Network Security

Cisco.com

- Ola Lundh
- ola.lundh@hh.se
- Schedule/ time-table: landris.hh.se/ (NetwoSec)
- Course home-page: hh.se/english/ide/education/student/coursewebpages/networksecurity
- cisco.netacad.net
  - Packet Tracer
    - *.pka find them under ”Tools”
  - Study guides
    - Find them under ”File Sharing”

Network Security

Cisco.com

- Eight lab-groups
- Some of them Swedish
- Fill in your name and e-mail IN BLOCK LETTERS
- Also fill in your Cisco login-name (if you have one)

Network Security

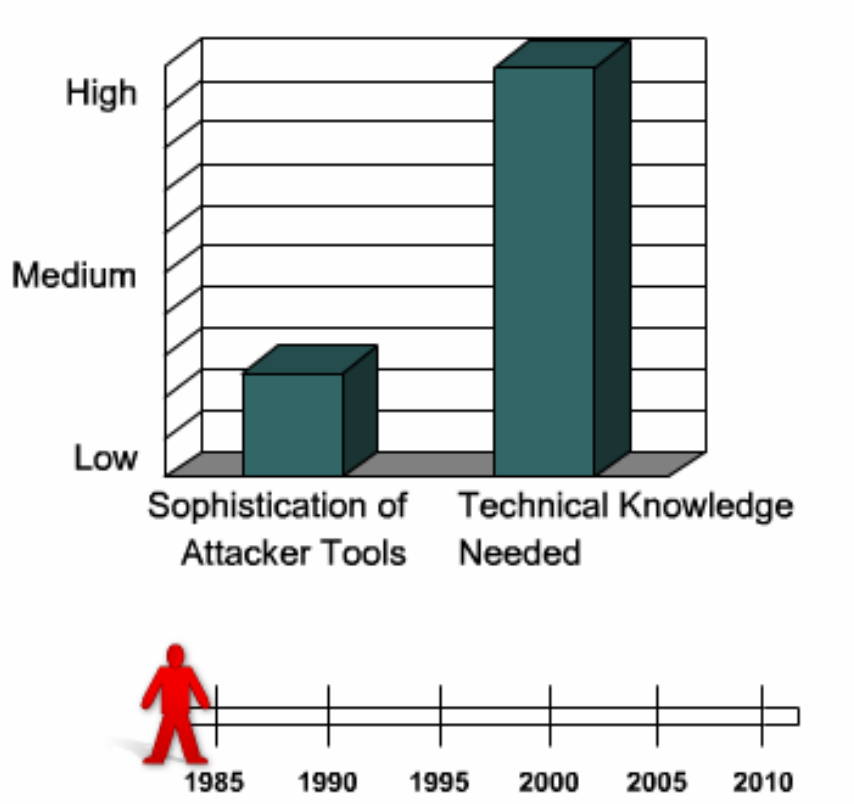
Cisco.com

- 1 Pass the course =>
  - Pass Written exam week 11
  - Pass Labs

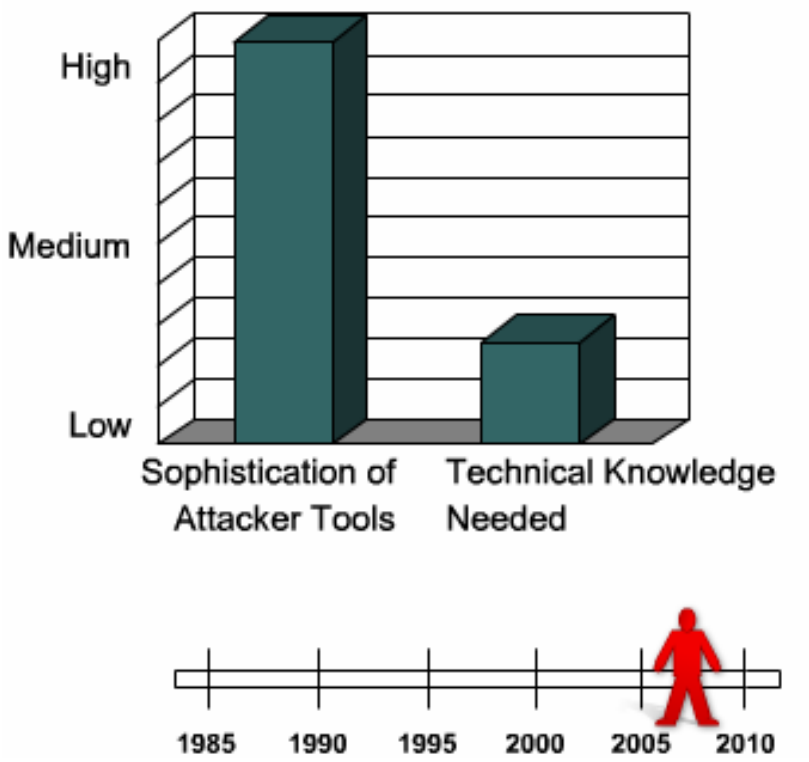
Network Security

- Protocols
- Technologies
- Devices
- Tools
- Techniques
- Secure data
- Mitigate threats

Network Security



Network Security

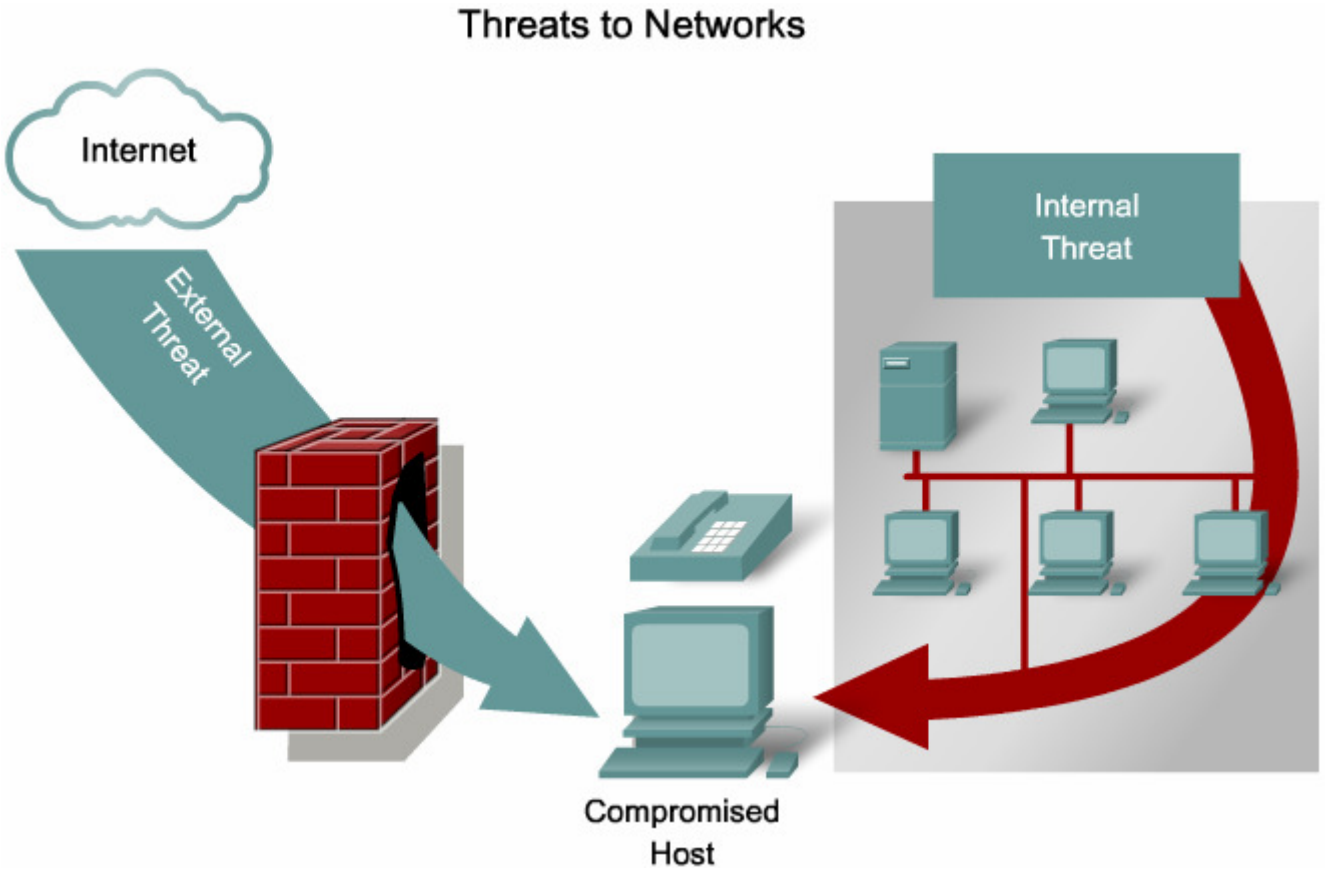


Network Security

- IDS provides real-time detection of certain types of attacks while they are in progress.
- IPS devices enable the detection of malicious activity and have the ability to automatically block the attack in real-time.
- For organizations that do not require a dedicated firewall, modern routers, like the Cisco Integrated Services Router (ISR), can be used as sophisticated stateful firewalls.

Network Security

Cisco.com



Network Security

- Each type – corresponding proocol - hide
- Cryptography
  - Wireless
  - VoIP
  - Computerfiles

Network Security

- Information security
  - Confidentiality
    - Encryption
  - Integrity
    - Hashing mechanisms
  - Availability
    - Network hardening
    - Backup

Domains of Network Security

Cisco.com

1. Risk assessment
2. Security policy
3. Organization of Information Security
4. Asset management
5. Human resources Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access control
9. Information Systems Acquisition, Development and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

Domains of Network Security

1. Risk assessment

This is the first step in the risk management process. It determines the quantitative and qualitative value of risk related to a specific situation or recognized threat.

Domains of Network Security

2. Security policy

A document that addresses the constraints and behaviors of members of an organization and often specifies how data can be accessed and what data is accessible by whom.

Domains of Network Security

3. Organization of Information Security

This is the governance model set out by an organization for information security.

Domains of Network Security

4. Asset management

This is an inventory of and classification scheme for information assets.

Domains of Network Security

5. Human resources Security

This addresses security procedures relating to employees joining, moving within, and leaving an organization.

Domains of Network Security

6. Physical and Environmental Security

This describes the protection of the computer facilities within an organization.

Domains of Network Security

7. Communications and Operations Management

This describes the management of technical security controls in systems and networks.

Domains of Network Security

8. Access control

This describes the restriction of access rights to networks, systems, applications, functions, and data.

Domains of Network Security

9. Information Systems Acquisition, Development and Maintenance

This describes the integration of security into applications.

Domains of Network Security

Cisco.com

10. Information Security Incident Management

This describes how to anticipate and respond to information security breaches.

Domains of Network Security

11. Business Continuity Management

This describes the protection, maintenance, and recovery of business-critical processes and systems.

