occur
- Firewall is a preventive control
  - Attempts to prevent the attacks before they occur.
- Intrusion Prevent System (IPS)
  - A preventive control
  - Will stop an attack in progress.

# Host- and Network-Based IDS

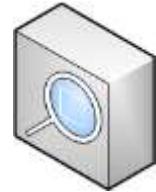
---

## HIDS

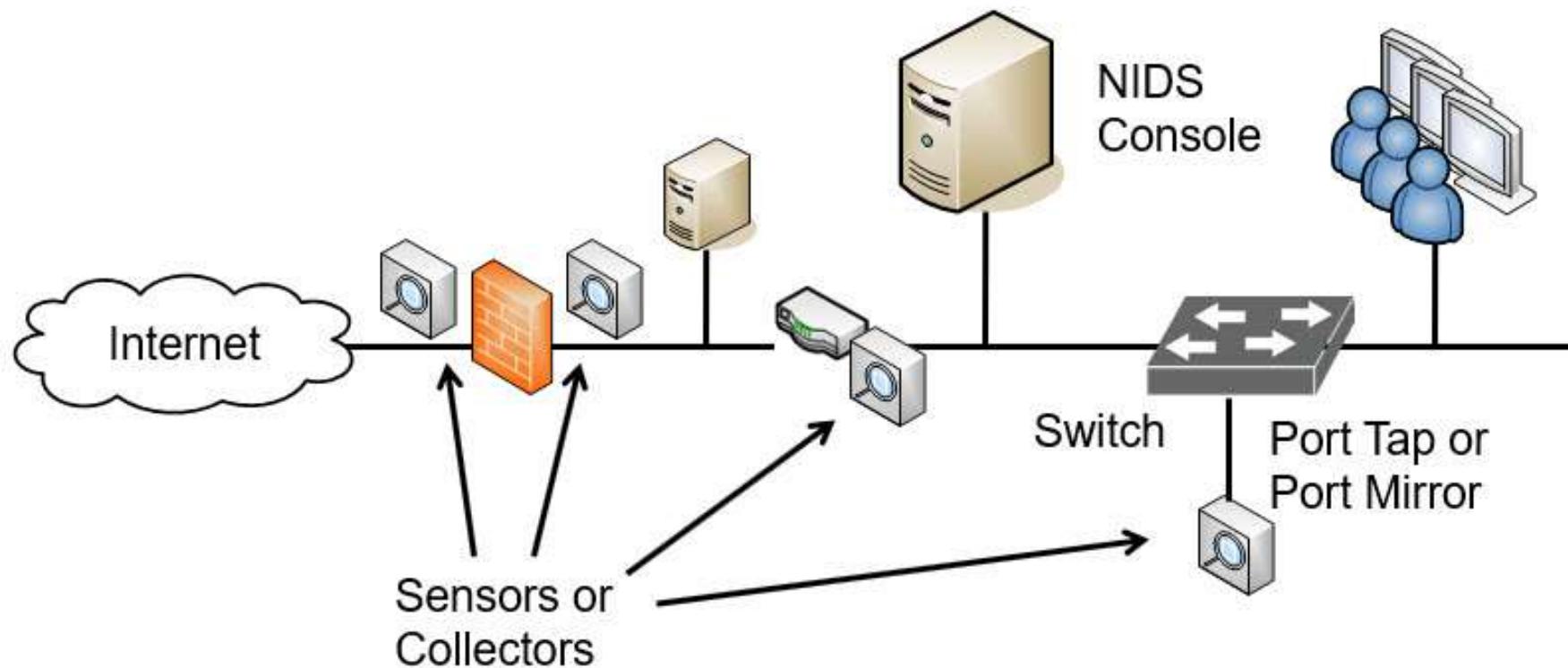
- Additional software on a workstation or server
- Can detect attacks on the local system
- Protects local resources on the host such as operating system files
- Cannot monitor network traffic

## NIDS

- Installed on network devices, such as routers or firewalls
- Monitors network traffic
- Can detect network-based attacks such as smurf attacks
- Cannot monitor encrypted traffic and cannot monitor traffic on individual hosts.



# Sensor and Collector Placement



# IDS Detection Methods

---

## Signature-based

- Also called definition-based
- Use a database of predefined traffic patterns (such as CVE list)
- Keep signature files up-to-date
- Most basic form of detection
- Easiest to implement

## Heuristic-, behavior-based

- Also called anomaly-based
- Starts with a performance baseline of normal behavior
- IDS compares activity against this baseline
- Alerts on traffic anomalies
- Update the baseline if the environment changes

# IDS Considerations

---

- Data sources and trends

|                                     |                         | IDS/IPS<br>Accurate                    | IDS/IPS<br>Not Accurate                           |
|-------------------------------------|-------------------------|----------------------------------------|---------------------------------------------------|
|                                     |                         | No Attack                              | Actual Attack                                     |
| No Attack                           | IDS/IPS<br>Accurate     | True Negative<br>(No alarm or alert)   | <b>False Positive</b><br>(Alarm or alert sent)    |
|                                     | IDS/IPS<br>Not Accurate | True Positive<br>(Alarm or alert sent) | <b>False Negative</b><br>(No alarm or alert sent) |
| Reporting                           |                         |                                        |                                                   |
| False positives                     |                         |                                        |                                                   |
| — Increase administrator's workload |                         |                                        |                                                   |
| False negatives                     |                         |                                        |                                                   |
| — No report during an incident      |                         |                                        |                                                   |

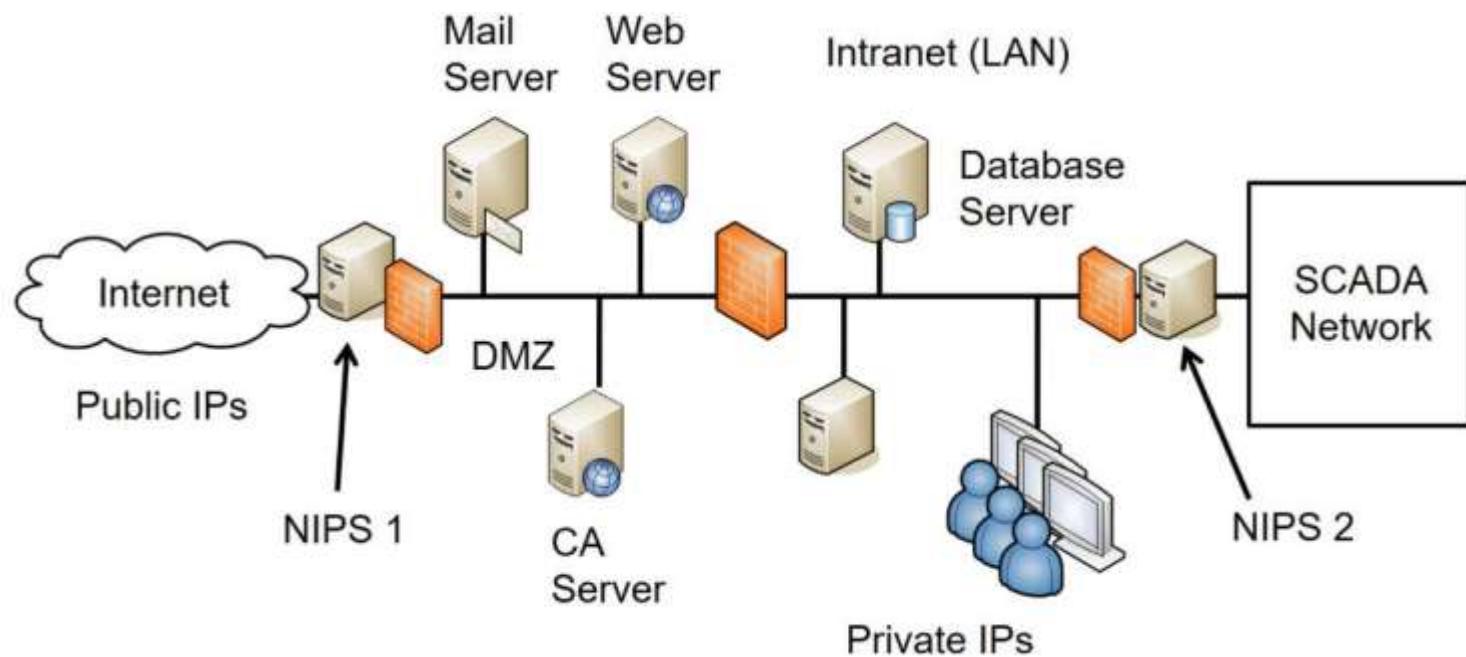
# IDS vs IPS

---

- IPS is a preventive control
  - Can actively monitor data streams
  - Can detect malicious content
  - Can stop attacks in progress

# IDS vs IPS

- IPS is placed in line with traffic



- In contrast IDS (not shown) is out of band

# Other Tools

---

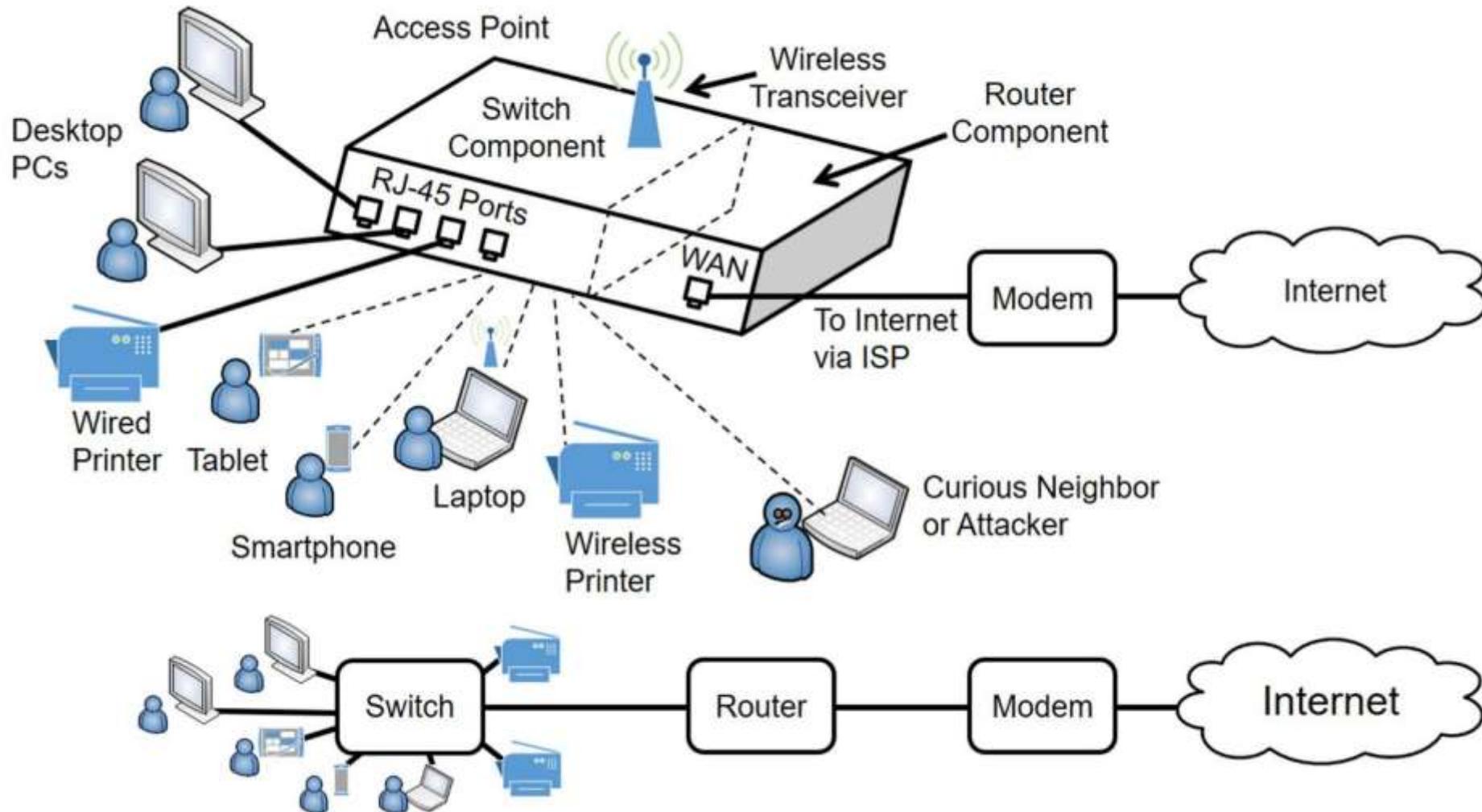
- Honeypots and Honeynets
  - Used to divert an attacker
  - Allow IT administrators an opportunity to observe methodologies
  - Can be useful to observe zero day exploits
- Honeyfile
  - Attract the attention of an attacker
- Fake Telemetry
  - Corrupts the data sent to monitoring systems and can disrupt a system

# Securing Wireless Networks

---

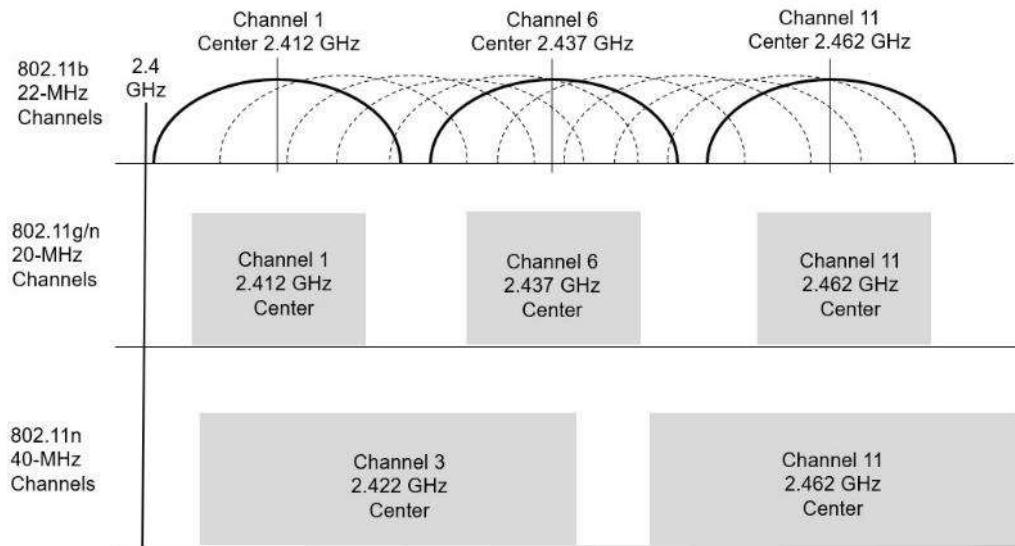
- WAPs and wireless routers
  - All wireless routers are WAPs
  - Not all WAPs are wireless routers

# Wireless Routers

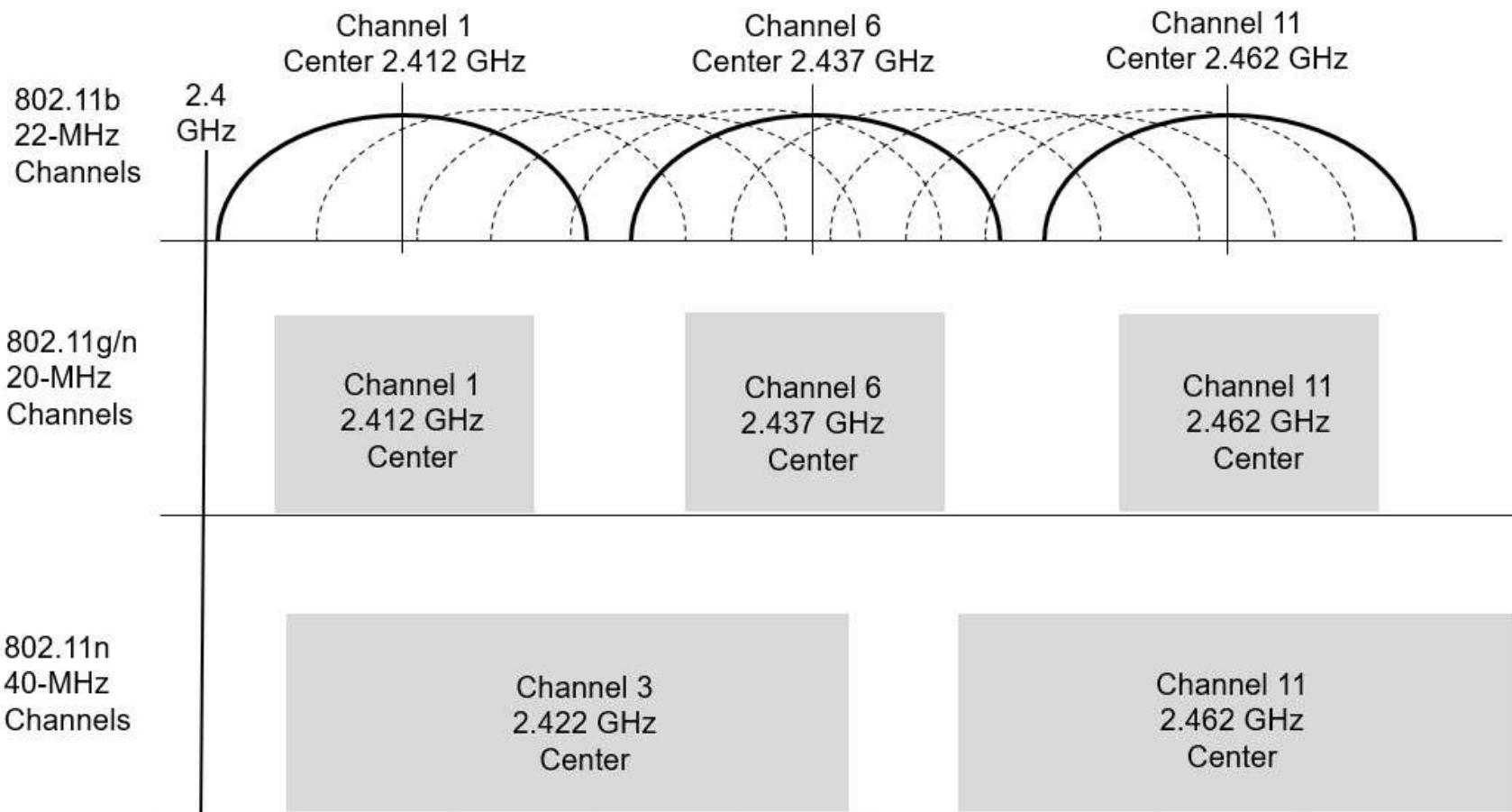


# Wireless Basics

- Band Selection and Channel Widths
  - 802.11b, 2.4 GHz
  - 802.11g, 2.4 GHz
  - 802.11n, 2.4 GHz, and 5 GHz
  - 802.11ac, 5 GHz
- MAC Filtering
  - MAC Cloning



# Wireless Basics



# Access Point SSID

---

- Network name
- Change default SSID
- Disabling SSID broadcast
  - Hides from some devices
  - Does not hide from attackers

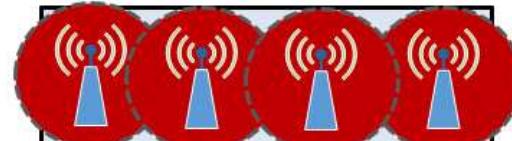
# Wireless Networks

- Site Surveys and Footprinting

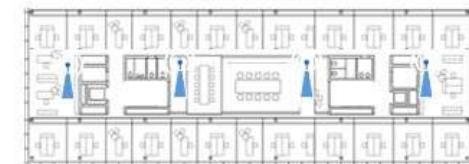
- Wi-Fi analyzer
  - heat map
  - Wireless footprinting



Organization 1



Organization 2



- Wireless Access Point Placement
  - Omnidirectional (or omni) antenna

# Wireless Cryptographic Protocols

---

- WPA2 and CCMP
- Open
- Pre-shared key (PSK)
- Enterprise modes
- WPA3 and Simultaneous Authentication of Equals

# Enterprise Modes

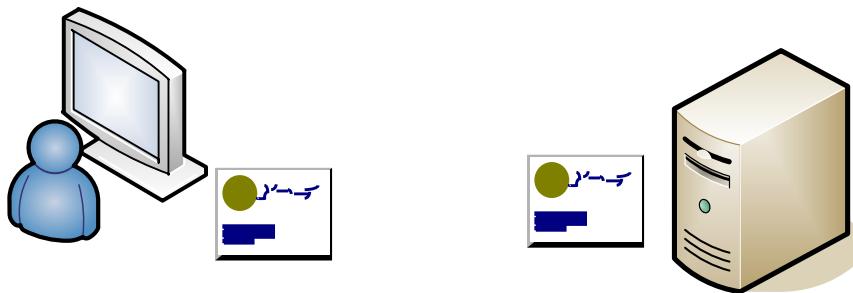
- RADIUS server
- RADIUS port
- Shared secret



# Authentication Protocols

---

- EAP-TLS
  - Most secure (compared to other EAP methods)
  - Provides mutual authentication
  - Requires certificate on 802.1x server
  - Requires certificate on the clients



# Authentication Protocols

---

- EAP
  - Uses pairwise master key
- EAP-FAST
  - Replaced LEAP
- PEAP
  - Requires certificate on server
- EAP-TTLS
  - Requires certificate on 802.1x server

# Wireless

---

- RADIUS federation
  - Provides single sign-on for two or more entities
  - Federation includes multiple 802.1x servers
  - Can use any of the EAP versions
- Captive Portals
  - Free Internet access
  - Paid Internet access
  - Alternative to IEEE 802.1x

# Wireless Attacks

---

- Disassociation attack
  - Removes a wireless client from a wireless network
- WPS
  - Streamlines process of configuring wireless clients
- WPS attack
  - Brute force method to discover WPS PIN
  - Reaver

# Wireless Attacks

---

- Rogue access points
  - Unauthorized AP
- Evil twins
  - Rogue AP with same SSID as legitimate AP
- Jamming attack
  - Broadcasts noise or other signals on same frequency

# Wireless Attacks

---

- IV attack
  - Attempts to discover PSK from the IV
- NFC attack
  - Uses an NFC reader to capture data



# Wireless Attacks

---

- Wireless replay attacks
  - Captures data
  - Attempts to use to impersonate client
- RFID attacks
  - Sniffing or eavesdropping
  - Replay
  - DoS

# Wireless Attacks

---

- War driving
  - Practice of looking for a wireless network
- War flying
  - Uses planes or drones instead of cars

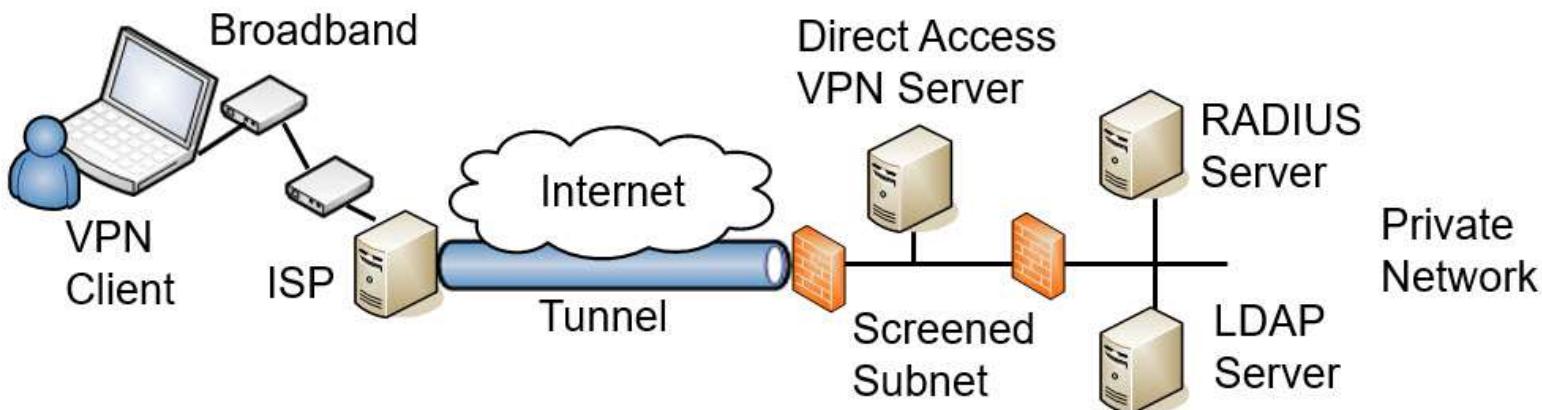
# Bluetooth Wireless

---

- Bluejacking
  - Unauthorized sending of text messages from a Bluetooth device
- Bluesnarfing
  - Unauthorized access to or theft of information from a Bluetooth device
- Bluebugging
  - Allows an attacker to take over a mobile phone

# Remote Access

- VPNs and VPN concentrators



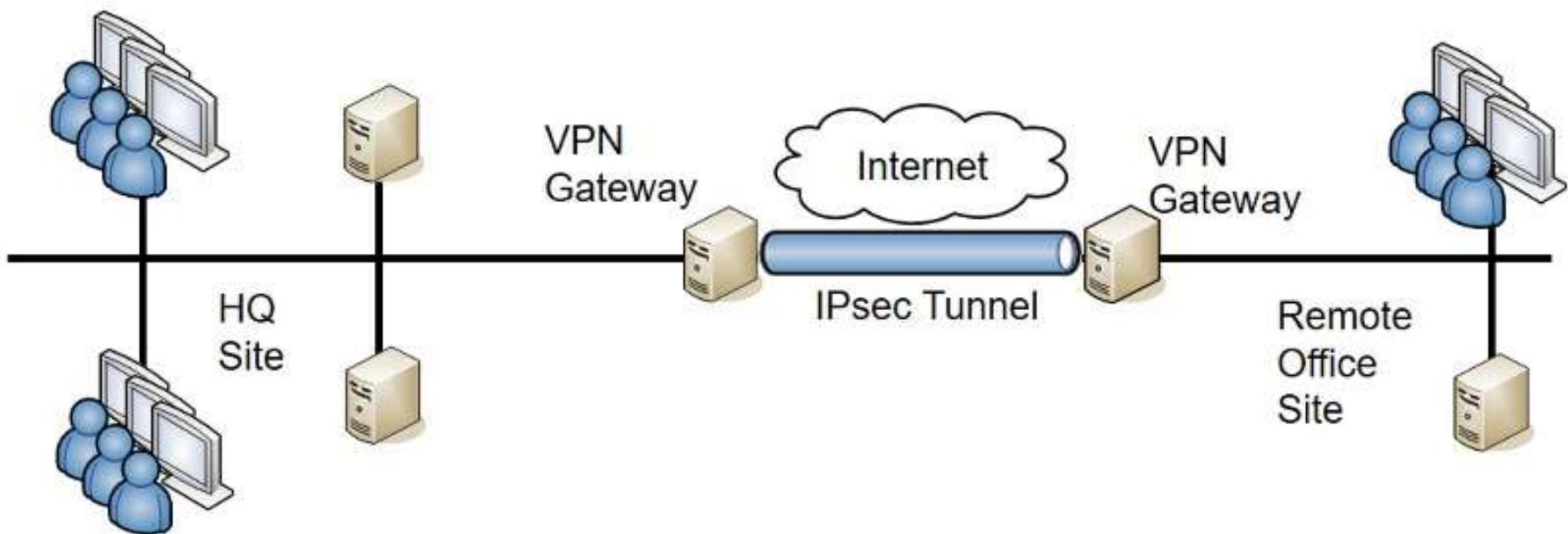
# Tunneling Protocols

---

- IPsec as a tunneling protocol
  - Authentication
    - AH provides authentication & integrity (protocol ID 51)
  - Encryption
    - ESP adds confidentiality (protocol ID 50)
      - Uses tunnel mode for VPNs with IKE over port 500
- TLS as a tunneling Protocol
  - Useful when VPN go through NAT
  - SSTP uses TLS over port 443

