Introduction to Network Security (Part-2)

By Dr. Md. Nadir Bin Ali

Lecture-4 Outline

1.0 Introduction

1.1 Securing Networks

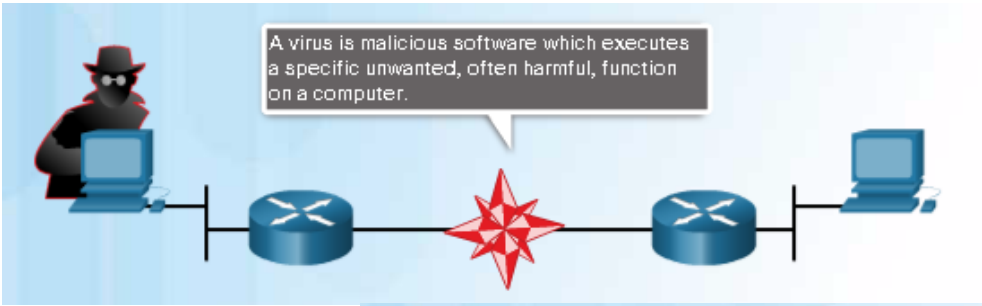
1.2 Network Threats

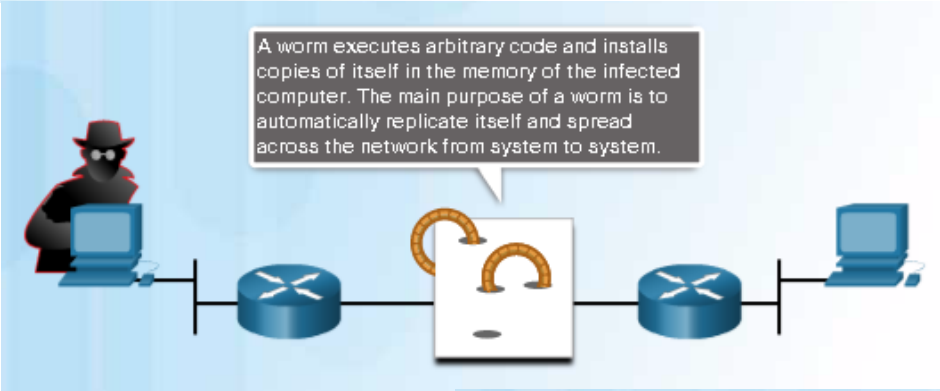
1.3 Mitigating Threats

