Security Concepts

Section 1: Network Threats

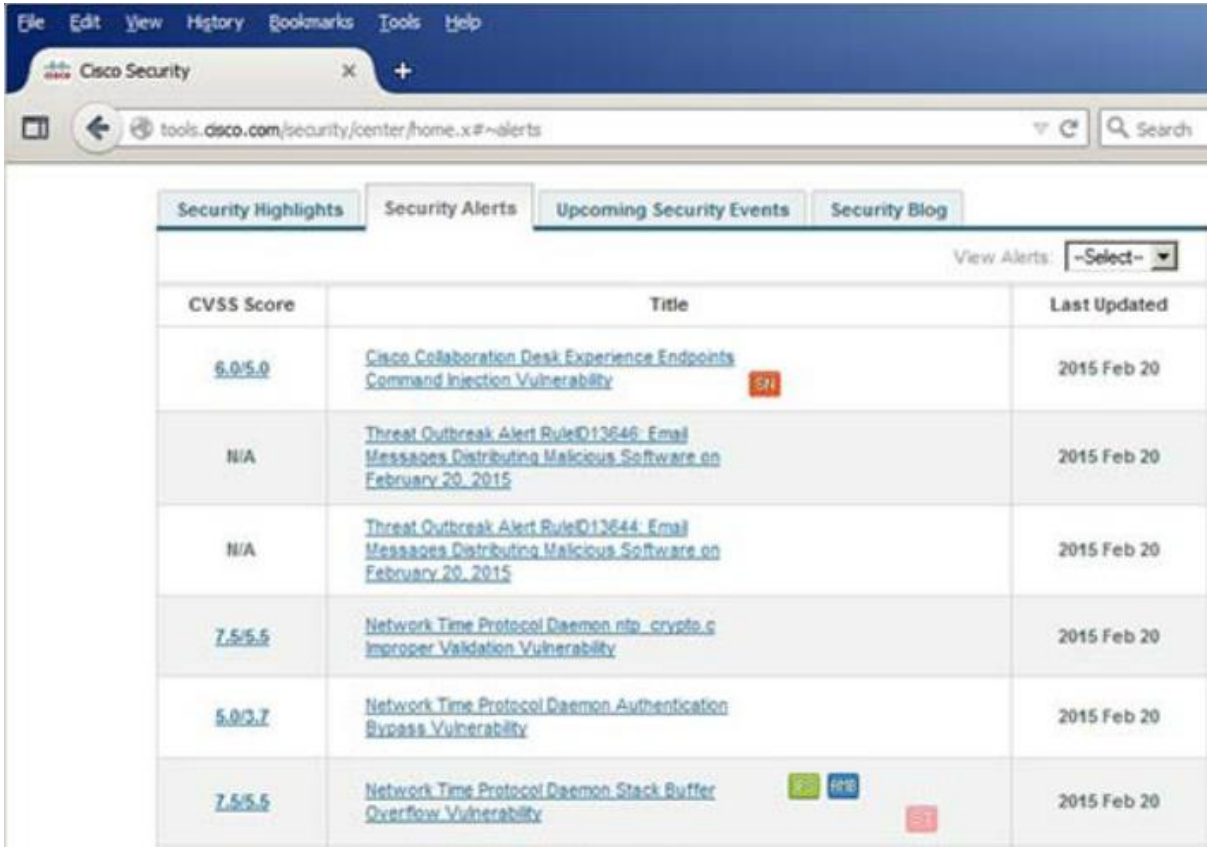
Upon completion of the section, you should be able to:

- Describe the evolution of network security.
- Describe the various types of attack tools used by hackers.
- Describe malware.
- Explain common network attacks.

Drivers for Network Security

Common network security terms:

- Threat
- Vulnerability
- Mitigation
- Risk



CVSS Score	Title	Last Updated
6.0/5.0	Cisco Collaboration Desk Experience Endpoints Command Injection Vulnerability SN	2015 Feb 20
N/A	Threat Outbreak Alert RuleID13646: Email Messages Distributing Malicious Software on February 20, 2015	2015 Feb 20
N/A	Threat Outbreak Alert RuleID13644: Email Messages Distributing Malicious Software on February 20, 2015	2015 Feb 20
7.5/5.6	Network Time Protocol Daemon ntp_crypto.c Improper Validation Vulnerability	2015 Feb 20
5.0/3.7	Network Time Protocol Daemon Authentication Bypass Vulnerability	2015 Feb 20
7.5/5.6	Network Time Protocol Daemon Stack Buffer Overflow Vulnerability	2015 Feb 20

The Hacker & The Evolution of Hackers

White Hat Hackers
Grey Hat Hackers
Black Hat Hackers

Modern hacking titles:

- Script Kiddies
- Vulnerability Brokers
- Hacktivists
- Cyber Criminals
- State-Sponsored Hackers

Evolution of Security Tools

Penetration testing tools:

- Password crackers
- Wireless hacking
- Network scanning and hacking
- Packet crafting
- Packet sniffers
- Rootkit detectors
- Fuzzers to search vulnerabilities
- Forensic
- Debuggers
- Hacking operating systems
- Encryption
- Vulnerability exploitation
- Vulnerability Scanners

Categories of Attack Tools

Network hacking attacks:

- Eavesdropping
- Data modification
- IP address spoofing
- Password-based
- Denial-of-service
- Man-in-the-middle
- Compromised-key
- Sniffer

Viruses

Virus Alert!

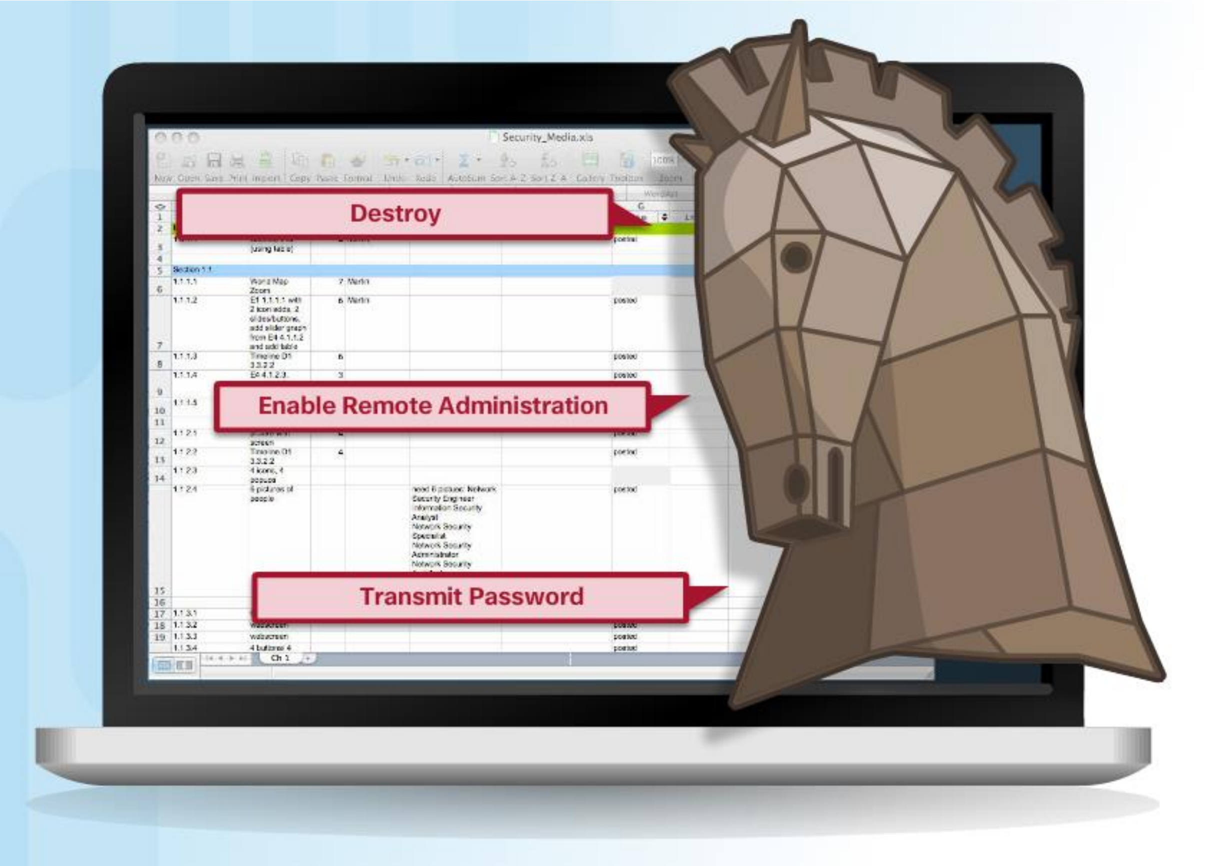
Warning! Threat detected!

