

Network Security 1

Module 1 – Overview of Network Security



Learning Objectives

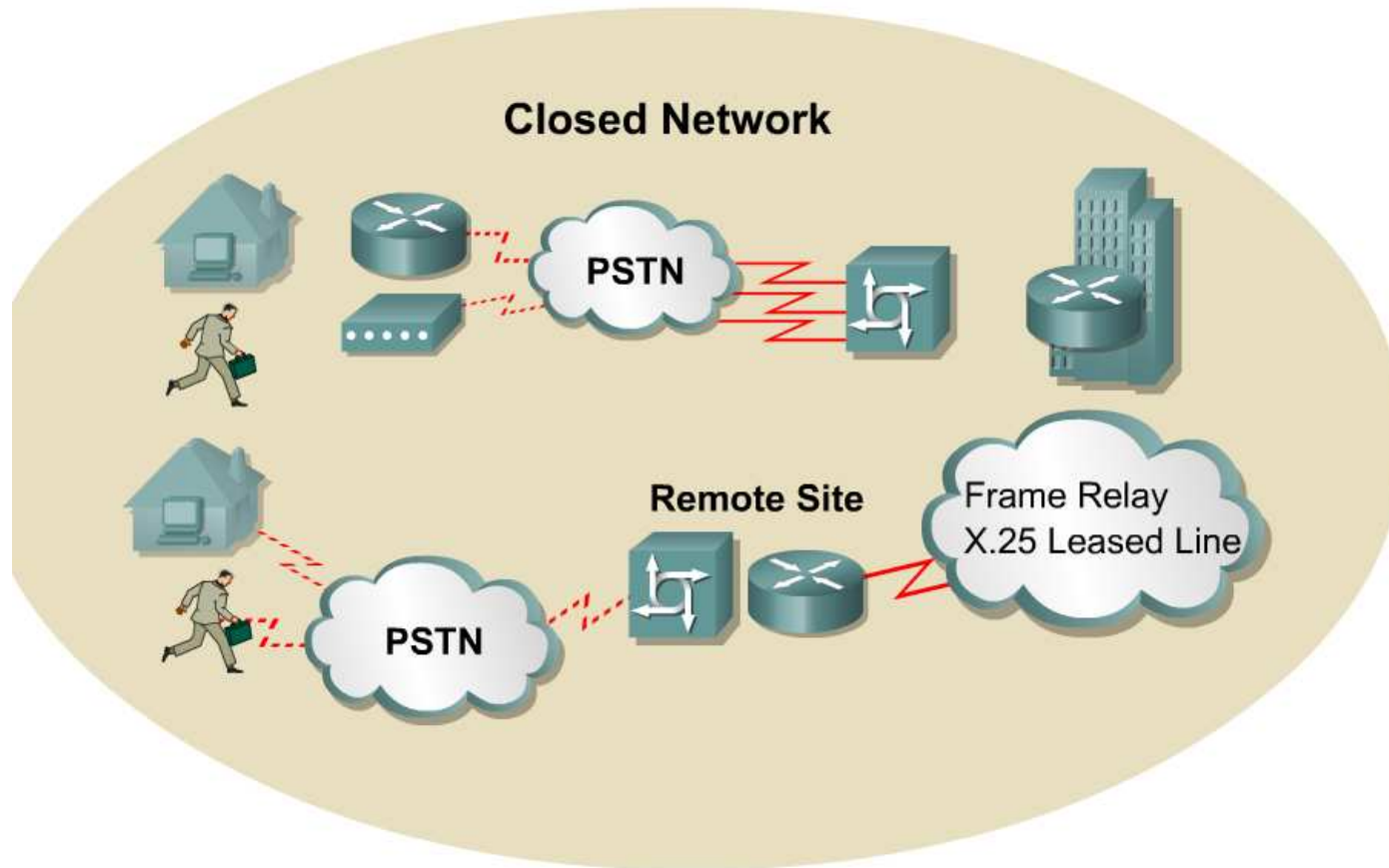


Cisco.com

- 1.1 Introduction to Network Security
- 1.2 Introduction to Vulnerabilities, Threats, and Attacks
- 1.3 Attack Examples
- 1.4 Vulnerability Analysis