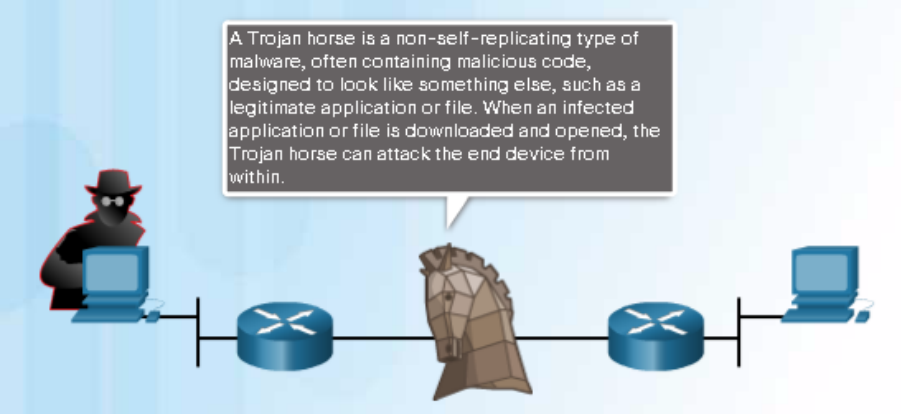
1.4 Summary

Malware

Various Types of Malware





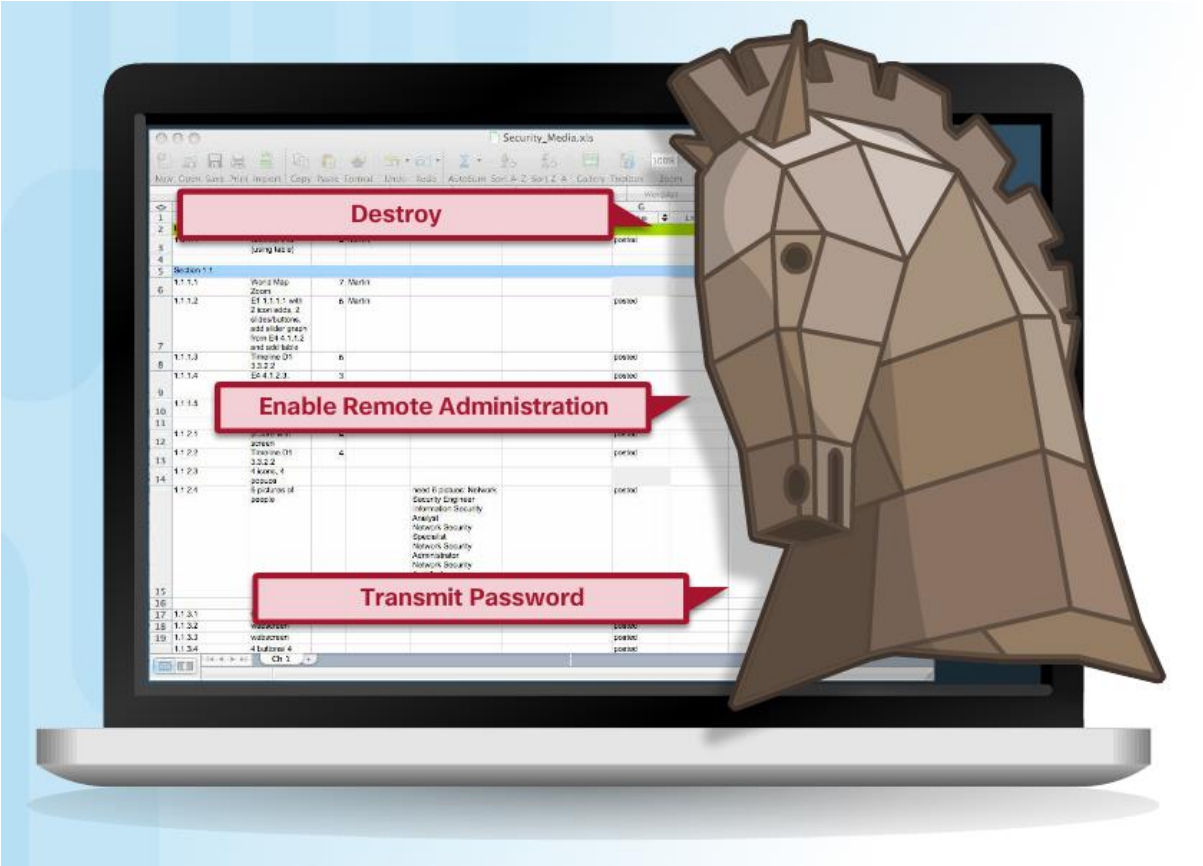


Viruses

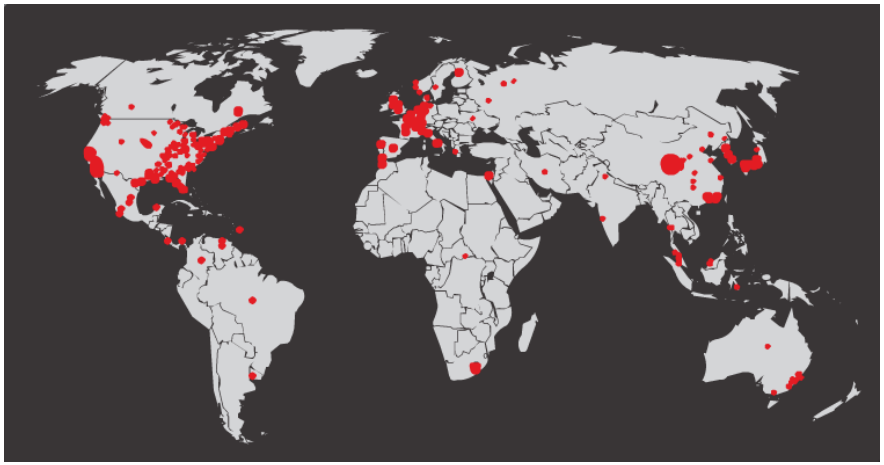
Trojan Horse Classification

Classifications:

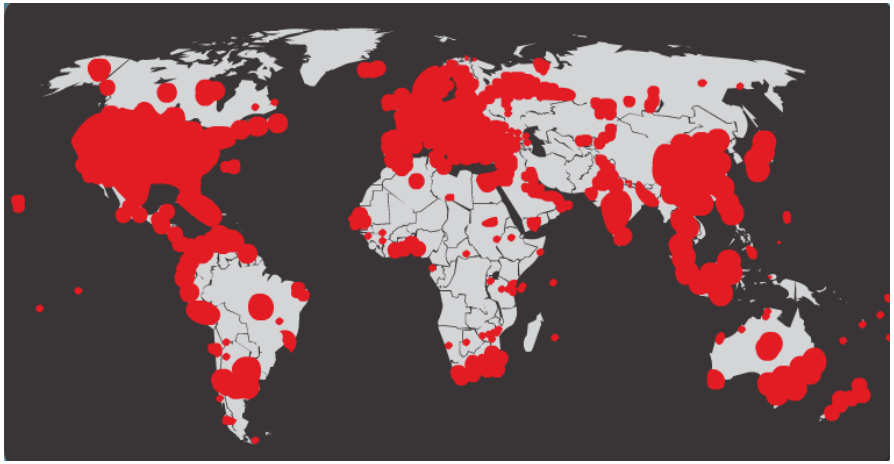
- Security software disabler
- Remote-access
- Data-sending
- Destructive
- Proxy
- FTP
- DoS



Worms



Initial Code Red Worm Infection

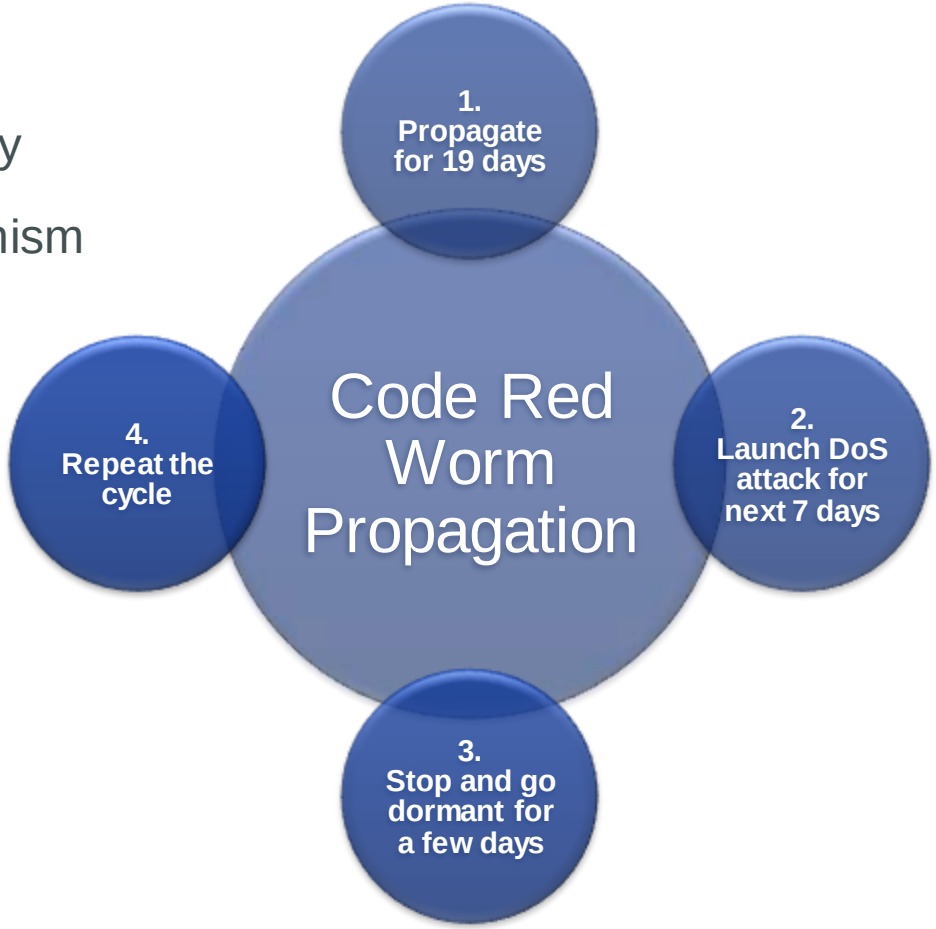


Code Red Worm Infection 19 Hours Later

Worm Components

Components:

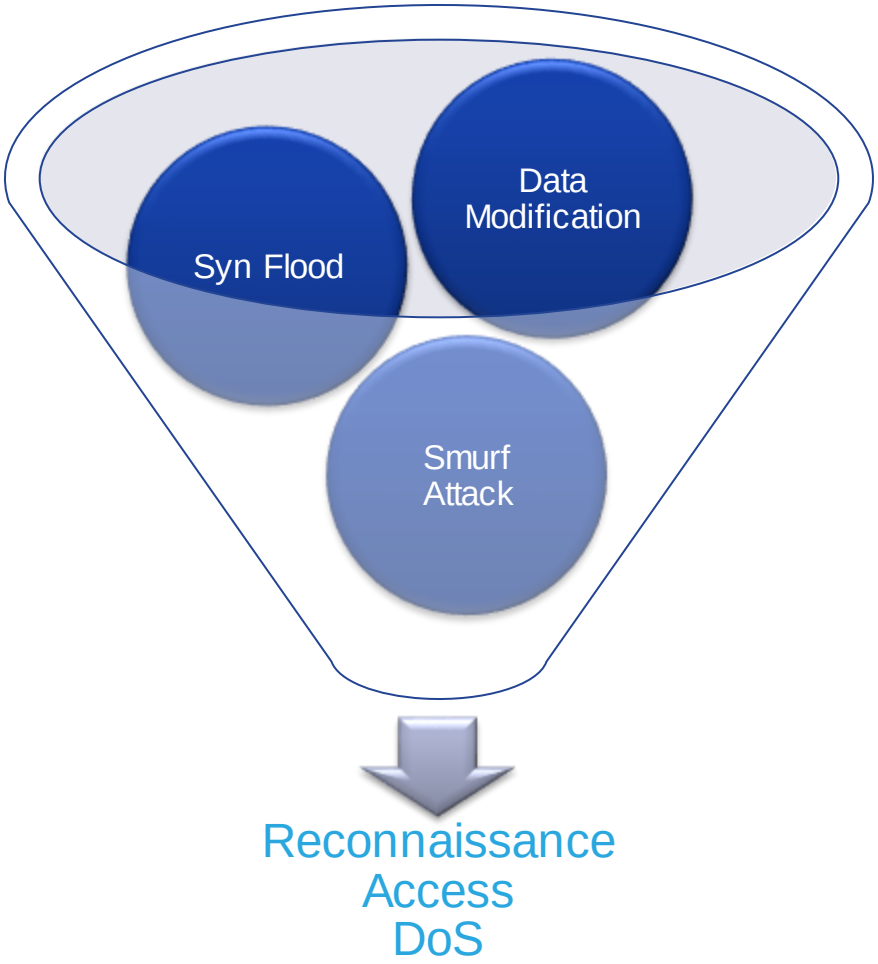
- Enabling vulnerability
- Propagation mechanism
- Payload



Other Malware

Common Network Attacks

Types of Network Attacks



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

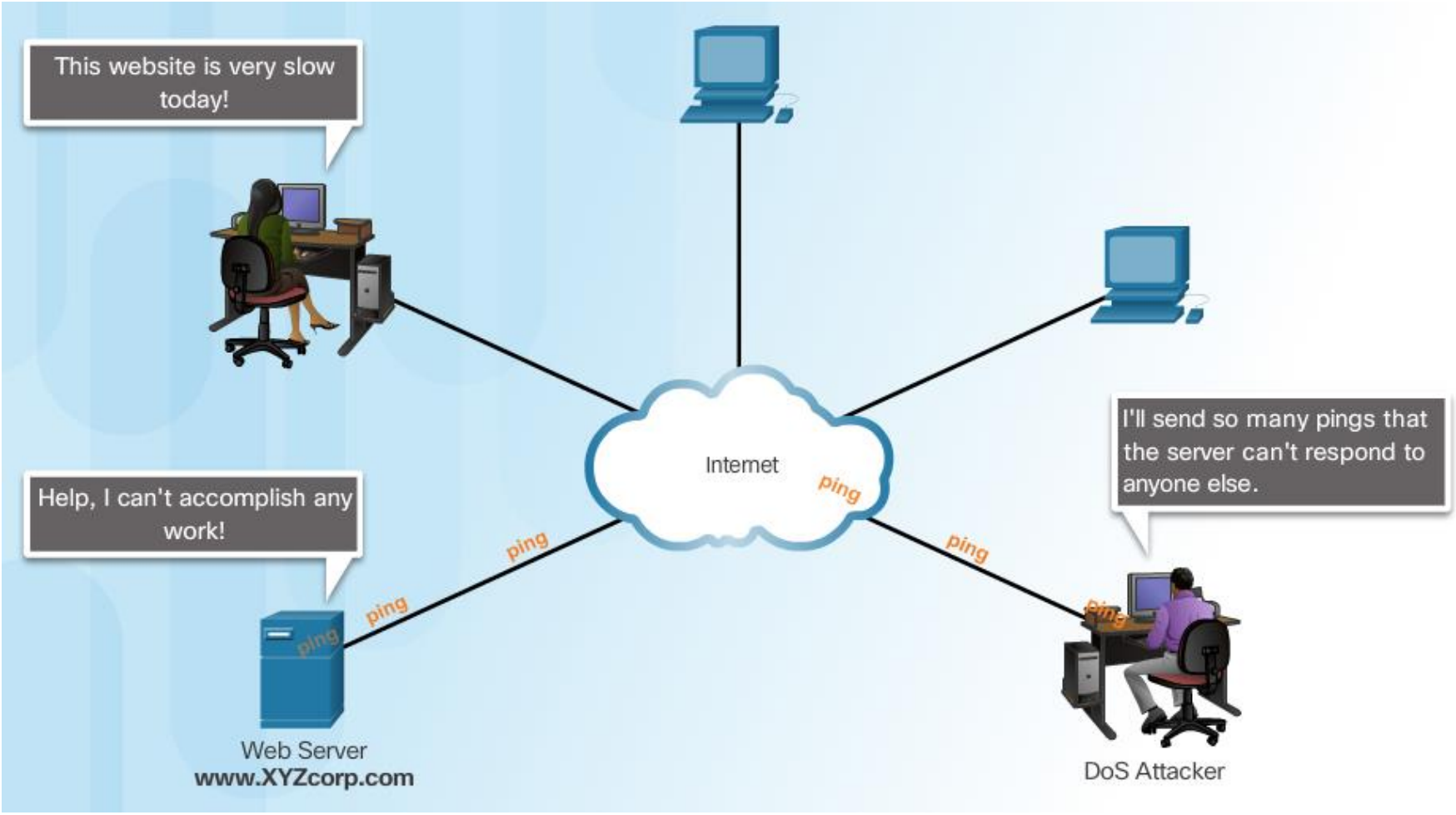
A few types of access attacks include:

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

Social Engineering Attacks

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

Denial of Service (DoS) Attacks



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

Mitigating Threats

Defending the Network

Network Security Professionals

Chief Information Officer (CIO)

Chief Information Security Officer (CISO)

Security Operations (SecOps) Manager

Chief Security Officer (CSO)