A malicious item has been detected!

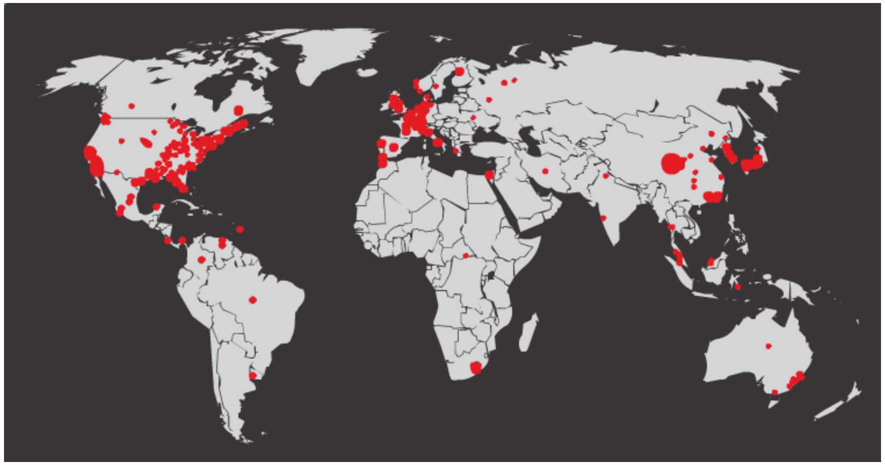
Trojan Horse Classification

Classifications:

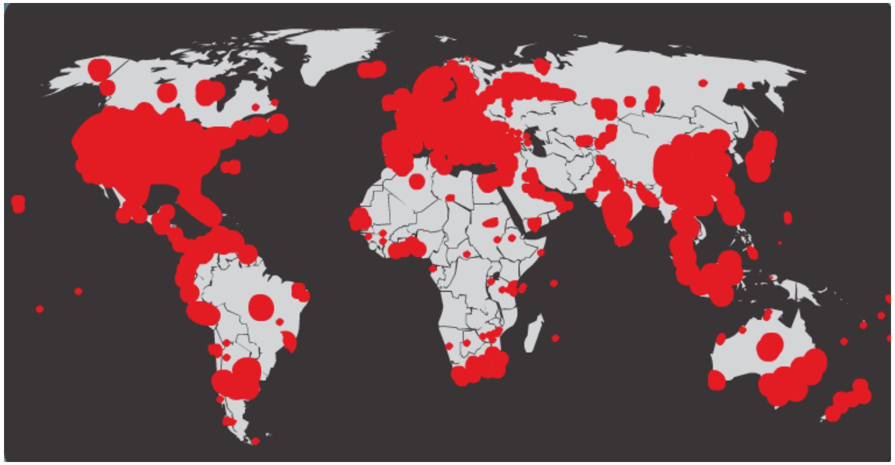
- Security software disabler
- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- DoS



Worms



Initial Code Red Worm Infection

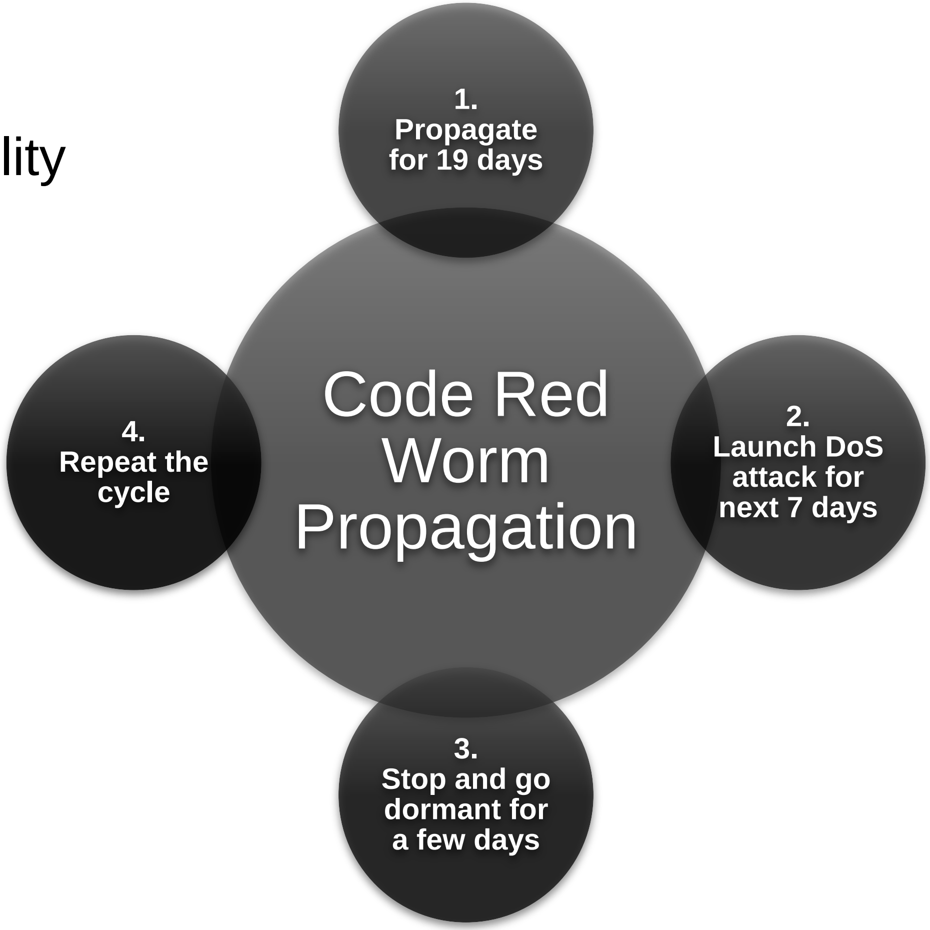


Code Red Worm Infection 19 Hours Later

Worm Components

Components:

- Enabling vulnerability
- Propagation mechanism
- Payload



Code Red Worm Propagation

1. Propagate for 19 days

2. Launch DoS attack for next 7 days

3. Stop and go dormant for a few days

4. Repeat the cycle

Other Malware

Ransomware

Spyware

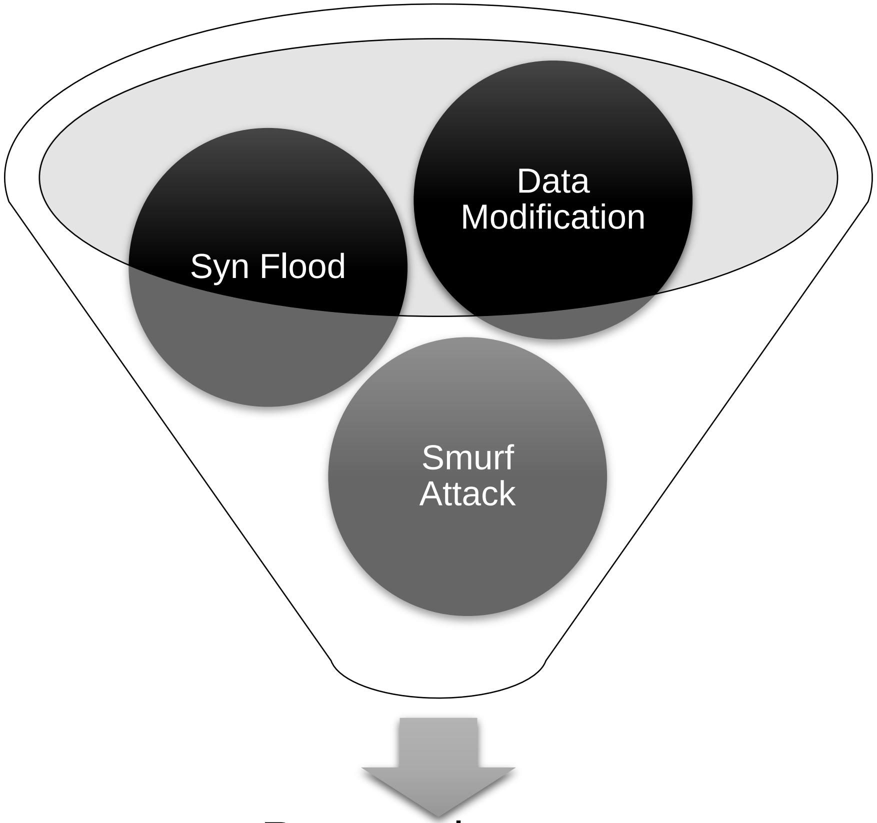
Adware

Scareware

Phishing

Rootkits

Types of Network Attacks



Reconnaissance
Access
DoS

Reconnaissance Attacks

- Initial query of a target
- Ping sweep of the target network
- Port scan of active IP addresses
- Vulnerability scanners
- Exploitation tools

