DCF255

Lecture 8 | Network Management and Security

Agenda

- Network Management
  - Service License Agreements (SLAs)
  - Reasons for Network Failures
- Security Management
- Plan Protect and Respond
  - Understanding the Threat Environment
- Hacker Motivation and Methodology
  - Types of Attacks

Network Management

Network Management Cost and Decision Making

Network Management

- Creating new networks and modifying existing networks on going job
- Management will select the least expensive technology to meet user needs.
- Networks are continually changing to meet organizational and personnel needs and goals
- Today we are building much larger networks than can be easily managed.

Cost and Decision Making

		Product·1¤		Product·2¤		¤
Criteria¤	Weight¤	Rating¤	Points¤	Rating¤	Points¤	¤
Price¤	5¤	10¤	50¤	8¤	40¤	¤
Ease·of·Installation¤	4¤	7¤	28¤	5¤	20¤	¤
Ease·of·Use¤	3¤	6¤	18¤	8¤	24¤	¤
Total¤	¤	¤	96¤	¤	84¤	¤

- Cost is a major constraint
- Riverbed Modeler used to create network simulations
- Weighted Criteria Table used to decide which product to buy

License Agreements (SLAs)

- SLAs are contractual agreements with 3rd party suppliers to provide a guaranteed quality of service (QoS)
- Failure to meet the minimum will result in payments to the company
- Two most common SLAs are speed and latency
  - Speed – not less than 512 Mbps of speed provided 99% of the time over a one year period
  - Latency – not more than 15ms of latency 99% of the time over one year

Reasons for Network Failures

Human Factors Poor Assumptions
Hardware/Software Misconfiguration Poor Policy Guidelines

Human Factors

- Major Reason for security failures
  - Deceived by hacker due to ignorance
  - Take advantage of people's helping nature – "Piggy-backing"
- User training can prevent failures due to ignorance
- Most secure buildings use a special code entered to alert security that an unauthorized person is entering the building.

Poor Assumptions

- Never trust user input
- Do not assume that the user will provide input in the format and length your application
  - Over trusting leads to SQL Injection attacks, Buffer Overflows
- Create a "choke-point" in your application where all input regardless of source, file, library, environment variable, is checked and validated before use
- Use Regular Expressions, stored procedures and string safe libraries

Hardware\Software Misconfigurations

- Multi-purpose servers are more likely to be misconfigured because the run multiple services

- 3 tier approach middle tier communicates with back end servers via sockets
  - Uses stored procedures information must be in length and format expected

Vulnerability – is a known weakness in the software
Exploit – is a tool designed to take advantage of a known vulnerability. A network break-in is also called an "exploit"

Poor Policy Guidelines

- **Security is a Management problem, NOT a technology problem**
- Must be top-down,comprehensive, relevant and consistent
  - Account policies
  - Storage of data
  - How to use company technology
  - How to respond to break-ins
- 85% of network break-ins caused by weak passwords
  - Complexity rules
  - Use password history
- Update hardware\software regularly – 28% of Canadian companies do it regularly

Password Complexity

Password Type	Exponent	Permutations
4 numeric pin	4^{10}	10,000
8 character same case	8^{26}	302231454903657293676544
8 characters mixed case	8^{52}	9.13438523331814323877303020447 68e+46
8 character mixed case and numbers	8^{62}	9.80797146154168869349342097376 2e+55
8 character mixed case, numbers and meta characters	8^{78}	2.76069853871622551497390234491 08e+70

- Each change in password increases complexity by about 70 times
- 8 character same case is 8^{26} – broken in 5 seconds
- 8 character mixed case is 8^{78} – broken in 9 hours
- An excellent web site is https://howsecureismypassword.net/