Security Manager

Network Security Engineer

Network Security Organizations

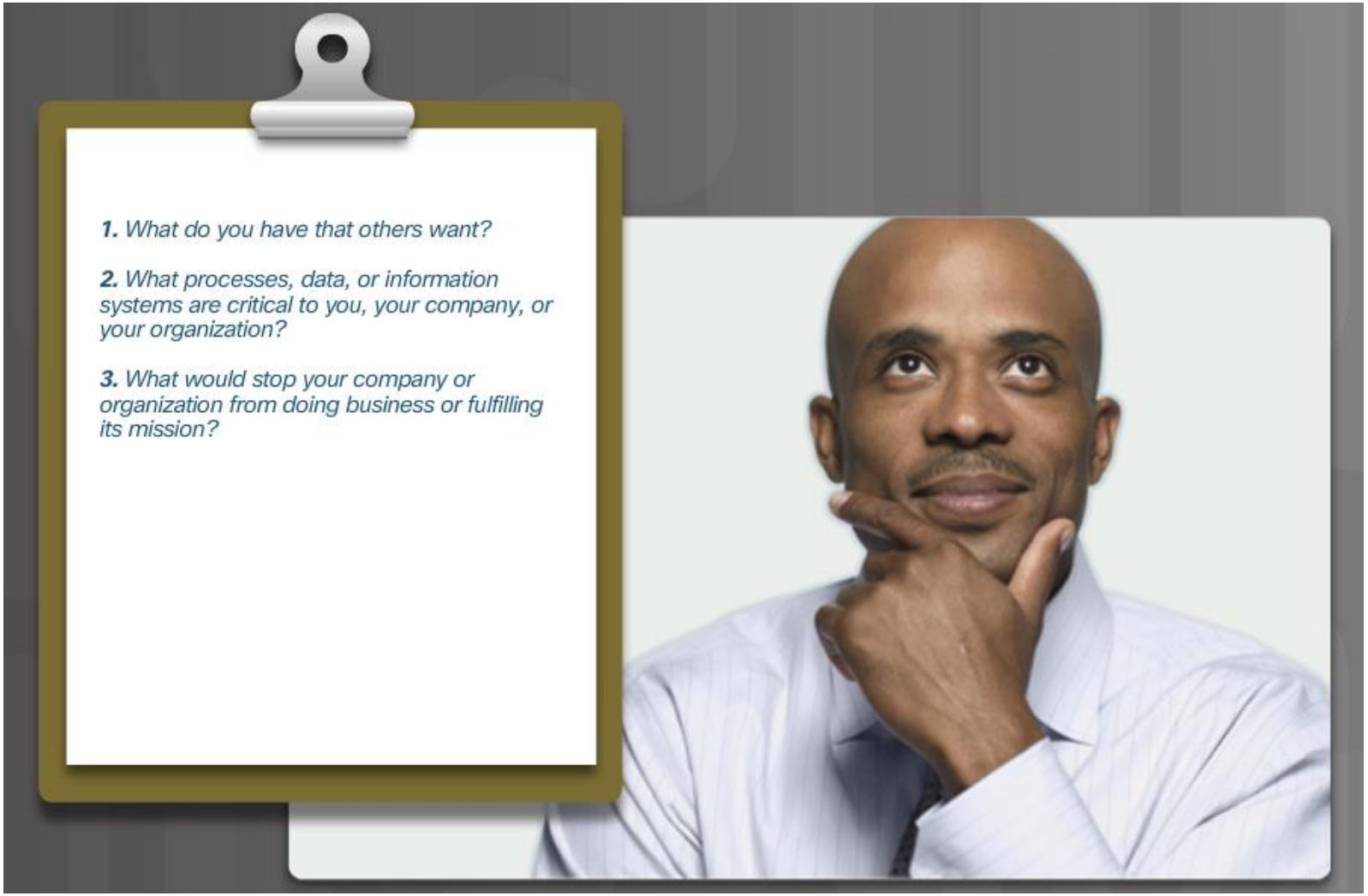
Domains of Network Security

Network Security Domains

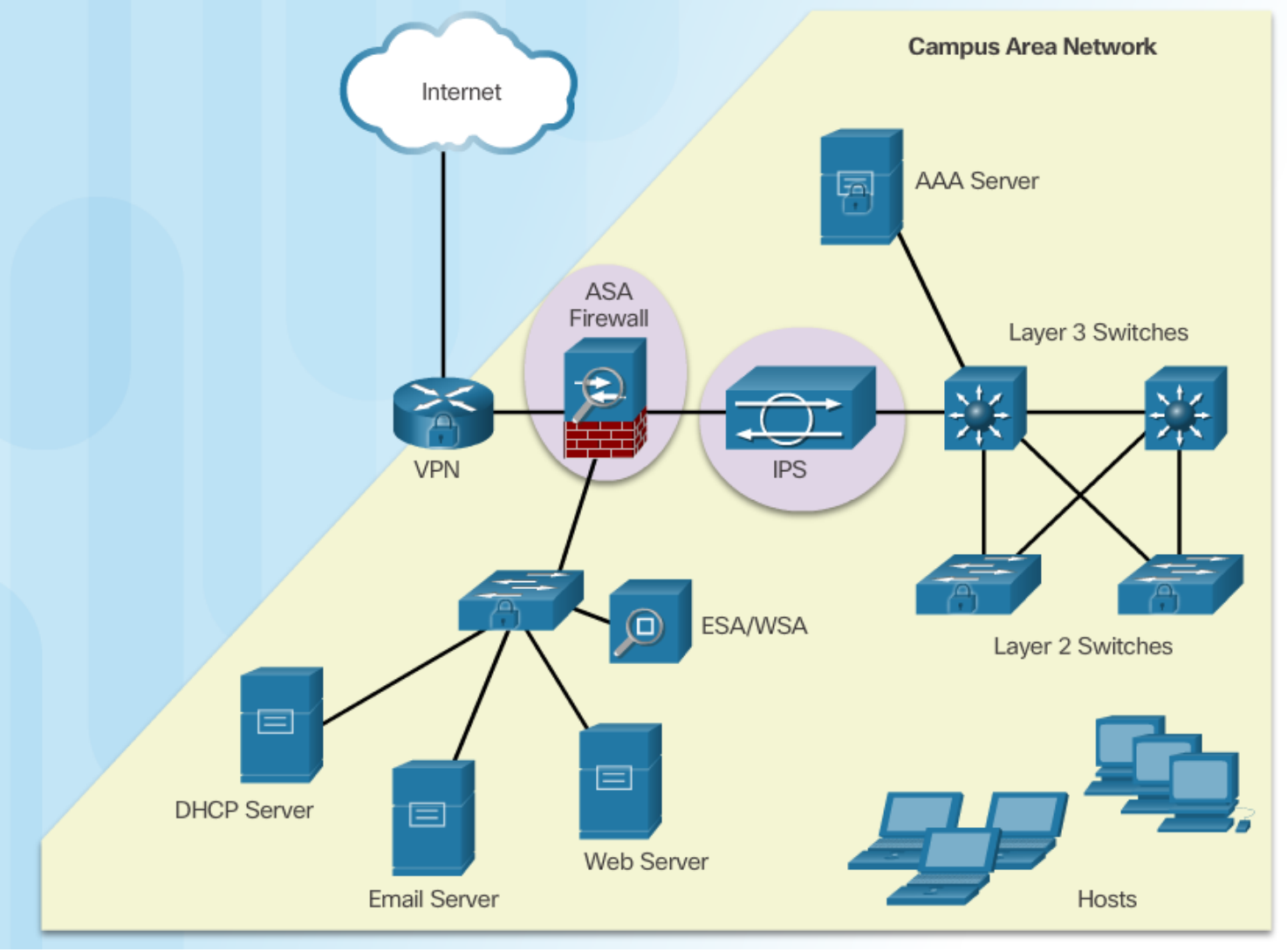
- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Information systems acquisition, development, and maintenance
- Access control
- Information security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

Network Security Policy

Network Security Policy Objectives



Evolution of Network Security Tools



Centralized Context-Aware Network Scanning Element

Defines security policies based on five parameters:

- Type of device being used for access
- Person's identity
- Application in use
- Location
- Time of access