Access Attacks

A few reasons why hackers use access attacks:

- To retrieve data
- To gain access
- To escalate access privileges

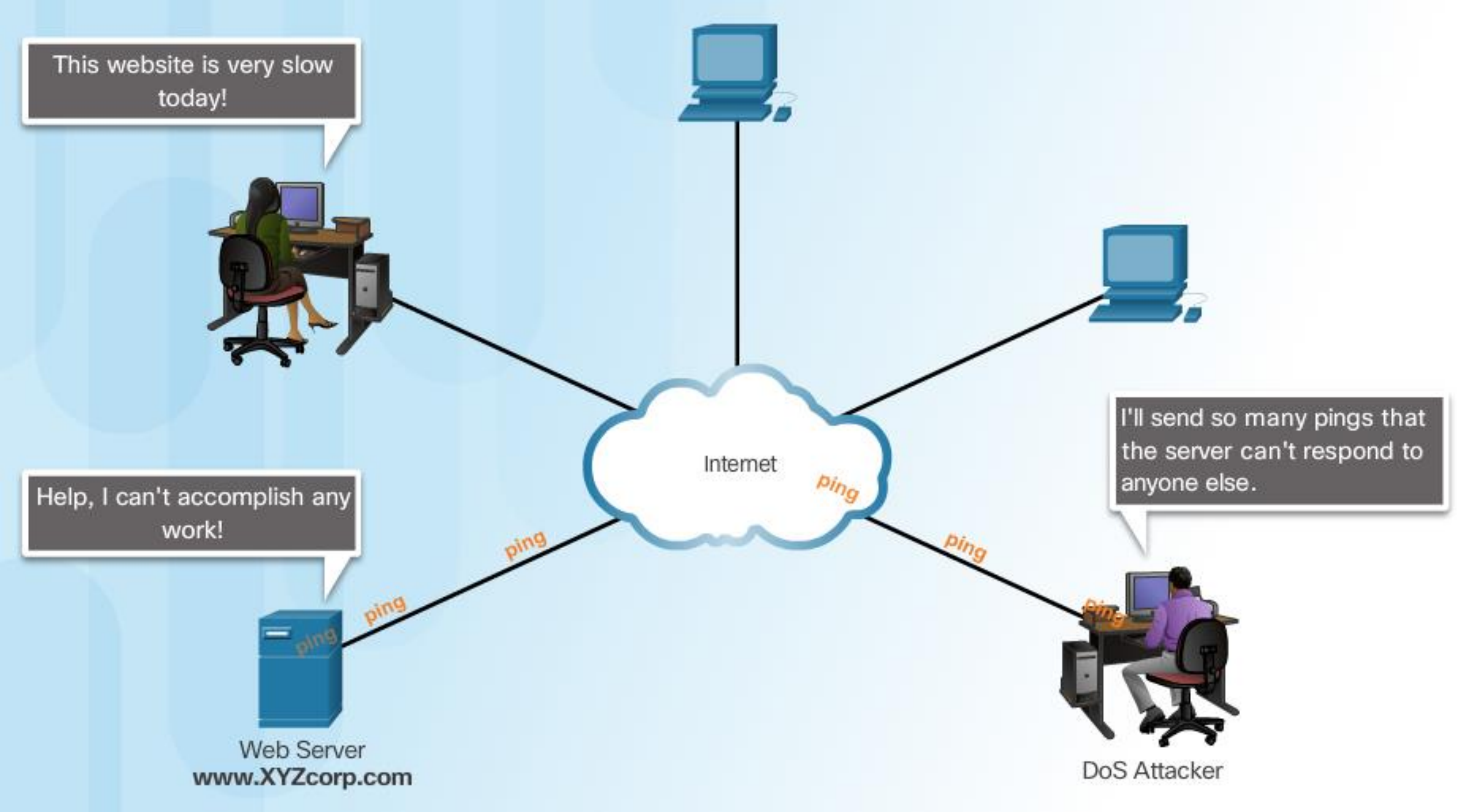
A few types of access attacks include:

- Password
- Trust exploitation
- Port redirection
- Man-in-the-middle
- Buffer overflow
- IP, MAC, DHCP spoofing

Social Engineering Attacks

- Pretexting
- Phishing
- Spearphishing
- Spam
- Tailgating
- Something for Something
- Baiting

Denial of Service Attacks


This website is very slow today!
Internet
ping
ping
ping
ping
ping
ping
Help, I can't accomplish any work!
I'll send so many pings that the server can't respond to anyone else.
Web Server
www.XYZcorp.com
DoS Attacker

DDoS Attacks

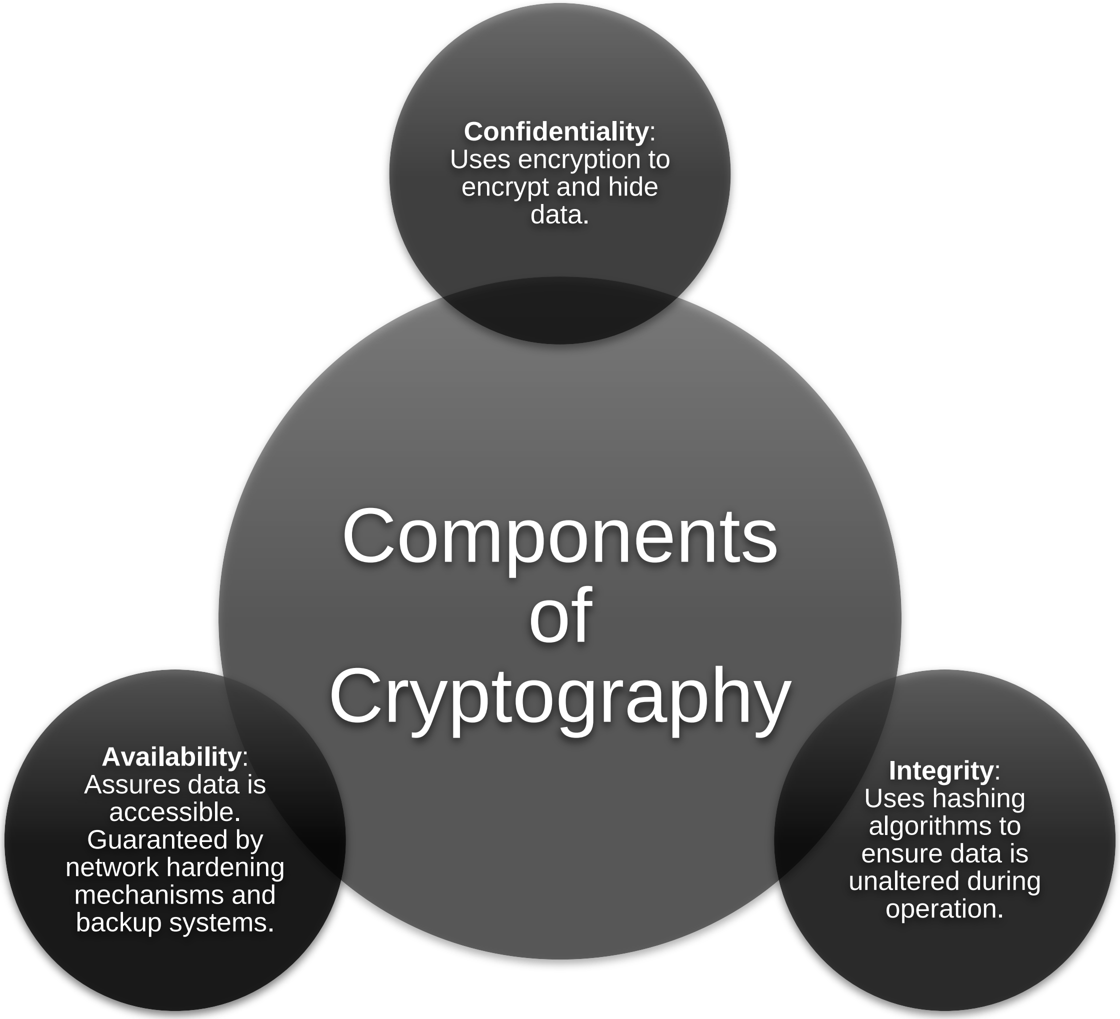
1. Hacker builds a network of infected machines
   - A network of infected hosts is called a botnet.
   - The compromised computers are called zombies.
   - Zombies are controlled by handler systems.
2. Zombie computers continue to scan and infect more targets
3. Hacker instructs handler system to make the botnet of zombies carry out the DDoS attack

Section 2:
Mitigating Threats

Upon completion of this section, you should be able to:

- Describe methods and resources to protect the networks.
- Describe a collection of domains for network security.
- Explain the purpose of the Cisco SecureX Architecture.
- Describe the techniques used to mitigate common network attacks.
- Explain how to secure the three functional areas of Cisco routers and switches.

