Cisco Systems
Networking Academy

Cisco.com

Network Security 1

Module 1 – Overview of Network Security

CCNA CISCO CERTIFIED ™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Learning Objectives

Cisco.com

–1.1 Introduction to Network Security

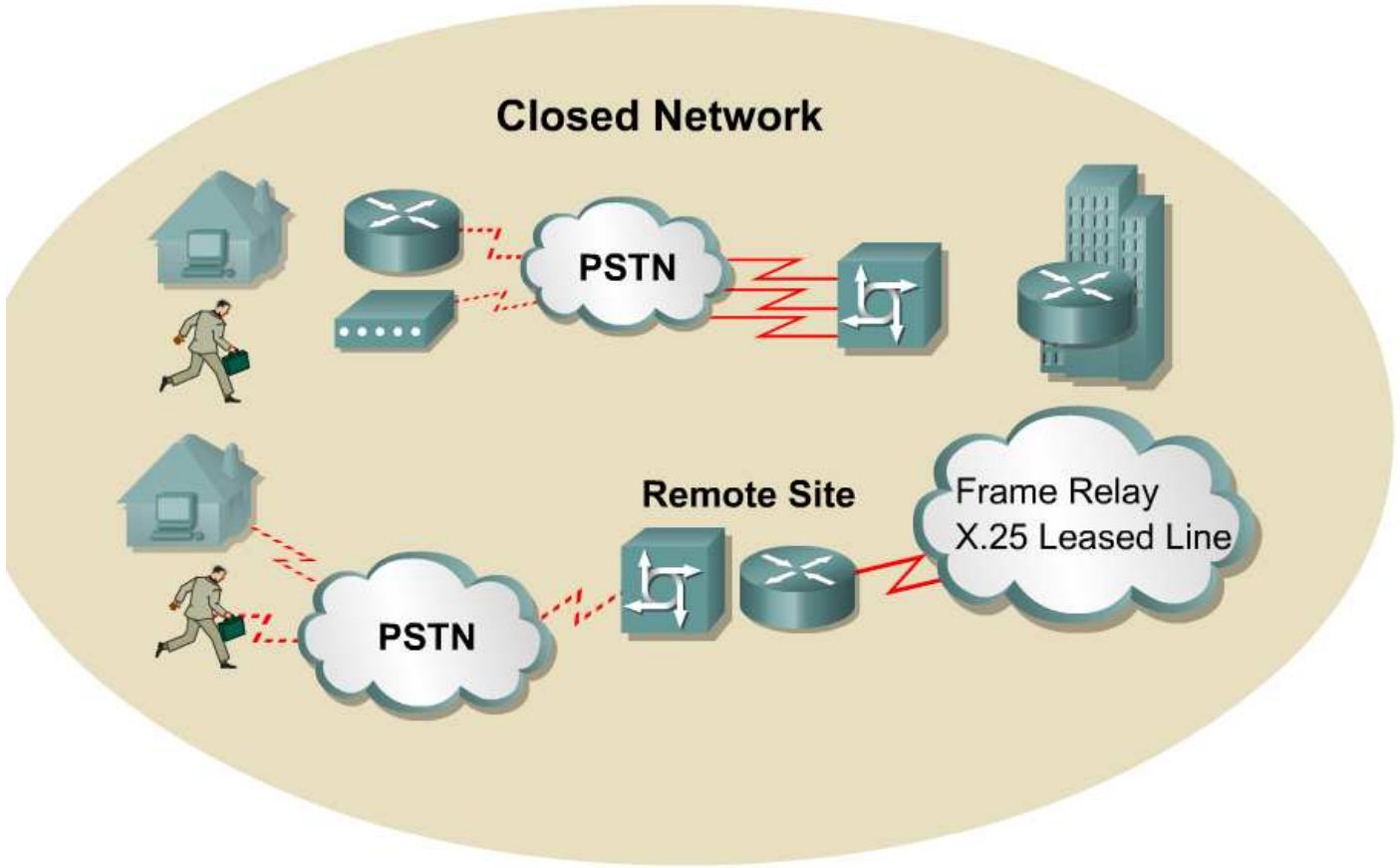
–1.2 Introduction to Vulnerabilities, Threats, and Attacks