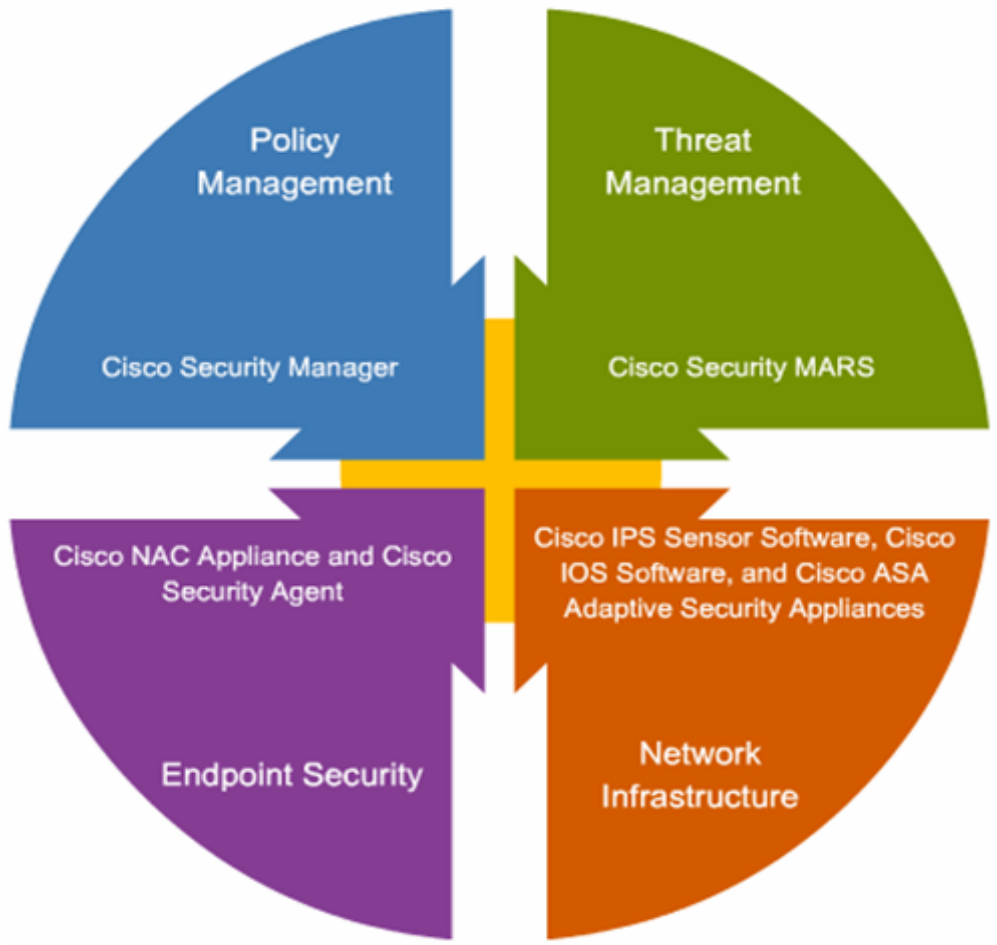
Domains of Network Security

12. Compliance

This describes the process of ensuring conformance with information security policies, standards, and regulations.