# Site-to-Site VPNs

- Gateways as VPN servers



# Always-On VPNs

---

- Site-to-site VPNs
- Regular VPNs for users
- Mobile devices

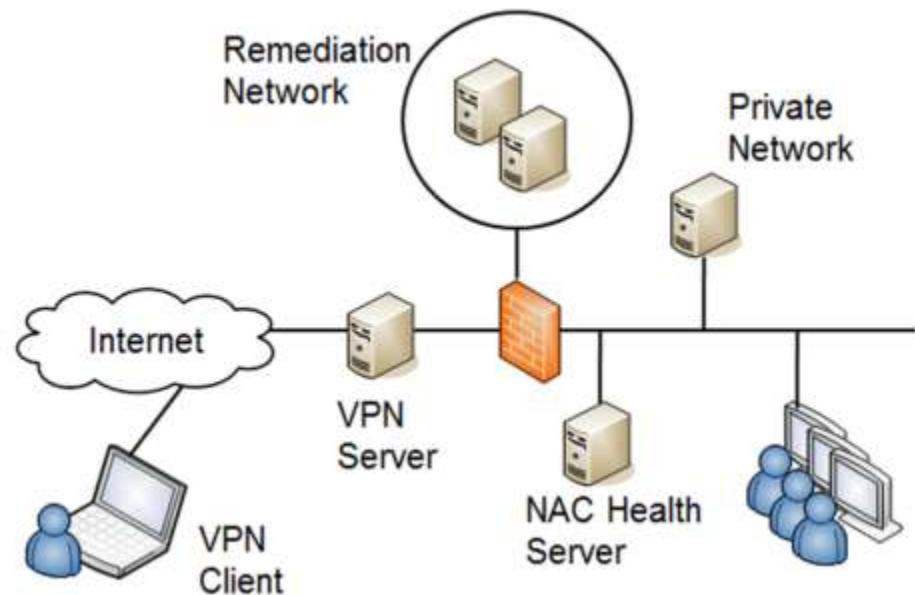
# Tunneling Protocols

---

- L2TP
  - not used by itself for VPN traffic
- HTML5 VPN Portal
  - allows users to connect to the VPN using their web browser

# Network Access Control

- Health agents
  - Inspects clients for predefined conditions
  - Restricts access of unhealthy clients to a remediation network
  - Used for VPN clients and internal clients



# NAC Agents

---

- Permanent (Agent)
  - Installed on client and remains on client
  - Persistent NAC agent
- Dissolvable (Agentless)
  - Does not stay on client
  - Downloaded to client when session starts
  - Removed during or after session
  - Commonly used for mobile devices

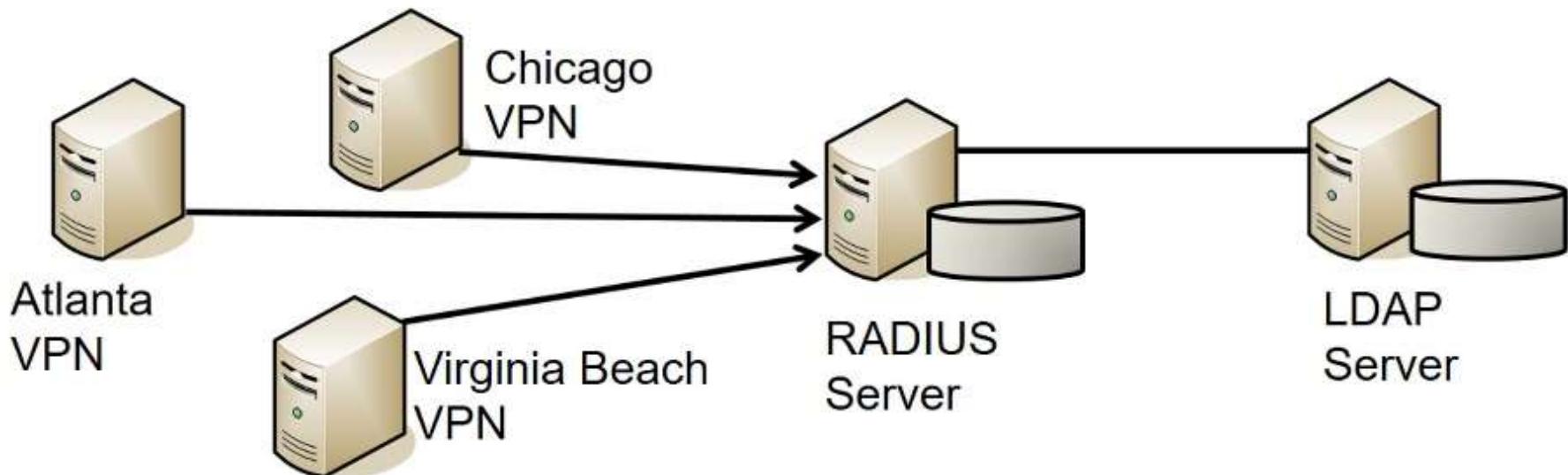
# Identity and Access Services

---

- PAP – Sends passwords in cleartext
- CHAP – uses shared secret
- TACACS+
  - Cisco alternative to RADIUS
  - Uses TCP port 49
  - Encrypts entire authentication process
  - Uses multiple challenges and responses

# Identity and Access Services

- RADIUS



# AAA Protocols

---

- Provide authentication, authorization, and accounting
  - Authentication verifies a user's identification
  - Authorization provides access
  - Accounting tracks user access with logs

# From Appendix C – Table 1

| Protocol                    | Port    | Protocol           | Port    |
|-----------------------------|---------|--------------------|---------|
| SMTP                        | TCP 25  | SMTP TLS/SSL       | TCP 587 |
| IMAP4                       | TCP 143 | Secure IMAP4       | TCP 993 |
| POP3                        | TCP 110 | Secure POP         | TCP 995 |
| SSH                         | TCP 22  | TLS                | TCP 443 |
| FTP data port (active mode) | TCP 21  | SFTP (uses SSH)    | TCP 22  |
| FTP (PASV) control          | TCP 21  | FTPS (uses TLS)    | TCP 989 |
| FTP control                 | TCP 20  | FTPS (uses TLS)    | TCP 990 |
| TFTP                        | UDP 69  | SCP (uses SSH)     | TCP 22  |
| HTTP                        | TCP 80  | HTTPS (uses TLS)   | TCP 443 |
| DNS name queries            | UDP 53  | DNS zone transfers | TCP 53  |

# From Appendix C – Table 2

| Protocol                  | Port          | Protocol                      | Port         |
|---------------------------|---------------|-------------------------------|--------------|
| NetBIOS (TCP rarely used) | TCP/UDP 137   | LDAP                          | TCP 389      |
| NetBIOS                   | UDP 138       | LDAPS                         | TCP 636      |
| NetBIOS                   | TCP 139       | Telnet (Not Recommended)      | TCP 23       |
| L2TP                      | UDP 1701      | IPsec (for VPN with IKE)      | UDP 500      |
| PPTP                      | TCP 1723      | Remote Desktop Protocol (RDP) | TCP/UDP 3389 |
| SNMP                      | UDP 161       | SNMP trap                     | UDP 162      |
| SIP                       | TCP 5060/5061 | SMB                           | TCP 445      |
| DHCP (client to server)   | UDP 67/68     | DHCP (server to client)       | UDP 68       |
| RADIUS                    | UDP 1812/1813 | RADIUS with EAP               | TCP 1812     |
| TACACS+                   | TCP 49        | Kerberos                      | TCP/UDP 88   |

# Chapter 4 Summary

---

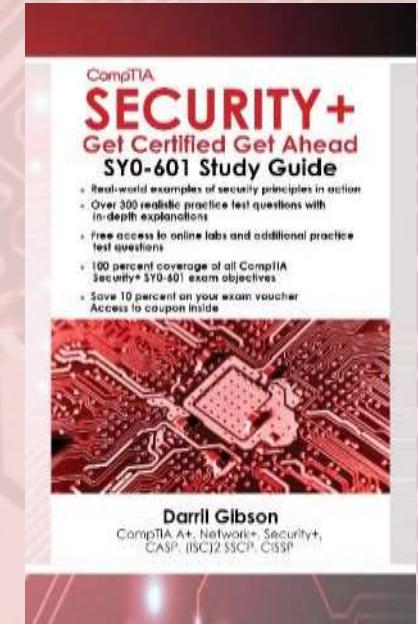
- Exploring Advanced Security Devices
- Securing Wireless Networks
- Understanding Wireless Attacks
- Using VPNs for Remote Access
- Check out the free online labs

# Chapter 5

## Securing Hosts and Data

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



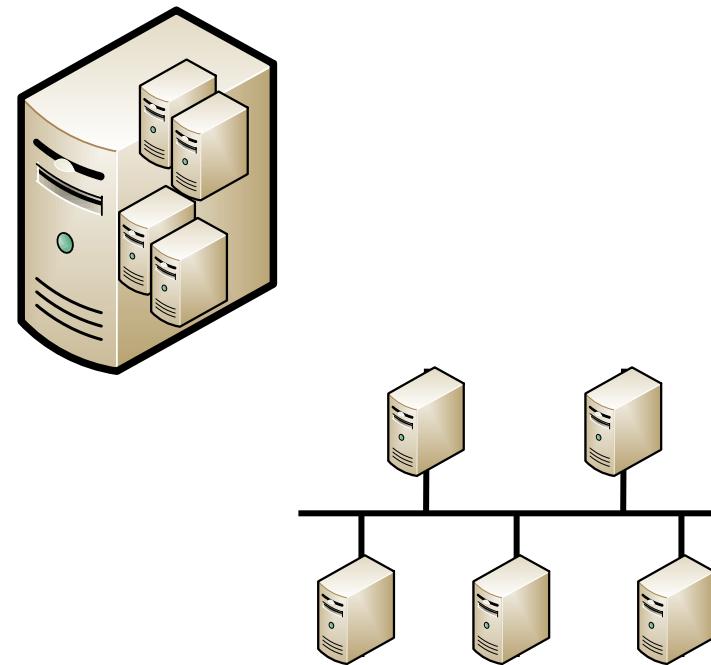
# Introduction

---

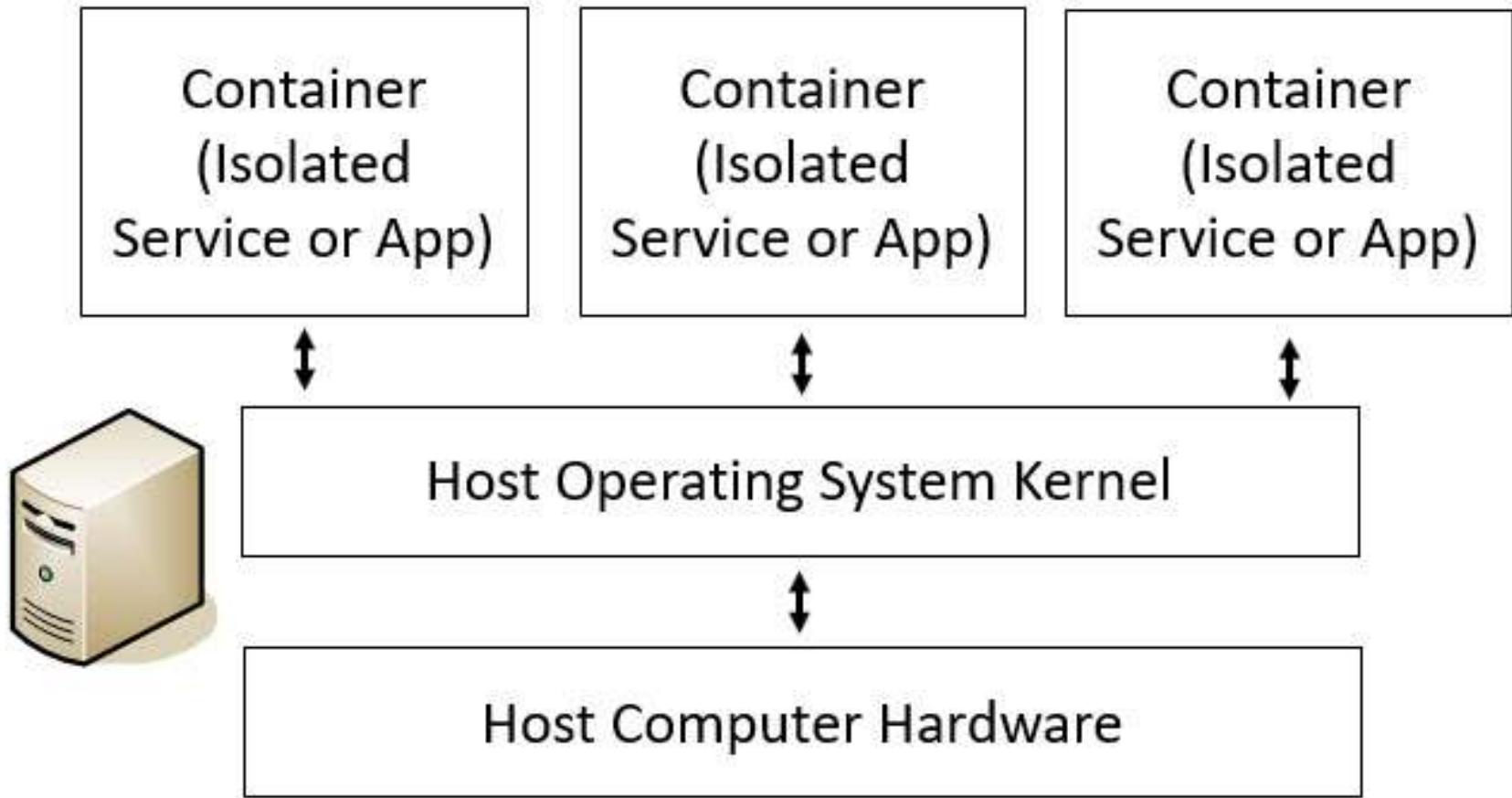
- Summarize Virtualization Concepts
- Implementing Secure Systems
- Summarizing Cloud Concepts
- Deploying Mobile Devices Securely
- Exploring Embedded Systems

# Virtualization

- VMs
  - Hypervisor
  - Host
  - Guest
  - Host scalability
  - Host elasticity
- Thin clients
- VDI



# Containers



# Virtualization

---

- VM escape
- VM sprawl
- Replication
- Snapshots
- Non-Persistence

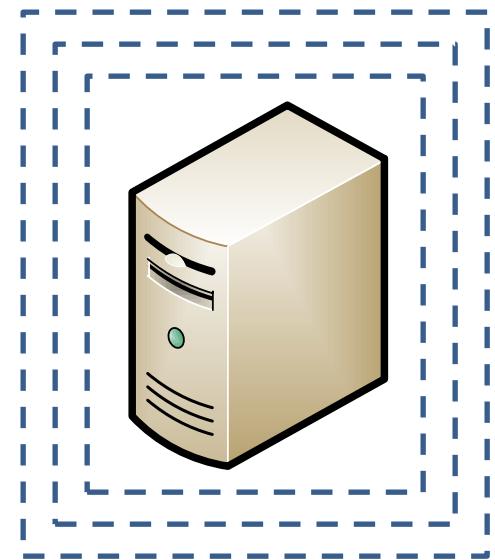
# Implementing Secure Systems

---

- Endpoints
  - Computing devices (servers, desktops, laptops, mobile devices, or IoT devices)
  - EDR tools
- Configuration management
  - Helps organizations deploy systems with secure configurations

# Hardening Systems

- Disabling unnecessary services
  - Improves security posture
  - Reduces attack surface
  - Reduces risks from open ports
- Disabling unneeded applications
- Disabling unnecessary accounts
- Protecting management interfaces and applications

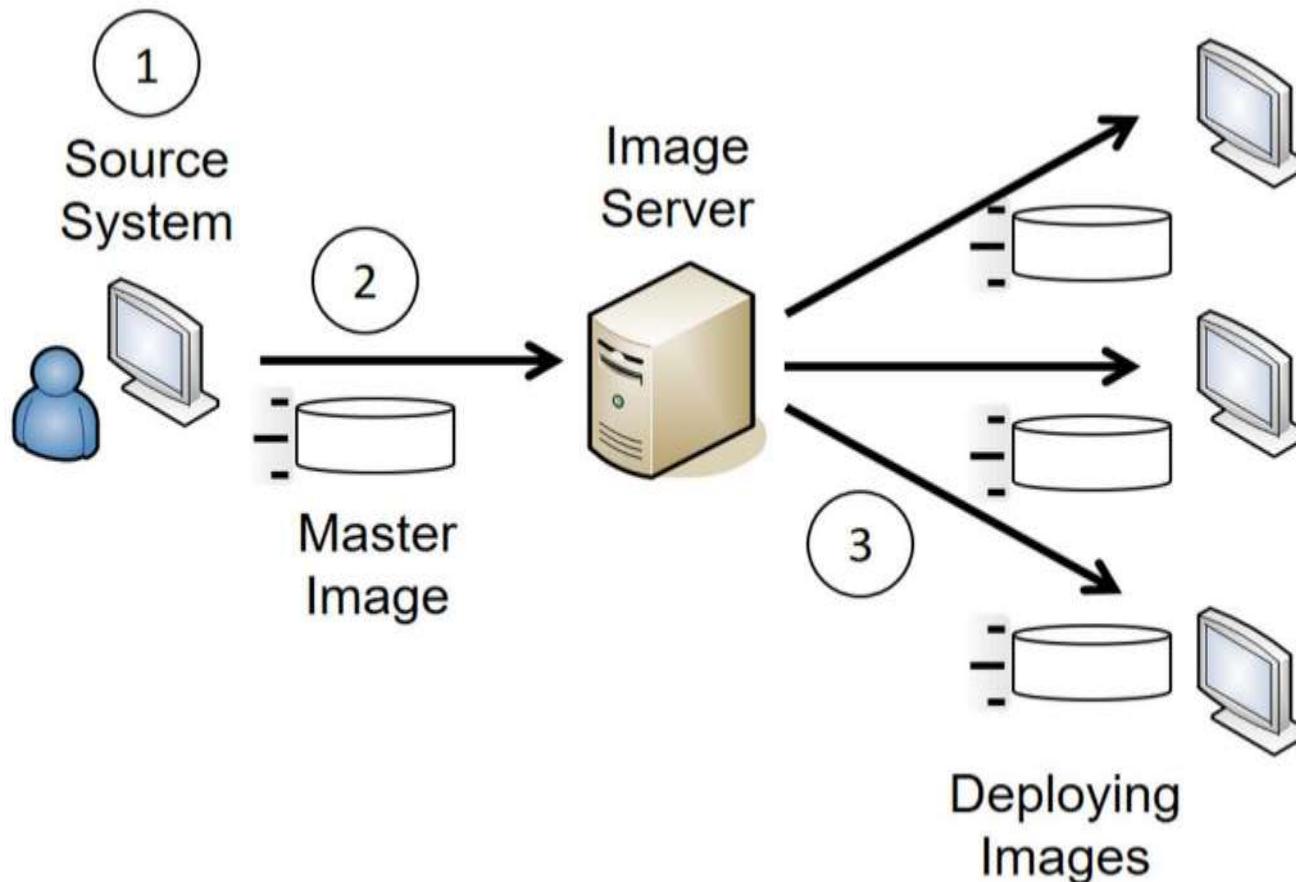


# Using Baselines

---

- Improve overall security posture
- Three steps
  1. Initial baseline configuration
    - Start in secure state
  2. Continuous security monitoring
    - Scan for and detect changes
  3. Remediation
    - Isolate or quarantine modified systems

# Master Images



Get(

©1 YCDA, LLC

# Implementing Patch Management

---

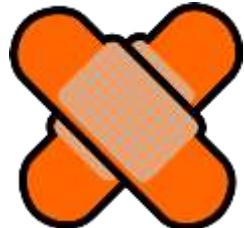
- Ensure that systems are up-to-date
- Protects system against known vulnerabilities
- Test patches in a test environment that mirrors the production environment



# Patch Management

---

- Automated deployment
- Controlled deployment
- Scheduling patch management
- Testing, deploying and verifying updates



# Change Management

---

- Helps ensure changes to IT systems do not result in unintended outages
- Provides an accounting structure or method to document all changes
- Changes are proposed and reviewed before implementation

# Allowing & Blocking Applications

---

- Application allow list
  - Blocks all applications NOT on the list
- Application block list
  - Blocks all applications on the list



# Implementing Secure Systems

---

- Application Programming Interface
  - Authentication
  - Authorization
  - Transport level security
- Microservices

# Encrypting Drives

---

- Full disk encryption (FDE)
  - Encrypts entire drive
- Self-encrypting drives (SEDs)
  - Automatically encrypts entire drive
  - Users typically need to log on to access drive

# Boot Integrity

---

- Unified Extensible Firmware Interface (UEFI)
- Trusted Platform Module (TPM)
- Hardware Security Module (HSM)

# DLP

---

- Data loss prevention (DLP) techniques & technologies
  - Rights management
  - Removable media
  - Data exfiltration
  - Encrypting data
  - Database encryption

# Summarizing Cloud Computing

---

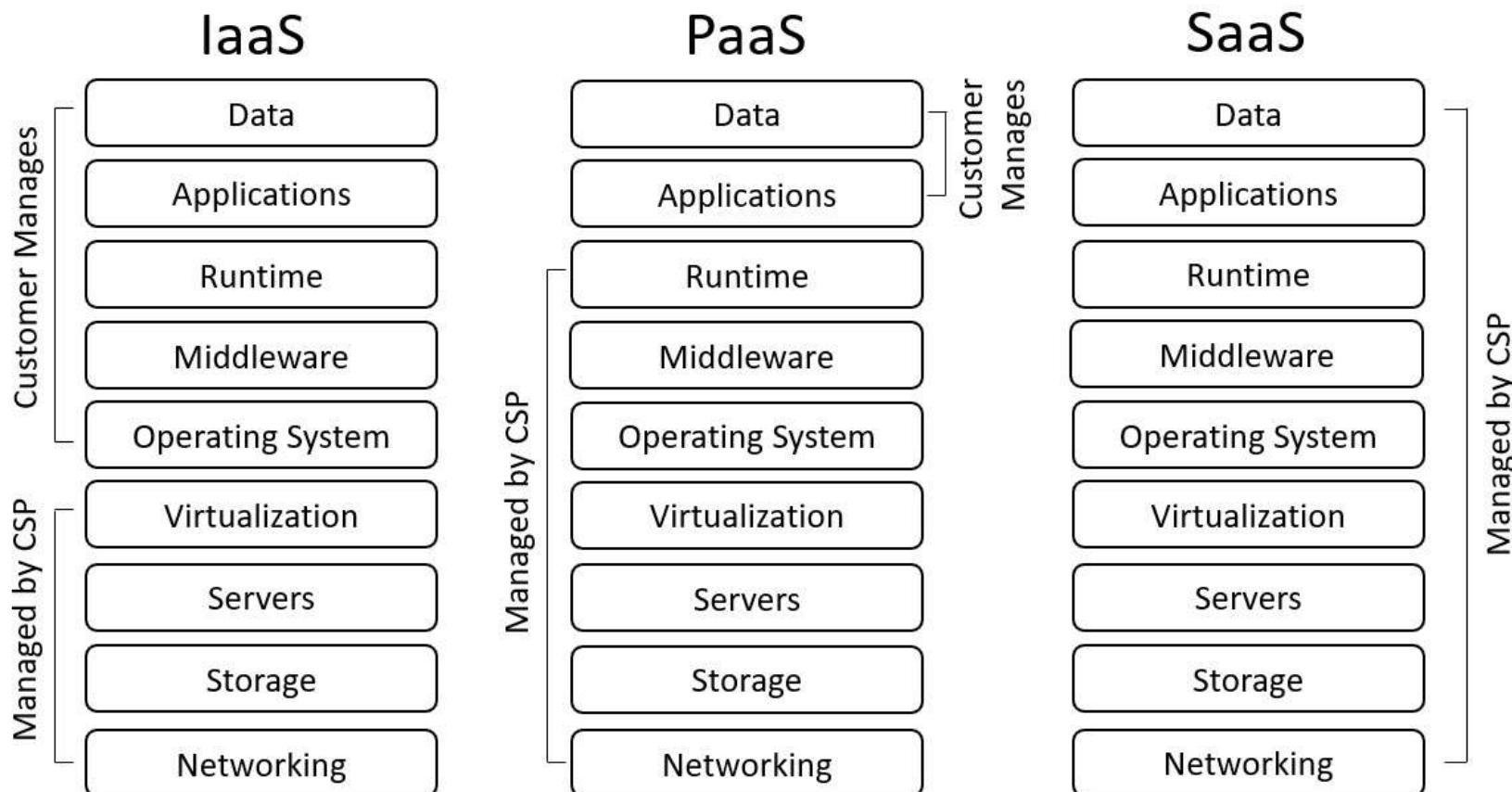
- Software as a Service (SaaS)
  - Applications provided over the Internet (such as web-mail accessed with a web browser)
- Platform as a Service (PaaS)
  - Provides customers with a fully managed platform
  - Vendor keeps platform up-to-date