–1.3 Attack Examples

–1.4 Vulnerability Analysis

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

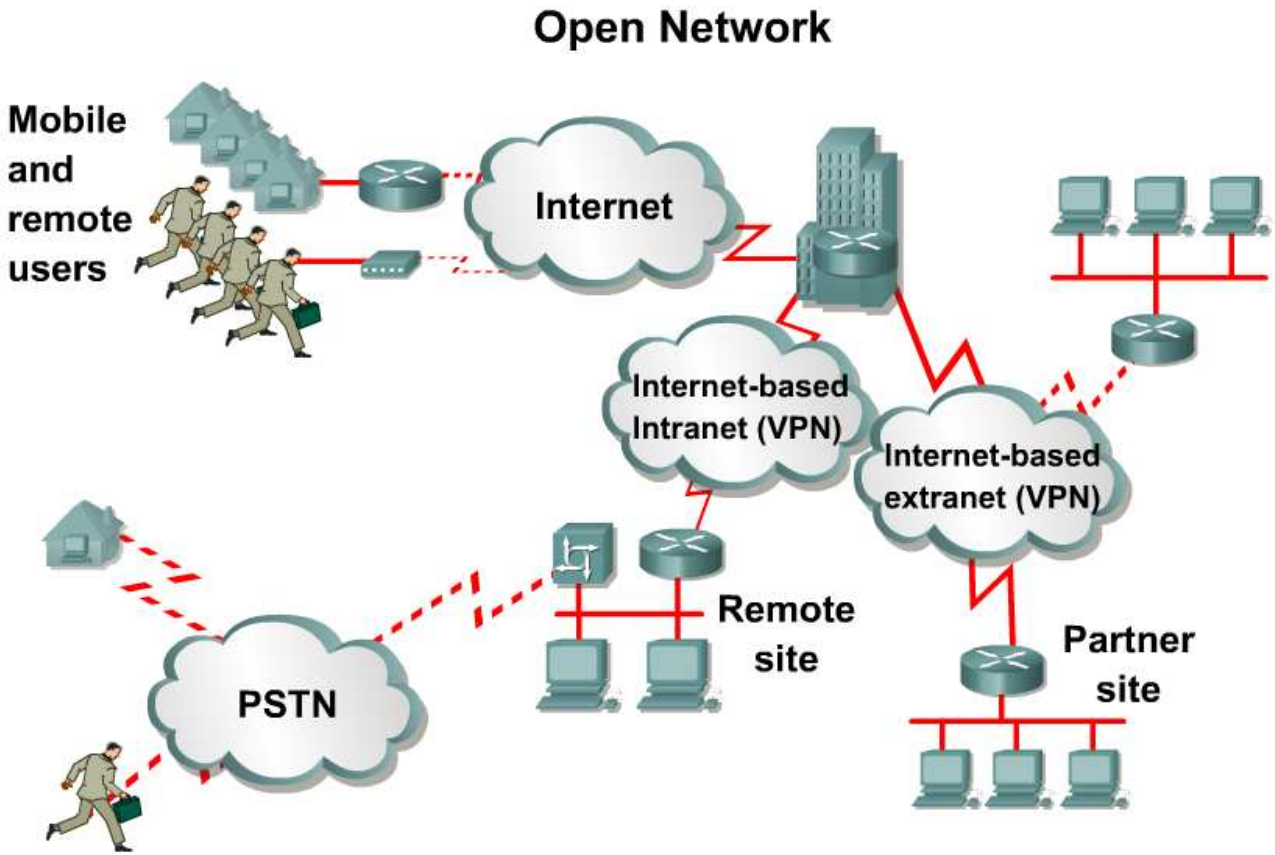
The Closed Network



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

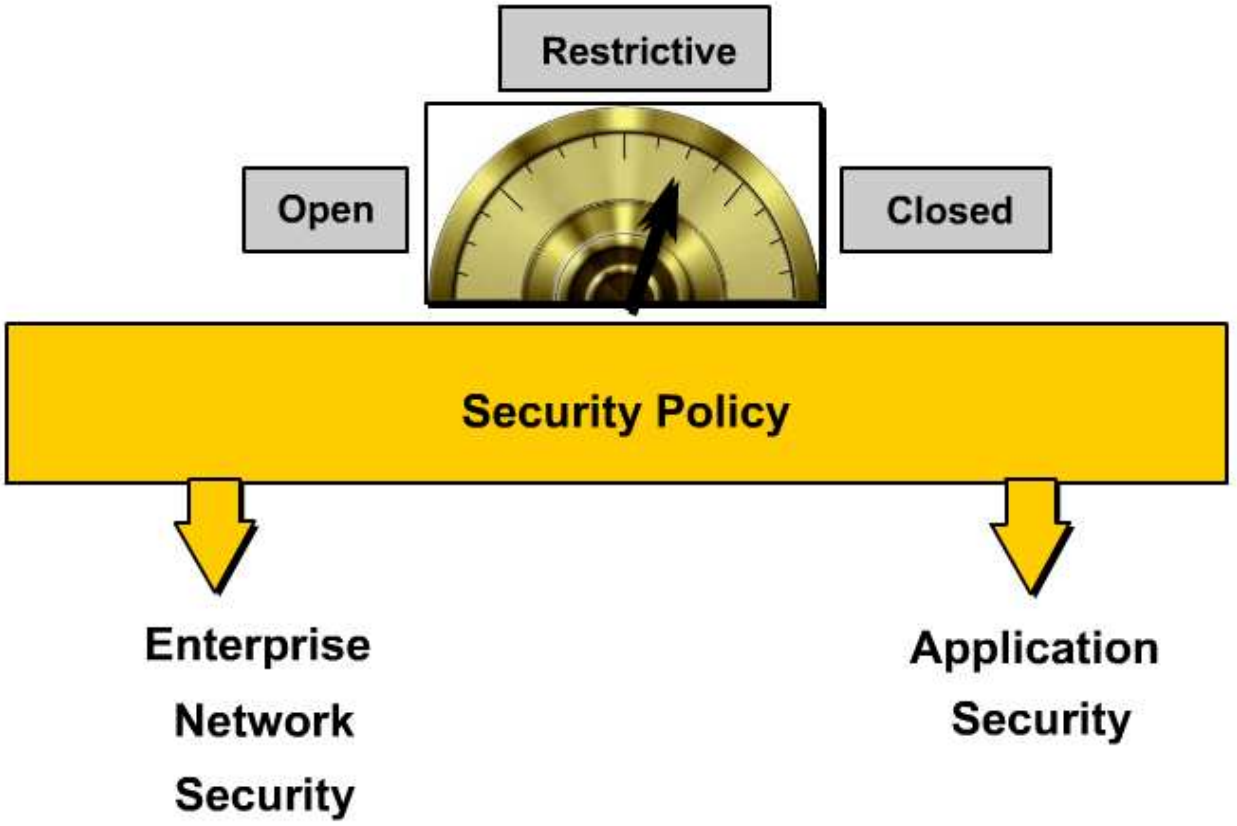
The Network Today

Cisco.com



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Network Security Models



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

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

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Overview of Network Security

1.2 Introduction to Vulnerabilities, Threats, and Attacks

CCNA CISCO CERTIFIED ™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

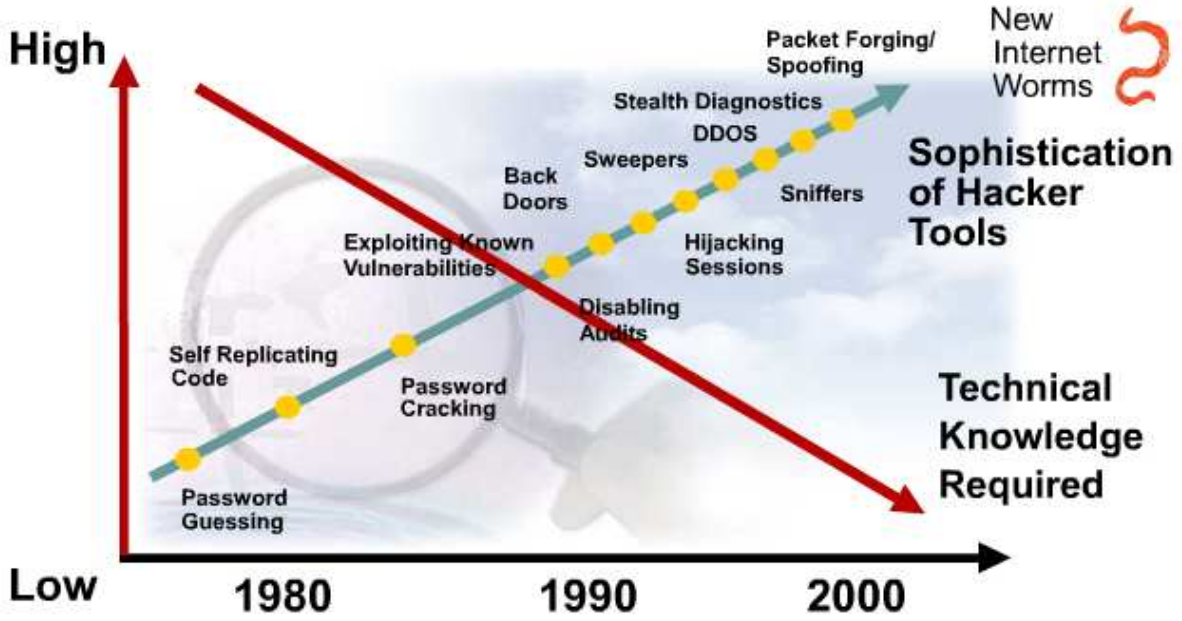
Network Vulnerabilities

Cisco.com

- Technology
- Configuration
- Policy

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Threat Capabilities—More Dangerous and Easier to Use



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

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Overview of Network Security

1.3 Attack Examples

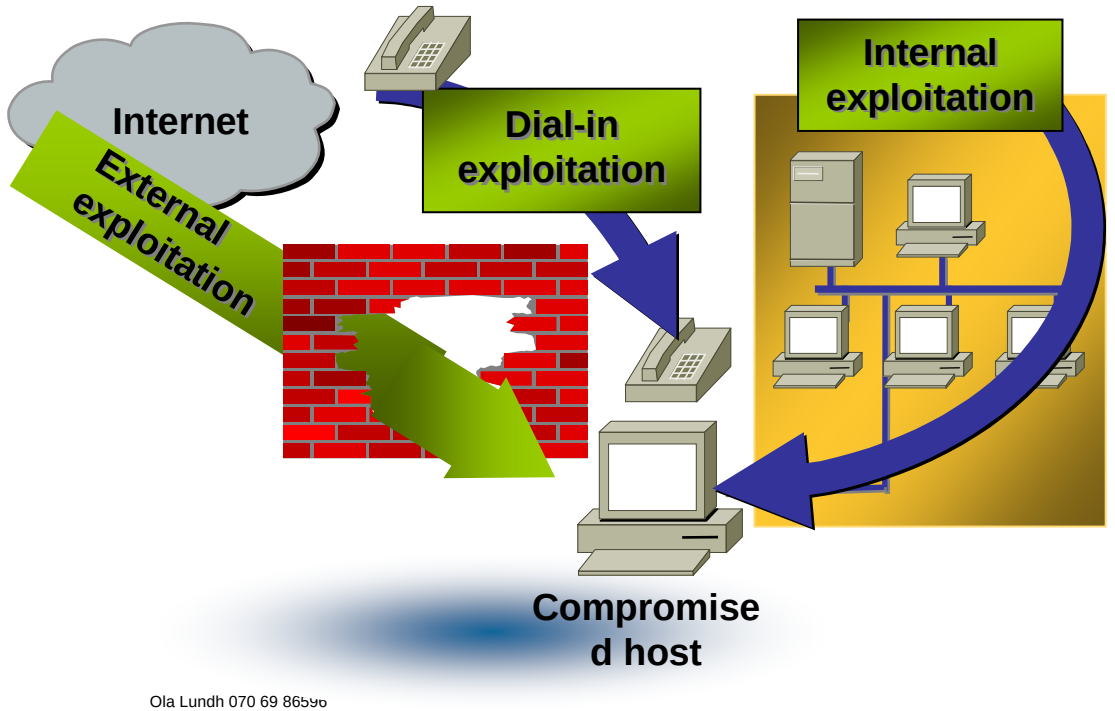
CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Network Threats

Cisco.com

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



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Four Classes of Network Attacks