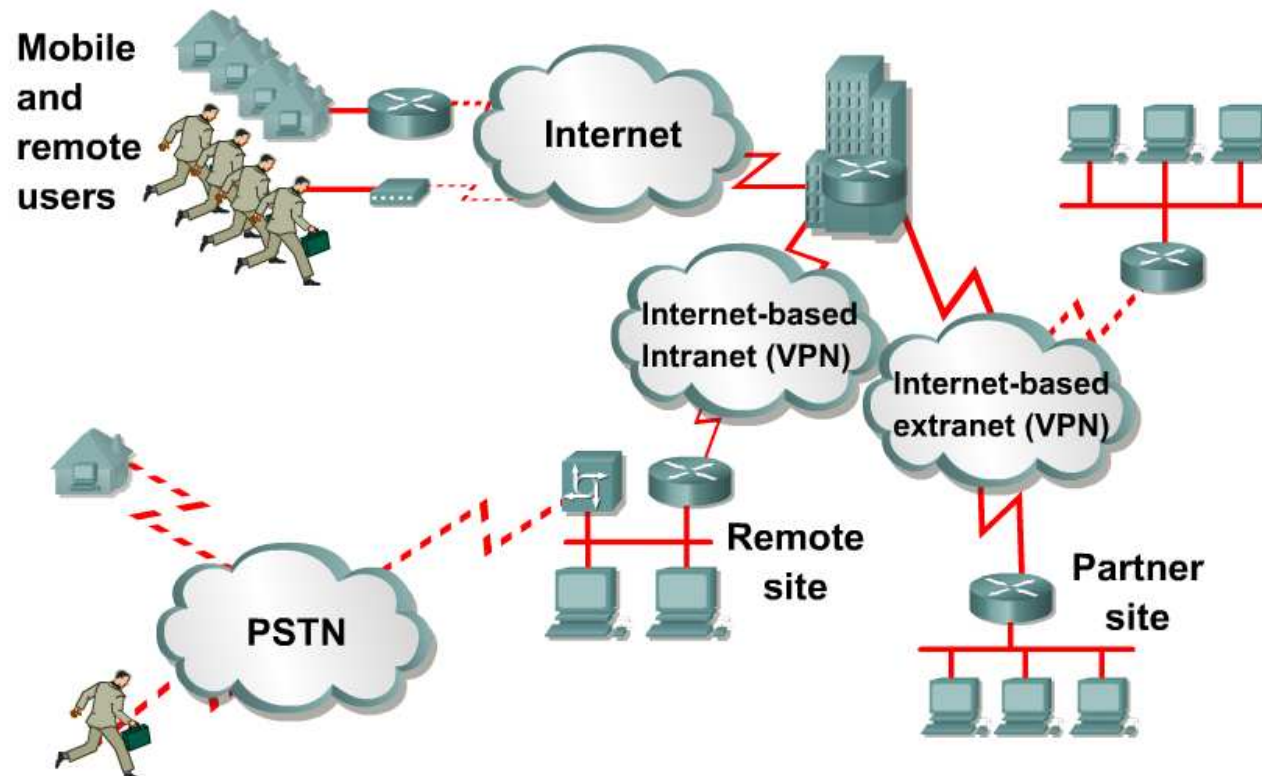


The Closed Network

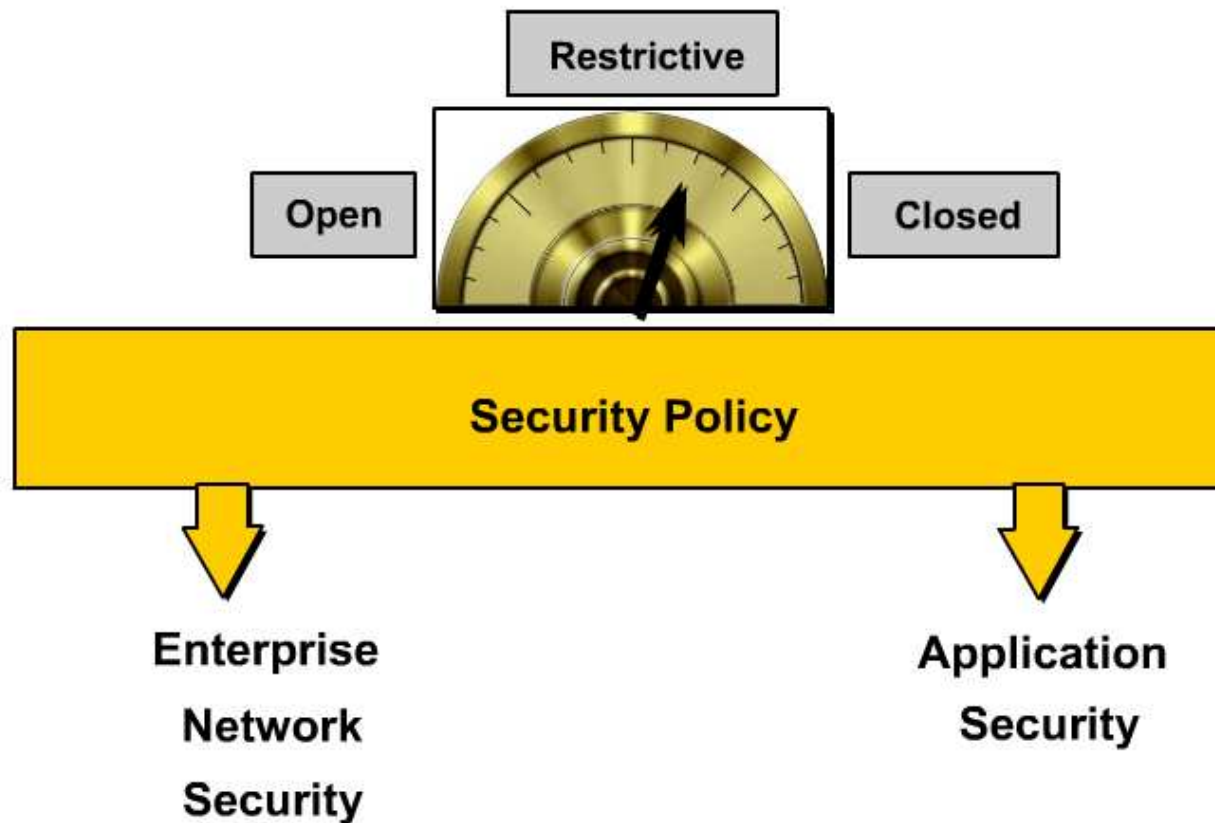


The Network Today

Open Network



Network Security Models



Trends that Affect Security



Cisco.com

- Increase of network attacks
- Increased sophistication of attacks
- Increased dependence on the network
- Lack of trained personnel
- Lack of awareness
- Lack of security policies
- Wireless access
- Legislation
- Litigation