Security Management

Plan Protect and Respond

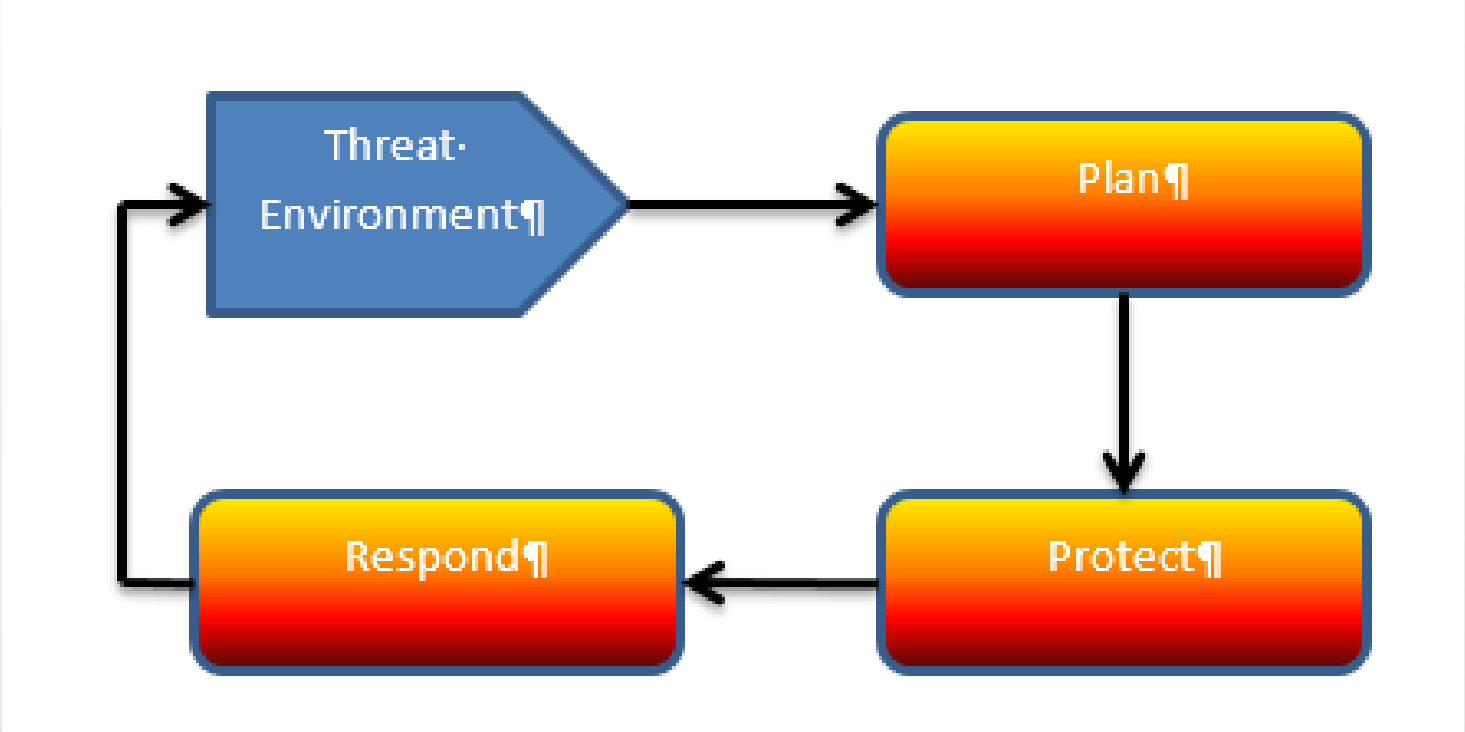
Security Management

- Guidelines – are regulations that should be followed but are not mandatory
- Standards – are regulations that must be followed and are backed by penalties for non-compliance

- Divide network into trust spheres
  - Administrators – most trusted
  - Users, DMZ – less trusted
  - Internet users, unauthorized and remote users - untrusted

Plan Protect Respond

- Plan
  - Risk Analysis
- Protect
  - Defense in Depth
- Respond
  - Comprehensive Security Policy



Planning: Risk Analysis

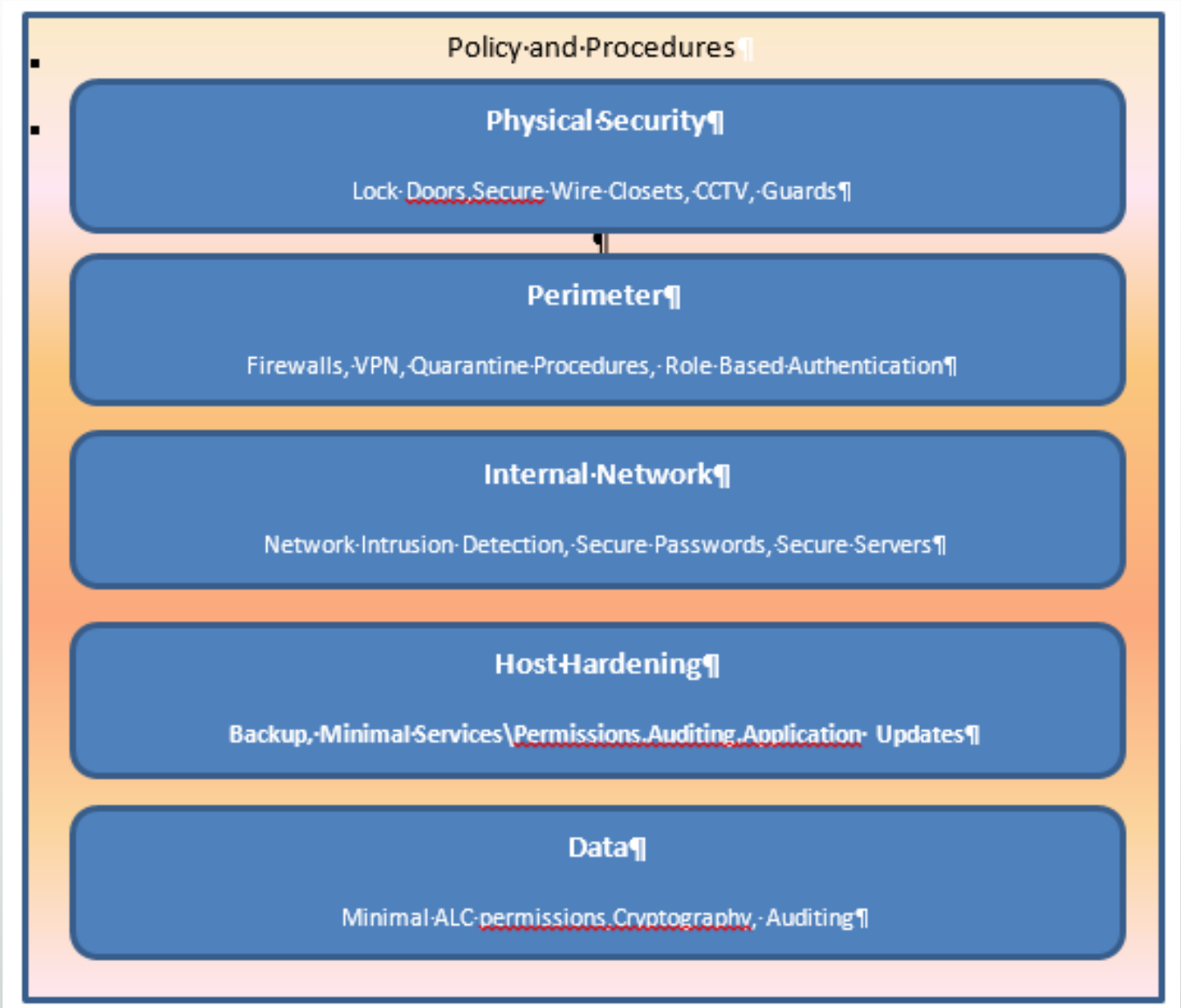
Description¤	Counter·Measure·A¤	Counter·Measure·B¤	Counter·Measure·C¤	¤
Success·Attack·Damage¤	$500,000¤	$1,000,000¤	$1,000,000¤	¤
Probability·of·an·Attack¤	20%¤	20%¤	20%¤	¤
Annual·Probability·of·Loss¤	$100,000¤	$200,000¤	$200,000¤	¤
·Cost·of·Counter·Measure¤	$25,000¤	$250,000¤	$50,000¤	¤
Net·Counter·Measure·Value¤	$75,000¤	-$50,000¤	$250,000¤	¤
Implement·Counter·Measure¤	Yes¤	No¤	Yes¤	¤

- Risk = Value of the Asset X the probability of loss
- Good Management is not to spend money on a counter measure if the cost is greater than the risk of loss

Protect: Defense in Depth

- Physical security
- Firewall
- Intrusion Detection
- Host Hardening
- ALC, Auditing, Cryptography

Note: Rights refer to what you can and cannot do on the network, such as the right to log in or shut down a PC
Permissions refer to what you can or cannot do with shared resources on the network, once you are authenticated on the network.



Respond: Comprehensive Security Policy

- ISO 17799 standard outlines the security policy process
- Certification shows partners and others you have policies to protect data, control machine usage and recover from disaster
- Review of the topics show its comprehensiveness

Security Policy
Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Organization of Information Security
Manage information security within the organization. Maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Asset Management
Achieve and maintain appropriate protection of organizational assets. Ensure that information receives an appropriate level of protection.

Human Resources Security
Ensure that employees, contractors, and third-party users (1) understand their responsibilities and are suitable for the roles they are considered for; (2) are aware of information security threats and concerns; (3) exit an organization or change employment in an orderly manner

Physical and Environmental Security
Prevent unauthorized physical access, damage, and interference to the organizations premises and information. Prevent loss, damage, theft, or compromise of assets and interruption to the organization's activities.

Communications and Operations Management
Develop controls for operational procedures, third-party service delivery management, system planning, malware protection, backup, network security management, media handling, information exchange, e-commerce services, and monitoring.

Access Control
Develop controls for business requirements for user access, user responsibilities, network access control, OS access control, application access control, and information access control.

Information Systems Acquisition, Development, and Maintenance
Develop controls for correct processing in applications, cryptographic functions, system file security, support process security, and vulnerability management.

Information Security Incident Management
Ensure information security events and weaknesses associated with information systems are communicated in a manner that allows timely corrective action to be taken. Ensure a consistent and effective approach is applied to the management of information security incidents.

Business Continuity Management
Counteract interruptions to business activities to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Compliance
Avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements. Ensure compliance of systems with organizational security policies and standards. Maximize the effectiveness of and minimize interference to and from the information systems audit process.

Threat Environment

Understanding What is hacking?

Hacking

- Hacking is when a person intentionally uses a computer resource without authorization or in excess of his/her authorization

- To protect a network you must understand the hacker motivation and methodology

Hacking Scenario 1

- You work in the School of Computer Studies and you find the username and password of the secretary on his/her desk. You log in with the secretary's user name and password, just to browse around and you are careful not to change anything. Are you hacking?

Yes, because finding the username and password did not give you authorization to use it. Most companies have an Acceptable use policy which strongly prevents a user from logging in to another users account for any purpose

Hacking Scenario 2

- You log into your authorized account and discover you can accidentally see sensitive information in your manager's directory. You spend a few minutes browsing around, but you did not change anything. Are you hacking?

Yes, because you did not have explicit authorization to read the information in another directory and therefore exceeded your level of authorization. This would be contrary to the company's Acceptable Use Policy.

Hacking Scenario 3

- Someone sends you an email with a link to a popular game site. When you click on the link, you find that you are logged into the i3 server. You log out immediately. Are you hacking?

No, you did not use the resource without authorization; you were the victim of a malicious payload which you were not aware of and you did not intentional try to log into the server. You logged out as some as you knew. Most network security training would require you to inform the IT staff of the malicious email.

Hacking Scenario 4

- The company you are working for does not have an Acceptable Use Policy and strong security policies. You wish to show management security weaknesses by demonstrating how you can log into the company server without authorization. Are you hacking?

Yes, you are hacking. Lack of a security policy did not mean that you had authorization to log into the server. Even if you did it to point out the company's weaknesses and had no malicious intent. You have created an illegal act and can be prosecuted by the company

Threat Environment

Understanding the hacker motivation and methodology

Hacker Motive and Methodology

- Traditional hacker has been adolescents who break-in or release malware for curiosity, and bragging rights among peers

- Today, this image changed to loosely organized criminal organizations who use “script-kiddies” as pones to lower the value of stock or steal personal information