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

CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Specific Attack Types

Cisco.com

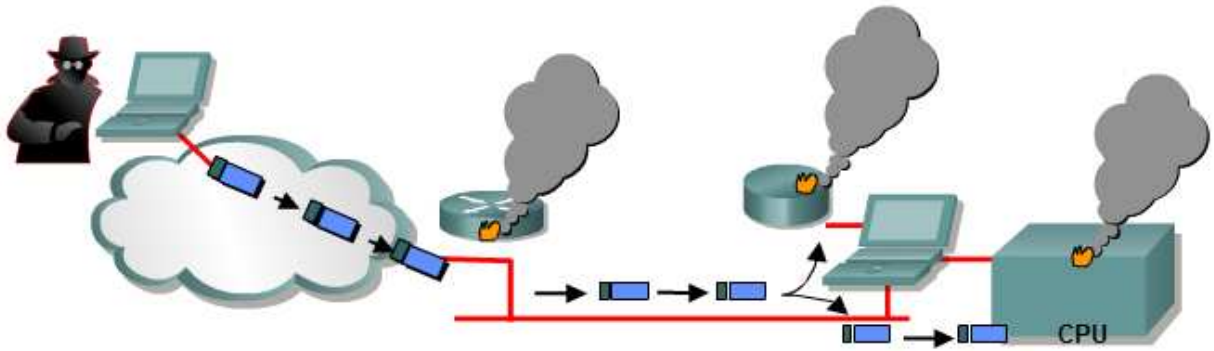
- All of the following can be used to compromise your system:
  - Packet sniffers
  - IP weaknesses
  - Password attacks
  - DoS or DDoS
  - Man-in-the-middle attacks
  - Application layer attacks
  - Trust exploitation
  - Port redirection
  - Virus
  - Trojan horse
  - Operator error
  - Worms

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

DoS Attacks

Cisco.com

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



Resource overloads

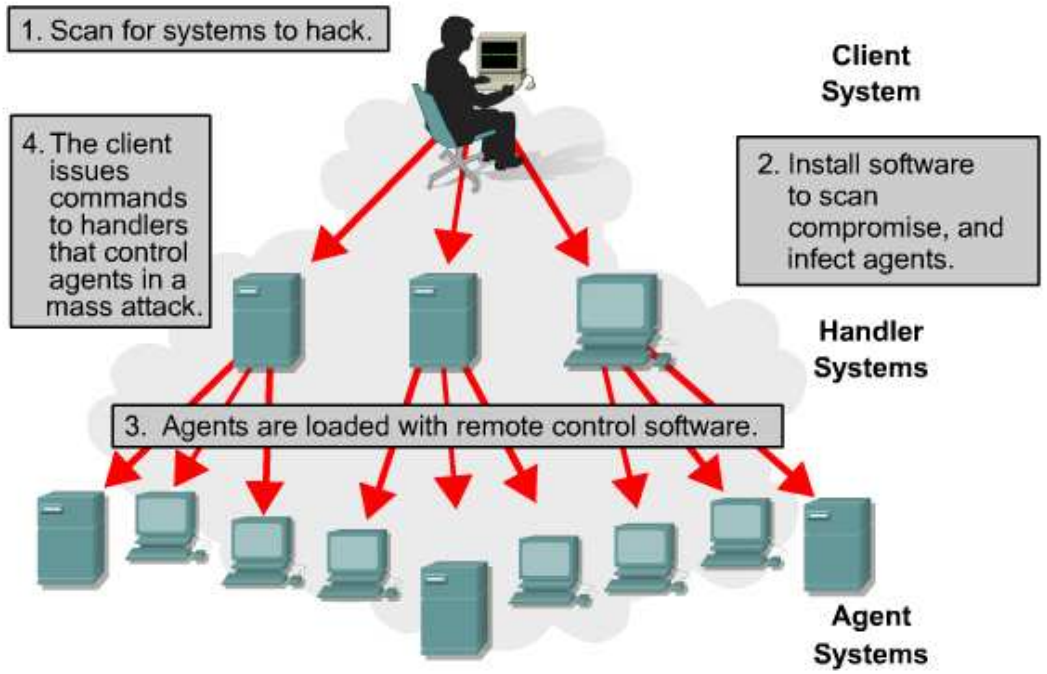
- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