Module 1 – Overview of Network Security

1.2 Introduction to Vulnerabilities, Threats, and Attacks



Network Vulnerabilities

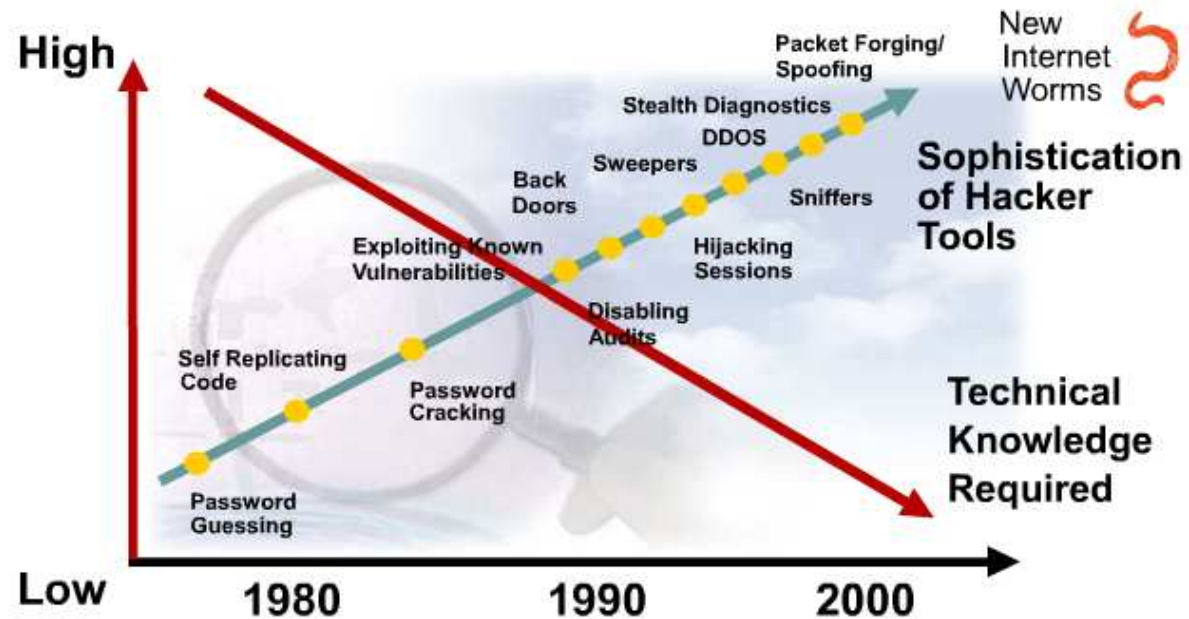


Cisco.com

- Technology
- Configuration
- Policy



Threat Capabilities—More Dangerous and Easier to Use



Threats continue to become more sophisticated as the technical knowledge required to implement attacks diminishes.



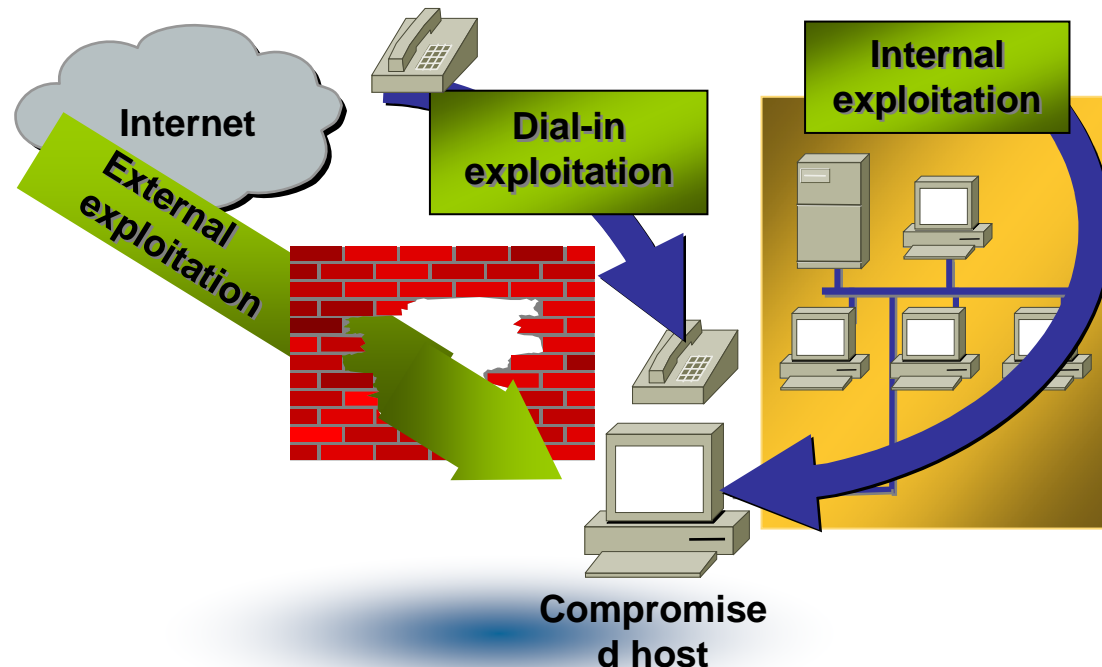
Module 1 – Overview of Network Security

1.3 Attack Examples



Network Threats

- There are four general categories of security threats to the network:
 - Unstructured threats
 - Structured threats
 - External threats
 - Internal threats



Four Classes of Network Attacks



Cisco.com

- Reconnaissance attacks
- Access attacks
- Denial of service attacks
- Worms, viruses, and Trojan horses