# Understanding Cloud Computing

---

- Infrastructure as a Service (IaaS)
  - Provides customers with access to hardware in a self-managed platform
  - Customers are responsible for keeping an IaaS system up to date
- Anything as a Service (XaaS)
  - Cloud services beyond SaaS, PaaS, and IaaS
  - Services that can be delivered via the cloud, such as communications, databases, desktops, storage, and security

# Cloud Service Provider Responsibilities



# Cloud Deployment Models

---

- Public – Available to anyone
- Private – Only available within a company
- Community – Cloud shared by two or more organizations
- Hybrid – Combination of any two models

# MSSP Services

---

- Patch management
- Vulnerability scanning
- Spam and virus filtering
- Data loss prevention (DLP)
- Virtual private network connections
- Proxy services for web content filtering
- Intrusion detection and prevention systems
- Unified threat management (UTM) appliances
- Advanced firewalls such as next-generation firewalls

# Cloud Security Controls

---

- Google Cloud and Amazon Web Services (AWS) documentation
  - High availability and high availability across zones
  - Resource policies
  - Secrets management
  - Integration and auditing
- Cloud-based storage characteristics
  - Permissions
  - Encryption
  - Replication

# Cloud-based Networks

---

- Virtual networks
- Public and private subnets
- Segmentation
- Security groups
- Dynamic resource allocation
- Instance awareness
- VPC endpoint
- Transit gateway
- Container security

# Cloud-based Networks

---

- Virtual networks
- Public and private subnets
- Security groups
- Dynamic resource allocation
- Segmentation
- Instance awareness
- VPC endpoint
- Transit gateway
- Container security

# On-Premises Versus Off-Premises

---

- On-premises
  - Cloud resources owned, operated, and maintained by an organization for its employees
- Off-premises
  - In the cloud
  - CSP maintains

# Cloud Computing Security

---

- Cloud access security broker (CASB)
  - Software tool or service
  - Placed between organization's network and the cloud provider
- Cloud-based DLP
- Secure web gateway (SWG)
- Cloud-based firewalls

# Cloud Computing

---

- Infrastructure as Code
  - Software defined network (SDN)
  - Software-defined visibility (SDV)
- Edge computing
- Fog computing
- Cloud Security Alliance (CSA)

# Mobile Device Deployment Models

---

- Models support connecting mobile devices to organization's network
  - Corporate-owned
  - COPE (corporate-owned, personally enabled)
  - BYOD (bring your own device)
    - Bring your own disaster
  - CYOD (choose your own device)
    - Limits supported devices (employee still buys)

# Mobile Device Connection Methods

---

- Cellular
- Bluetooth
- NFC (near field communication)
- RFID (radio frequency identification)
- WiFi
- Infrared
- USB (Universal Serial Bus)
- Point-to-point
- Point-to-multipoint

# Mobile Device Connection Methods

---

- Application management
- Content management
- Passwords and PINs
- Biometrics
- Screen locks
- Full device encryption
- Containerization
  - Good for BYOD
- Storage segmentation
- Remote wipe

# MDM Enforcement / Monitoring

---

- Unauthorized software
  - Third party app stores
  - Rooting and jailbreaking
  - OTA updates
  - Sideloaded
  - SMS and MMS
  - RCS

# MDM Enforcement / Monitoring

---

- Unauthorized software
  - OTA updates
  - Sideloaded
- Third party app stores
  - SMS
  - MMS
  - RCS
- Rooting and jailbreaking
- Device posturing
  - Checks device status (such OS, version, screen lock)

# MDM Enforcement / Monitoring

---

- Hardware control
  - USB OTG cables
- Unauthorized connections
  - Tethering
  - Wi-Fi Direct

# SEAndroid

---

- Security-enhanced Android
  - Uses Security-Enhanced Linux (SELinux) to enforce access security
  - Enforcing mode
    - Enforces SELinux policy
  - Permissive mode
    - Does not enforce SELinux policy
    - Logs all activity
    - Useful when testing the policy

# Embedded System

---

- Dedicated function with a computer system to perform that function
  - Compare to desktop PCs, laptops, and servers
    - All use central processing units (CPUs), operating systems, and applications to perform various functions
  - Embedded systems
    - Use CPUs, operating systems, and one or more applications to perform specific functions



# Embedded System

---

- Security implications and vulnerabilities
  - Keep up-to-date
    - Implement patch management processes
  - Avoid default configurations

# Embedded System

---

- Field programmable gate array (FPGA)
  - Programmable integrated circuit (IC) installed on a circuit board
- Arduino
  - Microcontroller board, and the circuit board contains the CPU, RAM, and ROM
- Raspberry Pi
  - Microprocessor-based mini-computer, and it uses the Raspberry Pi OS to run

# Comparing Embedded Systems

---

- Smart devices
- Internet of things (IoT)
  - Wearable technology
  - Home automation
- HVAC
- SoC
- RTOS
- Printers/MFDs
- Camera systems
- Special purpose
  - Medical devices
  - Vehicles
  - Aircraft/UAV

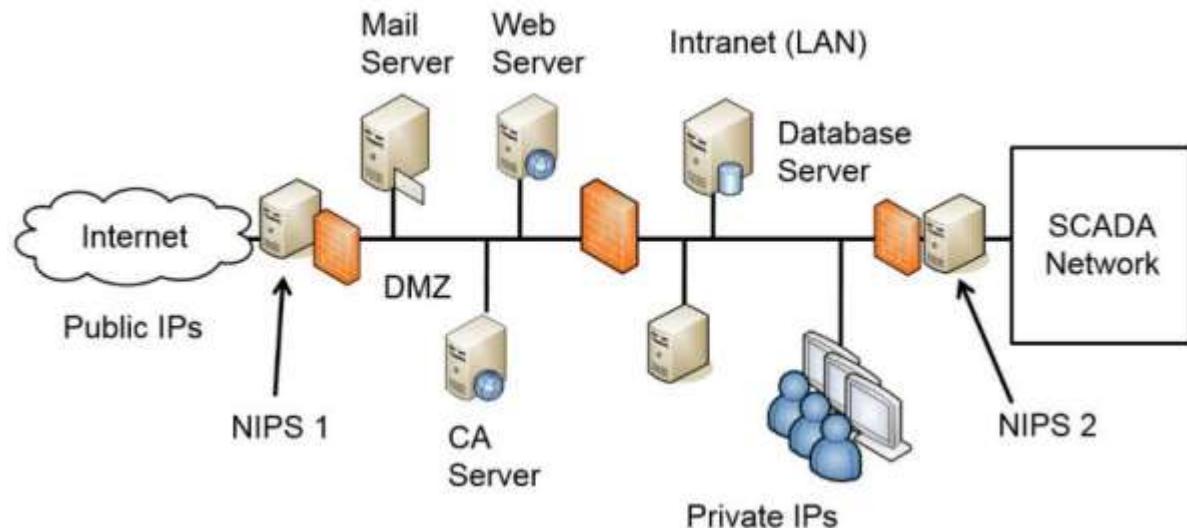
# Embedded System Constraints

---

- Compute
- Crypto
- Power
- Range
- Authentication
- Network
- Cost
- Inability to patch
- Implied trust
- Weak defaults

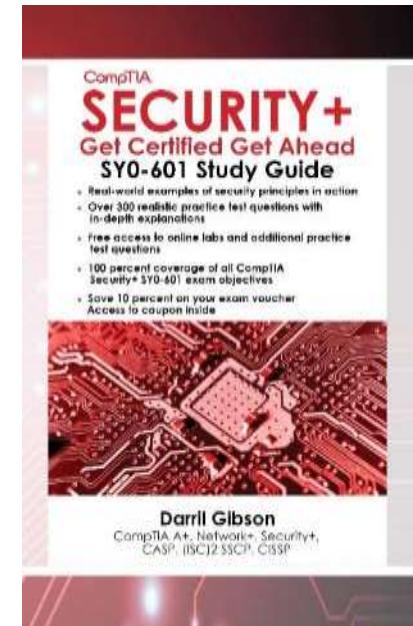
# SCADA/ICSs

- Manufacturing and industrial
- Facilities
- Energy
- Logistics
- Protect behind NIPS



# Chapter 5 Summary

- Summarize Virtualization Concepts
- Implementing Secure Systems
- Summarizing Cloud Concepts
- Deploying Mobile Devices Securely
- Exploring Embedded Systems
- Check out the free online resources

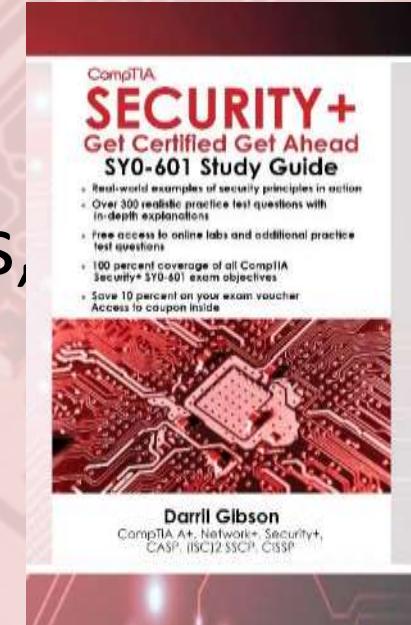


# Chapter 6

## Comparing Threats, Vulnerabilities, and Common Attacks

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Understanding Threat Actors
- Determining Malware Types
- Recognizing Common Attacks
- Blocking Malware and Other Attacks

# Threat Actors

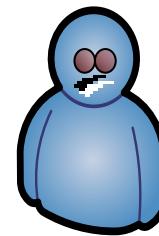
---

- Hacker
  - Malicious individuals who use their technical expertise to launch attacks
- Script kiddie
  - Little expertise, sophistication, or funding
- Hacktivist
  - Part of an activist movement
- Insider
  - Employee (can become a malicious insider)

# Threat Actors

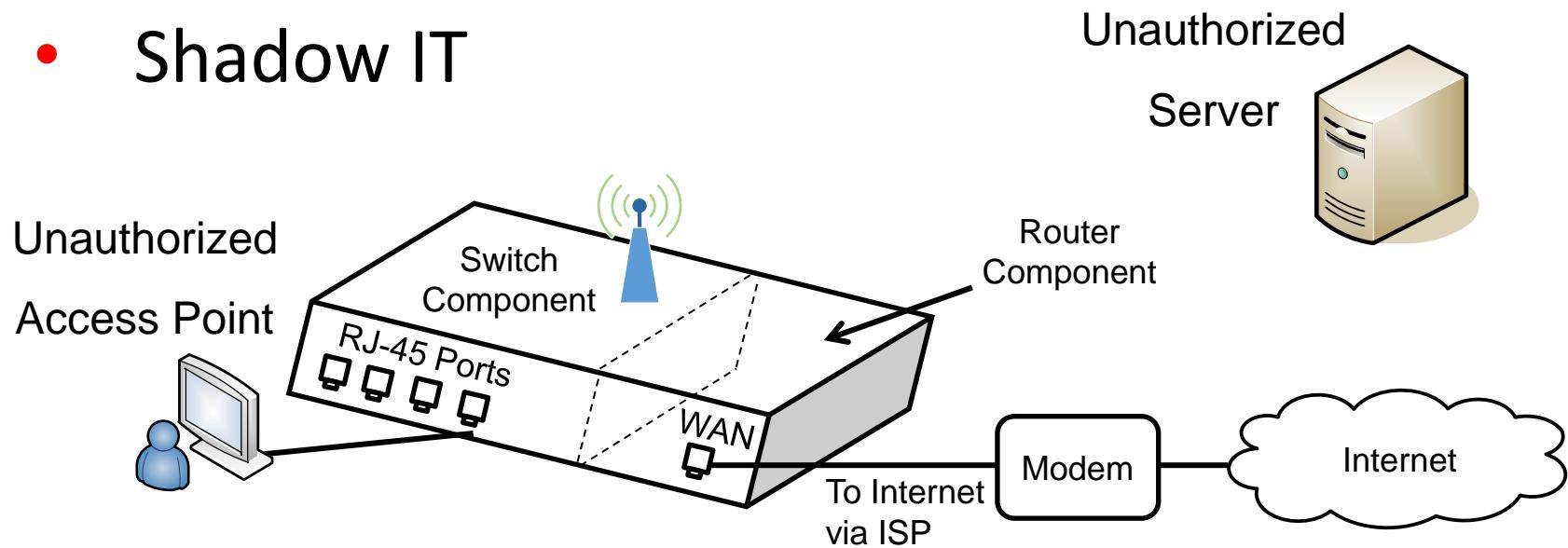
---

- Nation state/advanced persistent threat (APT)
  - Identify a target and persistently attack until they gain access
  - Often remain in network for months or years
  - China PLA Unit 61398
  - Russia APT 28 (Fancy Bear)
  - Russia APT 29 (Cozy Bear)



# Threat Actors

- Attack vectors
  - Email
  - Social media
- Shadow IT

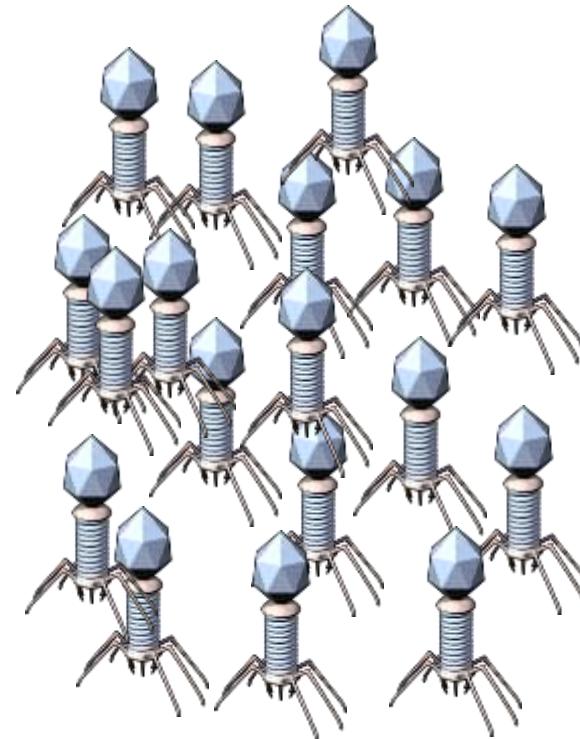


# Determining Malware Types

---

## Viruses

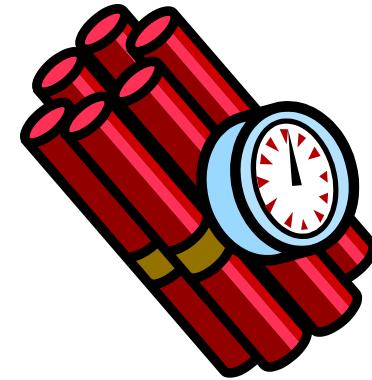
- Replication mechanism
- Activation mechanism
- Payload mechanism



# Determining Malware Types

---

- Worms
  - Self replicating
- Logic bombs
  - Executes in response to an event
- Backdoors
  - Provides an alternate method of access
  - Many types of malware create backdoors



# Determining Malware Types

---

- Trojan Horse
  - Appears to be useful but is malicious
  - Pirated software, rogueware, or games
  - Also infect systems via USB drives
- Drive-by downloads
  1. Attackers compromise a web site to gain control of it
  2. Attackers install a Trojan embedded in the web site's code
  3. Attackers attempt to trick users into visiting the site
  4. When users visit, the web site attempts to download the Trojan onto the users' systems
- Remote access Trojan (RAT)



# Determining Malware Types

---

- Keylogger
  - Capture's keystrokes
- Spyware
  - Can access a user's private data and result in loss of confidentiality



# Determining Malware Types

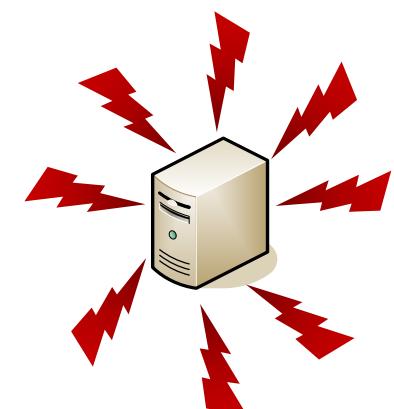
---

- Rootkits
  - System level or kernel access
  - Can modify system files and system access
  - Hide their running processes to avoid detection with hooking techniques
  - File integrity checker can detect modified files
  - Inspection of RAM can discover hooked processes

# Bots and Botnets

---

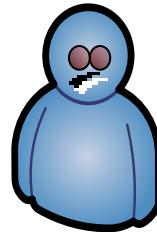
- Bots – software robots
- Botnets
  - Controlled by criminals (bot herders)
  - Manage command and control centers
  - Malware joins computers to robotic network
- Zombies or clones
  - Computers within botnet
  - Join after becoming infected with malware



# Determining Malware Types

---

- Ransomware
  - Takes control of user's system
  - Typically encrypts user's data
  - Attempts to extort payment



We have your data  
Pay up or you'll never see it again

# Determining Malware Types

---

- Potentially unwanted programs (PUPs)
  - Legitimate, but some are malicious, such as Trojans
- Fileless virus
  - Memory code injection
  - Script-based techniques
  - Windows Registry manipulation

# Social Engineering

---

- Flattery and conning
- Assuming a position of authority
- Encouraging someone to:
  - Perform a risky action
  - Reveal sensitive information
- Impersonating
- Tailgating



# Social Engineering

---

- Impersonating
  - Such as an authorized technician
- Shoulder Surfing
  - Can be in person looking at a computer
  - Can be with a remote camera
- Tricking users with hoaxes

# Social Engineering

---

- Tailgating
  - Closely following authorized personnel without providing credentials
  - Mitigated with mantraps
- Dumpster diving
  - Searching through trash looking for information
  - Mitigated by shredding or burning papers

# Social Engineering

---

- Zero-day vulnerabilities
  - Unknown to trusted sources, such as operating system and antivirus vendors
- Watering hole attack
  - Attacker identifies websites trusted by group of users
  - Attacker infects these websites
  - Users go to infected (but trusted) websites
  - Prompted to download files

# Social Engineering

---

- Typo squatting (called URL hijacking)
  - Hosting a malicious website
  - Earning ad revenue
  - Reselling the domain
- Elicitation
  - Active listening
  - Reflective questioning
  - False statements
  - Bracketing

# Attacks via Email and Phone

---

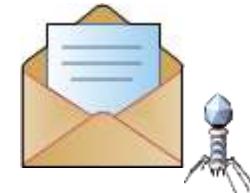
- Spam
  - Unwanted or unsolicited email
- Spam over internet messaging (SPIM)
  - Unwanted messages sent over instant messaging (IM) channels
- Phishing
  - Email from friends
  - Installing malware
  - Validating email address
  - Getting money



# Attacks via Email and Phone

---

- Spear Phishing
  - Targeted form of phishing
  - Attempts to target specific groups of users, or even a single user



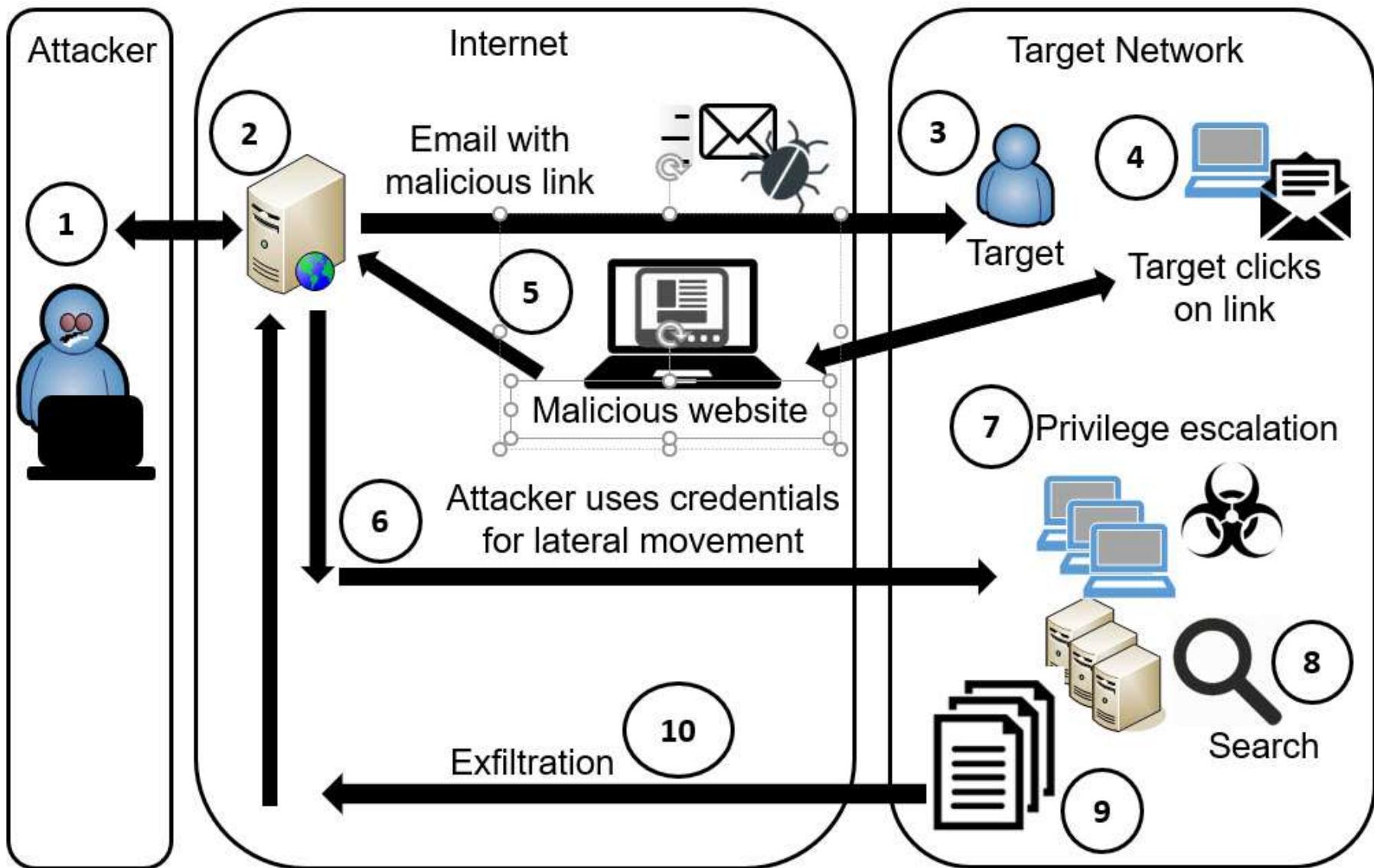
- Whaling
  - Form of spear phishing that attempts to target high-level executives

# Attacks via Email and Phone

---

- **Vishing**
  - use the phone system to trick users
- **Smishing**
  - a mashup of SMS and phishing
  - uses text instead of email

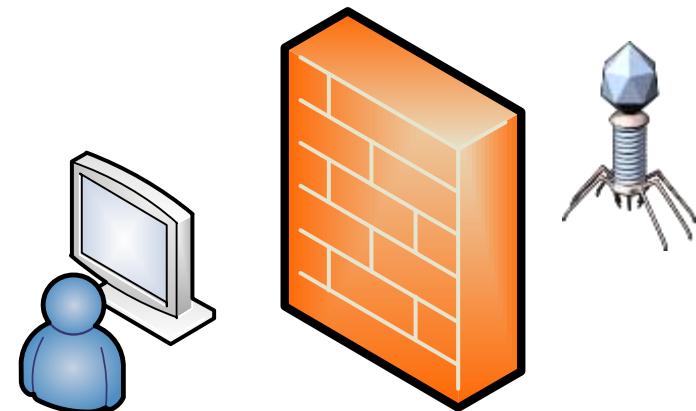
# One Click Lets Them In



# Blocking Malware

---

- Spam filter on mail gateways
- Anti-malware software on mail gateways
- Anti-malware software on all systems
- Block at boundaries
  - Firewalls
  - UTM systems



# Blocking Malware

---

- Antivirus software
  - Signature-based detection
    - Detects known malware based on signature definitions
  - Heuristic-based detection
    - Detects unknown malware based on behavior
  - File integrity monitors
  - Cuckoo sandbox

# Why Social Engineering Works

---

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust

# Common Types of OSINT

---

- Open source intelligence (OSINT)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - Structured Threat Information eXpression (STIX)
  - Public/private information sharing centers
  - Automated indicator sharing (AIS)
  - Indicators of compromise
  - Vulnerability databases
  - File/code repositories
  - Predictive analysis
  - Threat maps

# Research Sources

---

- Vendor
- Conferences
- Academic journals
- Local industry groups
- Request for comments (RFC)
- Public/private information sharing centers
- Social media

# Chapter 6 Summary

---

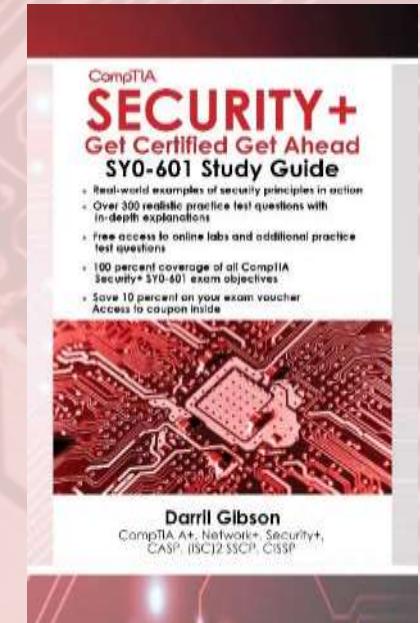
- Understanding Threat Actors
- Determining Malware Types
- Recognizing Common Attacks
- Blocking Malware and Other Attacks
- Check out the free online resources

# Chapter 7

## Protecting Against Advanced Attacks

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Understanding Attack Frameworks
- Identifying Network Attacks
- Summarizing Secure Coding Concepts
- Identifying Malicious Code and Scripts
- Identifying Application Attacks

# Attack Frameworks

---

- Cyber Kill Chain
  - includes seven elements tracking an attack from reconnaissance to performing actions
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control (C2)
    - Actions on Objectives