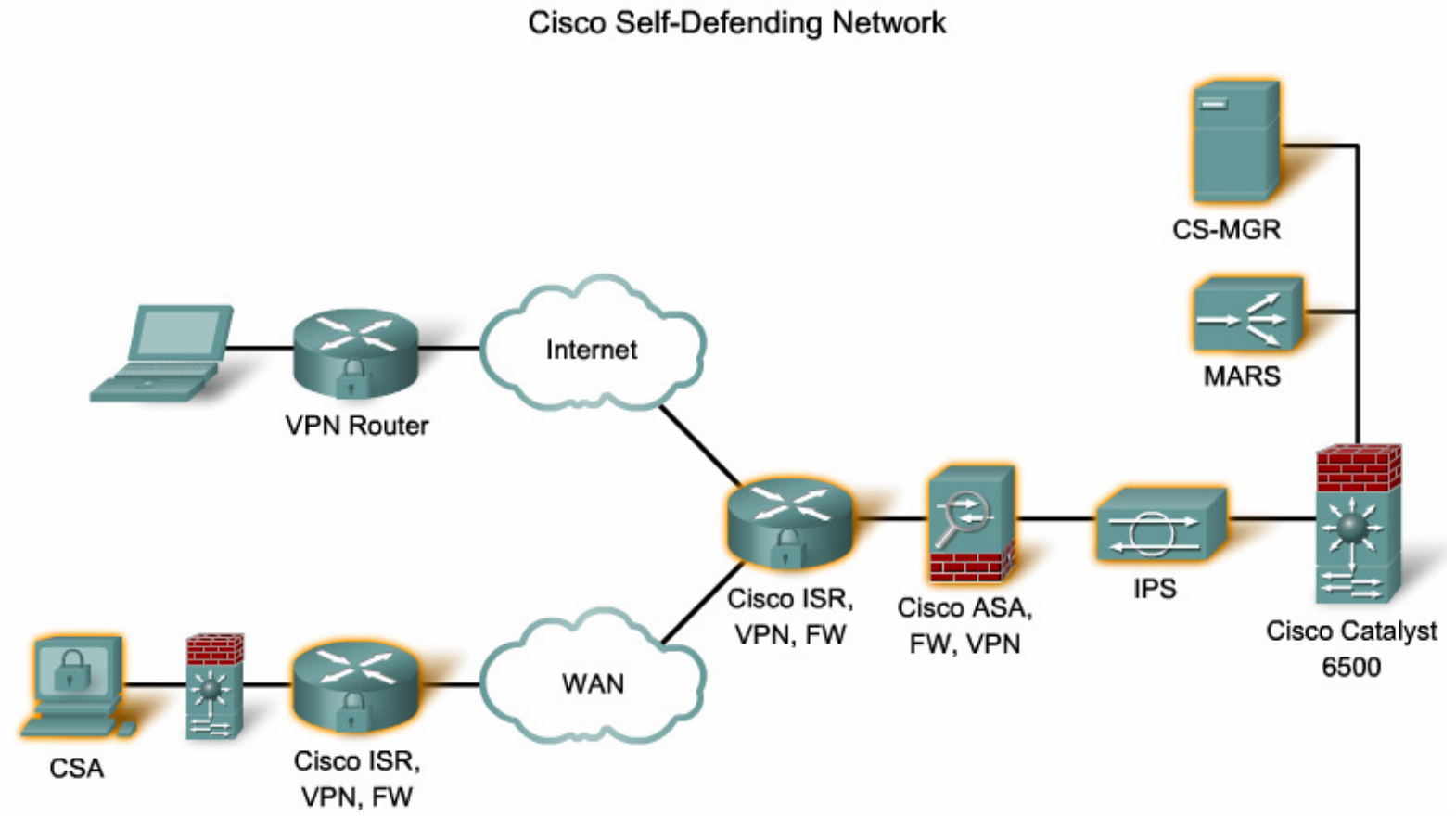
Cisco Self Defending Network

Cisco.com



Cisco Self Defending Network

Cisco.com



Threats

- Viruses
  - Attached to legitimate programs (hosts)
- Worms
  - Run by themselves
- Trojan horses
  - Masquerade as something legitimate
- Anti virus products
  - Host based
  - Networks still vulnerable

Reconnaissance Attacks

Internet queries

Ping sweeps

Port scans

Packet Sniffer

Access Attacks

- Password attack
  - Brute force
  - Trojan Horse
  - Packet sniffers
- Trust exploitation
- Port redirection
- Man in the middle
- Buffer overflow
- Ping of death
- Smurf attack
- TCP Syn flood

Reconnaissance Attack Mitigation

- 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.

Access Attack Mitigation

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

Mitigating DoS Attacks

- IPS and firewalls (Cisco ASAs and ISRs)
- Anti-spoofing technologies
- Quality of Service – traffic policing

Summary

- 1. Keep patches up to date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.
- 2. Shut down unnecessary services and ports.
- 3. Use strong passwords and change them often.
- 4. Control physical access to systems.
- 5. Avoid unnecessary web page inputs. Some websites allow users to enter usernames and passwords. A hacker can enter more than just a username. For example, entering "jdoe; rm -rf /" might allow an attacker to remove the root file system from a UNIX server. Programmers should limit input characters and not accept invalid characters such as | ; < > as input.
- 6. Perform backups and test the backed up files on a regular basis.
- 7. Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- 8. Encrypt and password-protect sensitive data.
- 9. Implement security hardware and software such as firewalls, IPSs, virtual private network (VPN) devices, anti-virus software, and content filtering.
- 10. Develop a written security policy for the company.