Security Intelligence Operations

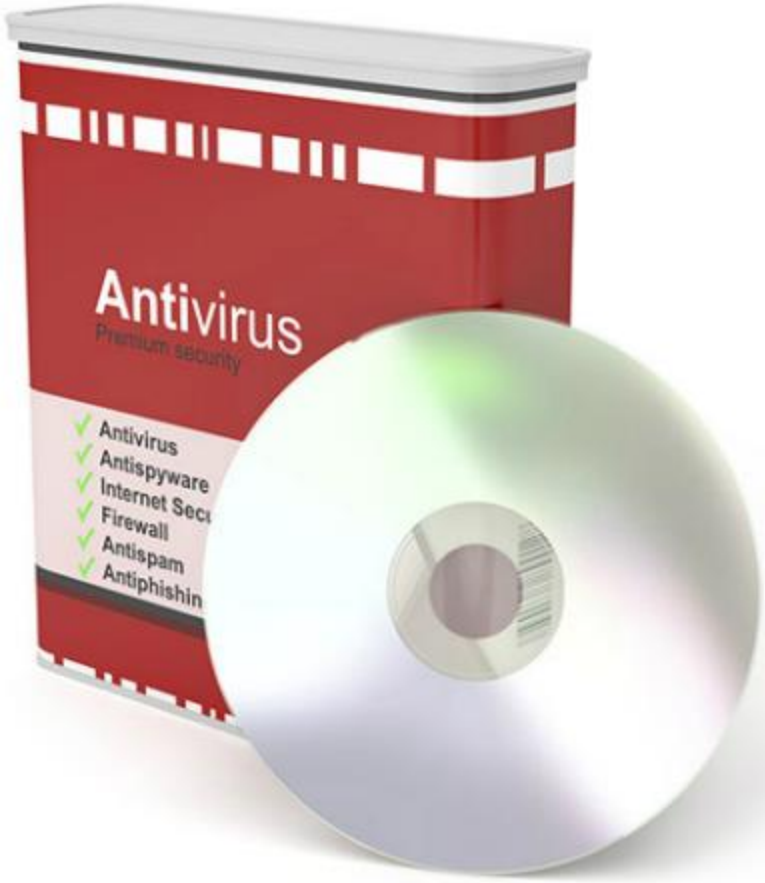
Mitigating Common Network Threats

Defending the Network

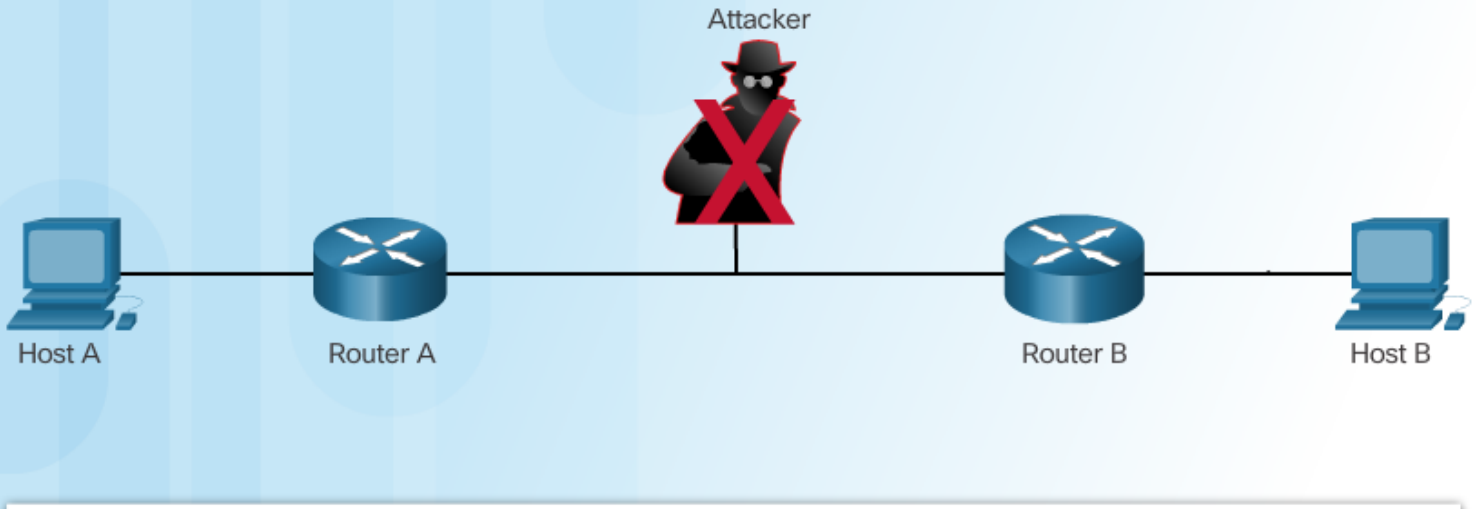
Best practices:

- 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 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

- 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

Thanks for today