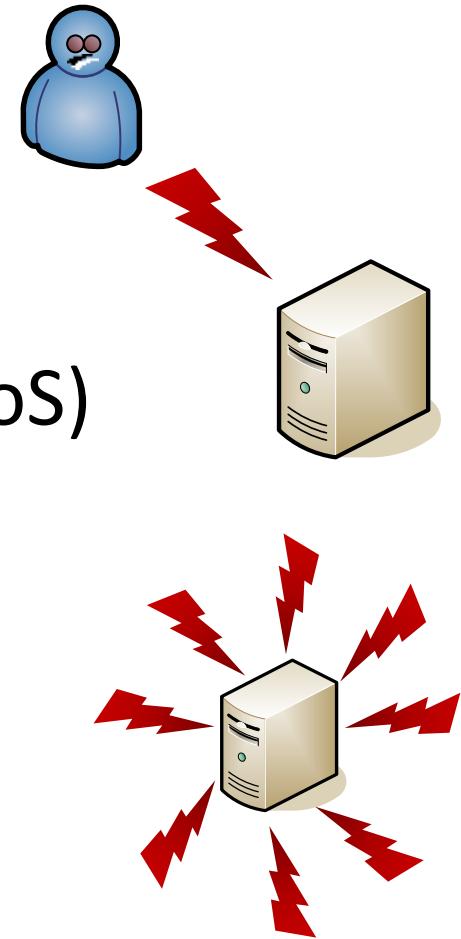
# Attack Frameworks

---

- Diamond Model of Intrusion Analysis
  - identifies four key components of every intrusion event
    - Adversary
    - Capabilities
    - Infrastructure
    - Victim
- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)
  - matrix of ten tactics and techniques attackers use to achieve each

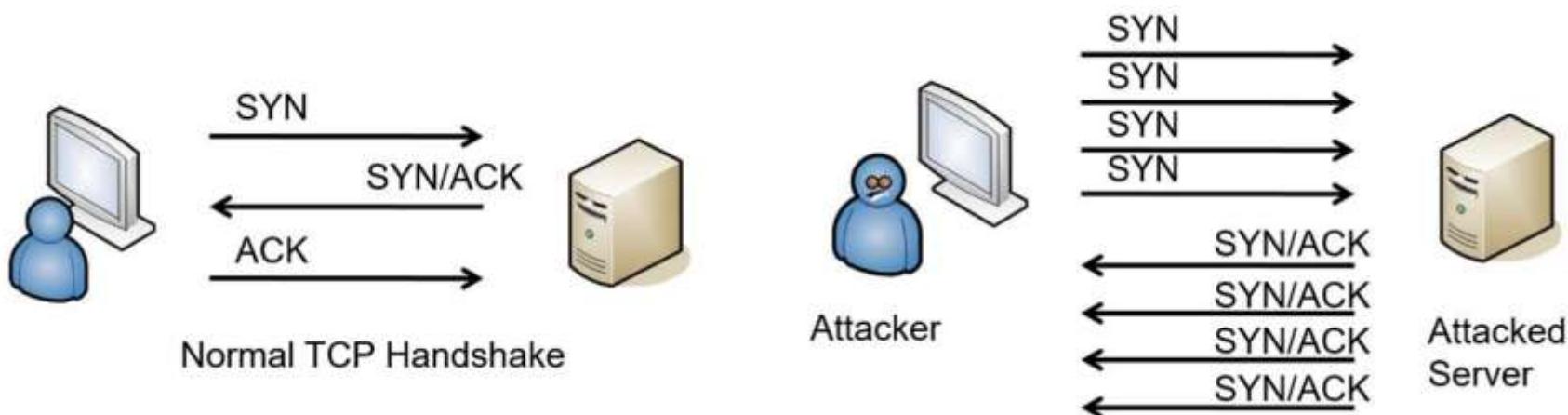
# Network Attacks

- Denial-of-service (DoS)
  - Comes from one system
- Distributed denial-of-service (DDoS)
  - Multiple attacking computers
  - Typically include sustained, abnormally high network traffic



# Network Attacks

- SYN flood attack
  - Common attack against Internet servers
  - Disrupts the TCP three-way handshake
  - Withholds 3<sup>rd</sup> packet



# Network Attacks

---

- Spoofing
  - Impersonating or masquerading as someone or something else
    - MAC spoofing
    - IP spoofing
- On-Path Attacks
  - sometimes referred to as a man-in-the-middle attack
  - is a type of proxy Trojan horse that infects vulnerable web browsers

# Network Attacks

---

- Secure Sockets Layer (SSL) stripping attack
  - Hypertext Transfer Protocol Secure (HTTPS) connection to a Hypertext Transfer Protocol (HTTP) connection
- Layer 2 Attacks
  - attempt to exploit vulnerabilities at the Data Link layer (Layer 2) of the Open Systems Interconnection (OSI) model

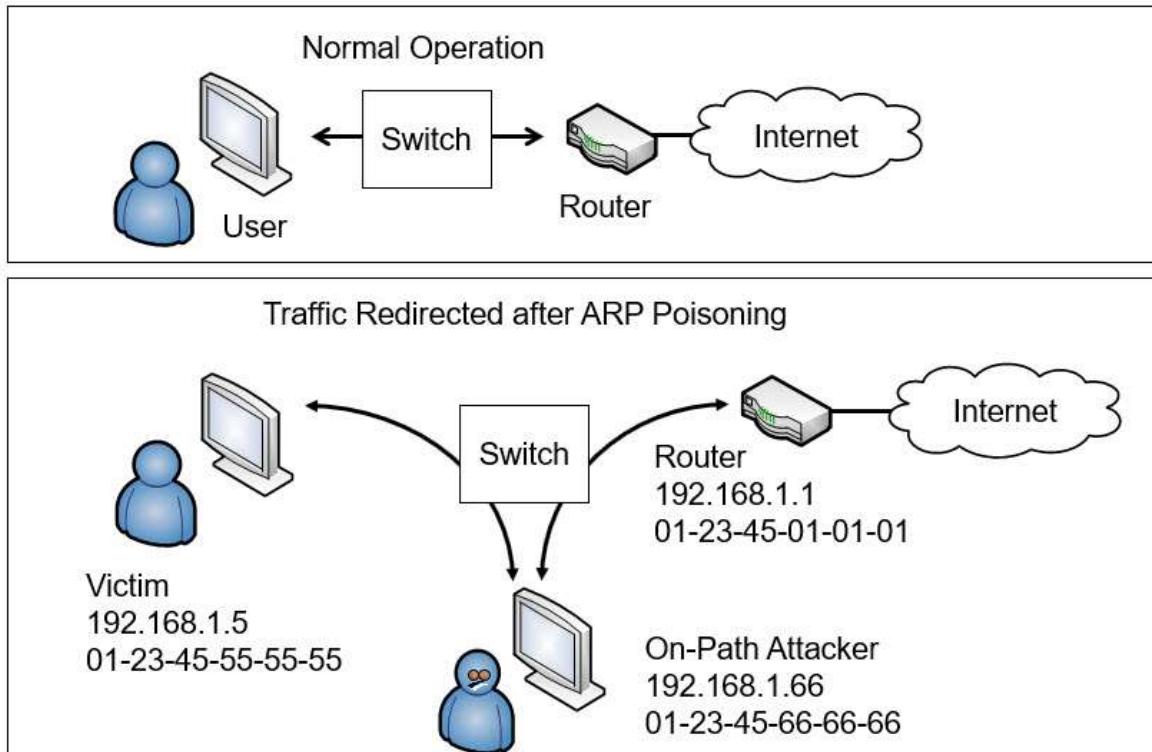
| Layer Number | Layer Name   | Mnemonic | Mnemonic   |
|--------------|--------------|----------|------------|
| 1            | Physical     | Please   | Processing |
| 2            | Data Link    | Do       | Data       |
| 3            | Network      | Not      | Need       |
| 4            | Transport    | Throw    | To         |
| 5            | Session      | Sausage  | Seem       |
| 6            | Presentation | Pizza    | People     |
| 7            | Application  | Away     | All        |

# OSI MODEL

| Layer Number | Layer Name   | Devices                                                                                                                 | Protocols                                                                                   |
|--------------|--------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1            | Physical     | Cables, hubs                                                                                                            | Ethernet, cabling protocols                                                                 |
| 2            | Data Link    | Switches                                                                                                                | MAC, ARP, VLANs                                                                             |
| 3            | Network      | Router, layer 3 switch                                                                                                  | IPv4, IPv6, IPsec, ICMP                                                                     |
| 4            | Transport    |                                                                                                                         | TCP, UDP                                                                                    |
| 5            | Session      |                                                                                                                         |                                                                                             |
| 6            | Presentation |                                                                                                                         |                                                                                             |
| 7            | Application  | Proxy servers, web application firewalls, next-generation firewalls, UTM security appliances, and web security gateways | DNS, FTP, FTPS, SFTP, TFTP, HTTP, HTTPS, IMAP4, LDAP, POP3, SFTP, SMTP, SNMP, SSH, and TFTP |

# ARP Poisoning

- ARP request
- ARP reply
- ARP on-path attacks
  - Previously known as man-in-the-middle attack



# Layer 2 Attacks

---

- MAC flooding
  - attack against a switch that attempts to overload it with different MAC addresses
  - sends a Simple Network Management Protocol (SNMP) trap or error message
- MAC Cloning
  - changing a system's MAC address to another MAC address

# DNS Attacks

---

- DNS poisoning
  - Attempt to corrupt DNS data
  - Protect against with DNSSEC
- URL redirection
  - used to redirect traffic to a different page within a site
- Domain hijacking
  - Attacker changes the registration of the domain name
  - Typically done by using social engineering techniques to guess owner's password

# DNS Attacks

---

- Domain reputation
  - helps ISPs determine an email is being sent by a legitimate organization
- DNS sinkhole
  - DNS server that gives incorrect results for one or more domain names
- DNS log files
  - record DNS quer

# Network Attacks

---

- Replay attacks/ session replays
  - capture data in a session to impersonate one of the parties in the session
  - can occur on both wired and wireless networks

# Secure Coding Concepts

---

- OWASP
  - Open Web Application Security Project
  - focused on improving the security of software
- Code reuse
  - saves time and helps prevent the introduction of new bugs
- Dead code
  - code that is never executed or used

# Input Validation

---

- Verifies validity of data before using it
  - Verifies proper characters
  - Uses boundary and/or range checking
  - Blocks HTML code
  - Prevents the use of certain characters
- Client-side vs server-side
  - Server-side is more secure (many sites use both)
- Input validation prevents
  - Buffer overflow, SQL injection, command injection, and cross-site scripting attacks

# Error and Exception Handling

---

- Catch errors and provides feedback
  - Prevent improper input from crashing an application providing information to attackers
  - Errors to users should be general
  - Logged information should be detailed

# Secure Coding Concepts

---

- Third-party libraries
- Software Development Kits (SDKs)
  - Provide software tools easy to reuse
- Code obfuscation
  - Camouflage code

# Secure Coding Concepts

---

- Avoid race conditions
  - Occur when two modules attempt to access the same resource
  - First module to complete the process wins
  - Database locks prevent race conditions

# Software Diversity

---

- Outsourced Code Development
- Data exposure
- HTTP headers
  - HTTP Strict-Transport-Security
  - Content-Security-Policy
  - X-Frame-Options
- Secure cookie
- Code signing

# Common Methods of Testing Code

---

- Static code analysis
  - examines the code without executing it
- Manual code review
  - static code analysis where someone goes through the code line by line
- Dynamic code analysis
  - checks the code as it is running
- Sandboxing
  - used to test applications within an isolated area

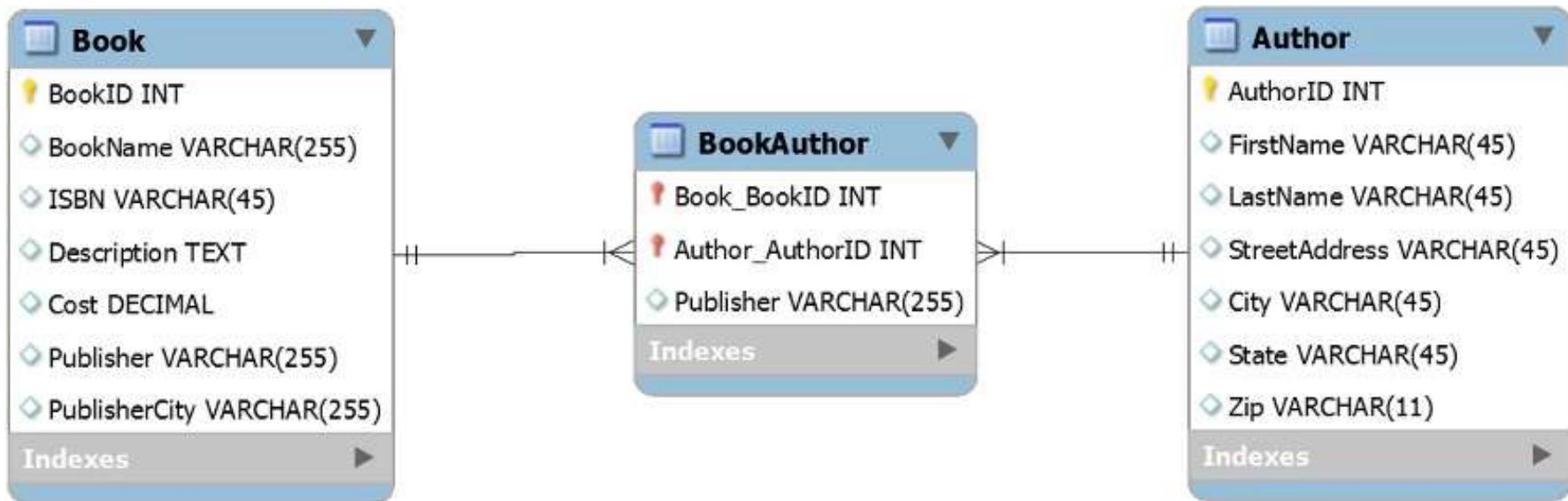
# Secure Coding Concepts

---

- Software version control
- Secure development environment
  - includes multiple stages
    - Development
    - Test
    - Staging
    - Production
    - Quality assurance

# Database concepts

- Tables related to each other with keys
- Database schema



# Database concepts

## Tables

- Rows (also called records or tuples)
- Columns (also called attributes)
- Cells hold individual values (such as “Lisa”)

Column  
↓

| AuthorID | FirstName | LastName | StreetAddress         | City        | State |       |
|----------|-----------|----------|-----------------------|-------------|-------|-------|
| 1        | Lisa      | Simpson  | 742 Evergreen Terrace | Springfield | IDK   | ← Row |
| 2        | Moe       | Szylak   | 1313 Walnut Street    | Springfield | IDK   | ← Row |
| 3        | Ned       | Flanders | 744 Evergreen Terrace | Springfield | IDK   | ← Row |

# Database concepts

---

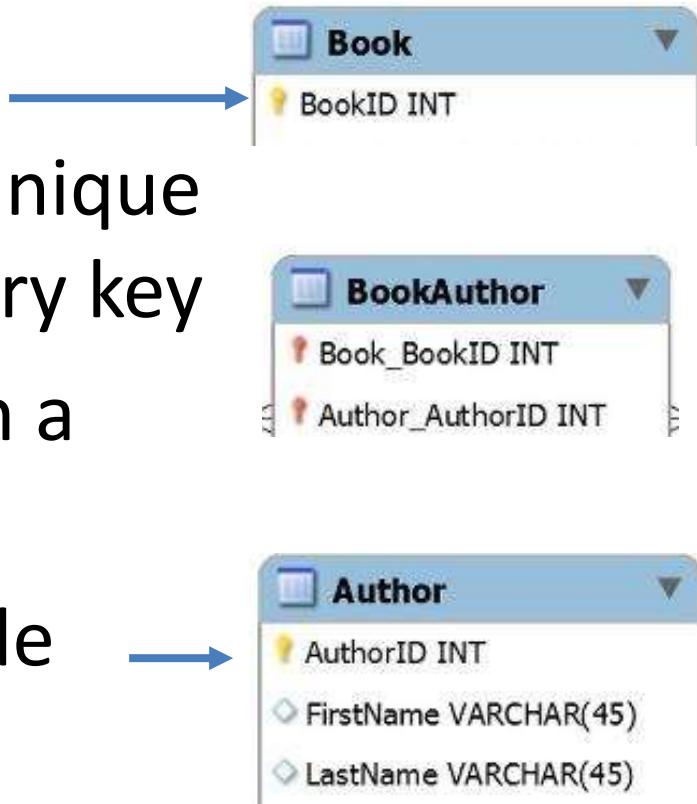
## Normalization

- Organizing tables and columns to reduce redundant data and improve performance
- First normal form (1NF)
- Second normal form (2NF)
- Third normal form (3NF)

# Database concepts

## 1NF

- Each row within a table is unique and identified with a primary key
- Related data is contained in a separate table
- None of the columns include repeating groups



# Database concepts

## 2NF (must be in 1NF)

- Non-primary key attributes are completely dependent on the composite primary key



# Database concepts

## 3NF (must be in 2NF and 1NF)

- All columns that aren't primary keys are only dependent on the primary key
- None of the columns in the table are dependent on non-primary key attributes.

PublisherCity column violates this rule  
It is dependent on the BookID column  
It is dependent on the Publisher column



| Book          |              |
|---------------|--------------|
| BookID        | INT          |
| BookName      | VARCHAR(255) |
| ISBN          | VARCHAR(45)  |
| Description   | TEXT         |
| Cost          | DECIMAL      |
| Publisher     | VARCHAR(255) |
| PublisherCity | VARCHAR(255) |
| Indexes       |              |

# SQL Queries

---

```
SELECT * FROM Customers WHERE name = 'Homer Simpson'
```

- Using SQL Injection

```
SELECT * FROM Customers WHERE name = '' or '1'='1' --'
```

- Result

```
SELECT * FROM Customers WHERE name = ''
```

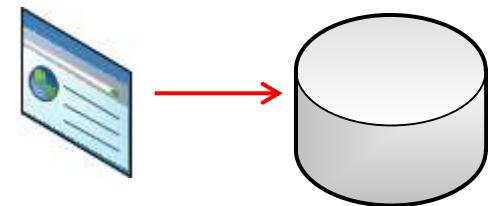
```
SELECT * FROM Customers WHERE '1'='1'
```



# SQL Injection Attack

---

- Used on unprotected web pages to access backend databases
- Often use the phrase ' or '1'='1 '
- Tricks database into providing information
- Best protection
  - Input validation & stored procedures
- XML injection (similar to SQL injection)



# SQL Injection Attack

---

- Protecting against SQL injection attacks
  - Input validation
  - Stored procedures
    - Group of SQL statements that execute as a whole
  - Parameterized stored procedures
    - Stored procedure that accepts input as a parameter
    - Stored procedure can perform input validation

# Secure Coding Concepts

---

- Provisioning and deprovisioning
  - typically refer to user accounts
- Integrity measurement
  - refers to the quality of the code
- Web server logs

# Scripting for Automation

---

- Automated courses of action
- Continuous monitoring
- Continuous validation
- Continuous integration
- Continuous delivery
- Continuous deployment

# Malicious Code and Scripts

---

- PowerShell
  - task-based command-line shell and scripting language that uses cmdlets
  - Invoke-Command
- Bash (short for Bourne-Again Shell)
  - command language interpreter for Unix and Unix-like operating systems
  - /bin/bash or /bin/sh

# Malicious Code and Scripts

---

- Python
  - interpreted programming language
- Macros
  - short instruction that will run a longer set of instructions
- Visual Basic for Applications (VBA)
  - event-driven tool

# Malicious Code and Scripts

---

- OpenSSL
  - software library used to implement SSL and TLS protocols
- SSH
  - OpenSSH is a suite of tools that simplify the use of SSH

# Application Attacks

---

- Zero day attack
  - Attempts to exploit zero-day vulnerabilities
  - Also known as zero day- exploit

# Memory Vulnerabilities

---

## Application bugs

- Memory leak
  - App consumes more and more memory
  - Can crash operating system
- Integer overflow
  - App attempts to use or create numeric value too big for the available storage
  - 8-bit storage
  - $95 \times 59 = 5,605$  (needs at least 13 bits to store)

# Memory Vulnerabilities

---

- Buffer overflow and buffer overflow attack
  - Occur when an application receives data that it can't handle
  - Exposes system memory
  - Often includes NOP instructions (such as x90)
  - Can then insert malicious code into memory
  - Input validation helps prevent buffer overflow attacks

# Memory Vulnerabilities

---

- Pointer/object dereference
  - A reference to a variable or object
  - Pointer is the memory address of the variable or object
  - If value is null results in error app tries to reference it
    - Some compilers catch it and throw an error
    - If compiler doesn't catch it, a failed dereference operation can cause app to crash

# Injection Attacks

---

- Dynamic Link Library (DLL) Injection
  - attack that injects a DLL into a system's memory and causes it to run
- Lightweight Directory Access Protocol Injection (LDAP)
  - specifies the formats and methods used to query databases of objects

# Injection Attacks

---

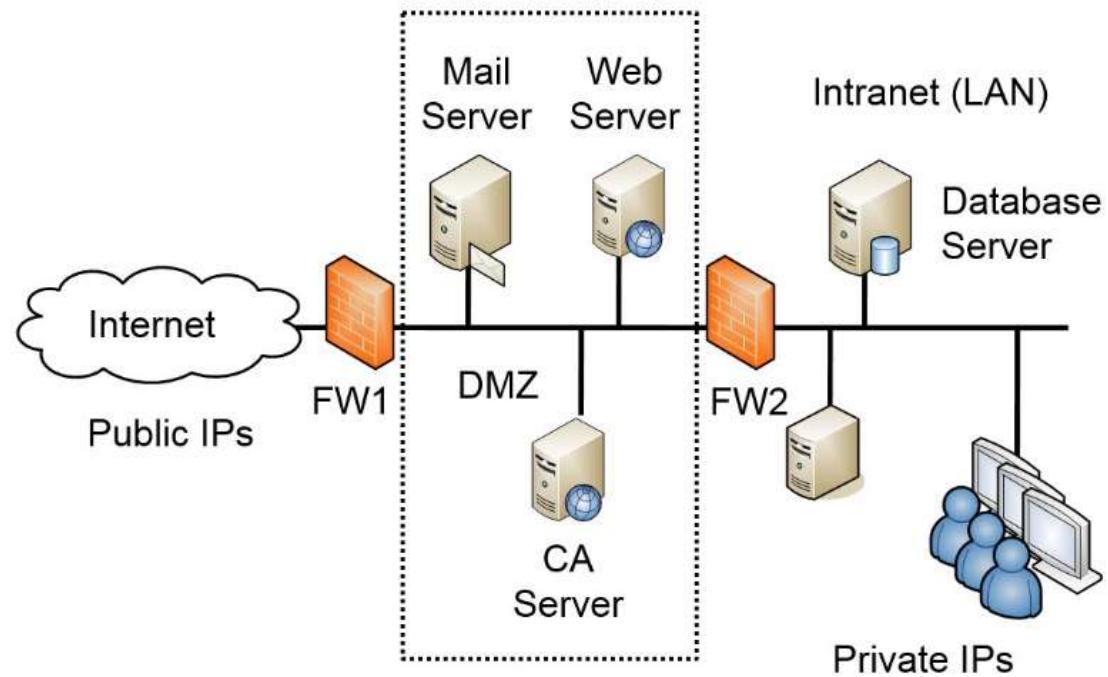
- Extensible Markup Language (XML) Injection
  - Markup language commonly used to transfer data
- Directory traversal
  - Attempts to access a file by including the full directory path

# Application Attacks

- Web servers host web sites

- Apache
  - IIS

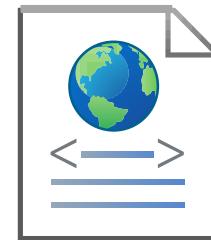
- Protected by placing in screened subnet



# Application Attacks

---

- Cross-site scripting (XSS)
  - Attackers embed malicious HTML or JavaScript code
  - Can be in web site or links in email
  - Prevented with server-side input validation
  - OWASP recommends use of library



# Application Attacks

---

- Cross-site request forgery (XSRF)
  - Causes users to perform actions on websites without their knowledge
  - Attackers can use to steal cookies and harvest passwords
  - XSRF tokens successfully block this attack

# Application Attacks

---

- Server-Side Request Forgeries (SSRF)
  - exploit how a server processes external information
- Client-Side Request Forgeries
  - occur if an attacker can inject code into the client-side webpage
  - use cookies

# Application Attacks

---

- Driver manipulation
  - Shimming
  - Refactoring code

# AI & ML

---

- Artificial intelligence (AI)
  - Intelligence that machines can demonstrate
  - Learn what works and keep doing it
  - Learn what doesn't work and stop
  - Try new things
- Machine Learning (ML)
  - Part of AI
  - Technologies that help computer systems improve with experience

# AI & ML

---

- Cybersecurity technologies
  - Google uses machine learning to block as many as 100 million spam emails daily
  - IBM's Watson uses machine learning to detect cyber threats as they're happening
  - The Balbix platform uses AI-powered risk predictions to protect networks

# AI & ML

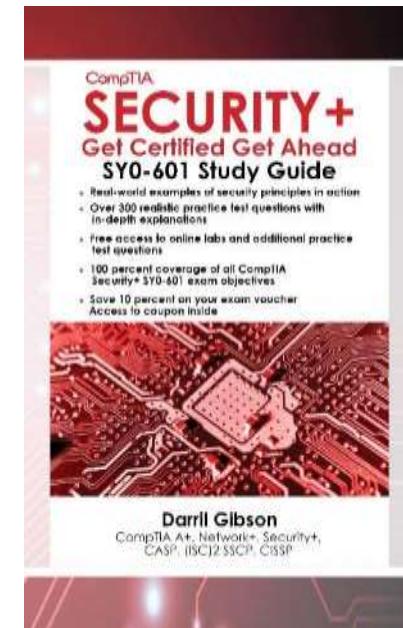
---

- Adversarial AI
  - Attempts to fool AI models by supplying it with deceptive input
- Tainted data (also known as data bias) for ML
  - Can cause AI and ML systems to give inconsistent results
- Machine Learning Algorithms
  - ML systems use algorithms to learn the environment

# Chapter 7 Summary

---

- Understanding Attack Frameworks
- Identifying Network Attacks
- Summarizing Secure Coding Concepts
- Identifying Malicious Code and Scripts
- Identifying Application Attacks
- Check out the free online resources