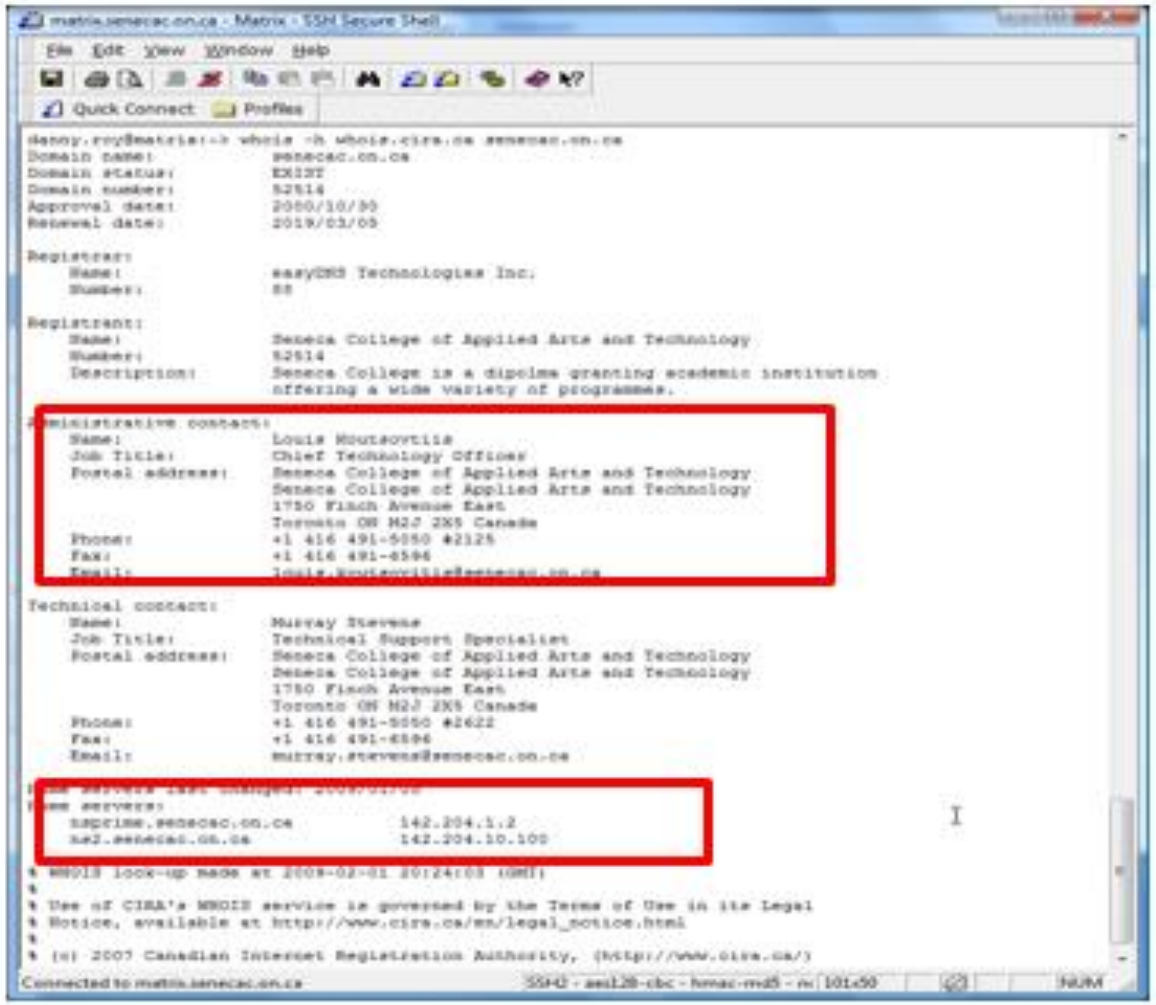
- Attacks today increasingly random and motivated by profit- attacks for hire, renting bot service or money laundering

Types of Attacks: Individual

- Criminal Attacks on Individuals
  - Steal personal information
  - Identify theft
- Viruses
- Worms
- Trojan horses

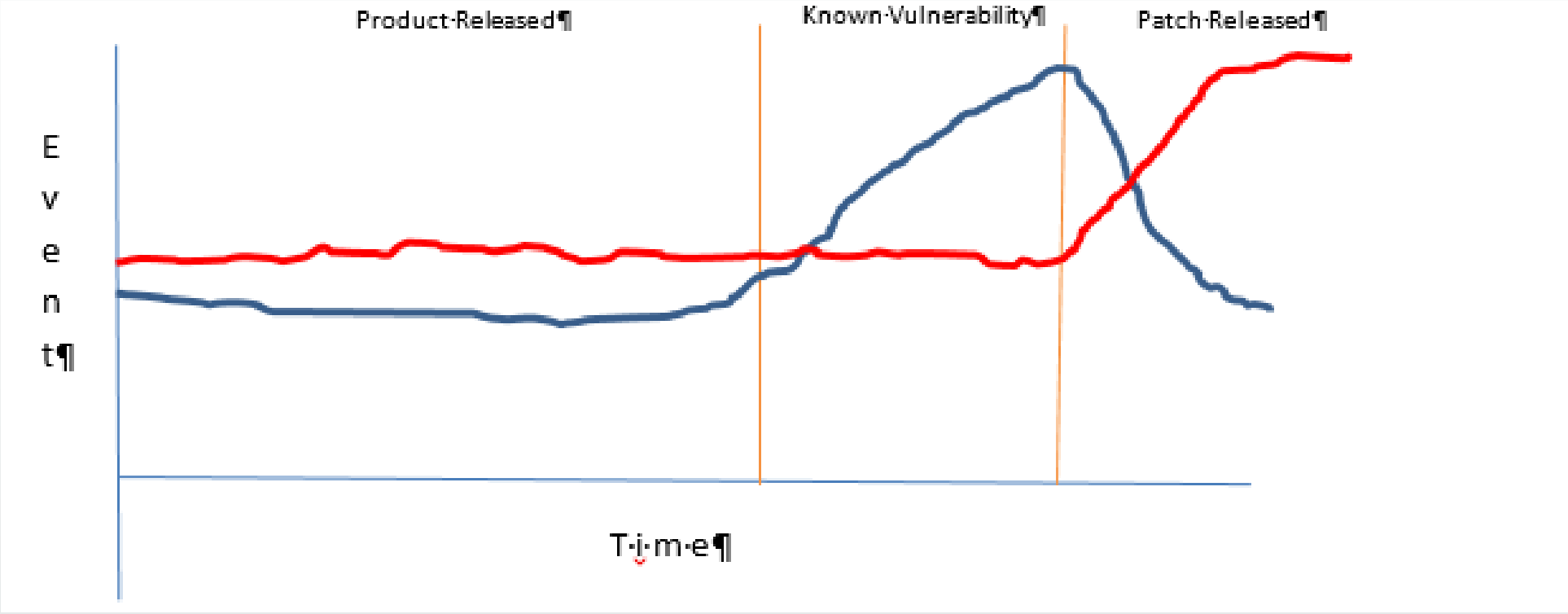
Types of Attacks: Corporation

- Criminal Attacks on Corporations
  - Stage 1
    - Gather public information
    - Web sites
    - Whois database
    - PING
    - Social Engineering to steal information



Types of Attacks: Corporation

- Stage 2



- Research known vulnerabilities
- Attacks increase AFTER patch released – all information to design a tool
- Trial and Error to find an exploit that works – use Metasploit

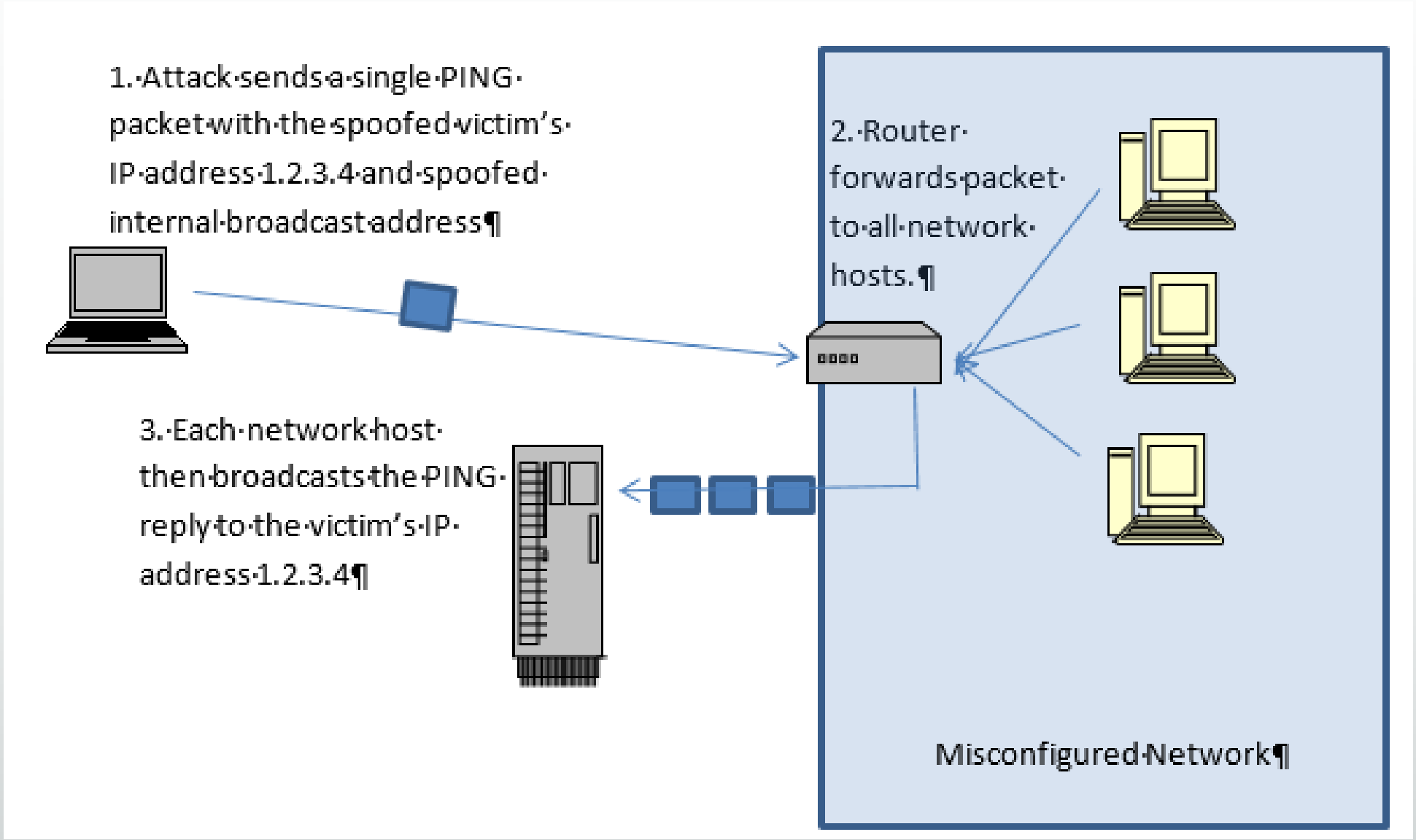
Types of Attacks: Corporation

- Stage 3
  - Create back door with known password and full privilege
  - Delete log files
  - Install “keylogger” to steal information or account information

Types of Attacks: Denial of Service

- DoS
  - Often used as a backup plan if a break-in was unsuccessful
  - Targets switches, routers, servers to prevent them from responding to authorized users

Types of Attacks: Smurf Attack



Summary

1. Creating or modifying networks is very expensive. To help management make cost decisions they use criteria tables to quantitative subjective decisions. Service License Agreements are often used to ensure quality of service by 3rd party suppliers

2. Network failures are the result of human errors of users, poor assumptions by developers, hardware\software misconfigurations and poor policy guidelines. Policies must be comprehensive, relevant and cover all aspects of network usage from account policies, to password complexity rules. Standards of practice should be enforcemented.

3. Good security management is based on Plan Protect and Respond (PPR). Planning involves conducting a risk assessment as to which assets need protection and to what extent. Protection is based on defense in depth which provides multiple levels of defense against an attack. Respond is based on having comprehensive policies which conform to ISO 17799 standard for writing and implementing security policies

4. The notion of a "hacker" is changing from young adolescents wanting bragging rights to criminal organizations that band together motivated solely for profit from stealing personal information or stealing intellectual property. Most attacks today are against individuals.

5. Attacks against corporations are based on a 3 stage process to establish a back door for future access, delete log files and install key-logger programs. If hackers can not break-in a network they will target the switches, routers or servers to create a denial of service attack.