Malformed data

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

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

DDoS Attack Example

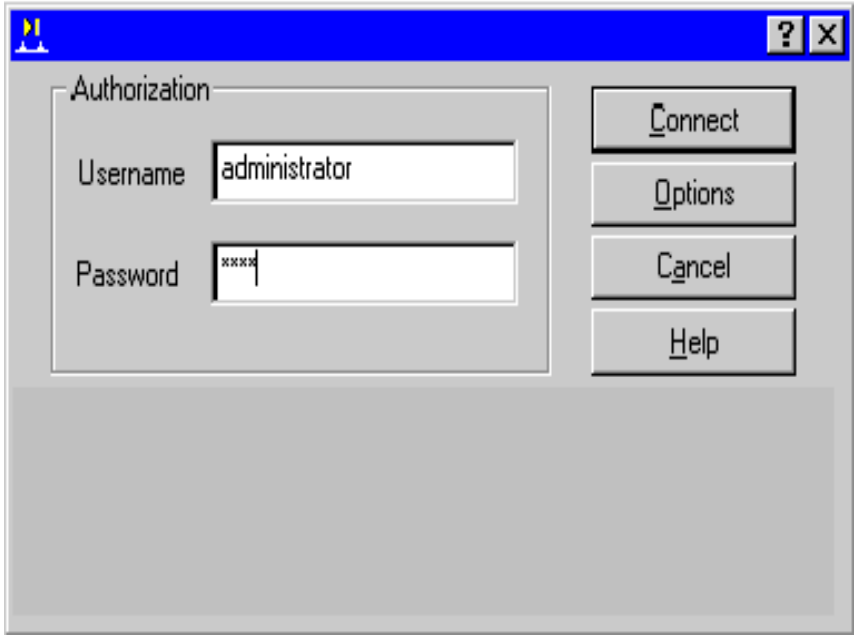


In a Distributed Denial of Service attack (DDoS) a hacker tricks other machines into flooding the target machine with nuisance traffic that robs system performance.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Password Attacks

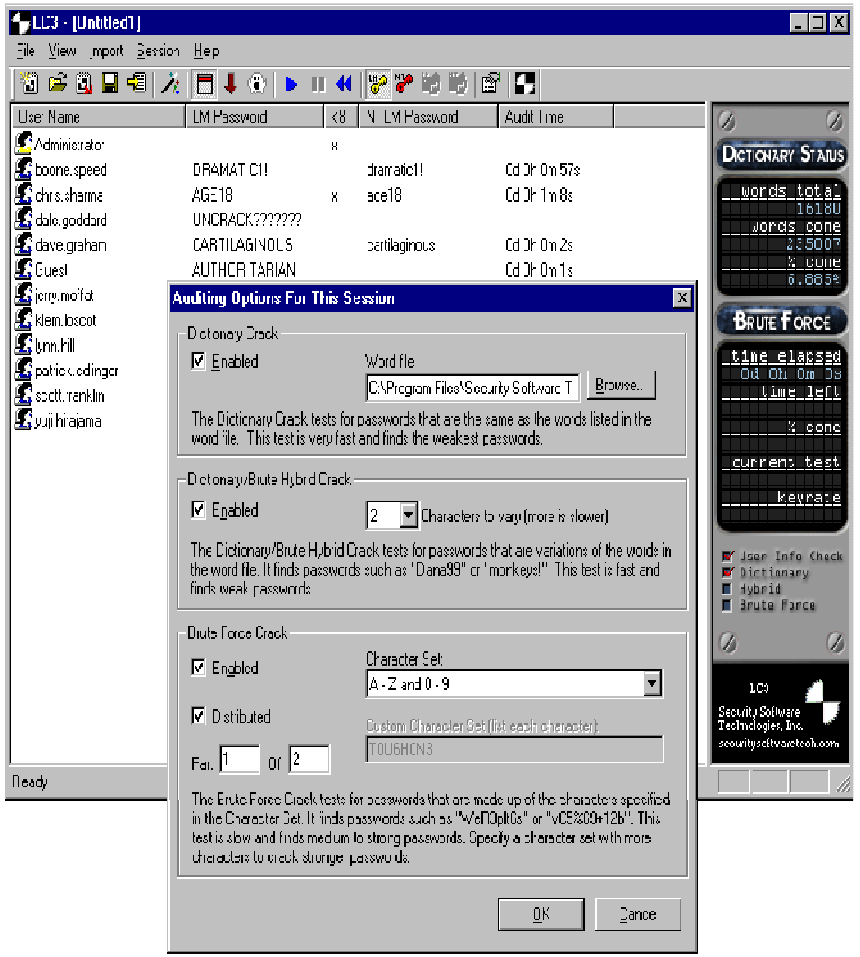
- Hackers can implement password attacks using several different methods:
  - Brute-force attacks
  - Dictionary Attacks
  - Trojan horse programs
  - IP spoofing
  - Packet sniffers



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

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



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Password Attacks Mitigation

- 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.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Virus and Trojan Horses

- 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.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Vulnerabilities Exist at all OSI Layers

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

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.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

© 2005, Cisco Systems, Inc. All rights reserved.