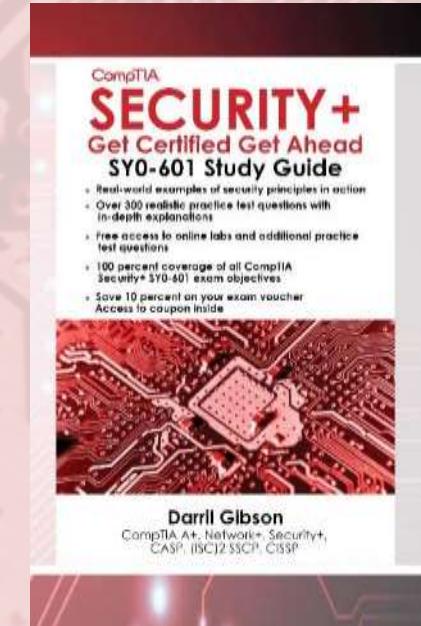


# Chapter 8

## Using Risk Management Tools

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Understanding Risk Management
- Comparing Scanning and Testing Tools
- Capturing Network Traffic
- Understanding Frameworks and Standards

# Understanding Risk Management

---

- Risk
  - Likelihood that a threat will exploit a vulnerability
- Vulnerabilities
  - Weaknesses
- Threats
  - Potential danger
- Impact
  - Magnitude of harm



# Threat

- Event that compromises confidentiality, integrity, or availability
- Malicious human threats
- Accidental human threats
- Environmental threats



# Threat

- Event that compromises confidentiality, integrity, or availability
- Manmade
- Internal
- External



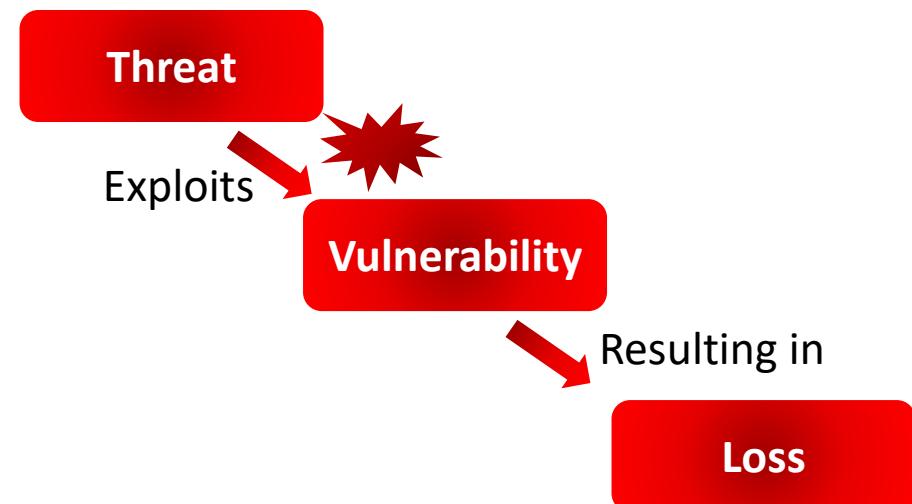
# Threat

- Event that compromises confidentiality, integrity, or availability
- Manmade
- Internal
- External



# Threat Assessment

- Helps identify and organize threats
- Attempts to identify:
  - Potential threats
  - Likelihood of threat (priority)
  - Potential impact
  - Security controls



# Vulnerabilities

- Flaw or weakness  
(in software, hardware, or process)
  - Lack of updates
  - Default configurations
  - Lack of up-to-date malware protection
  - No firewall
  - Lack of organizational policies



# Risk Management

---

- Practice of identifying, monitoring, and limiting risks to a manageable level
- Cannot eliminate risks
- Risk Terms
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite

# Risk Response Techniques

| Method                  | Comments                                                                                |
|-------------------------|-----------------------------------------------------------------------------------------|
| Avoid                   | Not participate in risky activity.                                                      |
| Mitigate                | Implement controls to reduce risks.<br>Antimalware reduced risk from malware            |
| Accept                  | Use if cost of control greater than the benefit<br>Remaining risk is residual risk      |
| Transfer                | Outsource. Purchase insurance.<br>Sometimes referred to as <i>sharing</i> risk.         |
| Cybersecurity Insurance | Helps protect businesses and individuals from losses related to cybersecurity incidents |

# Risk Assessments

---

- First steps
  - Identify assets and asset value
- Quantitative
  - Uses specific monetary amounts to identify cost and asset values
- Qualitative
  - Uses judgment to categorize risks based on probability and impact



# Quantitative Risk Assessment

---

- SLE (single loss expectancy)
  - Cost of any single loss
- ARO (annual rate of occurrence)
  - How many times the loss will occur annually
- ALE (annual loss expectancy)
  - $SLE \times ARO$



# Quantitative Risk Assessment

---

- Laptop cost \$2,000
- Employees lose one a month
- What is SLE?    SLE = \$2,000
- What is ARO?    ARO = 12
- What is ALE?    ALE = \$24,000

# Quantitative Risk Assessment

---

- Formulas
  - $ALE = SLE \times ARO$
  - $ARO = ALE / SLE$
  - $SLE = ALE / ARO$

# Qualitative Risk Assessment

---

- Likelihood of occurrence
  - Probability that an event will occur
  - Probability that a threat will attempt to exploit a vulnerability
- Impact
  - Magnitude of harm resulting from a risk
  - Negative result of the event
  - Loss of confidentiality, integrity, or availability of a system or data

# Qualitative Risk Assessment

---

- Web server selling products on the Internet
  - Probability of being attacked                      High (10)
  - Impact                                                  High (10)  
Risk score ( $10 \times 10 = 100$ )
- Library computer
  - Probability of being attacked                      Low (1)
  - Impact                                                  Low (1)  
Risk score ( $1 \times 1 = 1$ )

# Risk Assessments

---

- Documenting the assessment
- Results valuable
  - Help organization evaluate threats and vulnerabilities
  - Should be protected
  - Only accessible to management and security professionals



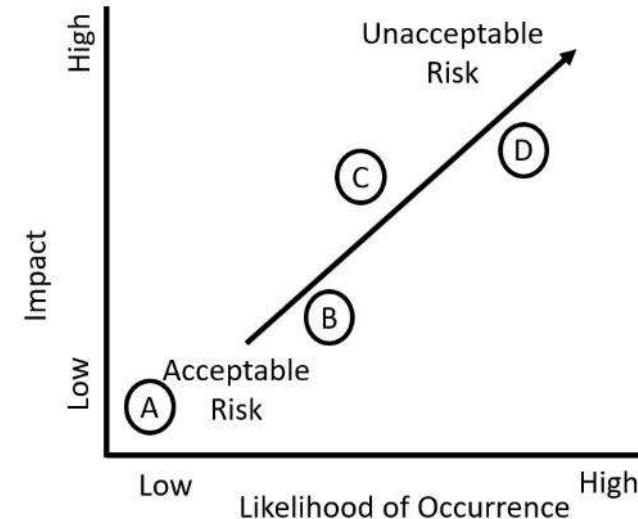
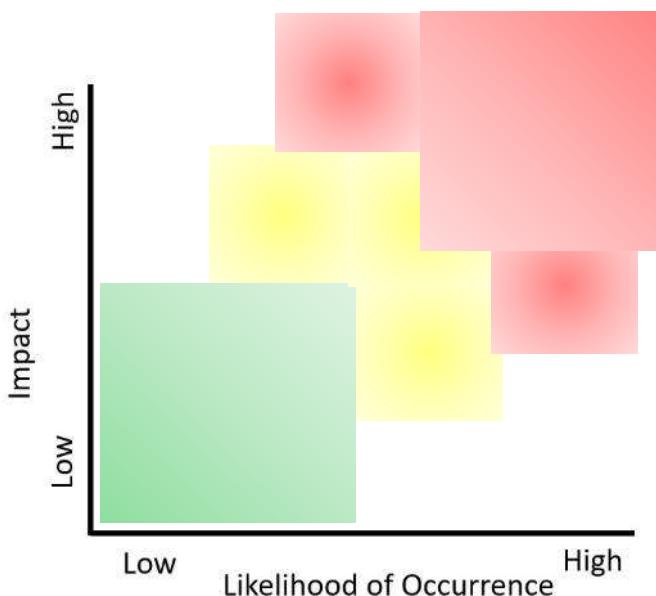
# Risk Register

---

- A record of information on identified risks
- A repository of information on risks
- Often recorded in a table
  - Category
  - Specific risk
  - Likelihood
  - Impact
  - Risk score
  - Security controls
  - Contingencies
  - Risk score (with controls)
  - Action assigned to
  - Action deadline

# Risk Matrix Versus Heat Map

- Risk matrix
  - Plots risks onto a graph or chart



- Heat map
  - Uses colors such as green and red

# Supply Chain Assessment

---

- Supply chain
  - Materials
  - All the processes required to create and distribute a product
- Assessment evaluates these elements
  - Identifies risks such as single point of failure

# Risk Management

---

- Threat Hunting
  - gathering data on the threat through threat intelligence
  - internal sources (device logs, IDS alerts, and data)
  - external sources
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTPs)

# Checking for Vulnerabilities

- Determines the security posture of a system
- Identifies vulnerabilities and weaknesses

**Identify assets and capabilities**



**Prioritize assets based on value**



**Identify vulnerabilities and prioritize them**



**Recommend controls to mitigate serious vulnerabilities**

# Checking for Vulnerabilities

---

- Password cracker
  - Attempts to discover passwords

MD5 Hash: 161ebd7d45089b3446ee4e0d86dbcf92

Password: P@ssw0rd

- Offline password cracker
- Online password cracker

# Checking for Vulnerabilities

---

- Network scanner
  - Nmap, Netcat, Nessus
  - Ping scan
  - Arp ping scan
  - Syn stealth scan
  - Service scan
  - OS detection



# Network Scanners

---

- Network scanner
  - Arp ping scan
  - Syn stealth scan
  - Port scan
  - Service scan
  - OS detection

# Vulnerability Scanning

---

- Identify vulnerabilities and misconfigurations
  - Open ports
  - Weak passwords
  - Default accounts
  - Sensitive data
  - Security and configuration errors

# Vulnerability Scanning

---

- Passively test security controls
  - Does not exploit vulnerabilities
- Identify lack of security controls
  - Systems without patches
  - Systems without antivirus software

# Vulnerability Scanning

---

- False positive
  - Scan detected a vulnerability
  - But the vulnerability doesn't actually exist
- False negative
  - Vulnerability exists
  - But the scan did not detect it

# Vulnerability Scanning

---

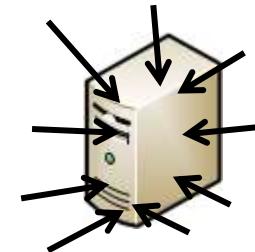
- Credentialed scan
  - Non-credentialed scan
  - Configuration compliance scans
- 
- Obtaining authorization
    - A penetration test can cause system instability
    - Without consent you may be perceived as an attacker



# Penetration Testing

---

- Assesses deployed security controls
- Determine the impact of a threat
- Starts with passive reconnaissance (such as a vulnerability scan)
- Follows with attempt to exploit vulnerabilities



# Penetration Testing

---

- Passive reconnaissance
  - Collects information
  - Often uses open-source intelligence
- Active reconnaissance
  - Uses tools to gather information
  - Typically includes vulnerability and network scans
- Initial exploitation
  - Exploits vulnerabilities

# Penetration Testing

---

- Passive reconnaissance
  - Collects information
  - Often uses open-source intelligence
- Active reconnaissance
  - Uses tools to gather information
  - Typically includes vulnerability and network scans
- Initial exploitation
  - Exploits vulnerabilities

# Penetration Testing

---

- Network Reconnaissance and Discovery
  - IP scanner
  - Nmap
  - Netcat
  - Scanless
  - Dnsenum
  - Nessus
  - hping
  - Sn1per
  - Curl
- Footprinting
- Fingerprinting

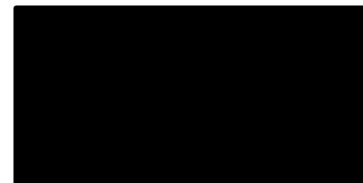
# Penetration Testing

---

- Persistence
  - Take steps to retain presence on network
- Lateral movement
  - Refers to the way attackers maneuver throughout a network
- Pivot
  - Use exploited system to exploit other systems
- Cleanup

# Penetration Testing

- Unknown environment
  - Testers have zero knowledge of the environment prior to the test
  - Often use fuzzing
- Known environment
  - Testers have full knowledge of the environment
- Partially known environment
  - Testers have some knowledge of the environment



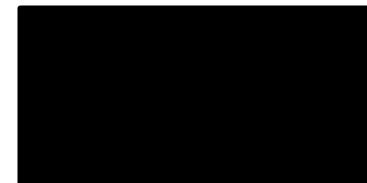
Documentation  
source code  
login details

Some  
information

# Penetration Testing

---

- Unknown environment
  - Previously called black box
- Known environment
  - Previously called white box
- Partially known environment
  - Previously called gray box



Documentation  
source code  
login details

Some  
information

# Scanning and Testing Tools

---

- Bug Bounty
- Intrusive Versus Non-Intrusive Testing
- Exercise types
  - Red team - Attacks
  - Blue team - Defends
  - Purple team – Members can attack or defend
  - White team – Establish the rules

# Wireshark

Intel DC21140 PCI Fast Ethernet Adapter (not tcp port 3389) [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

| No. | Time     | Source        | Destination   | Protocol | Length | Info                                                    |
|-----|----------|---------------|---------------|----------|--------|---------------------------------------------------------|
| 120 | 5.829743 | 192.168.1.130 | 192.168.1.134 | SMB      | 117    | Read AndX Request, FID: 0x172e, 23 bytes at offset 0    |
| 121 | 5.830763 | 192.168.1.134 | 192.168.1.130 | SMB      | 140    | Read AndX Response, FID: 0x172e, 23 bytes               |
| 122 | 5.831676 | 192.168.1.130 | 192.168.1.134 | SMB      | 180    | Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, |
| 123 | 5.832208 | 192.168.1.134 | 192.168.1.130 | SMB      | 158    | Trans2 Response, \\DARRIL\GIBS\on...P@ss w0rd           |

Frame 121: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)  
Ethernet II, Src: WesternND\_82:4b:5f (00:90:a9:82:4b:5f), Dst: Microsoft\_b3:73:6c (00:03:ff:  
Internet Protocol Version 4, Src: 192.168.1.134 (192.168.1.134), Dst: 192.168.1.130 (192.1  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Cap  
Total Length: 126  
Identification: 0x5504 (21764)  
Flags: 0x02 (Don't Fragment) ← ①  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0x611d [correct]  
Source: 192.168.1.134 (192.168.1.134)  
Destination: 192.168.1.130 (192.168.1.130)  
Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 51701 (51701), Seq:  
NetBIOS Session Service  
SMB (Server Message Block Protocol)

Middle Pane

Bottom Pane

File: "C:\Users\Darri\AppData\Local\Temp\..." Packets: 155 Displayed: 155 Marked: 0 Dropped: 0 Profile: Default

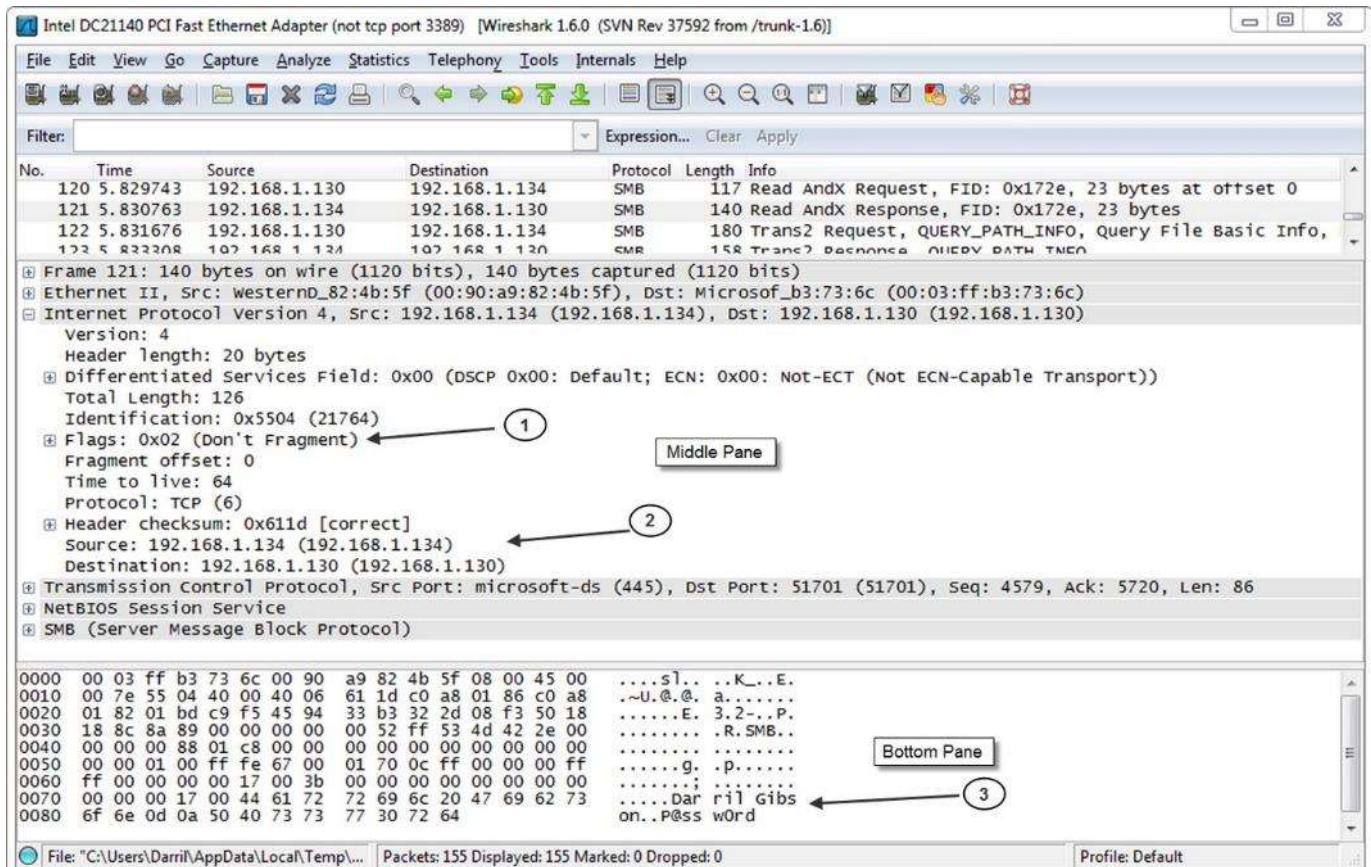
① Points to the 'Flags' field in the TCP header.  
② Points to the 'Source' and 'Destination' fields in the TCP header.  
③ Points to the 'Data' pane showing the captured SMB response.

.....s1.. ..K..E.  
.~U.@@. a.....  
.....E. 3.2-..P.  
..... .R.SMB..  
.....  
.....g. .p.....  
.....;  
.....Dar ril Gibs  
on...P@ss w0rd

0000 00 03 ff b3 73 6c 00 90 a9 82 4b 5f 08 00 45 00 .....s1.. ..K..E.  
0010 00 7e 55 04 40 00 40 06 61 1d c0 a8 01 86 c0 a8 .~U.@@. a.....  
0020 01 82 01 bd c9 f5 45 94 33 b3 32 2d 08 f3 50 18 .....E. 3.2-..P.  
0030 18 8c 8a 89 00 00 00 00 00 52 ff 53 4d 42 2e 00 ..... .R.SMB..  
0040 00 00 00 88 01 c8 00 00 00 00 00 00 00 00 00 00 .....g. .p.....  
0050 00 00 01 00 ff fe 67 00 01 70 0c ff 00 00 00 ff .....  
0060 ff 00 00 00 00 17 00 3b 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 17 00 44 61 72 72 69 6c 20 47 69 62 73 .....Dar ril Gibs  
0080 6f 6e 0d 0a 50 40 73 73 77 30 72 64 on...P@ss w0rd

# Network Traffic

- Packet Capture and Replay



# Network Traffic

---

- Packet Capture and Replay
- Tcpreplay
  - Includes tcpreplay, tcpprep, tcprewrite, and more
- Tcpdump
  - A command-line protocol analyzer
- NetFlow, sFlow, and IPFIX

# Key Frameworks

---

- ISO 27001 Information Security Management
- ISO 27002 Information Technology Security Techniques
- ISO 27002 Privacy Information Management System (PIMS)
- ISO 31000 Family of standards related to risk management

# Key Frameworks

---

- The Statement on Standards for Attestation Engagements (SSAE)
- System and Organization Controls (SOC) 2 report
  - Covers organizational cybersecurity controls
- SOC 2 Type I
  - Specific date
- SOC 2 Type II
  - Range of dates (such as 12 months)

# Risk Management Framework Steps

---

- Prepare
- Categorize information systems
- Select security controls
- Implement security controls
- Assess security controls
- Authorize information systems
- Monitor security controls

# Frameworks and Standards

---

- Reference Architecture
  - Document or set of documents that provides a set of standards
- Exploitation Frameworks
  - Metasploit Framework
  - BeEF (Browser Exploitation Framework)
  - w3af (Web Application Attack and Audit Framework)
- Benchmarks and Configuration Guides

# Chapter 8 Summary

---

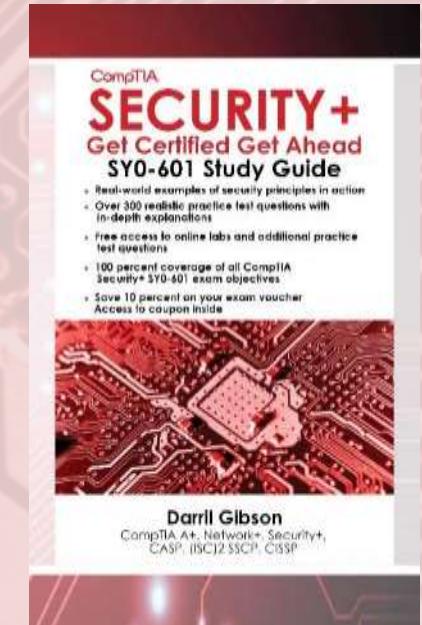
- Understanding Risk Management
- Comparing Scanning and Testing Tools
- Capturing Network Traffic
- Understanding Frameworks and Standards
- Check out the free online resources

# Chapter 9

## Implementing Controls to Protect Assets

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Comparing Physical Security Controls
- Adding Redundancy and Fault Tolerance
- Protecting Data with Backups
- Comparing Business Continuity Elements

# Physical Security Controls

---

- Perimeter
- Buildings
- Secure work areas
- Server rooms
- Hardware (such as cable locks)



# Physical Security Controls

---

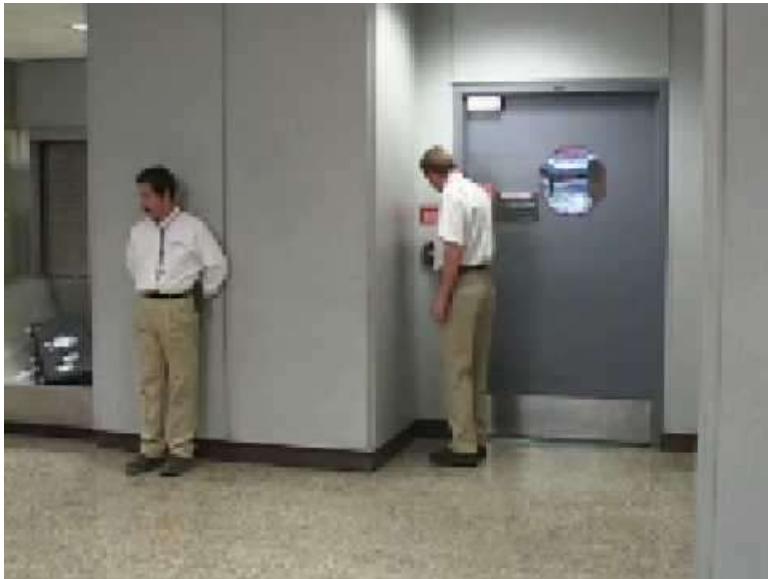
- Door access systems
  - Proximity cards
- Locks
  - Physical locks
  - Physical cipher locks
  - Biometric locks
  - Cable locks



# Physical Security Controls

---

- Tailgating and access control vestibules



- Security guards

# Physical Security Controls

---

- Personnel
  - Two-person integrity
- Cameras
- Fencing, lighting, and alarms



# Sensors

---

- Motion detection
- Noise detection
- Temperature
- Moisture detection
- Proximity reader
- Cards

# Physical Security Controls

---

- Barricades
  - Bollards
- Signage
- Drones



# Asset Management

---

- Architecture weaknesses
- Design weaknesses
- System sprawl
- Undocumented assets

# Diversity

---

- Defense in depth
  - Also known as layered security
- Vendor diversity
- Technology diversity
- Control diversity

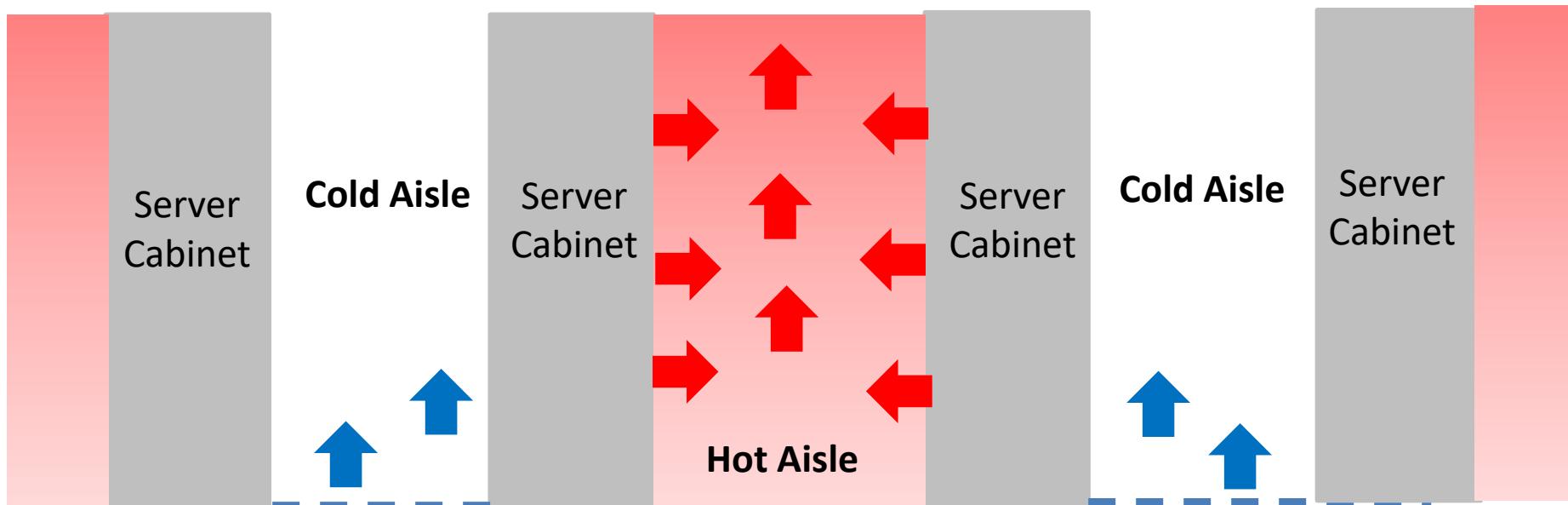
# Secure Areas

---

- Air gap
- Vaults
- Faraday Cage
- Safes

# Environmental Controls

- Hot and cold aisles
  - Regulate the cooling



# Physical Attacks

---

- Malicious Universal Serial Bus (USB) cable
- Malicious flash drive
- Card skimming
- Card cloning

# Fire Suppression

---

- Remove the heat
  - Fire extinguishers
- Remove the oxygen
  - Carbon dioxide (CO<sub>2</sub>)
- Remove the fuel
  - Fire-suppression
- Disrupt the chain reaction

# Redundancy and Fault Tolerance

---

- Single point of failure
  - Any component whose failure results in the failure of an entire system
- Remove single points of failure with
  - RAID (disk)
  - Failover clustering (server)
  - UPS and generators (power)
  - Personnel
- Single points of failure are often overlooked until a disaster occurs

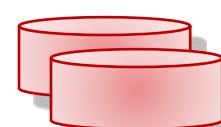
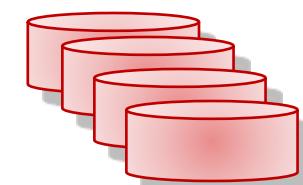
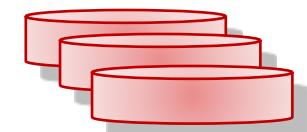
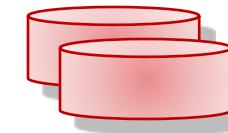
# Disk Redundancies

---

- Inexpensive
- Adds fault tolerance and increases availability
- Hardware RAID more efficient than software RAID

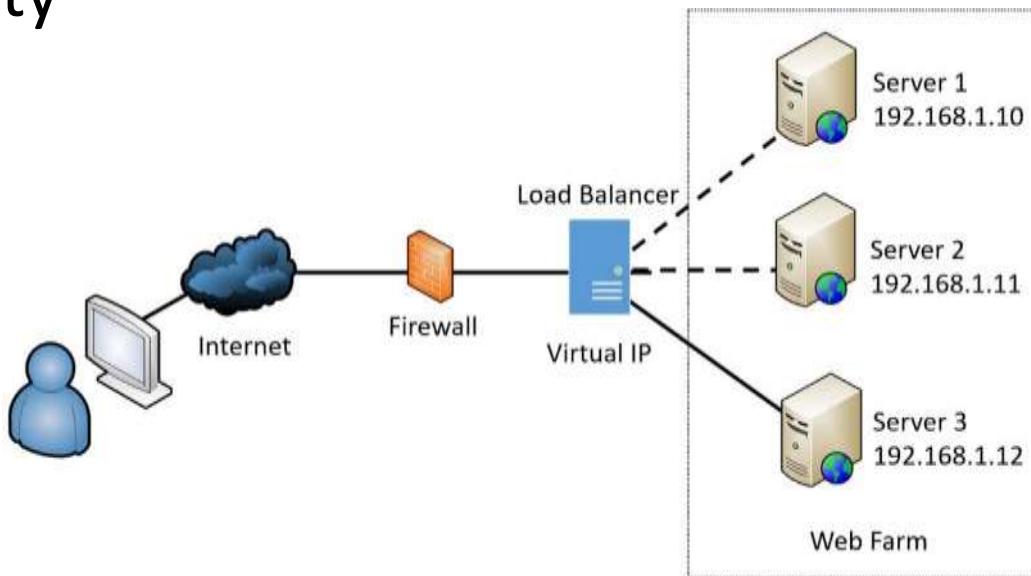
# Disk Redundancies

- RAID-0 no redundancy
  - Two or more disks
- RAID-1 uses two disks as a mirror
  - Two disks
- RAID-5 can survive failure of one disk
  - Three or more disks
- RAID-6 can survive failure of two disks
  - Four or more disks
- RAID-10 combines RAID-1 and RAID-0
  - Even number of disks



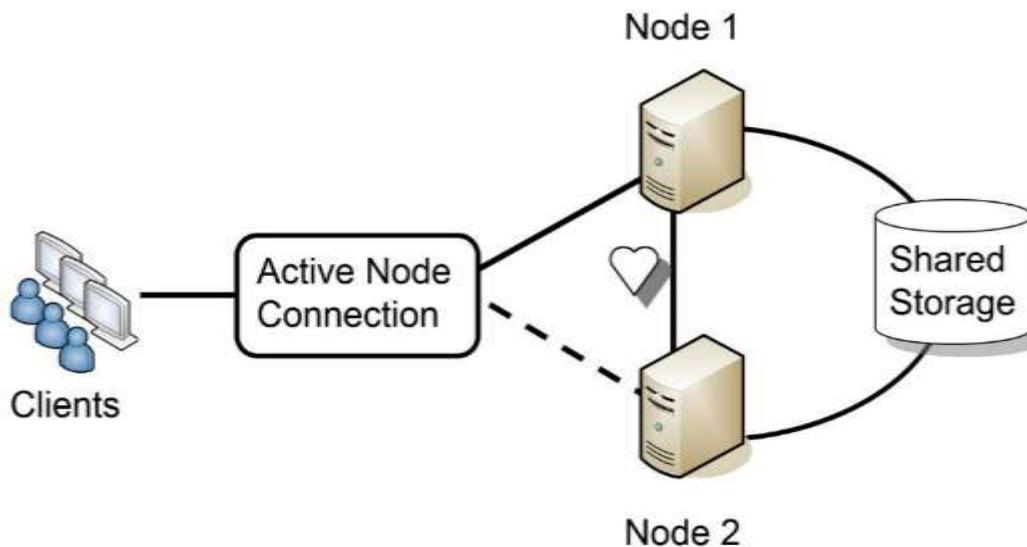
# Load Balancers

- Active/active load balancer
  - Affinity



# Load Balancers

- Active/passive load balancer



# Power Redundancies

---

- UPS
  - Provides short-term fault tolerance for power
  - Can protect against power fluctuations
- Dual supply
- Generators provide long-term fault tolerance for power
- Managed power distribution units

# Protecting Data with Backups

---

- Backup media
  - Network-attached storage (NAS)
  - Storage area network (SAN)
  - Cloud
- Online backups
- Offline backups

# Backups Types

---

- Full backups
  - Fastest recovery time
- Differential backup
  - Backs up all the data that has changed since the last full or differential backup
- Incremental backup
  - Backs up all the data that has changed since the last full or incremental backup

# Protecting Data with Backups

---

- Snapshot backup
- Image backup
- Copy backup
- Testing backup

# Geographic Considerations

---

- Off-site storages
- Distance
- Location selection
- Legal implications
- Data sovereignty

# Business Continuity Elements

---

- Protect against disasters and outages
  - Fires
  - Attacks
  - Power outages
  - Data loss from any cause
  - Hardware and software failures
  - Natural disasters, such as hurricanes, floods, tornadoes, and earthquakes

# Business Continuity Elements

---

- Business impact analysis (BIA) identifies:
  - Systems and components that are essential to the organization's success (must continue to operate)
  - Maximum downtime limits for these systems and components
  - Scenarios that can impact these systems and components
  - Potential losses from an incident
  - Assets to include in recovery plans

# Business Continuity Elements

---

- Impact
- Recovery Time Objective (RTO)
  - Identifies maximum amount of ***time*** it should take to restore a system after an outage
  - Derived from maximum allowable outage ***time*** identified in the BIA
- Recovery Point Objective (RPO)
  - Refers to the amount of ***data*** an organization can afford to lose

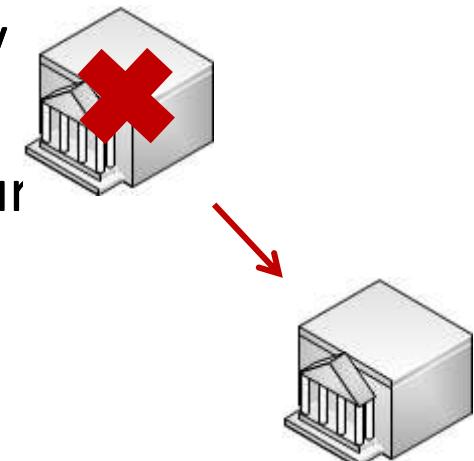
# Risk Metrics

---

- Mean time between failures (MTBF)
  - Provides a measure of a system's reliability
  - Usually represented in hours
  - MTBF indicates the device can be repaired
- Mean time to recover or mean time to repair (MTTR)
  - The time it takes to restore a failed system
  - Often specified in contracts as a target

# Continuity of Operations Sites

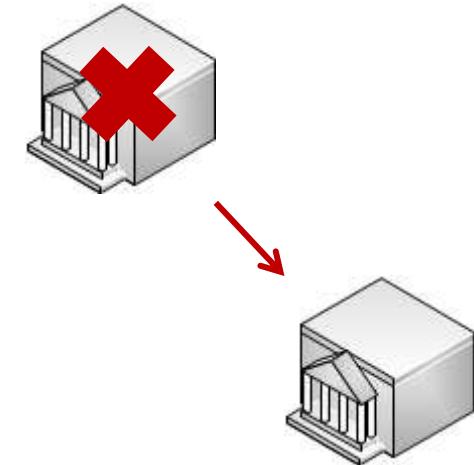
- Provides an alternate location for operations after a critical outage
- Most common sites are hot, cold, and warm sites
- Hot site
  - Includes personnel, equipment, software, and communications capabilities of the primary
  - All the data is up to date
  - Can take over for a failed site within an hour
  - Most effective disaster recovery solution for an alternate site
  - Most expensive to maintain



# Continuity of Operations Sites

---

- Cold site
  - Has power and connectivity needed for COOP activation, but little else
  - Least expensive and hardest to test
- Warm site
  - Compromise between a hot site and a cold site
- Order of restoration
  - Return least critical functions first



# Disaster Recovery Plan (DRP)

---

- Part of BCP
- Includes a hierarchical list of critical systems
- Prioritizes services to restore after an outage
- Testing validates a DRP
- Recovered systems tested before returning to operation
  - Can include a comparison to baselines

# Disaster Recovery Plan (DRP)

---

- Phases
  - Activate the disaster recovery plan
  - Implement contingencies
  - Recover critical systems
  - Test recovered systems
  - After-action report
    - Includes a review to identify any lessons learned
    - May include an update of the plan

# BCP and DRP Testing

---

- Validate BCPs and DRPs through testing
- Tabletop exercises
  - Discussion-based only
  - Typically performed in a classroom or conference setting
- Simulations
  - simple simulations to full-blown tests

# Chapter 9 Summary

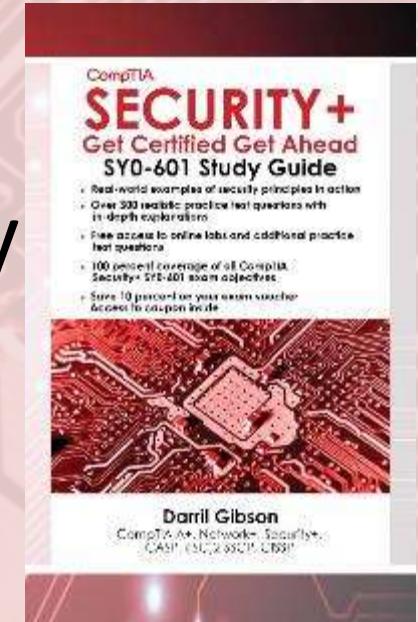
---

- Comparing Physical Security Controls
- Adding Redundancy and Fault Tolerance
- Protecting Data with Backups
- Comparing Business Continuity Elements
- Check out the free online resources

# Chapter 10

## Understanding Cryptography and PKI

CompTIA Security+  
Get Certified Get Ahead  
By Darril Gibson



# Introduction

---

- Introducing Cryptography Concepts
- Providing Integrity with Hashing
- Understanding Password Attacks
- Providing Confidentiality with Encryption
- Using Cryptographic Protocols
- Exploring PKI Components

# Cryptography Concepts - Integrity

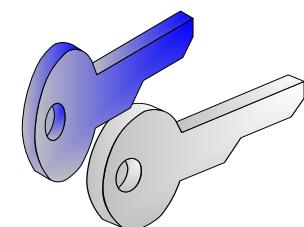
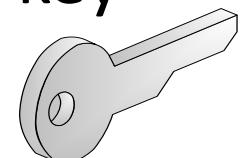
---

- Provides assurances that data has not been modified
- Hashing ensures that data has retained integrity
- A hash is a number derived from performing a calculation on data
- If the data is unchanged the hash will always be the same number
- Common hashing algorithms include MD5, SHA, HMAC
- Each algorithm creates a fixed-size string of bits
  - Example: MD5 creates a hash of 128 bits

# Cryptography Concepts - Confidentiality

---

- Ensures only authorized users can view data
- Encryption protects the confidentiality of data
- Encryption ciphers data to make it unreadable
- Encryption normally includes algorithm and key
- Symmetric encryption
  - Uses the same key to encrypt and decrypt data
- Asymmetric encryption
  - Uses two keys (public and private) created as a matched pair



# Cryptography Concepts

---

- Authentication validates an identity
- Non-repudiation
  - Prevents a party from denying an action
- Digital signatures
  - Provide authentication, non-repudiation, and integrity
  - Users sign emails with a digital signature
    - Digital signature is a hash of an email message encrypted with the sender's private key
    - Only the sender's public key can decrypt the hash
    - Provides verification it was encrypted with the sender's private key

# Providing Integrity with Hashing

---

- Hashing provides integrity for data
  - Email, downloaded files, files stored on a disk
  - A one-way function that creates a string of characters
- A hash is a number
  - Sometimes called a checksum
  - You cannot reverse the hash
  - You cannot re-create the original data from the hash
  - Created with a hashing algorithm
    - Message Digest 5 (MD5)
    - Secure Hash Algorithm (SHA) family
    - HMAC

# Hashing Protocols

---

- To verify integrity
  - MD5 (use is discouraged)
  - SHA (SHA-3 previously known as Keccak)
- To verify integrity and authenticity
  - HMAC (HMAC-MD5 and HMAC-SHA1)
    - Uses a shared secret
    - IPsec and TLS use HMAC-MD5 and HMAC-SHA1

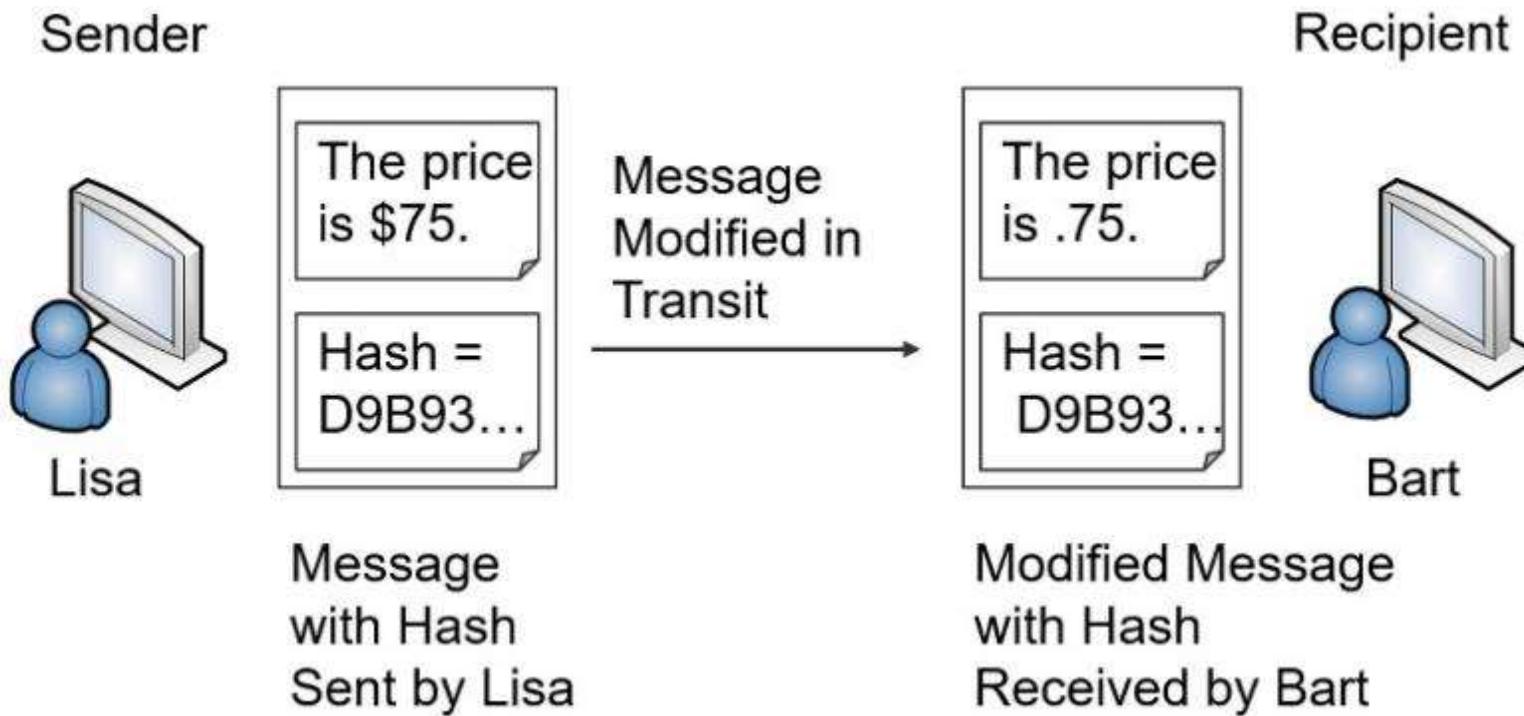
# Hashing Passwords

---

- Passwords often stored as hashes
- Password attacks attempt to discover passwords
  - Guess a password
  - Hash the guessed password
  - Compare the hash to the original hash

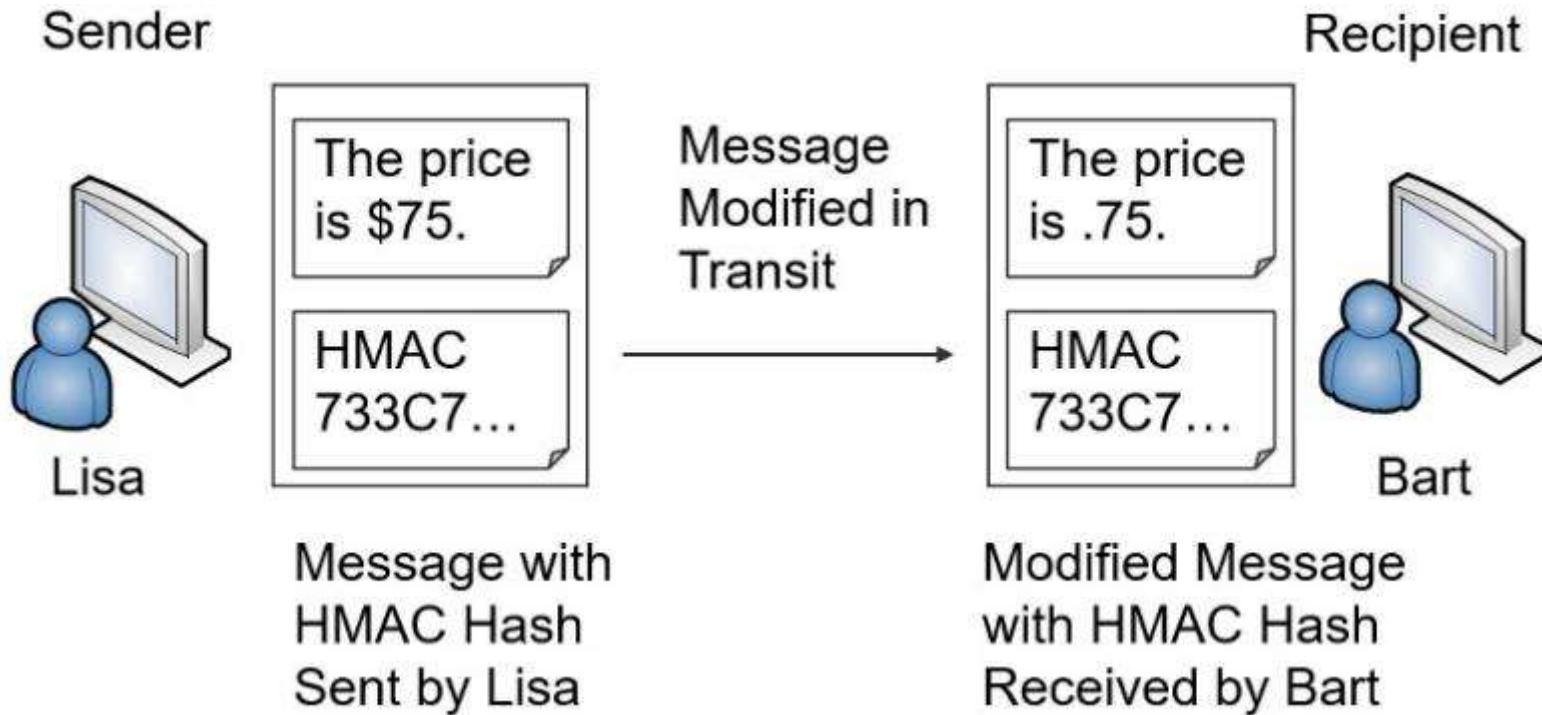
# Hashing Messages

- Hashing detects modified message



# Hashing Messages with HMAC

- HMAC prevents attacker from modifying hash



# Hash Collisions

---

- Hashing algorithm creates the same hash from different inputs
  - MD5 (highly susceptible)

# Understanding Password Attacks

---

- Attempt to discover, or bypass, passwords used for authentication
  - Online password attack (guess the password of an online system)
  - Offline password attack (guess the password stored within a downloaded file, such as a database)

# Password Attacks

---

- Dictionary attacks
  - Uses a dictionary of words
  - Attempts every word in the dictionary to see if it works
- Brute force
  - Attempts to guess all possible character combinations

# Password Attacks

---

- Spraying attacks
  - Special type of brute force or dictionary attack designed to avoid being locked out
- Pass the hash
  - Attempts to use an intercepted hash to access an account
- Birthday attacks
  - Attempts to create a password that produces the same hash as the user's actual password

# Password Attacks

---

- Rainbow table attacks
  - Attempts to discover the password from the hash
- Salting passwords
  - Prevent rainbow table attacks, along with other password attacks
- Key stretching
  - Used to increase the strength of stored passwords (Bcrypt, PBKDF2, and Argon2)

# Providing Confidentiality with Encryption

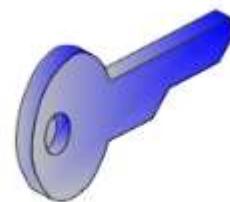
---

- Encryption provides confidentiality
  - Helps ensure only authorized users can view data
  - Applies to any type of data
    - Data-at-rest (files, in a database, and so on)
    - Data-in-transit or data in motion (sent over a network)
  - Data-in-processing (sometimes called data in use\_
    - Not encrypted while in use
    - If sensitive should be purged after use

# Providing Confidentiality with Encryption

---

- Two basic components of encryption
  - Algorithm
    - Performs mathematical calculations on data
    - Algorithm always the same
  - Key
    - A number that provides variability
    - Either kept private and/or changed frequently



# Symmetric Encryption

---

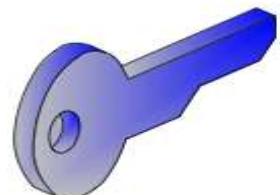
- Uses the same key to encrypt and decrypt data
  - When transmitting encrypted data
    - Uses key to encrypt data before transmission
    - Uses same key to decrypt data when received
- Much more efficient encrypting large amounts of data than asymmetric encryption
- RADIUS uses symmetric encryption



# Simple Symmetric Encryption Example

---

- Encryption algorithm uses substitution cipher
  - Move forward \_\_\_\_ spaces to encrypt
  - For example, move forward 3 spaces to encrypt
- Decryption algorithm
  - Move back \_\_\_\_ spaces to decrypt
  - For example, move back 3 spaces to decrypt
- With the key of 3
  - Message is PASS and encrypted it is SDVV
- ROT13 always uses a key of 13



# Block vs. Stream Ciphers

---

- Block ciphers
  - Encrypts data in specific sized blocks
    - Often 64-bit blocks or 128-bit blocks
  - Divides large files or messages into these blocks
  - Encrypts each block separately
- Stream ciphers
  - Encrypt data as a single bit or byte at a time in a stream
  - An important principle when using a stream cipher
    - Encryption keys should never be reused
    - If a key is reused, it is easier to crack the encryption

# Symmetric Algorithms

---

- Advanced Encryption Standard (AES)
  - Fast, efficient, strong symmetric block cipher
  - 128-bit block cipher
  - Uses 128-bit, 192-bit, or 256-bit keys
- Blowfish and Twofish
  - Strong symmetric block cipher (widely used)
  - 64-bit blocks
  - Supports between 32 and 448 bits

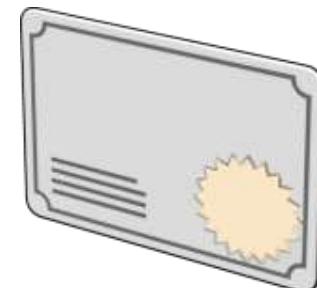
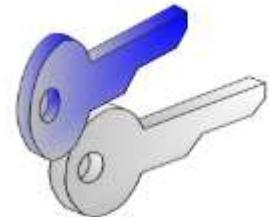
# Symmetric Algorithms

---

- 3DES
  - 64-bit block cipher
  - Originally designed as a replacement for DES
  - Uses multiple keys and multiple passes
  - Not as efficient as AES
  - 3DES is still used in some applications, such as when hardware doesn't support AES

# Asymmetric Encryption

- Private Key / Public Key matched pair
  - One key encrypts, the other key decrypts
  - Only a private key can decrypt information encrypted with a matching public key
  - Only a public key can decrypt information encrypted with a matching private key
  - Private key stays private
  - Public key shared in a certificate
  - Asymmetric encryption methods require certificate and PKI



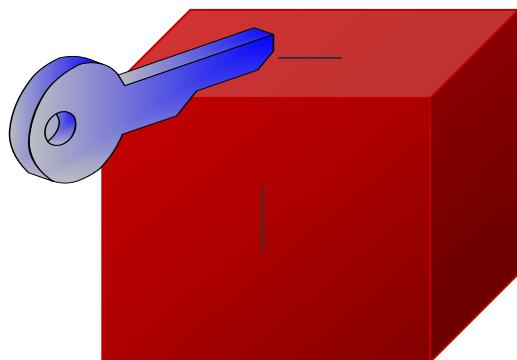
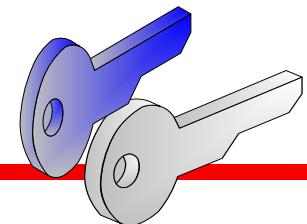
# Asymmetric Encryption

---

- Key exchange
  - Used to share cryptographic keys between two entities
  - Asymmetric encryption uses key exchange to share a symmetric key

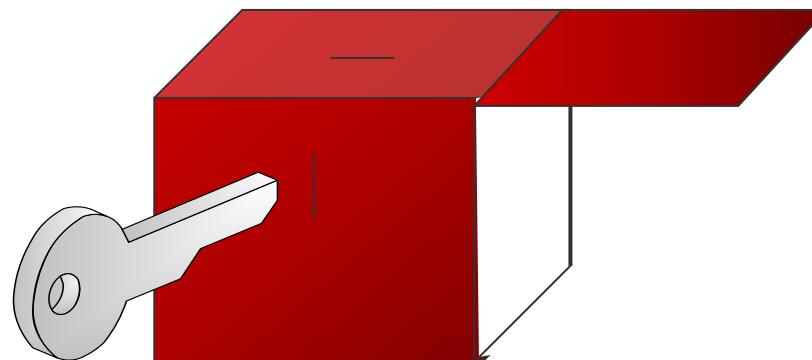
# Asymmetric Encryption

- Rayburn Box



**Rayburn Box**

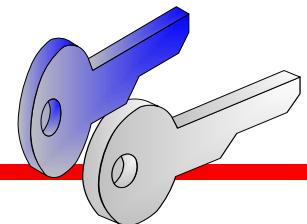
**Locked by one key**



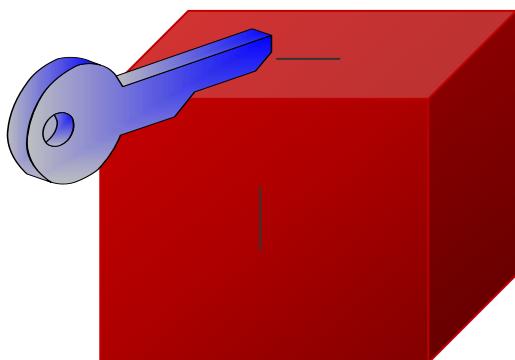
**Rayburn Box**

**Unlocked by the other key**

# Asymmetric Encryption

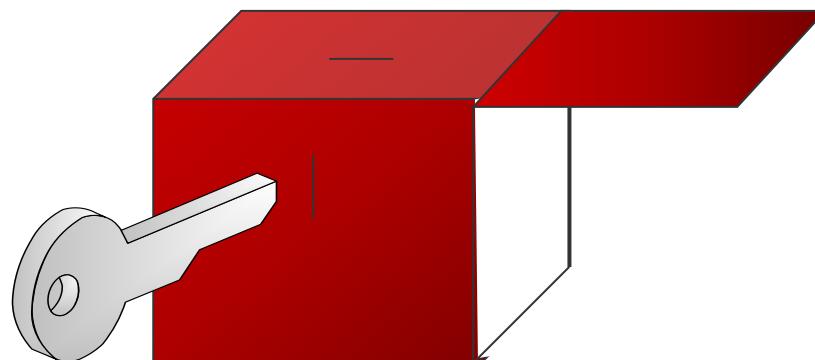


- Rayburn box used to send secrets
  - Encryption



**Rayburn Box**

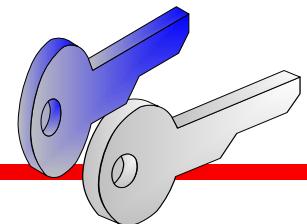
**Locked by one key**



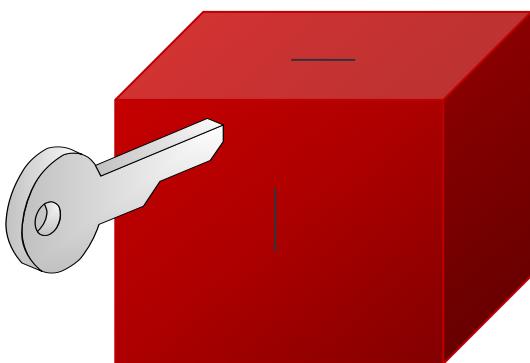
**Rayburn Box**

**Unlocked by the other key**

# Asymmetric Encryption

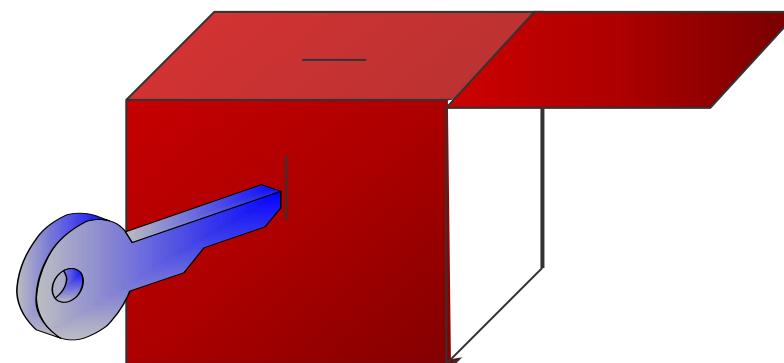


- Rayburn box used for authentication
  - Digital signature



**Rayburn Box**

**Locked by one key**

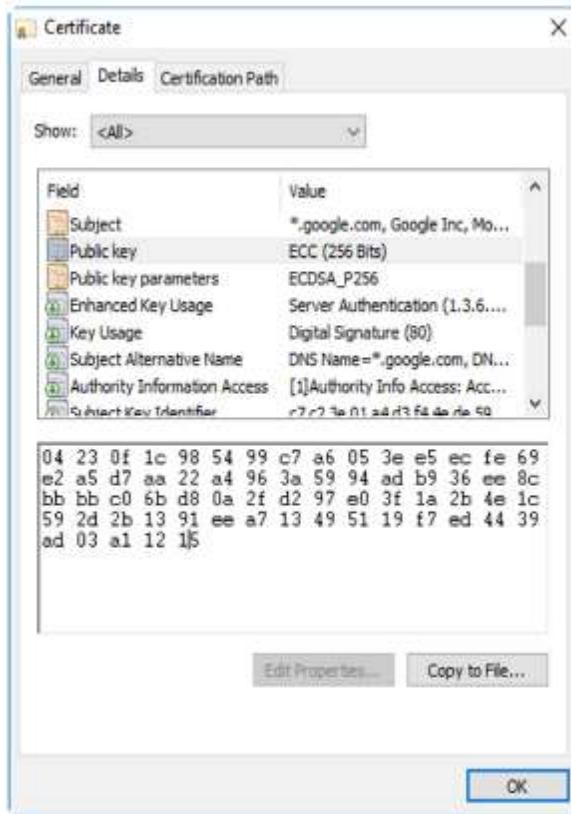


**Rayburn Box**

**Unlocked by the other key**

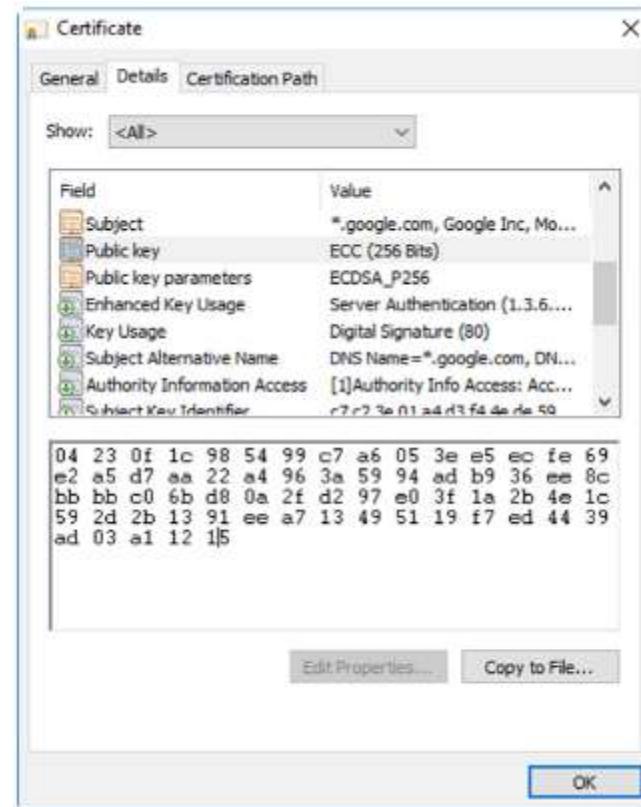
# Certificates

- Used for
  - Encryption
  - Authentication
  - Digital signatures



# Certificates

- Includes
  - Serial number
  - Issuer
  - Validity dates
  - Subject
  - Public key
  - Usage



# Asymmetric Encryption

---

- Ephemeral keys
  - Short lifetimes
  - Re-created for each session
  - Perfect forward secrecy
- Elliptic curve cryptography (ECC)
  - Commonly used with small wireless devices
  - Uses smaller key sizes requires less processing power



# Other Encryptions

---

- Quantum computing
  - Quantum key distribution (QKD)
  - Post-quantum cryptography
- Lightweight Cryptography
  - Deployed to smaller devices (RFID tags, sensor nodes, smart cards, IoT devices)

# Other Encryptions

---

- Key length
  - RSA (Rivest-Shamir-Adleman)
- Modes of operation
  - Authenticated, counter, and unauthenticated
- Steganography
  - Audio, image, video steganography

# Using Cryptographic

---

- Email digital signatures
  - The sender's private key encrypts (or signs)
  - The sender's public key decrypts
- Email encryption
  - The recipient's public key encrypts
  - The recipient's private key decrypts

Knowing which key encrypts and which key decrypts will help you answer many questions.

# Using Cryptographic Protocols

---

- Website encryption
  - The website's public key encrypts
    - It encrypts a symmetric key
  - The website's private key decrypts
    - It decrypts a symmetric key
  - The symmetric key encrypts data in the website session

Knowing which key encrypts and which key decrypts will help you answer many questions.

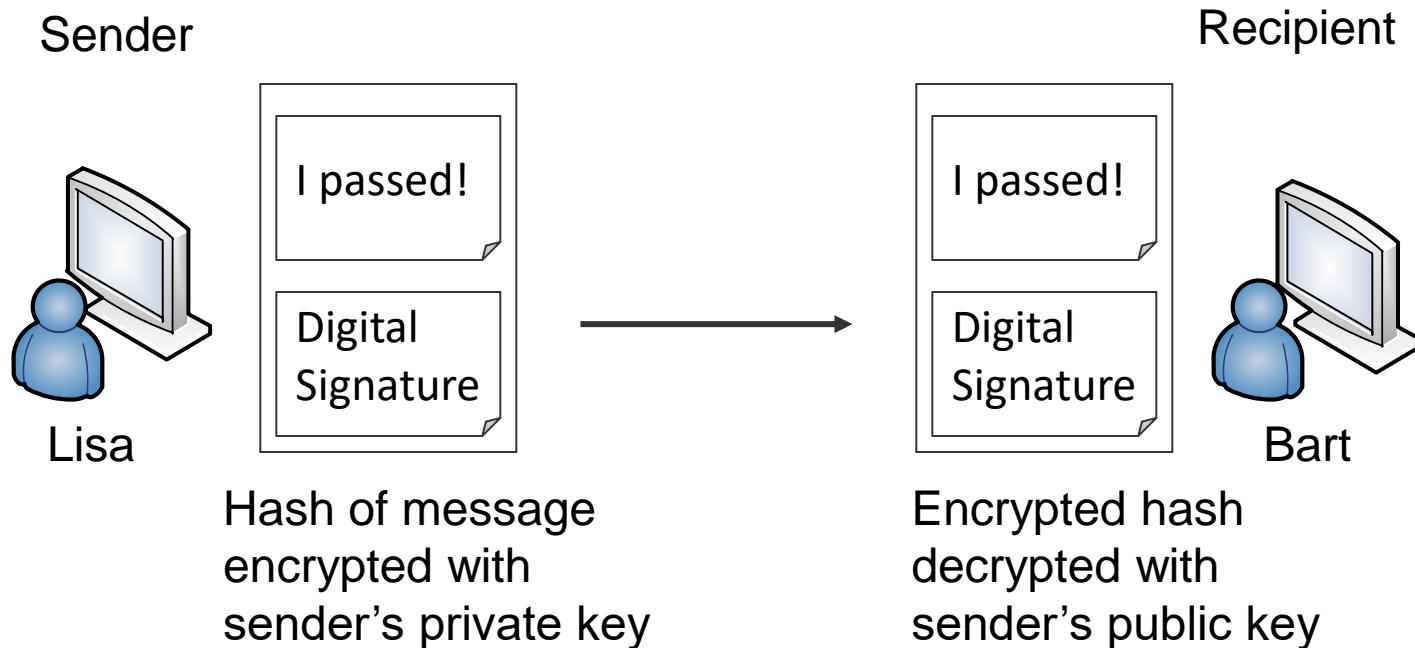
# Digital Signature

---

- Encrypted hash of a message
  - The sender's private key encrypts the hash
  - Recipient decrypts hash with sender's public key
  - Provides
    - Authentication – identifies the sender
    - Non-repudiation – prevents the sender from denying the action
    - Integrity – verifies the message has not been modified

# Digital Signature

- Signing email with a digital signature



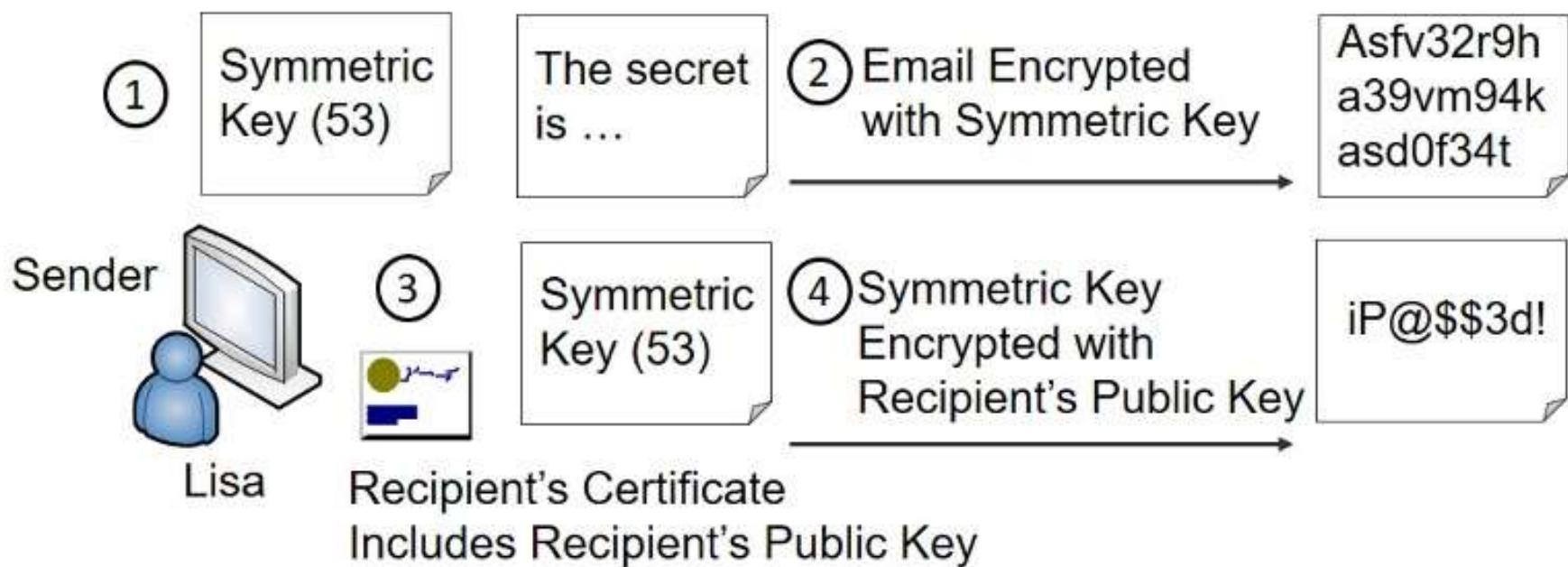
# Encrypting Email

---

- Using only asymmetric encryption  
(Not common)
1. Lisa retrieves a copy of Bart's certificate that contains his public key
  2. Lisa encrypts the email with Bart's public key
  3. Lisa sends the encrypted email to Bart
  4. Bart decrypts the email with his private key

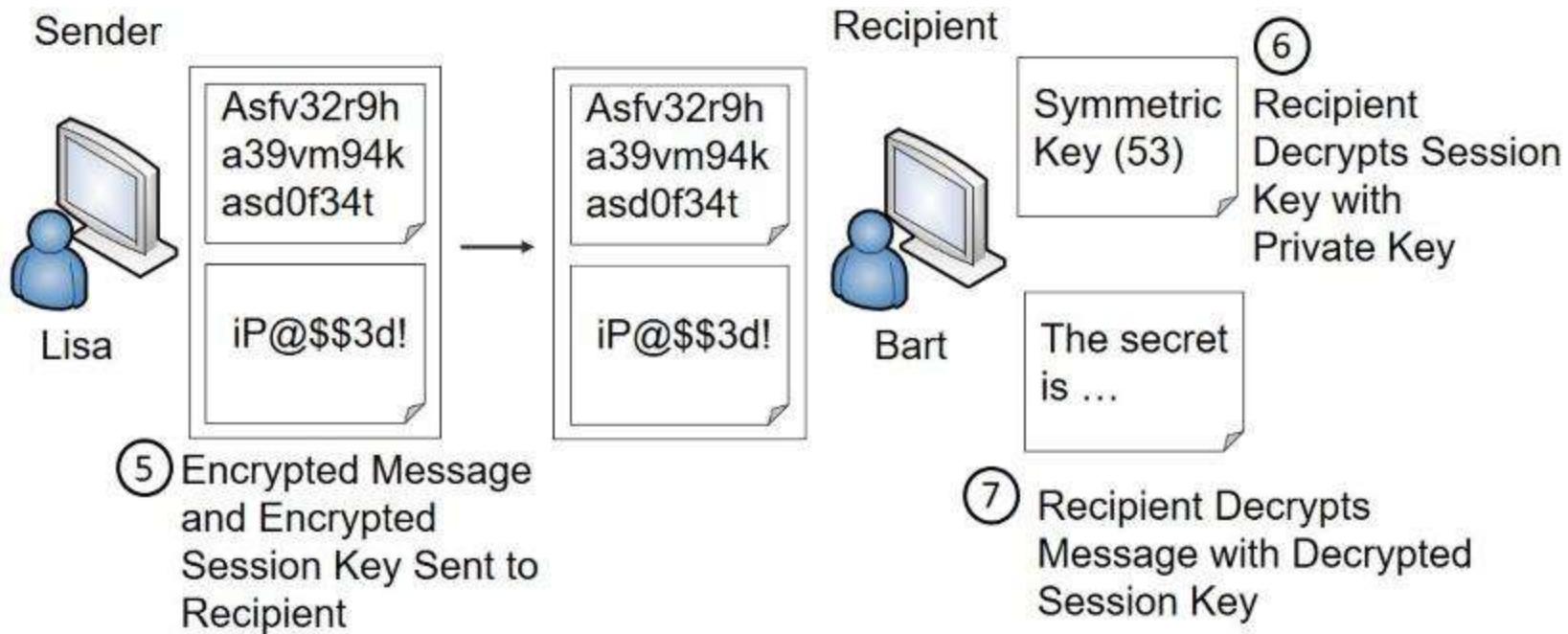
# Encrypting Email

- Using symmetric and asymmetric encryption



# Decrypting Email

- Using symmetric and asymmetric encryption



# Protecting Email

---

- S/MIME and PGP/GPG
- Both:
  - Use RSA algorithm
  - Use public and private keys for encryption and decryption
  - Use certificates
  - Can digitally sign and encrypt email
    - Including email at rest and in transit
  - OpenPGP (PGP-based standard)

# Transport Encryption

---

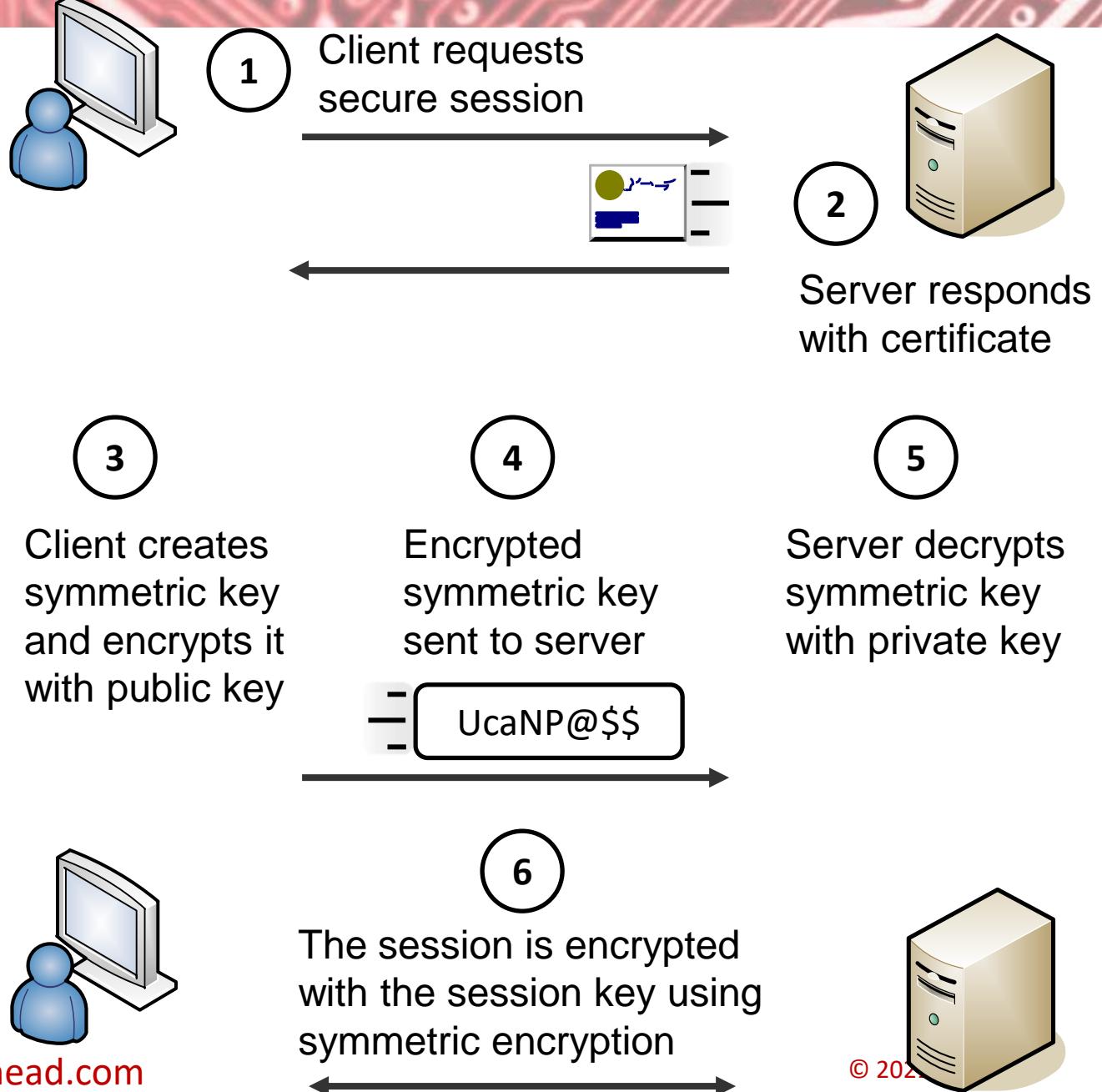
- Protects confidentiality of transmitted data
  - SSH, IPsec, HTTPS, SSL, and TLS
  - IPsec must use HMAC for authentication and integrity
  - IPsec can use either AES or 3DES for encryption
  - IPsec's ESP encrypts the entire packet
  - Creates an additional IP header

# TLS and SSL

---

- TLS is the replacement for SSL
  - SSL deprecated
  - Both require certificates issued by CAs
- TLS used in HTTPS
  - HTTPS uses a combination of symmetric and asymmetric encryption to encrypt HTTPS sessions

# Encrypting HTTPS traffic with TLS



# Other Cryptographic Protocols

---

- Blockchain
  - Public record-keeping technology
  - Distributed, decentralized, public ledger
- Crypto Diversity
  - Using different methods to protect security keys

# Other Cryptographic Protocols

---

- Limitations
  - Resource versus security constraint
  - Speed and time
  - Size and computational overhead
  - Entropy
  - Predictability
  - Weak keys
  - Longevity
  - Reuse

# Other Cryptographic Protocols

---

- Plaintext attack
  - Also called a known plaintext
  - Attacker has some known plaintext data and the ciphertext created from this plaintext
- Use cases