Confidentiality, Integrity, Availability



Confidentiality: Uses encryption to encrypt and hide data.

Components of Cryptography

Availability: Assures data is accessible. Guaranteed by network hardening mechanisms and backup systems.

Integrity: Uses hashing algorithms to ensure data is unaltered during operation.

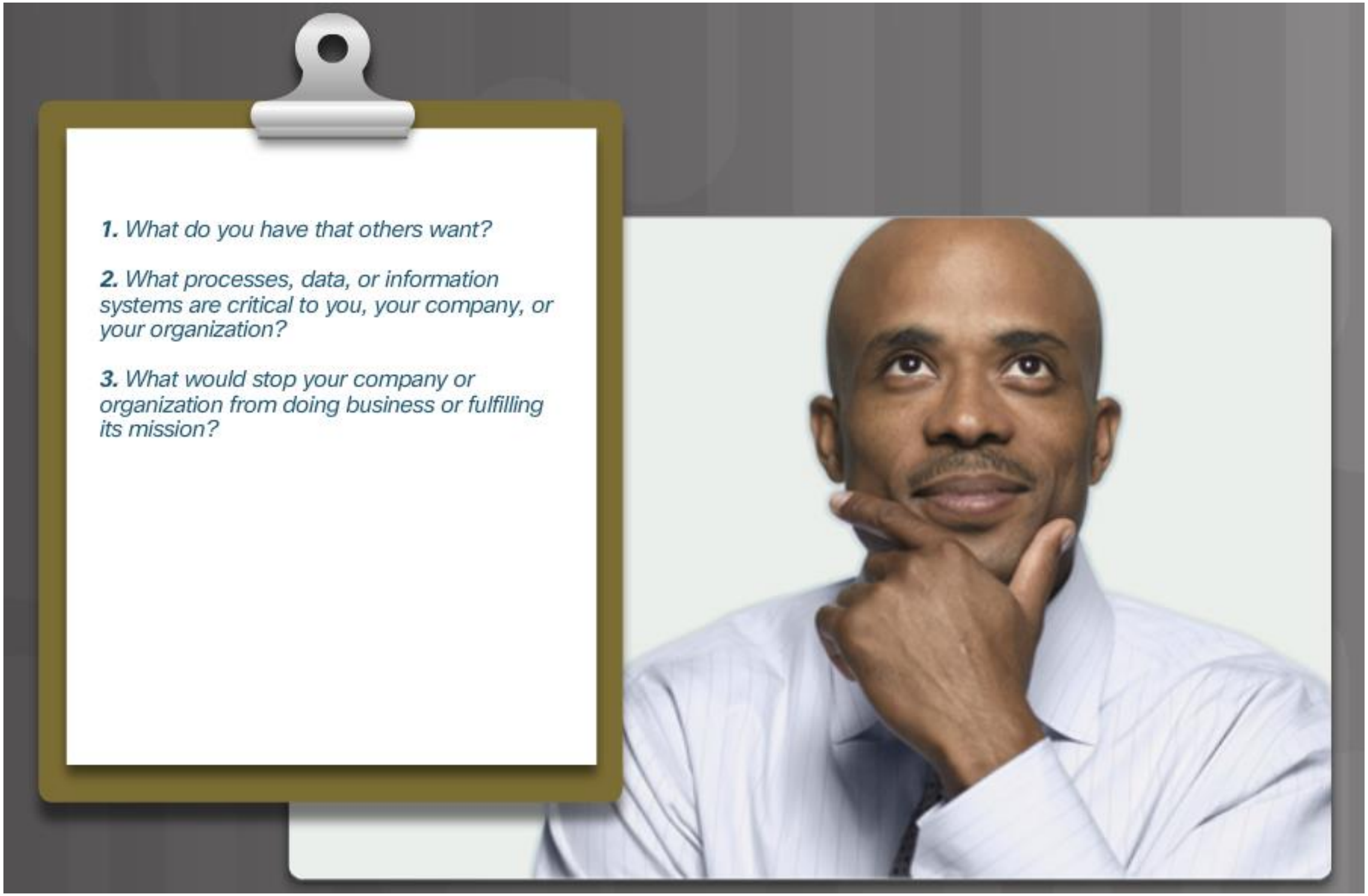
Network Security Domains

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Information systems acquisition, development, and maintenance
- Access control
- Information security incident management
- Business continuity management
- Compliance

Network Security Policy

The next item on the security policy that we need to discuss is the rules for network access.
We must keep in mind that we have remote workers. They will have different access rules than our onsite employees.

Network Security Policy Objectives



1. *What do you have that others want?*

2. *What processes, data, or information systems are critical to you, your company, or your organization?*

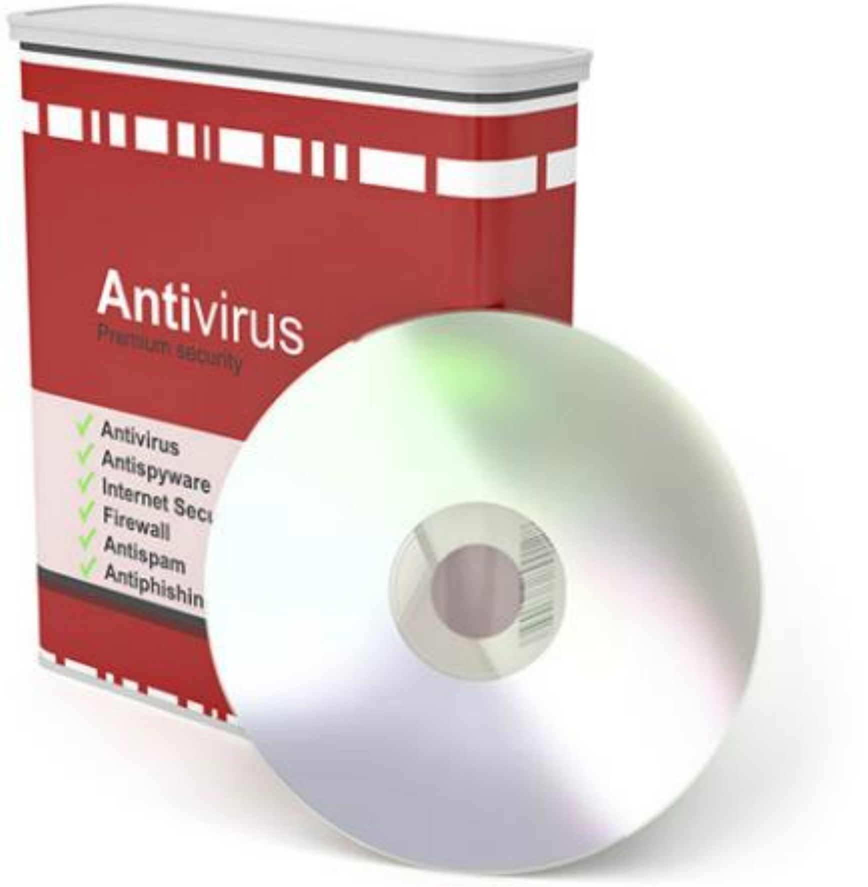
3. *What would stop your company or organization from doing business or fulfilling its mission?*

Defending the Network

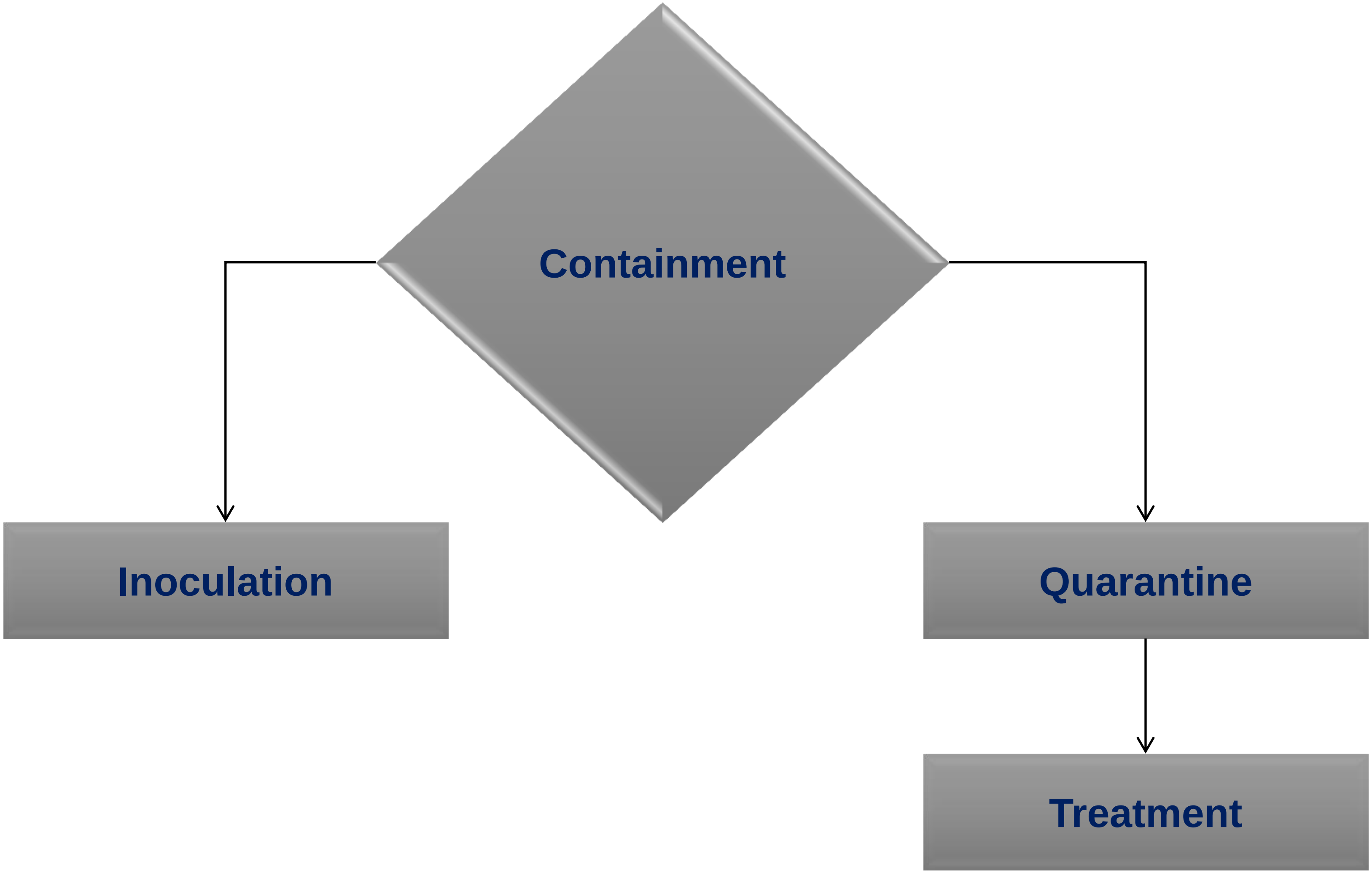
Best practices:

- Develop a written security policy.
- Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- Control physical access to systems.
- Use strong passwords and change them often.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software.
- Perform backups and test the backed up files on a regular basis.
- Shut down unnecessary services and ports.
- Keep patches up-to-date by installing them weekly or daily to prevent buffer overflow and privilege escalation attacks.
- Perform security audits to test the network.