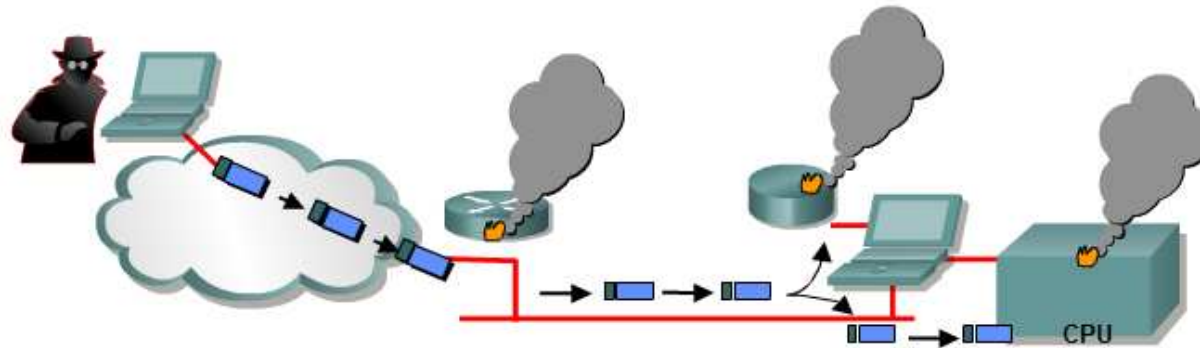
Specific Attack Types

- All of the following can be used to compromise your system:
 - Packet sniffers
 - IP weaknesses
 - Password attacks
 - DoS or DDoS
 - Man-in-the-middle attacks
 - Application layer attacks
 - Trust exploitation
 - Port redirection
 - Virus
 - Trojan horse
 - Operator error
 - Worms



DoS Attacks

DoS attacks prevent authorized people from using a service by using up system resources.



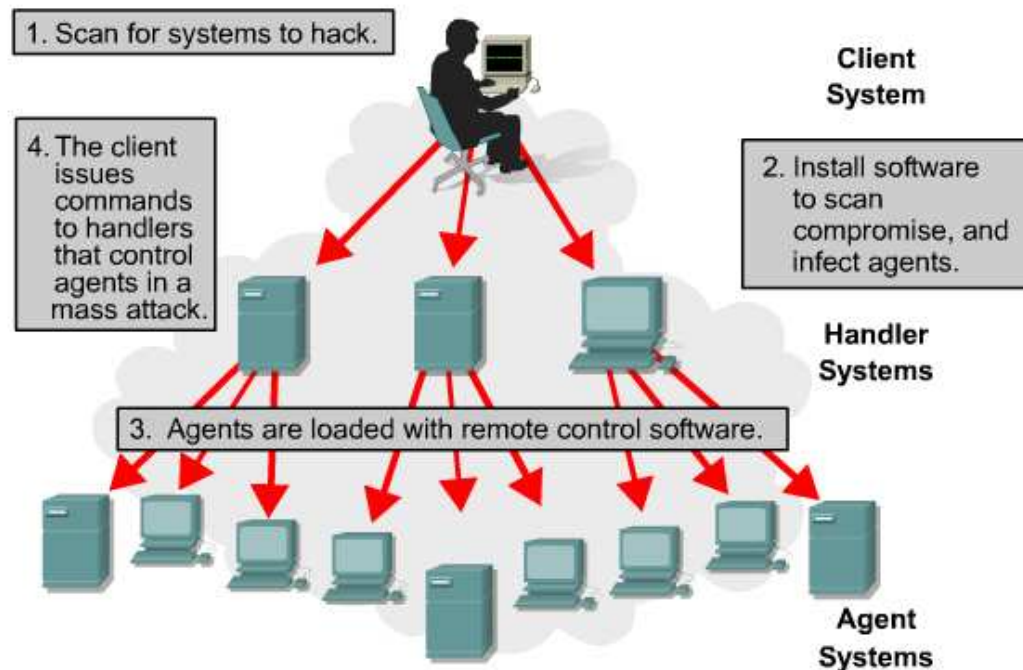
Resource overloads

- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

Malformed data

- Oversized packets: ping of death, and so on.
- Overlapping packets: winuke, and so on.
- Un-handled data: teardrop, and so on.