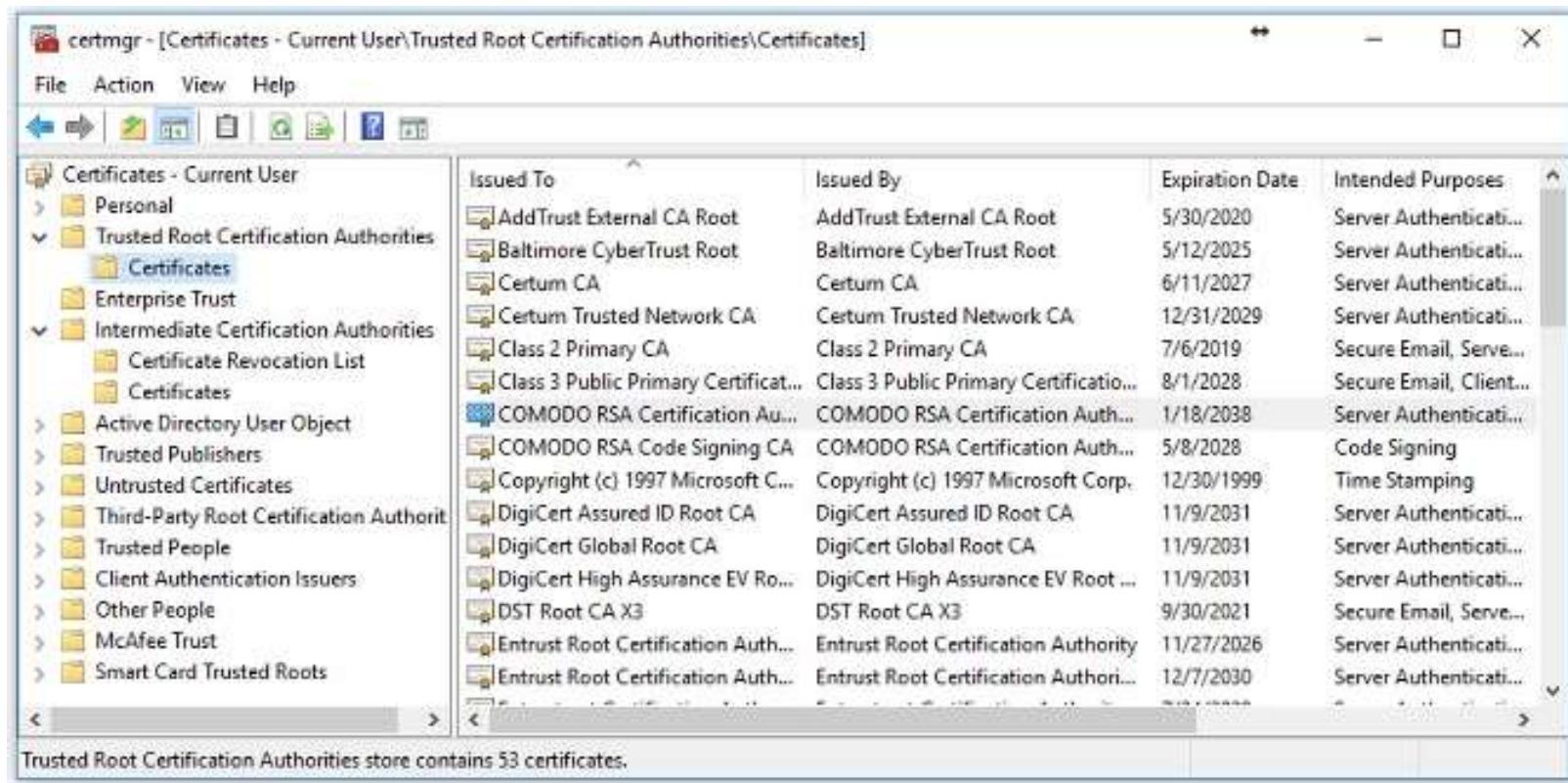
# Exploring PKI Components

---

- Public Key Infrastructure
  - Includes components required for certificates
  - Allows two entities to privately share symmetric keys without any prior communication
- Certificate Authority (CA)
  - Issues, manages, validates, and revokes certificates

# Certificate Trust Models

- Trusted root certification authorities



The screenshot shows the Windows Certmgr application window titled "certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]". The left pane displays a tree view of certificate categories, with "Trusted Root Certification Authorities" expanded to show its sub-categories: "Certificates" (selected), "Enterprise Trust", and "Intermediate Certification Authorities". The right pane is a grid table listing 53 certificates. The columns are: "Issued To", "Issued By", "Expiration Date", and "Intended Purposes". The table includes entries from well-known CAs like AddTrust, Baltimore CyberTrust, Certum, COMODO, DigiCert, and Entrust.

| Issued To                            | Issued By                            | Expiration Date | Intended Purposes     |
|--------------------------------------|--------------------------------------|-----------------|-----------------------|
| AddTrust External CA Root            | AddTrust External CA Root            | 5/30/2020       | Server Authentication |
| Baltimore CyberTrust Root            | Baltimore CyberTrust Root            | 5/12/2025       | Server Authentication |
| Certum CA                            | Certum CA                            | 6/11/2027       | Server Authentication |
| Certum Trusted Network CA            | Certum Trusted Network CA            | 12/31/2029      | Server Authentication |
| Class 2 Primary CA                   | Class 2 Primary CA                   | 7/6/2019        | Secure Email, Server  |
| Class 3 Public Primary Certificate   | Class 3 Public Primary Certificate   | 8/1/2028        | Secure Email, Client  |
| COMODO RSA Certification Authority   | COMODO RSA Certification Authority   | 1/18/2038       | Server Authentication |
| COMODO RSA Code Signing CA           | COMODO RSA Certification Authority   | 5/8/2028        | Code Signing          |
| Copyright (c) 1997 Microsoft Corp.   | Copyright (c) 1997 Microsoft Corp.   | 12/30/1999      | Time Stamping         |
| DigiCert Assured ID Root CA          | DigiCert Assured ID Root CA          | 11/9/2031       | Server Authentication |
| DigiCert Global Root CA              | DigiCert Global Root CA              | 11/9/2031       | Server Authentication |
| DigiCert High Assurance EV Root CA   | DigiCert High Assurance EV Root CA   | 11/9/2031       | Server Authentication |
| DST Root CA X3                       | DST Root CA X3                       | 9/30/2021       | Secure Email, Server  |
| Entrust Root Certification Authority | Entrust Root Certification Authority | 11/27/2026      | Server Authentication |
| Entrust Root Certification Authority | Entrust Root Certification Authority | 12/7/2030       | Server Authentication |

Trusted Root Certification Authorities store contains 53 certificates.

# Trust Models

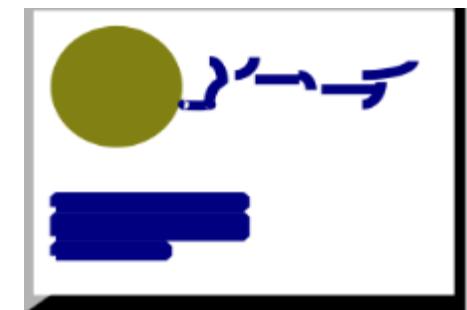
- Certificate chain
  - Root CA
  - Intermediate CAs
  - Child CAs
  - All certificates issued by trusted CAs are trusted
  - Errors when a site uses an untrusted certificate



# Registration Authority and CSRs

---

- Certificate signing request (CSR)
  - PKCS #10 format
  - Create the RSA-based private key, which is used to create the public key
  - Include the public key in the CSR
  - The CA will embed the public key in the certificate.



# Other PKI Components

---

- Online Versus Offline CAs
  - Online (accessible over a network, it's possible to submit the CSR using an automated process)
  - Offline (to reduce the risk of compromise)
- Updating certificates

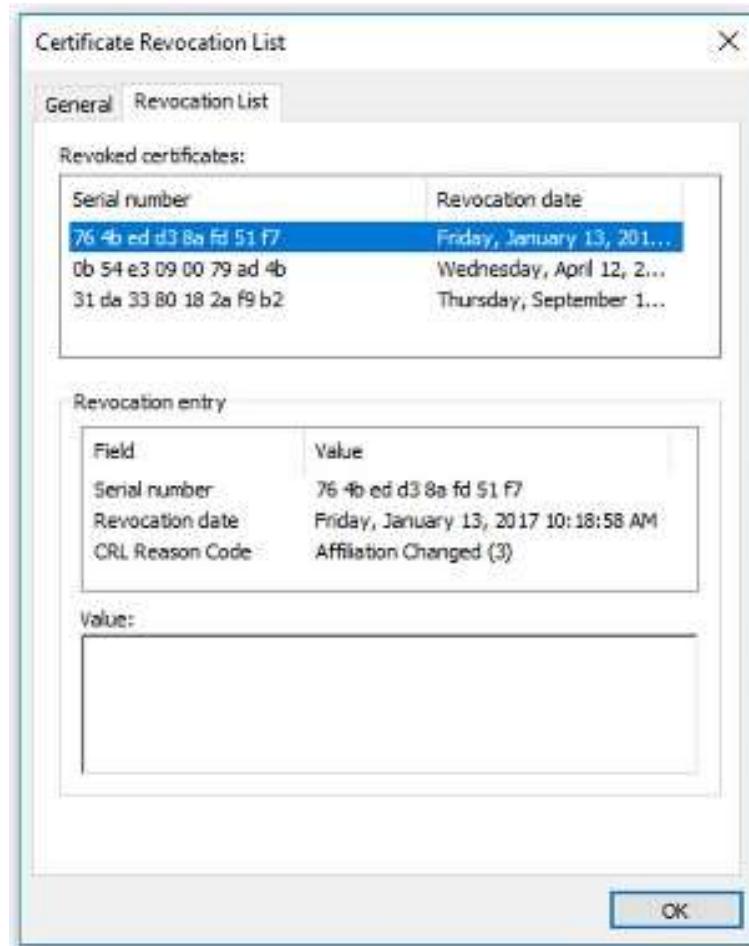
# Revoking Certificates

---

- Reasons
  - Key or CA Compromise
  - Change of Affiliation
  - Cease of Operation
  - Employee Leaves
  - Superseded
  - Certificate Hold
- Revoked certificates
  - Revoked by serial number
  - Published in Certificate Revocation List (CRL)
  - Publicly available

# Certificate Revocation List

- Issued in a version 2 certificate



# Certificate Revocation List (CRL)

**Certificate Revocation List**

General | Revocation List

**Certificate Revocation List Information**

| Field                 | Value                               |
|-----------------------|-------------------------------------|
| Version               | V2                                  |
| Issuer                | sec-plus-SUCCESS-CA, sec-plus, com  |
| Effective date        | Friday, July 29, 2011 1:10:12 PM    |
| Next update           | Friday, July 29, 2011 2:45:12 PM    |
| Signature algorithm   | sha1RSA                             |
| Authority Key Iden... | KeyID=9b fd e2 d9 68 89 3b b0 9c... |
| CA Version            | V0.0                                |
| CRL Number            | 38                                  |
| Next CRL Publish      | Friday, July 29, 2011 2:20:12 PM    |

Value:

Learn more about [certificate revocation list](#)

OK

**Certificate Revocation List**

General | Revocation List

**Revoked certificates:**

| Serial number                 | Revocation date            |
|-------------------------------|----------------------------|
| 11 b7 19 c2 00 00 00 00 00 03 | Tuesday, July 26, 2011 ... |

**Revocation entry**

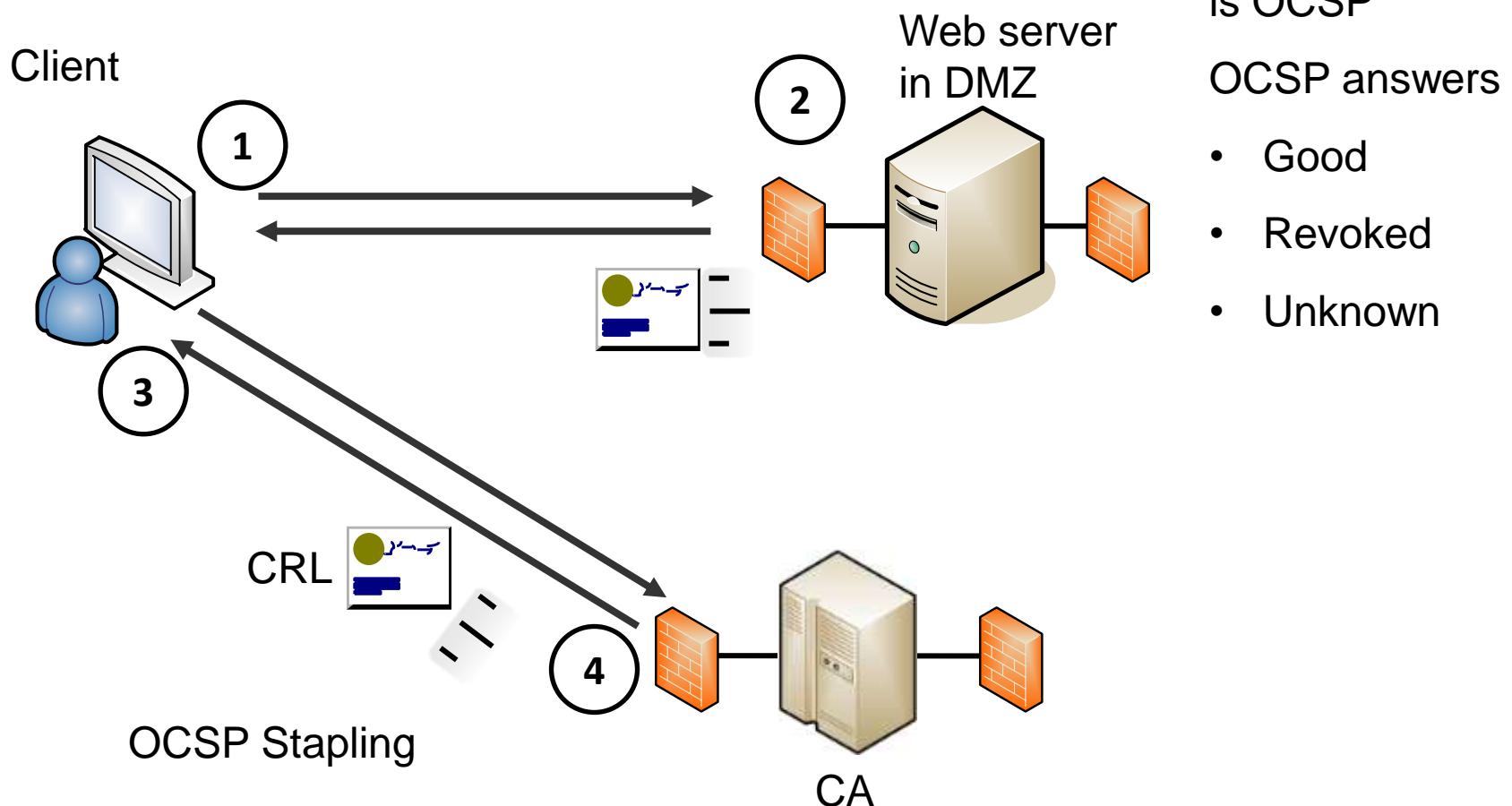
| Field | Value |
|-------|-------|
|       |       |

Value:

Learn more about [certificate revocation list](#)

OK

# Validating Certificates



# Certificates

---

- Public key pinning
  - Helps prevent web site impersonation
- Key escrow
  - Maintains a copy of a private key for recovery
  - Used if the original is lost
- Key management
  - Steps taken to manage public and private keys

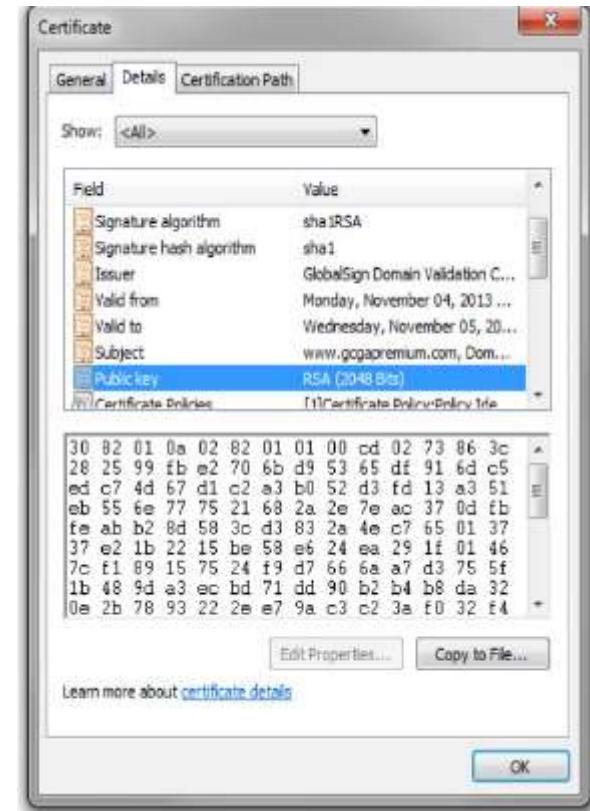
# Certificate Types

---

- Machine/computer
- User
- Email
  - Encryption and digital signatures
- Code signing
  - Validates authentication of code
- Self-signed
  - Not issued by CA
- Root
  - Issued by the root CA

# Certificate Types

- Wildcard
  - Same root domain
- Subject Alternative Name (SAN)
  - Different root domains, but same organization
- Domain validation
  - CA takes extra steps to contact requestor
- Extended validation
  - Additional steps beyond domain validation



# Certificate Formats

| Type       | Common Extensions         | Format                         | Common Purpose                                            | Can Contain                                                         |
|------------|---------------------------|--------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------|
| CER        | .cer                      | ASCII                          | Used for ASCII certificates                               | Varies                                                              |
| DER        | .der                      | Binary                         | Used for binary certificates                              | Varies                                                              |
| PEM        | .pem, .cer,<br>.crt, .key | Binary (DER)<br>or ASCII (CER) | Can be used for almost any<br>certificate purpose         | Server certificates, certificate chains,<br>keys, CRL               |
| P7B        | .p7b, .p7c                | ASCII (CER)                    | Used to share the public key                              | Certificates, certificate chains, CRL,<br>but never the private key |
| P12<br>PFX | .p12, .pfx                | Binary (DER)                   | Commonly used to store<br>private keys with a certificate | Certificates, certificate chains, and<br>private keys               |

# Chapter 10 Summary

---

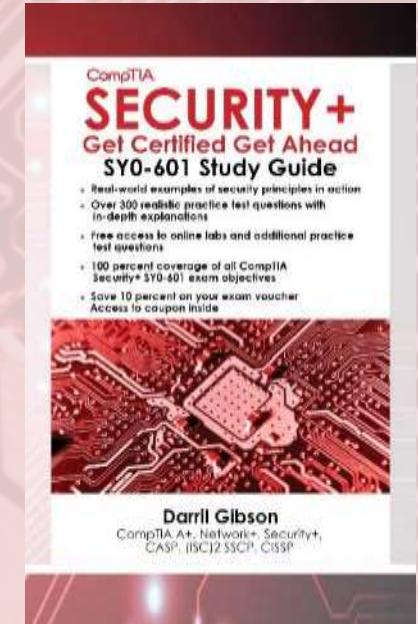
- Introducing Cryptography Concepts
- Providing Integrity with Hashing
- Understanding Password Attacks
- Providing Confidentiality with Encryption
- Using Cryptographic Protocols
- Exploring PKI Components
- Check out the free online labs

# Chapter 11

## Implementing Policies to Mitigate Risks

CompTIA Security+  
Get Certified Get Ahead

By Darril Gibson



# Introduction

---

- Exploring security policies
- Incident response policies
- Understanding digital forensics
- Protecting data
- Training users

# Exploring Security Policies

---

- Security policies
  - Written documents that identify a security plan
  - personnel within the organization create plans and procedures to support the policies



# Personal Policies

---

- Acceptable use policy
  - Defines proper system usage
  - Users often required to read and sign an AUP when hired and periodically
- Mandatory vacations
  - Require employees to take time away from the job
  - Helps reduce fraud and discover malicious activities while the employee is away



# Personal Policies

---

- Separation of duties
  - Prevents any single person or entity from being able to complete all the functions of a process
  - Divides tasks between employees
- Least Privilege
  - Grants only those rights and permissions needed
  - Limits potential losses if any individual or process is compromised



# Personal Policies

---

- Job rotation
  - Require employees to change roles on a regular basis
  - Helps ensure that employees cannot continue with fraudulent activity indefinitely
- Background check
  - Varies based on job

# Personal Policies

---

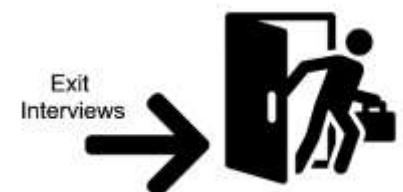
- Clean desk policy
  - Requires users to organize their areas
  - Reduces risk of possible data theft
  - Reminds users to secure sensitive data
  - May include a statement about not writing down passwords



# Personal Policies

---

- Onboarding
  - Granting individuals access to an organization's computing resources after being hired
- Offboarding
  - Removing an employee's access when he leaves the company



# Personal Policies

---

- Non-disclosure agreement (NDA)
  - NDAs prohibit data sharing
- Social Media Analysis
  - Monitoring employee activity on social media networks



# Personal Policies

---

- Measurement Systems Analysis (MSA)
  - Evaluates processes and tools used to make measurements
- Third-Party Risk Management
  - Supply Chain and Vendors (elements required to produce and sell products and services)
  - Third-Party Agreements (help identify various responsibilities)

# Personal Policies

---

- Third-Party Risk Management
  - Supply Chain and Vendors (elements required to produce and sell products and services)
  - Third-Party Agreements (help identify various responsibilities)
- Terms of Agreement
  - Indicates the period that an agreement shall be in effect



# Incident Response Policies

---

- Incident response
  - Helps personnel identify and respond to incidents
- Security incident
  - An adverse event or series of events
  - Can negatively affect the confidentiality, integrity, or availability of data or systems

# Incident Response Policies

---

- Examples
  - Data breach
  - Release of malware
  - Security policy violations
  - Inappropriate usage of systems

# Incident Response Plan

---

- Incident response plan
  - Provides organizations with a formal, coordinated plan that personnel can use when responding to an incident
- Incident types
- Cyber-incident response teams
- Roles and responsibilities

# Incident Response Plan

---

- Communication plan
  - Provides direction on how to communicate issues related to an incident
- First responders
- Reporting requirements
- External communication
- Law enforcement
- Customer communication

# Incident Response Plan

---

- Data breach responses
- Stakeholder management
  - Creating and maintaining positive relationships with stakeholders

# Incident Response Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned



# Understanding SOAR

---

- SOAR
  - Internal tools used to respond to low-level security events automatically
  - Uses playbooks and runbooks
- Examples
  - Respond to phishing emails
  - Verify potentially malicious traffic

# Understanding Digital Forensics

---

- Digital forensic techniques
  - Help an organization collect and analyze data as evidence
- Computer forensics techniques
  - Analyze evidence from computers to gather details on computer incidents

# Key Aspects of Digital Forensics

---

- Admissibility of documentation and evidence
  - Tags
  - Chain of custody
  - Legal hold
  - Video
  - Interviews
  - Event logs
  - Sequence of events
  - Reports

# Key Aspects of Digital Forensics

---

- On-Premises Versus Cloud Concerns
  - Right to audit clauses
  - Regulatory Jurisdiction
  - Data breach notification laws

# Acquisition and Preservation

---

- Data acquisition
  - Ensures that the evidence is preserved in case it is needed in a legal proceeding
- Order of volatility
  - Ensures that the evidence is preserved in case it is needed in a legal proceeding

# Acquisition and Preservation

---

- Forensic tools
  - Capturing data
  - Verifying integrity
- Electronic discovery
  - eDiscovery is the identification and collection of electronically stored information
- Data recovery
  - Restoring lost data

# Strategic Intelligence and Counterintelligence

---

- Digital forensic intelligence
  - Knowledge and information which has value to investigative personnel
- Digital forensics strategic intelligence
  - Collecting, processing, and analyzing digital forensic data to create long-term cybersecurity goals

# Protecting Data

---

- Classifying data types
- PII and Health Information
- Impact assessment
- Data governance
- Privacy enhancing technologies
- Data retention policies
- Data sanitization

# Classifying Data Types

---

- Information classification
  - Helps ensure users understand the value of data
  - Helps protect sensitive data
  - Classifications defined in security policy
    - Public data
    - Private data
    - Confidential data
    - Proprietary data
    - Financial information
    - Customer data

# PII and Health Information

---

- Personally identifiable information (PII)
  - Includes information such as:
    - Full name, birthdate, biometric data, identifying numbers
  - Requires special handing
  - Employees should be trained not to give out PII
  - Many laws mandate the reporting of PII data losses
- Personal Health Information (PHI)
  - PII that includes health information
  - Includes information on employee health plans

# PII and Health Information

---

- Some examples of PII are:
  - Full name
  - Birthday and birthplace
  - Medical and health information
  - Street or email address information
  - Personal characteristics (biometrics data)
  - Any type of identification number

# Data Governance

---

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- General Data Protection Regulation (GDPR)

# Privacy Enhancing Technologies

---

- Data Masking
- Anonymization
- Pseudo-Anonymization
- Tokenization

# Data Retention Policies

---

- Storage and retention policies
  - Identify where data is stored
  - Identify how long it is retained
  - Retention policies
    - May limit a company's exposure to legal proceedings
    - May reduce the amount of labor required to respond to court orders

# Data Sanitization

---

- File shredding
- Wiping
- Erasing or overwriting
- Paper shredding
- Burning



# Data Sanitization

---

- Pulping
- Pulverizing
- Degaussing
- Third-party solutions

# Training Users

---

- Training personnel on security policies
- Training to help ensure personnel remain up to date with current technologies and threats
- Computer-based training
  - Any training where an individual interacts with an application on a computer
  - Students can learn at their own pace

# Training Users

---

- Phishing campaigns
  - Personnel to learn new phishing campaigns
- Phishing simulations
  - Sends out fake phishing emails to employees
  - To know if any of their employees will be tricked by phishing emails

# Training Users

---

- Gamification
  - Often used in courseware and online training
  - Game-design elements within user training
- Capture the Flag
  - Example of gamification
  - Includes several challenges that players can solve

# Training Users

---

- Role-based Training
  - Targeted to users based on their roles
    - Data owner
    - Data controller
    - Data processor
    - Data custodian/steward
    - Data protection officer



# Chapter 11 Summary

---

- Exploring Security Policies
- Incident Response Policies
- Understanding Digital Forensics
- Protecting Data
- Training Users
- Check out the free online labs