Mitigating Malware



Mitigating Worms



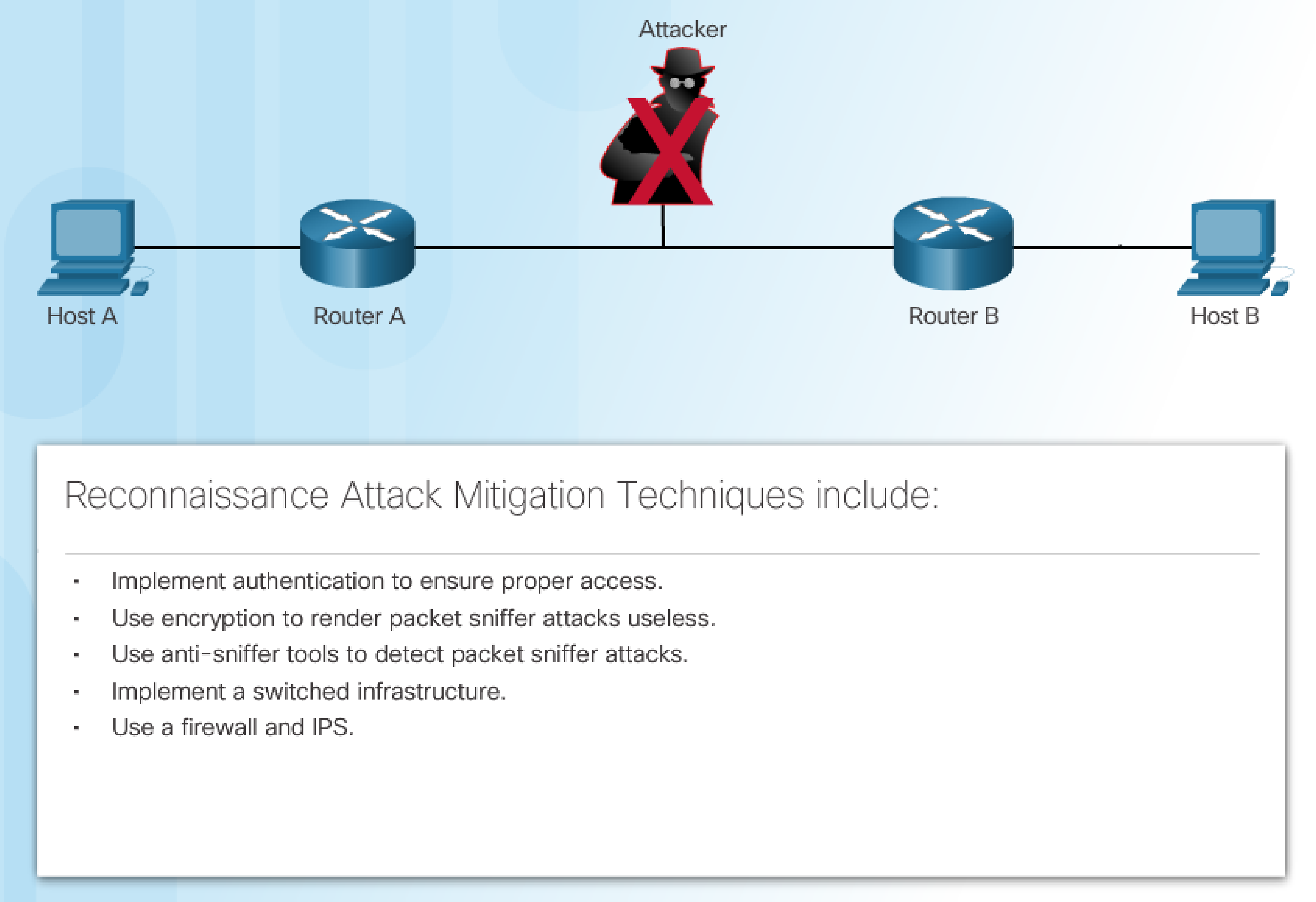
Containment

Inoculation

Quarantine

Treatment

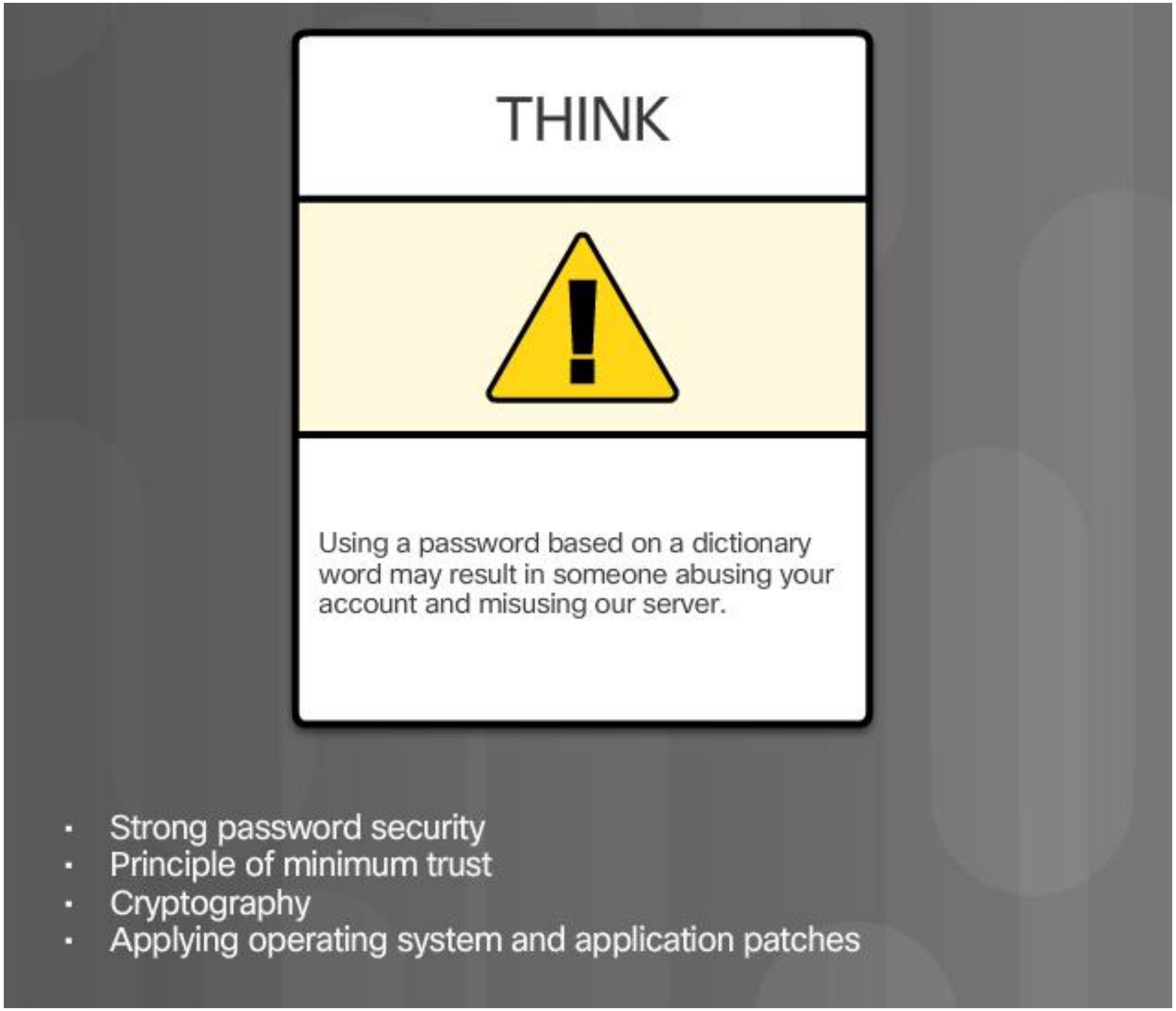
Mitigating Reconnaissance Attacks



Reconnaissance Attack Mitigation Techniques include:

- Implement authentication to ensure proper access.
- Use encryption to render packet sniffer attacks useless.
- Use anti-sniffer tools to detect packet sniffer attacks.
- Implement a switched infrastructure.
- Use a firewall and IPS.

Mitigating Access Attacks



THINK

Using a password based on a dictionary word may result in someone abusing your account and misusing our server.

- Strong password security
- Principle of minimum trust
- Cryptography
- Applying operating system and application patches

Mitigating DoS Attacks

- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

Section 3:
Securing Network Devices

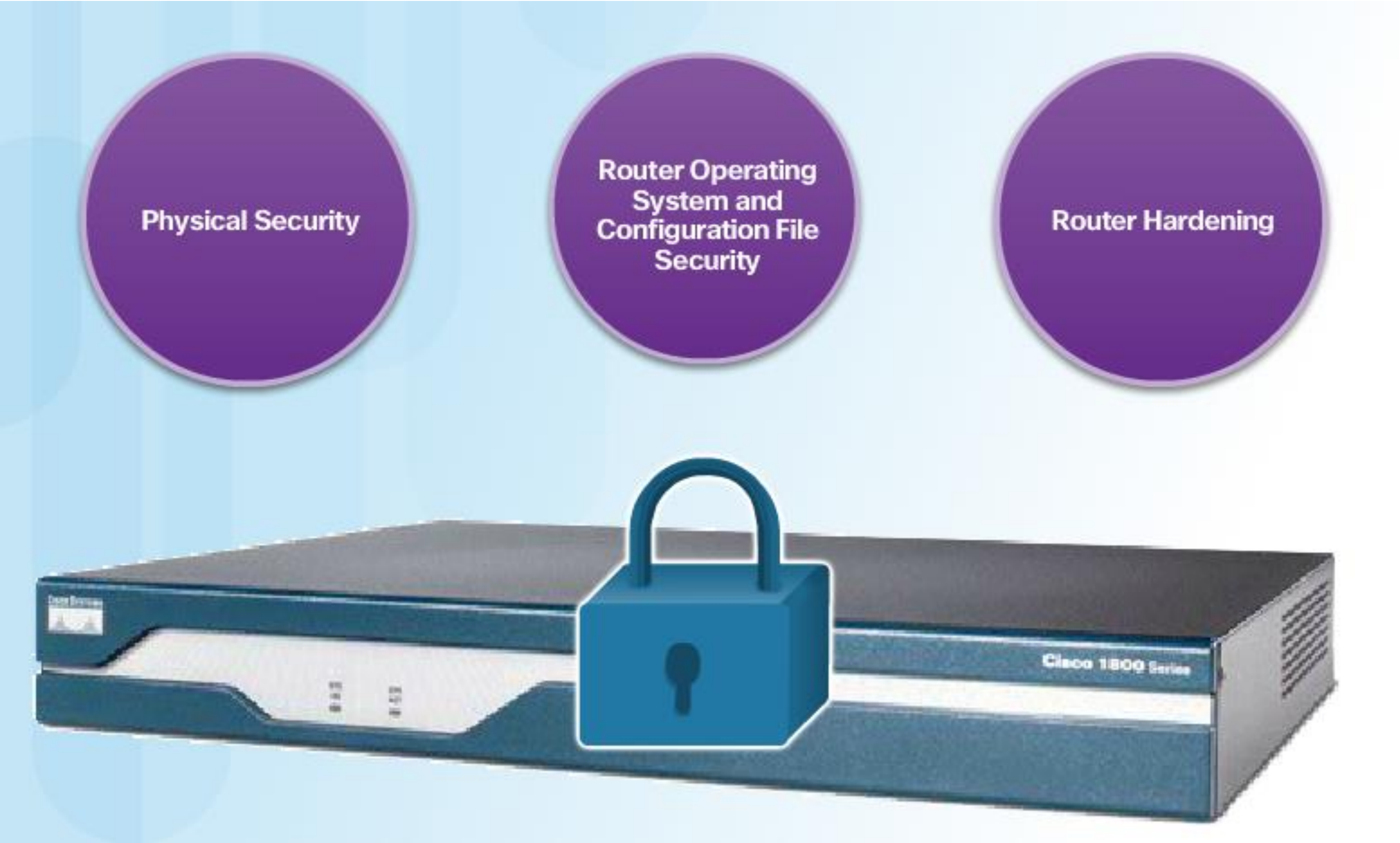
Upon completion of this section, you should be able to:

- Secure Access in Network Infrastructure
- Configure administrative privilege levels to control command availability

Securing the Network Infrastructure

```
R1#erase startup-config
R1#reload in 5
Proceed with reload?
[confirm]
R1#
***
*** -- SHUTDOWN in 0:05:00 --
***
R1#
```

Three Areas of Router Security



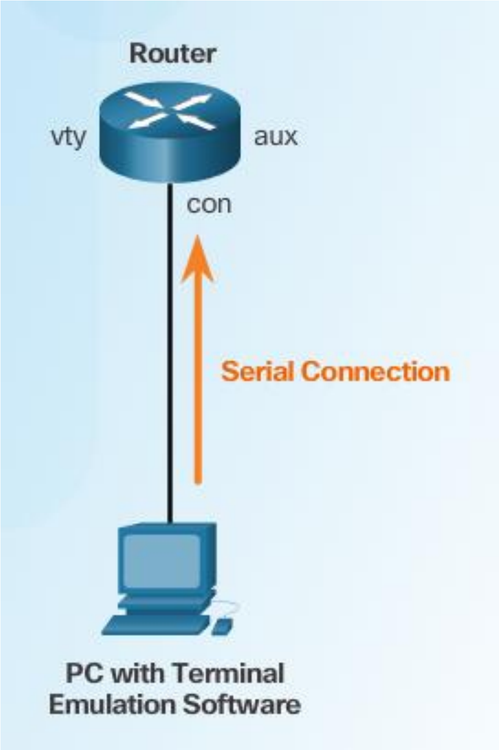
Secure Administrative Access

Tasks:

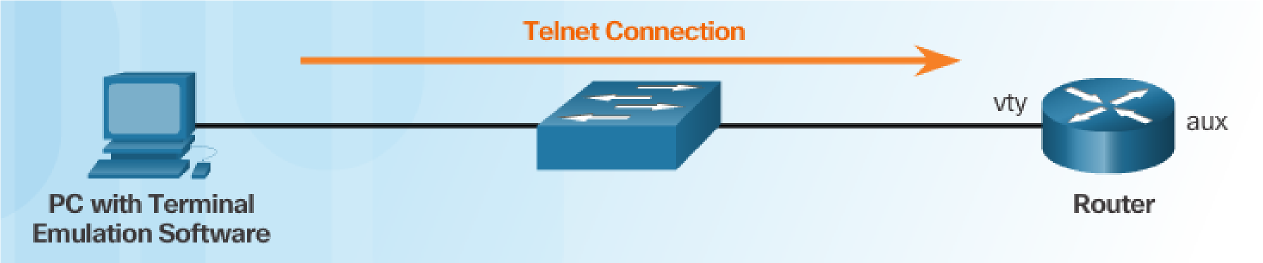
- Restrict device accessibility
- Log and account for all access
- Authenticate access
- Authorize actions
- Present legal notification
- Ensure the confidentiality of data

Secure Local and Remote Access

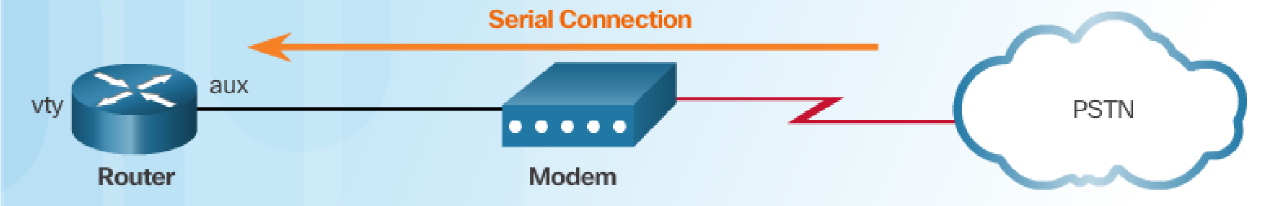
Local Access



Remote Access Using Telnet



Remote Access Using Modem and Aux Port



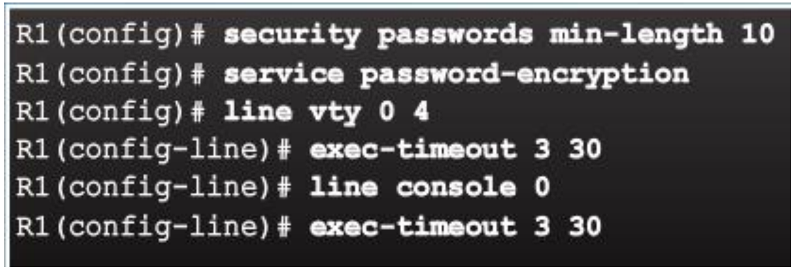
Strong Passwords

Guidelines:

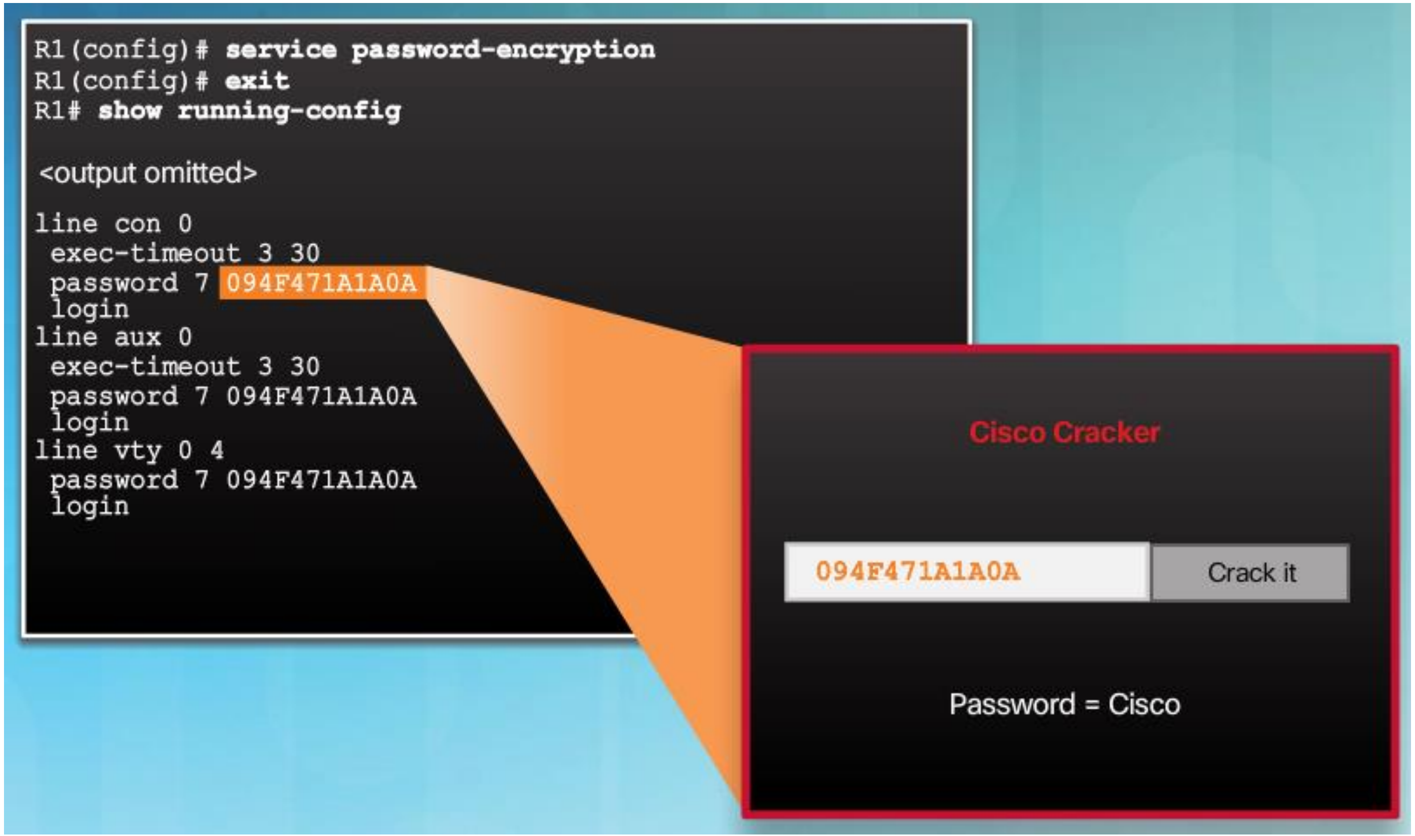
- Use a password length of 10 or more characters.
- Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on easily identifiable pieces of information.
- Deliberately misspell a password (Smith = Smyth = 5mYth).
- Change passwords often.
- Do not write passwords down and leave them in obvious places.

Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother’s maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

Increasing Access Security



```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```



```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

 <output omitted>

line con 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line vty 0 4
 password 7 094F471A1A0A
 login
```

Cisco Cracker

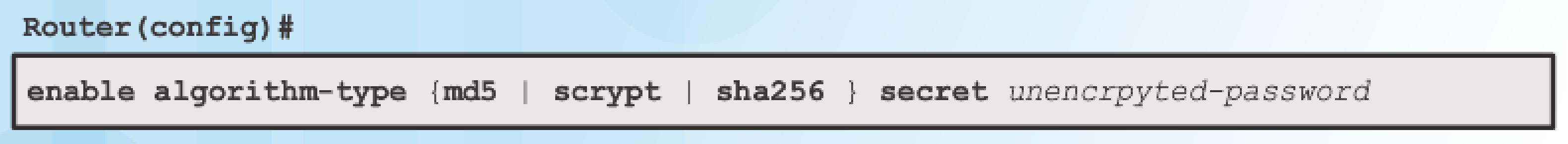
094F471A1A0A

Password = Cisco

Secret Password Algorithms

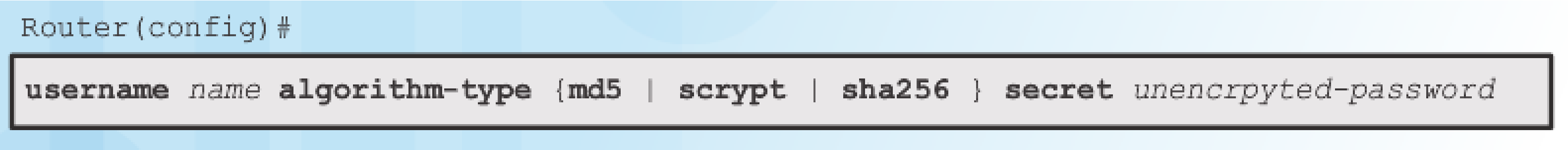
Guidelines:

- Configure all secret passwords using type 8 or type 9 passwords
- Use the enable algorithm-type command syntax to enter an unencrypted password



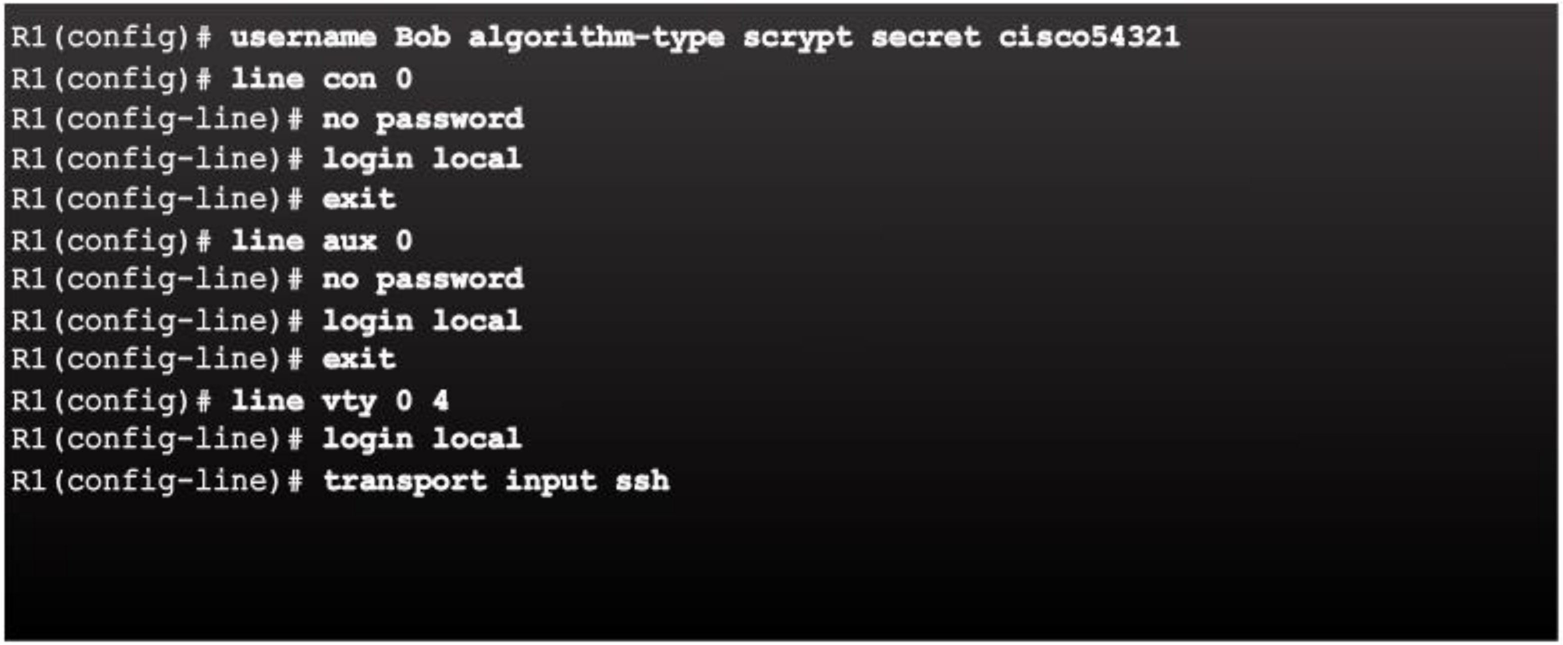
```
Router(config)#
enable algorithm-type {md5 | scrypt | sha256 } secret unencrpyted-password
```

- Use the username name algorithm-type command to specify type 9 encryption



```
Router(config)#
username name algorithm-type {md5 | scrypt | sha256 } secret unencrpyted-password
```

Securing Line Access



```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

Limiting Command Availability

Privilege levels:

- Level 0: Predefined for user-level access privileges.
- Level 1: Default level for login with the router prompt.
- Level 2-14: May be customized for user-level privileges.
- Level 15: Reserved for the enable mode privileges.

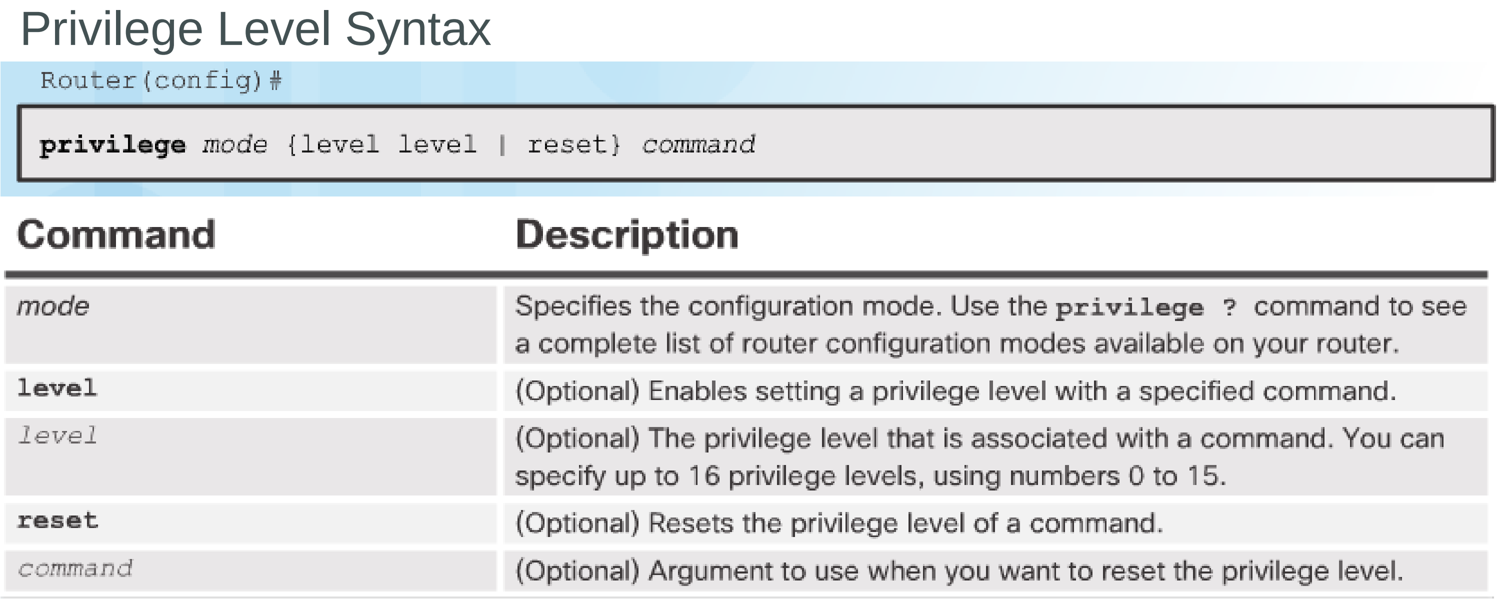
Levels of access commands:

User EXEC mode (privilege level 1)

- **Lowest EXEC mode user privileges**
- **Only user-level command available at the router> prompt**

Privileged EXEC mode (privilege level 15)

- **All enable-level commands at the router# prompt**



Privilege Level Syntax

```
Router(config)#
privilege mode {level level | reset} command
```

Command	Description
mode	Specifies the configuration mode. Use the **privilege ?** command to see a complete list of router configuration modes available on your router.
level	(Optional) Enables setting a privilege level with a specified command.
level	(Optional) The privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) Resets the privilege level of a command.
command	(Optional) Argument to use when you want to reset the privilege level.

Limitations of Privilege Levels

No access control to specific interfaces, ports, logical interfaces, and slots on a router

Commands available at lower privilege levels are always executable at higher privilege levels

Commands specifically set at higher privilege levels are not available for lower privilege users

Assigning a command with multiple keywords allows access to all commands that use those