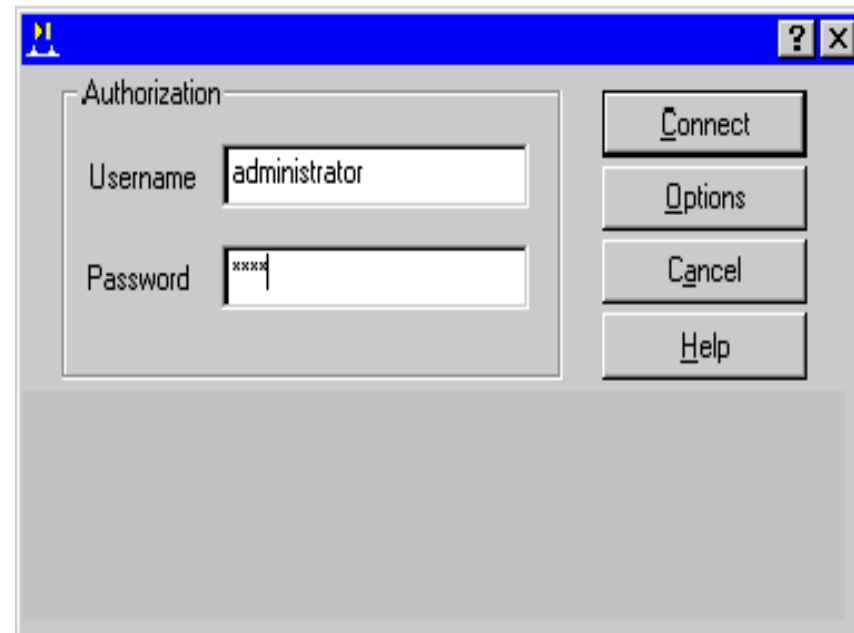
DDoS Attack Example



In a Distributed Denial of Service attack (DDoS) a hacker tricks other machines into flooding the target machine with nuisance traffic that robs system performance.

Password Attacks

- Hackers can implement password attacks using several different methods:
 - Brute-force attacks
 - Dictionary Attacks
 - Trojan horse programs
 - IP spoofing
 - Packet sniffers



Password Attack Example

- L0phtCrack can take the hashes of passwords and generate the clear text passwords from them.
Passwords are computed using two different methods:
 - Dictionary cracking
 - Brute force computation

The screenshot shows the L0phtCrack application window. The main window displays a list of users and their corresponding LM hashes and passwords. An 'Auditing Options For This Session' dialog box is open, showing settings for Dictionary Crack, Dictionary/Brute Hybrid Crack, and Brute Force Crack.

User Name	LM Password	<8	>8	LM Password	Audit Time
Administrator		x			
boone.speed	DRAMATIC		x	dramat1	Cd 3f 0m 57s
chris.shaine	AGE18	x		ace18	Cd 3f 1m 0s
dale.goddard	UNCRACK??????				
dave.grahan	CARTILAGINOLS			cartilaginous	Cd 3f 0m 2s
Guest	AUTHORITARIAN				Cd 3f 0m 1s
larry.moffat					
klem.boscot					
lunn.hill					
patric.edinger					
scott.ranklin					
wuji.hirajana					

Auditing Options For This Session

Dictionary Crack:
 Enabled
Word file: C:\Program Files\Security Software T...
The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack:
 Enabled
2 Characters to vary (more is slower)
The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as 'Dane99' or 'monkey!' This test is fast and finds weak passwords.

Brute Force Crack:
 Enabled
Character Set: A-Z and 0-9
 Distributed
For: 1 or 2
The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as 'wef0pl0s' or 'vCE&00+12b'. This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.



Password Attacks Mitigation



Cisco.com

- The following are mitigation techniques:
 - Do not allow users to use the same password on multiple systems.
 - Disable accounts after a certain number of unsuccessful login attempts.
 - Do not use plain text passwords. OTP or a cryptographic password is recommended.
 - Use “strong” passwords. Strong passwords are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.



Virus and Trojan Horses



Cisco.com

- Viruses refer to malicious software that are attached to another program to execute a particular unwanted function on a user's workstation. End-user workstations are the primary targets.
- A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. A Trojan horse is mitigated by antivirus software at the user level and possibly the network level.



Vulnerabilities Exist at all OSI Layers



Cisco.com



Auto Secure

To secure the management and forwarding planes of the router, use the auto secure command in privileged EXEC mode.

```
auto secure [management | forwarding]
           [no-interact]
```

Syntax Description

- `management` (Optional) Only the management plane will be secured.
- `forwarding` (Optional) Only the forwarding plane will be secured.
- `no-interact` (Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.



CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION