ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Network Security

1

About this course

- Course ID: IT4262E
- Course name: Network Security 2(2-0-0-4)
- Evaluation:
  - Midterm (50%): Quiz
  - Final exam(50%): Quiz

2

References

1. **Security in Computing, 5th edition,** *Charles P. Pfleeger - Pfleeger Consulting Group, Shari Lawrence Pfleeger*, Prentice Hall 2015
2. **Cryptography and Network Security Principles and Practices, Global edition,** *William Stallings,* Prentice Hall 2017
3. **Security Engineering, 3rd edition,** *Ross J. Anderson,* Wiley 2020

3

About lecturer

Dr. Nguyen Duc Toan,

Computer Engineering Department, SoICT, HUST

Email: toannd@soict.hust.edu.vn

Working place: Room 801 – B1 – BKHN

Website: https://soict.hust.edu.vn/en/ph-d-nguyen-duc-toan.html

4

Objectives

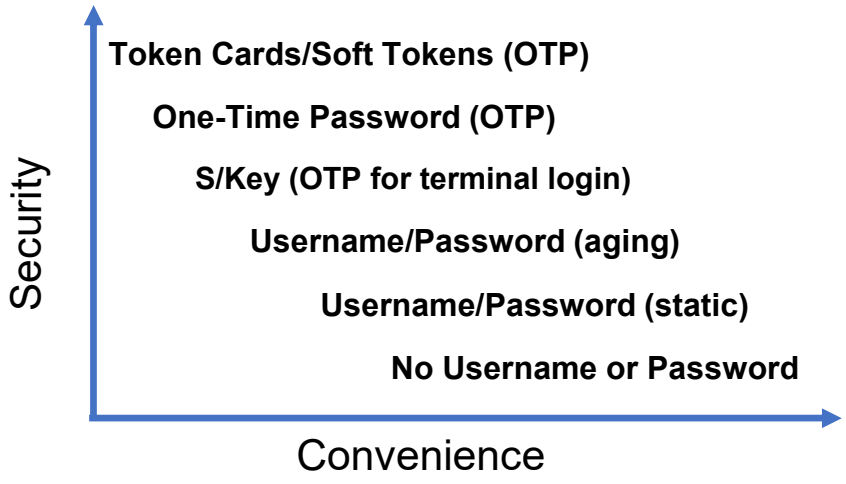
1. Describe the rationale for network security
2. Identify risks, threats, vulnerabilities and countermeasures
3. Discuss the states of information, identify threats and appropriate countermeasures for each state
4. Differentiate between security policies, standards and guidelines

5

1. Introduction

6

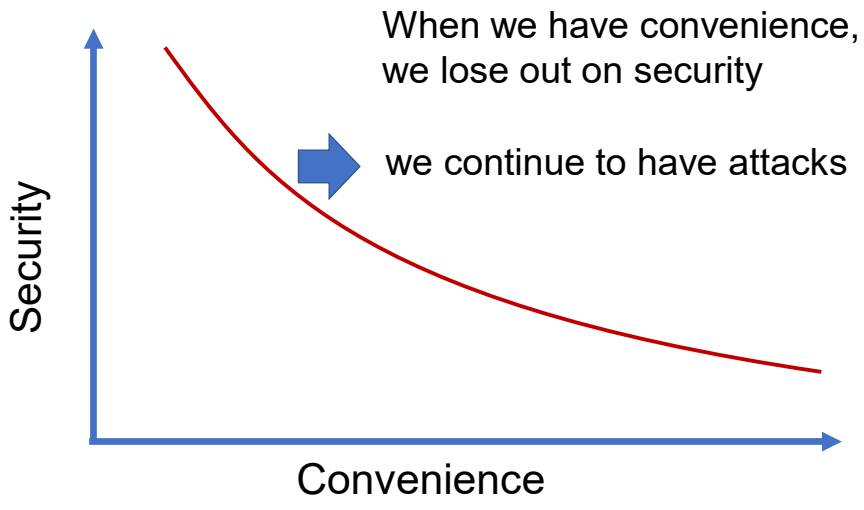
What your choice?



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

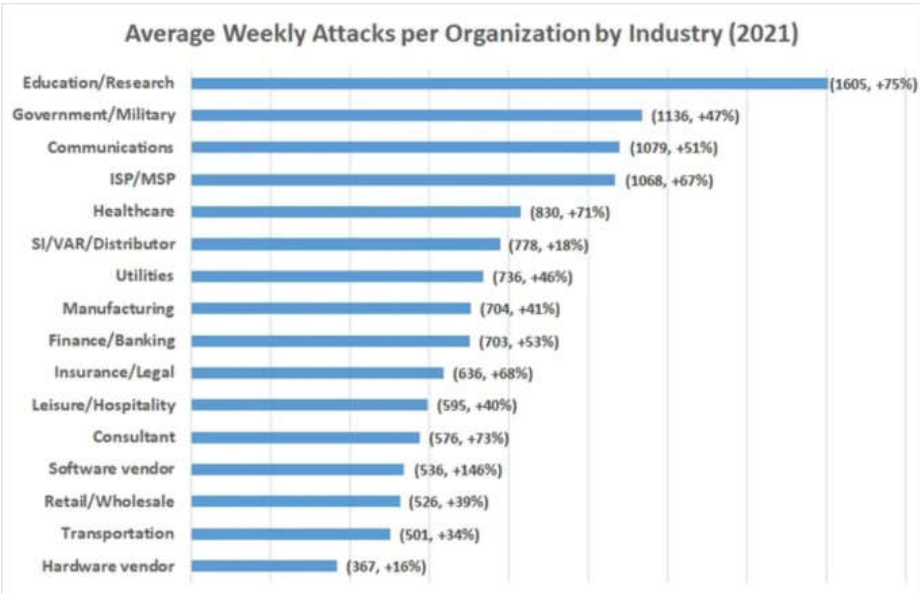
7

What your choice?



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

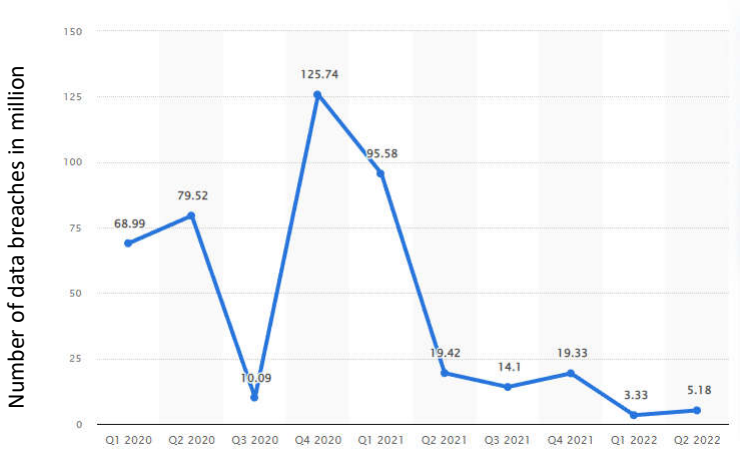
8



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

9

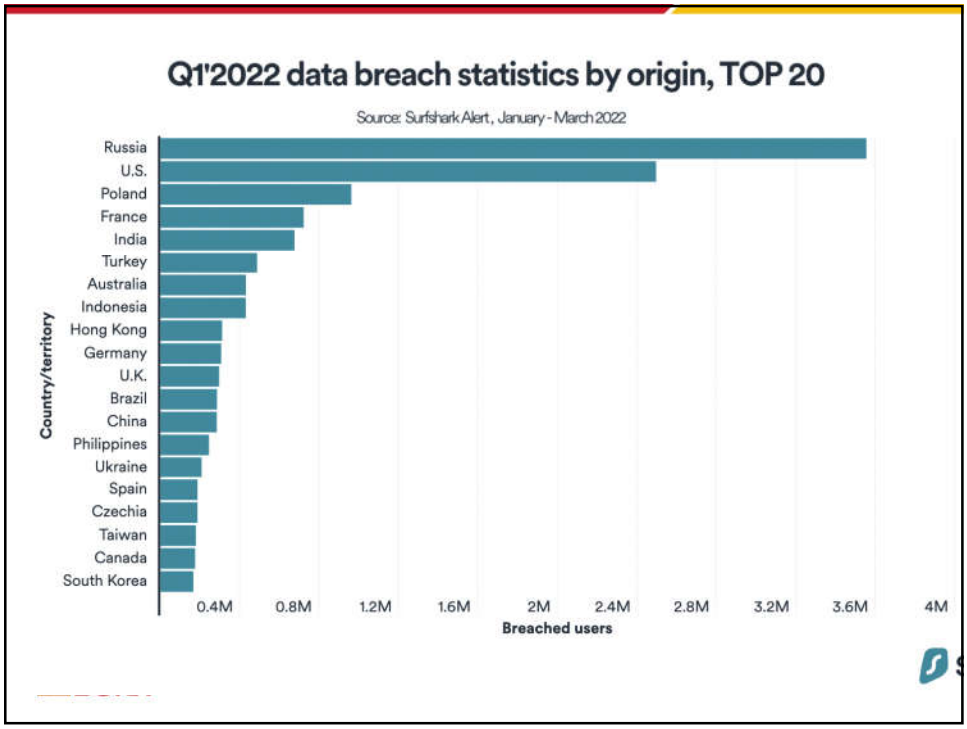
Number of data records exposed



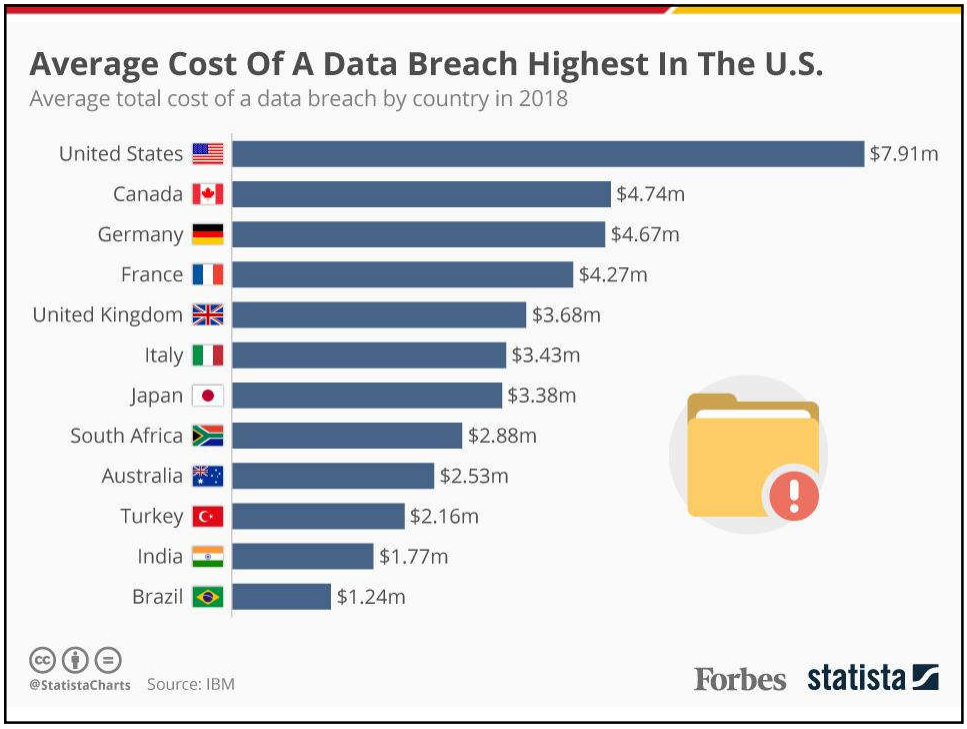
https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

10


Q1'2022 data breach statistics by origin, TOP 20
Source: Surfshark Alert, January - March 2022
Country/territory
Russia
U.S.
Poland
France
India
Turkey
Australia
Indonesia
Hong Kong
Germany
U.K.
Brazil
China
Philippines
Ukraine
Spain
Czechia
Taiwan
Canada
South Korea
0.4M
0.8M
1.2M
1.6M
2M
2.4M
2.8M
3.2M
3.6M
4M
Breached users

11


Average Cost Of A Data Breach Highest In The U.S.
Average total cost of a data breach by country in 2018
United States $7.91m
Canada $4.74m
Germany $4.67m
France $4.27m
United Kingdom $3.68m
Italy $3.43m
Japan $3.38m
South Africa $2.88m
Australia $2.53m
Turkey $2.16m
India $1.77m
Brazil $1.24m
@StatistaCharts
Source: IBM
Forbes
statista

12

Information security

Act of protecting data and information from unauthorized access, unlawful modification and disruption, disclosure, and corruption, and destruction.

13

Information system security

Act of protecting the systems that hold and process our critical data.

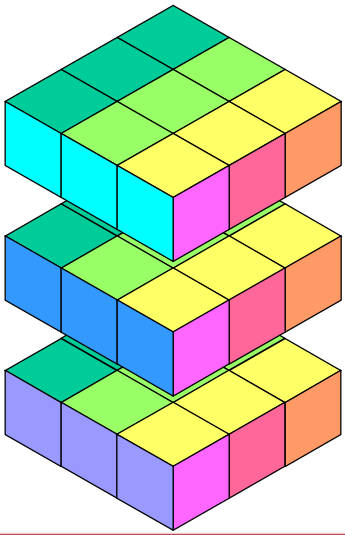
14

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

1.1. Basic Concepts

15

Information Security Properties



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

16

Confidentiality in physical world

17

Confidentiality in digital world

18

Confidentiality – Balance view

19

Confidentiality - Balance change

20

Integrity

21

Integrity – User

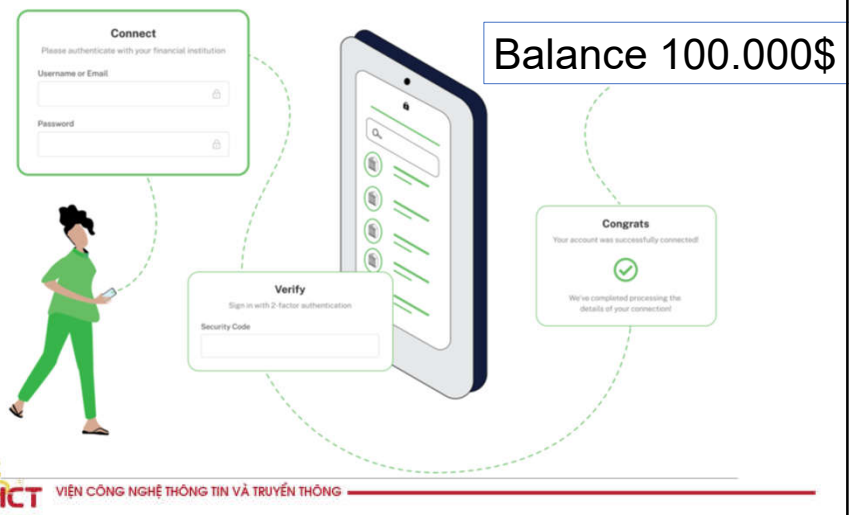
Breach of integrity

Balance 1000$

Only the bank has the authorization to change the balance.

22

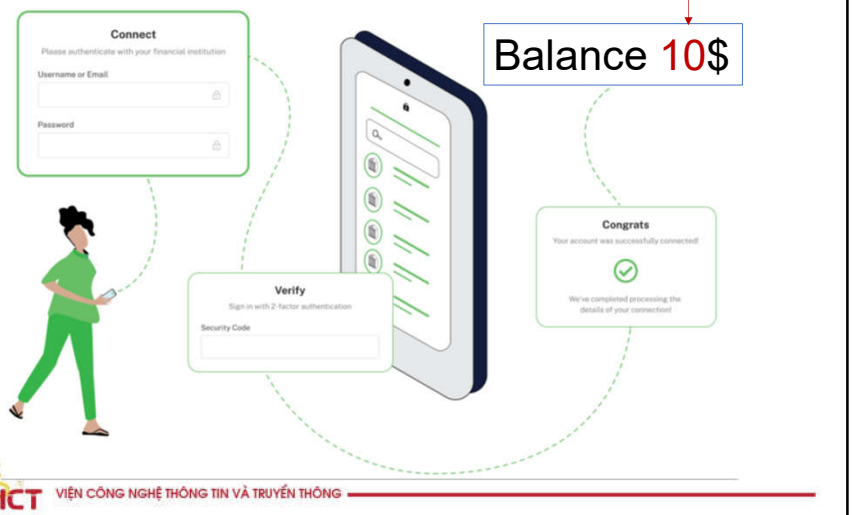
Integrity – Bank



23

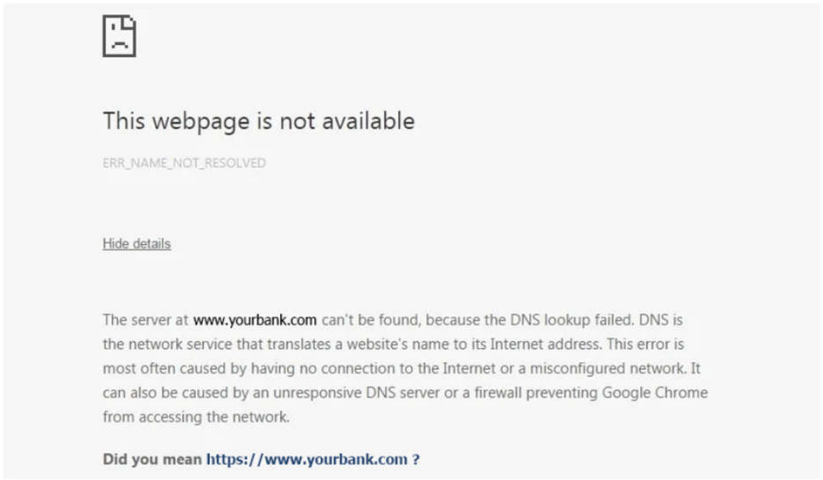
Integrity – Bank

Breach of integrity



24

Availability



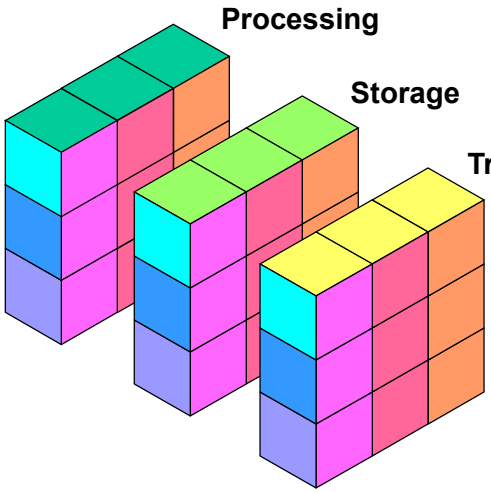
25

Goals of an Information Security Program

- **Confidentiality**
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- **Integrity**
  - The protection of system information or processes from intentional or accidental modification
- **Availability**
  - The assurance that systems and data a accessible by authorized users when ne

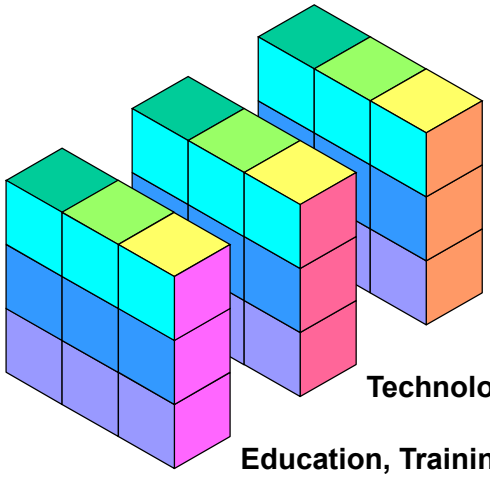
26

Information States



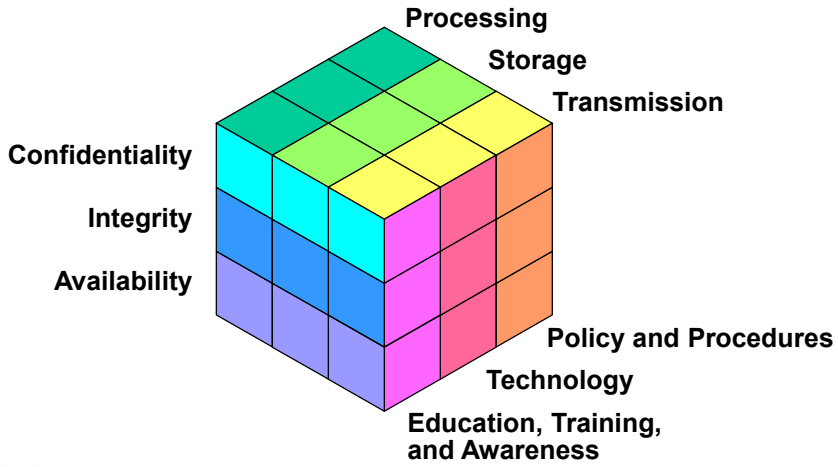
27

Security Measures



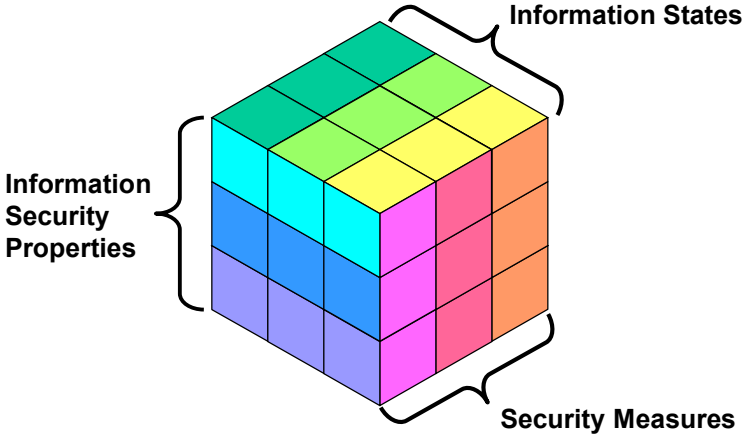
28

Information Security Model



29

Information Security Model



NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

30

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

1.2. Network Security model

31

What is Network Security?

Network security is the **protection** of **information**, **systems** and **hardware** that **use, store, and transmit** that information.

Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources.

National Security Telecommunications and Information Systems Security Committee (NSTISSC)

32

Network Security challenge

- Open system
- Distribution resource
- Anonymous
- TCP/IP was NOT designed for security
  - No authentication
  - No authorization, not all data are encrypted

33

"On the Internet, nobody knows you're a dog."

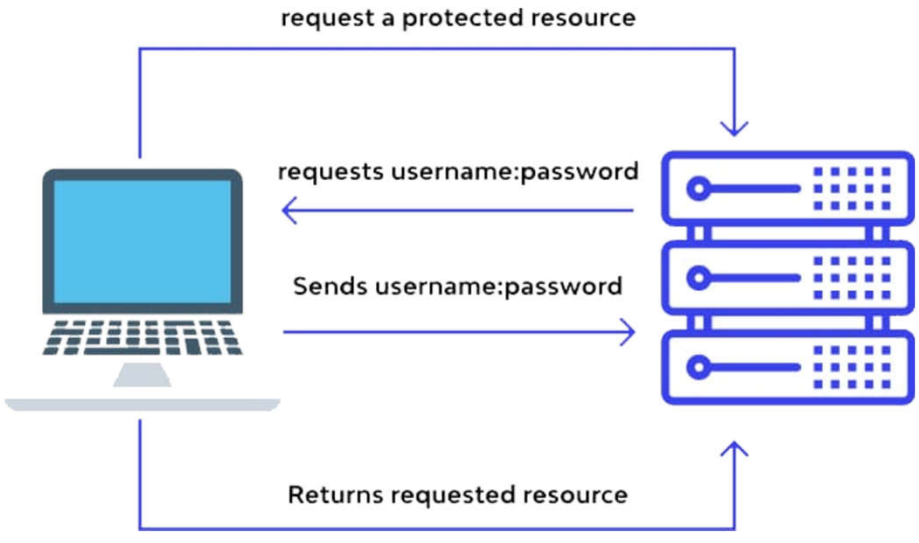
34

Network Security Architecture

- Authentication
  - Who are you?
  - "I am user *student* and my password *validateme* proves it"
- Authorization
  - What can you do? What can you access?
  - "User *student* can access host *NT_Server* with *Telnet*"
- Accounting
  - What did you do? How long did you do it? How often did you do it?
  - "User *student* accessed host *NT_Server* with *Telnet* 15 times"

35

Authentication



36

Authorization

Authorization

What you can do

Authentication

Who you are

37

Accounting

```
HP Switch(config)# show logging
 Keys:   W=Warning   I=Information
         M=Major     D=Debug E=Error
----  Event Log listing: Events Since Boot  ----
I 10/28/09 21:45:42 00061 system:  AM1: ----------

I 10/28/09 21:45:42 00062 system:  AM1: Mgmt Module 1 went down without saving
          crash information
M 10/28/09 21:45:42 03002 system:  AM1: System reboot due to Reset Switch
I 10/28/09 21:45:42 02759 chassis: AM1: Savepower LED timer is OFF.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot A configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot B configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot C configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot D configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot E configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot F configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot G configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot H configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot I configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot J configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot K configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot L configured ON.
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 1 inserted
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 2 inserted
I 10/28/09 21:45:43 00092 dhcp: AM1: Enabling Auto Image Config Download via
           DHCP and turning off auto-tftp if enabled
I 10/28/09 21:45:43 00690 udpf: AM1: DHCP relay agent feature enabled
I 10/28/09 21:45:43 02637 srcip: AM1: TACACS admin policy is 'outgoing interface
           '
I 10/28/09 21:45:43 02638 srcip: AM1: TACACS oper policy is 'outgoing interface'
```

AM1 = Active management module in slot 1
AM2 = Active management module in slot 2
SM1 = Standby management module in slot 1
SM2 = Standby management module in slot 2

38

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

1.3. Why Network Security is Important?

39

Rationale for Network Security

- Network security **initiatives** and network security **specialists** can be found in private and public, large and small companies and organizations.
- The need for network security and its growth are driven by many factors:
  1. Internet connectivity is 24/7 and is worldwide
  2. Increase in cyber crime
  3. Impact on business and individuals
  4. Legislation & liabilities
  5. Proliferation of threats
  6. Sophistication of threats

40

What is Cyber Crime?

The adopted definition of Cyber Crime is:

- ***Cyber Dependent Crimes*****,** where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to commit further crime).
- ***Cyber Enabled Crimes***. 'Existing' crimes that have been transformed in scale or form by their use of the Internet. The growth of the Internet has allowed these crimes to be carried out on an industrial scale.
- The use of the Internet to facilitate drug dealing, people smuggling and many other 'traditional' crime types.

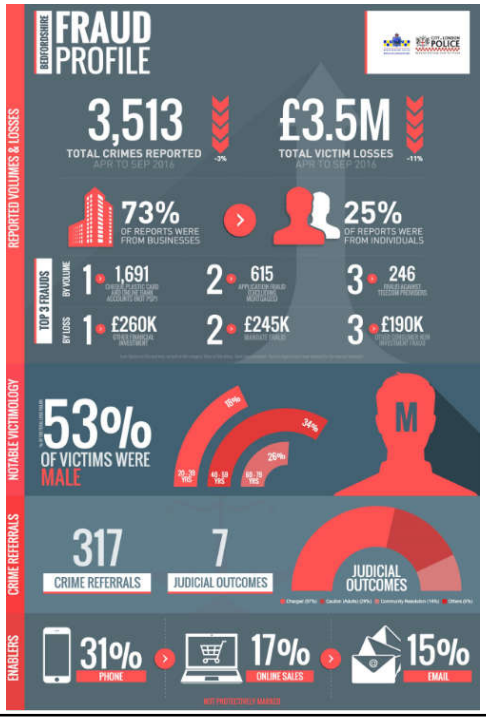
41

Cyber element?

42

Highest reported incidents:

+ Online fraud
+ Mandate
+ Ransomware
+ Romance frauds



43

Which of these is a cyber threat?

POTENTIALLY ALL OF THEM!

44

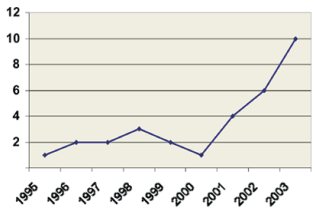
Current Scams

- Invoice emails – i.e. new vendors, changes to current vendors, Apple [little mix]
- Vouchers - Supermarkets, on line stores
- Account updates – amazon, Sky, Virgin, Utilities.
- Advice – any unsolicited emails. Do not press that link; simply delete. Go via normal website. Send to phishing email address for company
- Mandate fraud – Bedford company lost £100K put 27 staff at risk. £1M in Luton in September. Bedford company had windows 365 compromised with poor PW. L/Buzzard company 17 fake invoices by post in Jan17.
- Solicitor companies being targeted – Luton March 2017, Bedford Dec
- Advice - Slow down, check via second source. Get copy of our advice
- Ransomware – Luton Hotel attacked over New year – pay and enter suckers list

45

Other cybercrime

- Identity Theft
- Child Pornography
- Theft of Telecommunications Services
- Electronic Vandalism, Terrorism and Extortion



WASHINGTON, D.C. — An estimated 3.6 million households, or about 3 percent of all households in the nation, learned that they had been the victim of at least one type of identity theft during a six-month period in 2004, according to the Justice Department's Bureau of Justice Statistics

46

What are some of the biggest threats?

- Insider Threat (theft/fraud/data breach)
- Malware by phishing attacks
- Data Breach
- DDoS
- Social Engineering leading to scams
- Theft/fraud by Customers or vendors.

47

Some good news!!

80% is easily preventable

Ultimately it depends on the business, how it is set up, the infrastructure and the policies and procedures, and protect mechanisms in place.

48

Business Impact

1. Decrease in productivity
2. Loss of sales revenue
3. Release of unauthorized sensitive data
4. Threat of trade secrets or formulas
5. Compromise of reputation and trust
6. Loss of communications
7. Threat to environmental and safety systems
8. Loss of time

49

Legislation

- Federal and local government has passed legislation that holds organizations and individuals liable for mismanagement of sensitive data.
- Luật an ninh mạng

50

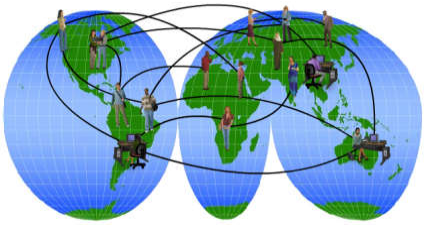
Proliferation of Threats

In 2001, the National Infrastructure Protection Center at the FBI released a document summarizing the **Ten Most Critical Internet Security Vulnerabilities**.

Thousands of organizations rely on this list to prioritize their efforts so they can close the most dangerous holes first.

The threat landscape is very dynamic, which in turn makes it necessary to adopt newer security measures.

Just over the last few years, the kinds of **vulnerabilities** that are being exploited are very different from the ones being exploited in the past.



51

What is Vulnerability

- A network vulnerability is a **weakness** in a system, technology, product or policy
- In today's environment, several organizations track, organize and test these vulnerabilities
- Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- The **common vulnerability exposure** (CVE) list also publishes ways to prevent the vulnerability from being attacked

52

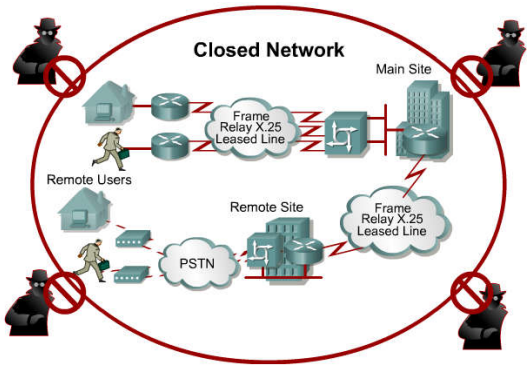
Vulnerability Appraisal

- It is very important that **network security specialists** comprehend the importance of vulnerability appraisal
- A vulnerability appraisal is a **snapshot** of the current security of the organization as it now stands
- What **current security weaknesses** may expose the assets to these threats?
- Vulnerability scanners are tools available as free Internet downloads and as commercial products
  - These tools compare the asset against a database of known vulnerabilities and produce a discovery report that exposes the vulnerability and assesses its severity

53

Purpose of Security

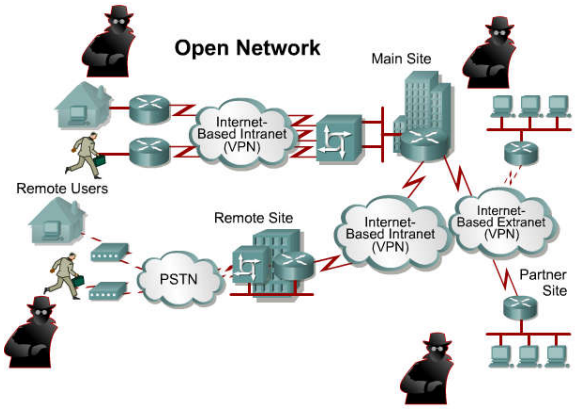
- To protect assets!
  - Historically done through physical security and closed networks.



54

The Network Today

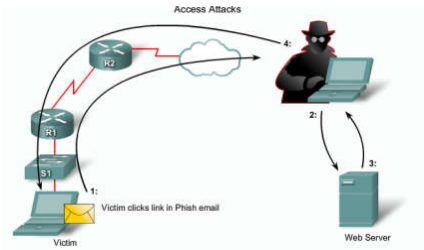
- With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open.



55

What is Threat

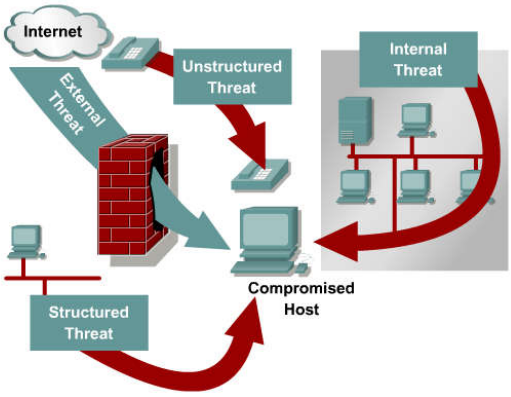
- A **potential danger** to information or a system
- E.g: the ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network
- There may be **weaknesses** that greatly increase the likelihood of a threat manifesting
- Threats may include equipment failure, structured attacks, natural disasters, physical attacks, theft, viruses and many other potential events causing danger or damage



56

Threats

- There are four primary classes of threats to network security:
  - Unstructured threats
  - Structured threats
  - External threats
  - Internal threats



57

Types of Attacks

Structured attack

Come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

Unstructured attack

Consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

58

Types of Attacks

External attacks

Initiated by individuals or groups working outside of a company. They do not have authorized access to the computer systems or network. They gather information in order to work their way into a network mainly from the Internet or dialup access servers.

Internal attacks

More common and dangerous. Internal attacks are initiated by someone who has authorized access to the network. According to the FBI, internal access and misuse account for 60 to 80 percent of reported incidents. These attacks often are traced to disgruntled employees.

59

Types of Attacks

- **Passive Attack**
  - Listen to system passwords
  - Release of message content
  - Traffic analysis
  - Data capturing
- **Active Attack**
  - Attempt to log into someone else's account
  - Wire taps
  - Denial of services
  - Masquerading
  - Message modifications

60

Specific Network Attacks

- ARP Attack
- Brute Force Attack
- Worms
- Flooding
- Sniffers
- Spoofing
- Redirected Attacks
- Tunneling Attack
- Covert Channels


Internet queries


Ping sweeps


Port scans

61

Attack Methodology

Stages - the methodology of network attacks is well documented and researched. This research has led to greater understanding of network attacks and an entire specialization of engineers that test and protect networks against attacks (Certified Ethical Hackers/Penetration Testers)

Tools - penetration testers have a variety of power tools that are now commercially available. They also have may open source free tools. This proliferation of powerful tools has increased the threat of attack due to the fact that even technical novices can now launch sophisticated attacks.

62

Stages of an Attack

- Today's attackers have an abundance of targets. In fact their greatest challenge is to select the most vulnerable victims. This has resulted in very well- planned and structured attacks. These attacks have common logistical and strategic stages. These stages include;
  - Reconnaissance
  - Scanning (addresses, ports, vulnerabilities)
  - Gaining access
  - Maintaining Access
  - Covering Tracks

63

Tools of the Attacker

- The following are a few of the most popular tools used by network attackers:
  - Enumeration tools (dumpreg, netview and netuser)
  - Port/address scanners (AngryIP, nmap, Nessus)
  - Vulnerability scanners (Meta Sploit, Core Impact, ISS)
  - Packet Sniffers (Snort, Wire Shark, Air Magnet)
  - Root kits
  - Cryptographic cracking tools (Cain, WepCrack)
  - Malicious codes (worms, Trojan horse, time bombs)
  - System hijack tools (netcat, MetaSploit, Core Impact)

64

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

2. Risk managêmnt

65

Risk Management

- Risk Analysis
- Threats
- Vulnerabilities
- Countermeasures

66

Risk Management

- The process of assessing and quantifying risk and establishing an acceptable level of risk for the organization
- Risk can be **mitigated**, but cannot be **eliminated**

67

Risk Assessment

- Risk assessment involves determining the likelihood that the vulnerability is a risk to the organization
- Each vulnerability can be ranked by the scale
- Sometimes calculating anticipated losses can be helpful in determining the impact of a vulnerability

68

Asset Identification

- Categories of assets
  - Information Assets (people, hardware, software, systems)
  - Supporting Assets (facilities, utilities, services)
  - Critical Assets (can be either of those listed above)
- Attributes of the assets need to be compiled
- Determine each item's relative value
  - How much revenue/profit does it generate?
  - What is the cost to replace it?
  - How difficult would it be to replace?
  - How quickly can it be replaced?

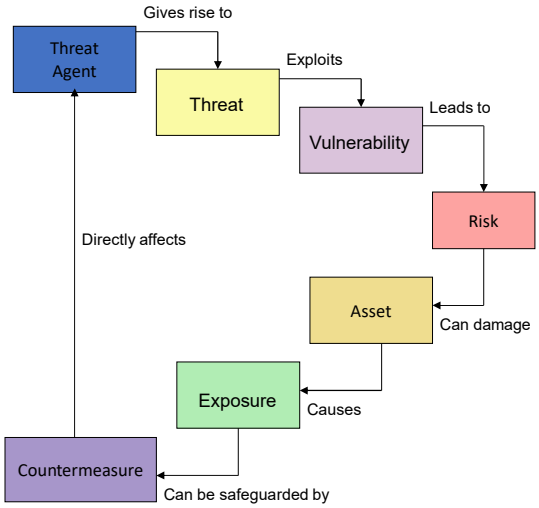
69

Risk Management Terms

- Vulnerability – a system, network or device weakness
- Threat – potential danger posed by a vulnerability
- Threat agent – the entity that indentifies a vulnerability and uses it to attack the victim
- Risk – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- Exposure – potential to experience losses from a threat agent
- Countermeasure – put into place to mitigate the potential risk

70

Understanding Risk



71

Qualitative Risk Analysis

Probability X Severity = Exposure

Exposure values prioritize the order for addressing risks

RISK	Probability	Severity	Exposure
A new worm	7	7	49
Web site defacement	2	8	16
Fire protection system Floods datacenter	1	10	10

72

Quantitative Risk Analysis

- Exposure Factor (EF)
  - % of loss of an asset
- Single Loss Expectancy (SLE)
  - EF x Value of asset in $
- Annualized Rate of Occurrence (ARO)
  - A number representing frequency of occurrence of a threat
    Example: 0.0 = Never 1000 = Occurs very often
- Annualized Loss Expectancy (ALE)
  - Dollar value derived from: SLE x ARO

73

Countermeasures

- DMZ/NAT
- IDS/IPS
- Content Filtering/NAC
- Firewalls/proxy services
- Authentication/Authorization/Accounting
- Self-defending networks
- Policies, procedures, standards guidelines
- Training and awareness

74

Countermeasure Selection

- Cost /benefit calculation

  (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company

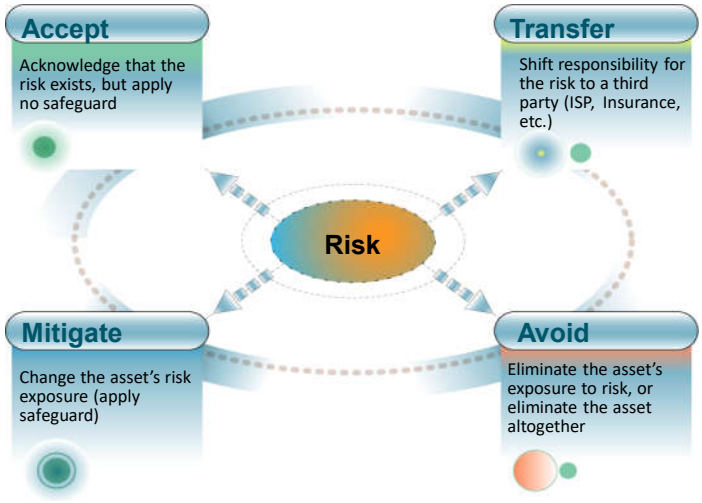
- Evaluating cost of a countermeasure

  - Product costs
  - Design/planning costs
  - Implementation costs
  - Environment modifications
  - Compatibility
  - Maintenance requirements

  - Testing requirements
  - Repair, replacement, or update costs
  - Operating and support costs
  - Effects of productivity

75

Managing Risks



76

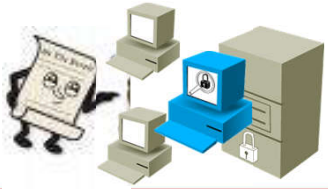
ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

3. Security Policy

77

What Is a Security Policy?

- A document that states how an organization plans to protect its tangible and intangible information assets
  - Management instructions indicating a course of action, a guiding principle, or appropriate procedure
  - High-level statements that provide guidance to workers who must make present and future decisions
  - Generalized requirements that must be written down and communicated to others



78

Change Drivers

- Built into the information security program
- Events that cause us to revisit policies, procedures, standards, and guidelines
  - Changes in technology
  - Changes in senior level personnel
  - Acquisition of other companies
  - New products, services, or business lines

79

Documents Supporting Policies

- Standards – dictate specific minimum requirements in our policies
- Guidelines – suggest the best way to accomplish certain tasks
- Procedures – provide a method by which a policy is accomplished (the instructions)

80

Example: The Policy

- All users must have a unique user ID and password that conforms to the company password standard
- Users must not share their password with anyone regardless of title or position
- Passwords must not be stored in written or any readable form
- If a compromise is suspected, it must be reported to the help desk and a new password must be requested

81

Example: The Standards

- Minimum of 8 upper- and lowercase alphanumeric characters
- Must include a special character
- Must be changed every 30 days
- Password history of 24 previous passwords will be used to ensure passwords aren't reused

82

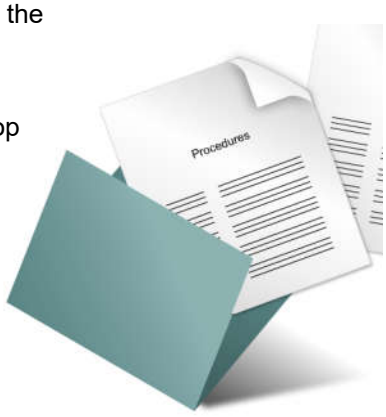
Example: The Guideline

- Take a phrase
  Up and At 'em at 7!
- Convert to a strong password
  Up&atm@7!
- To create other passwords from this phrase, change the number, move the symbol, or change the punctuation mark

Example: The Procedure

Procedure for changing a password

1. Press Control, Alt, Delete to bring up the log in dialog box
2. Click the "change password" button
3. Enter your current password in the top box
4. …



Policy Elements

- Statement of Authority – an introduction to the information security policies
- Policy Headings – logistical information (security domain, policy number, name of organization, effective date, author, change control documentation or number)
- Policy Objectives – states *what* we are trying to achieve by implementing the policy
- Policy Statement of Purpose – *wh*y the policy was adopted, and *how* it will be implemented

85

Policy Elements, 2

- Policy Audience – states *who* the policy is intended for
- Policy Statement – *how* the policy will be implemented (the rules)
- Policy Exceptions – special situations calling for exception to the normal, accepted rules
- Policy Enforcement Clause – consequences for violation
- Policy Definitions – a “glossary” to ensure that the target audience understands the policy

86

Policy Example

Subsection	6.1 PERSONNEL SECURITY Change Control #: 1.0
Policy	6.1.3 Confidentiality Agreements Approved by: SMH
Objectives	Confidentiality of organizational data is a key tenet of our information security program. In support of this goal, ABC Co will require signed confidentiality agreements of all authorized users of information systems. This agreement shall conform to all federal, state, regulatory, and union requirements.
Purpose	The purpose of this policy is to protect the assets of the organization by clearly informing staff of their roles and responsibilities for keeping the organization's information confidential.
Audience	ABC Co confidentiality agreement policy applies equally to all individuals granted access privileges to an ABC Co Information resources
Policy	This policy requires that staff sign a confidentiality policy agreement prior to being granted access to any sensitive information or systems. Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organization. The agreements will be provided to the employees by the Human Resource Dept.
Exceptions	At the discretion of the Information Security Officer, third parties whose contracts include a confidentiality clause may be exempted from signing individual confidentiality agreements.
Disciplinary Actions	Violation of this policy may result in disciplinary actions, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution.

87

Network Security Organizations

www.infosyssec.com

www.sans.org

www.cisecurity.org

www.cert.org

www.isc2.org

www.first.org

www.infragard.net

www.mitre.org

www.cnss.gov

INFOSYSSEC Information System Security

CERT

SANS

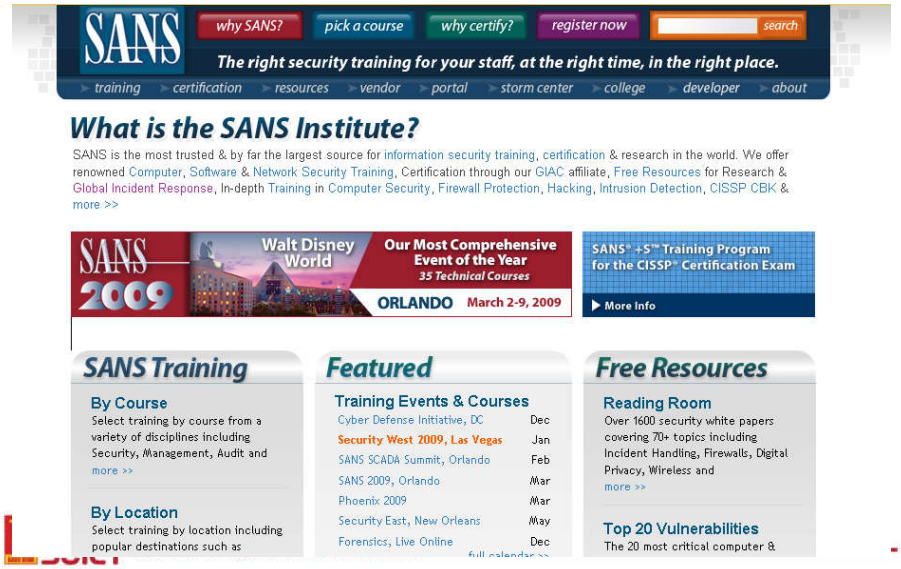
FIRST Forum of Incident Response and Security Teams

the CENTER for INTERNET SECURITY

(ISC)² SECURITY TRANSCENDS TECHNOLOGY

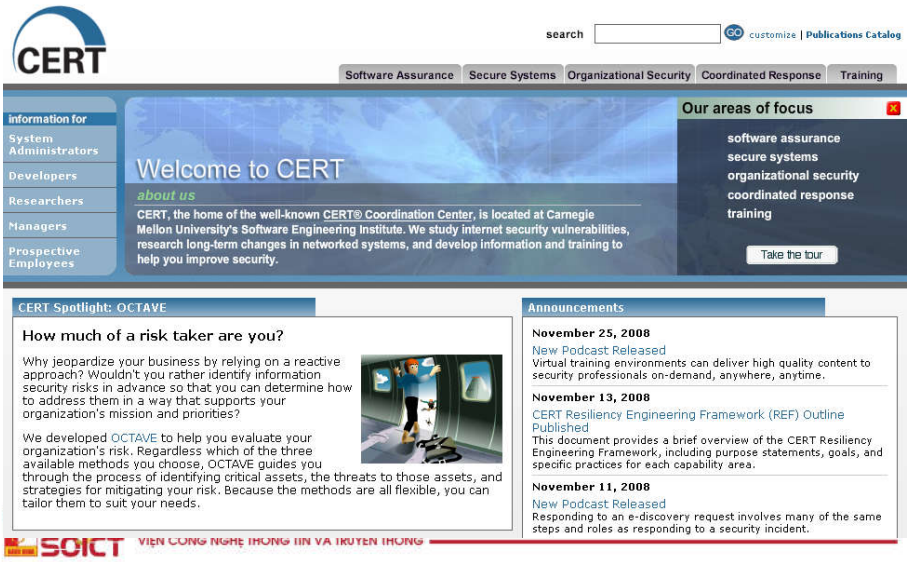
88

SANS



89

CERT



90

ISC2

Information security certifications Offered by (ISC)2

Systems Security Certified Practitioner (SCCP)

Certification and Accreditation Professional (CAP)

Certified Secure Software Lifecycle Professional (CSSLP)

Certified Information Systems Security Professional (CISSP)

91

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

4. Evolution of Hacking

92

Hacker Titles

- Phreaker
  - An individual that manipulates the phone network in order to cause it to perform a function that is normally not allowed such as to make free long distance calls.
  - Captain Crunch (John Drapper)
- Spammer
  - Individual that sends large quantities of unsolicited email messages.
  - Spammers often use viruses to take control of home computers to send out their bulk messages.
- Phisher
  - Individual uses email or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords.

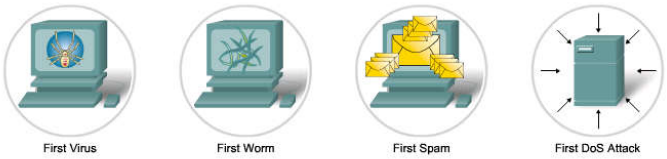
93

Evolution of Hacking

- 1960s - Phone Freaks (Phreaks)
- 1980s - Wardialing (WarGames)
- 1988 - Internet Worm
- 1993 - First def Con hacking conference held
- 1995 - First 5 year federal prison sentence for hacking
- 1997 - Nmap released
- 1997 - First malicious scripts used by script kiddies
- 2002 - Melissa virus creator gets 20 months in jail

94

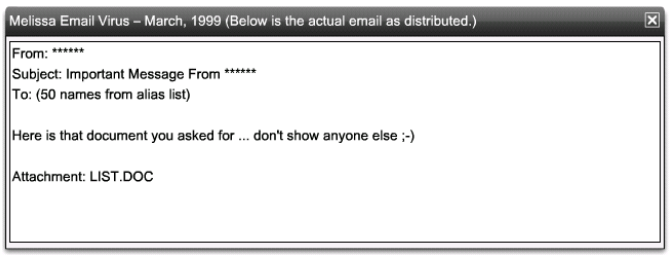
Security firsts …



95

First Email Virus

- The first email virus, the Melissa virus, was written by David Smith and resulted in memory overflows in Internet mail servers.
  - David Smith was sentenced to 20 months in federal prison and a US$5,000 fine.



96

First Worm

- Robert Morris created the first Internet worm with 99 lines of code.
  - When the Morris Worm was released, 10% of Internet systems were brought to a halt.

The Morris Internet Worm

All the following events occurred on the evening of Nov. 2, 1988.
6:00 PM - At about this time the Worm is launched.
8:49 PM - The Worm infects a VAX 8600 at the University of Utah (cs.utah.edu).
9:09 PM - The Worm initiates the first of its attacks to infect other computers from the infected VAX.
9:21 PM - The load average on the system reaches 5. (Load average is a measure of how hard the computer system is working. At 9:30 at night, the load average of the VAX was usually 1. Any load average higher than 5 causes delays in data processing.)
9:41 PM - The load average reaches 7.
10:01 PM - The load average reaches 16.
10:06 PM - At this point there are so many worms infecting the system that no new processes can be started. No users can use the system anymore.
10:20 PM - The system administrator kills off the worms.
10:41 PM - The system is reinfected and the load average reaches 27.
10:49 PM - The system administrator shuts down the system. The system is subsequently restarted.
11:21 PM - Reinfestation causes the load average to reach 37.

97

First SPAM

First Spam on ARPAnet – 1978 (Below is the actual spam message as distributed on ARPAnet.)

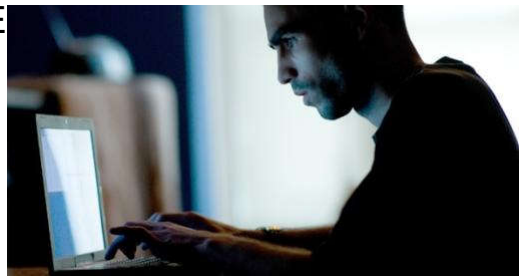
To: Everyone
From:
Subject: Presentation Today

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE

98

First DoS Attack

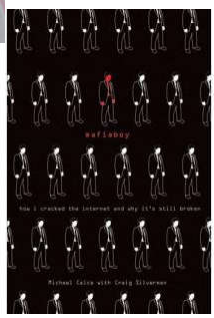
- MafiaBoy was the Internet alias of Michael Calce, a 15 year old high school student from Montreal, Canada.
- He launched highly publicized DoS attacks in Feb 2000 against Yahoo!, Amazon.com, Dell, Inc., E*TRADE



99

Mafiaboy

- In 2001, The Montreal Youth Court sentenced him on September 12, 2001 to eight months of "open custody," one year of probation, restricted use of the Internet, and a small fine.
- In 2005, Mr. Calce wrote as a columnist on computer security topics for the Francophone newspaper Le Journal de Montréal.
- In 2008, he published Mafiaboy: “How I Cracked the Internet and Why It's Still Broken.”
- He has also made numerous TV appearances.



100

Trends Driving Network Security

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

101

Legal and Governmental Policy Issues

- Organizations that operate vulnerable networks will face increasing and substantial liability.
  - http://en.wikipedia.org/wiki/Information_security#Laws_and_regulations
- US Federal legislation mandating security includes the following:
  - Gramm-Leach-Blilely (GLB) bill financial services legislation
  - Government Information Security Reform Act
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Children Internet Protection Act (CIPA)
  - The Payment Card Industry Data Security Standard (PCI DSS)
  - Sarbanes-Oxley Act of 2002

102

How to Keep on Top?

- Network security professionals must collaborate with professional colleagues more frequently than most other professions.
  - Attending workshops and conferences that are often affiliated with, sponsored or organized by local, national, or international technology organizations.
- Must also know about various security organizations which provide help on:
  - Detecting and responding to both established and emerging information security threats.
  - Operating system weaknesses, best practices for security, and security training and certification information is also available.

103

5. Network Attacks

104

Types of Attacks

- There are four categories of attacks:
  - **Malicious Code**: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - Access Attacks
  - Denial of Service (DoS) Attacks

105

Malware

- "Malicious software" is software designed to infiltrate a computer without the owner's informed consent.
- Malware includes:
  - Computer viruses
  - Worms
  - Trojan horses
  - Rootkits
  - Backdoors (Method of bypassing normal authentication procedures and usually installed using Trojan horses or worms.)
  - For profit (Spyware, botnets, keystroke loggers, and dialers)

106

Spyware

- Spyware is a strictly for-profit category of malware designed to:
  - Monitor a users web browsing.
  - Display unsolicited advertisements.
  - Redirect affiliate marketing revenues to the spyware creator.
- Spyware programs are generally installed by exploiting security holes or as Trojan horse programs such as most peer-to-peer applications.

107

Why Write Malicious Code?

- Most early worms and viruses were written as experiments or pranks generally intended to be harmless or merely annoying rather than to cause serious damage to computers.
- Young programmers learning about viruses and the techniques wrote them for the sole purpose that they could or to see how far it could spread.
  - In some cases the perpetrator did not realize how much harm their creations could do.
- As late as 1999, widespread viruses such as the Melissa virus appear to have been written chiefly as pranks.

108

Malicious Code Writing Today

- Malicious code writing has changed for profitable reasons.
  - Mainly due to the Internet and broadband access.
  - Since 2003 the majority of viruses and worms have been designed to take control of users' computers for black-market exploitation.
  - Infected "zombie computers" are used to send email spam, to host contraband data, or to engage in DDoS attacks as a form of extortion.
- In 2008, Symantec published:
  - The release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications.

109

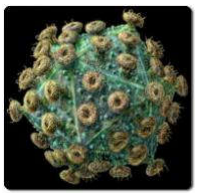
Viruses, Trojan horses, and Worms

- A **virus** is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
- A **worm** executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.
- 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.

110

Viruses

- A computer virus is a malicious computer program (executable file) that can copy itself and infect a computer without permission or knowledge of the user.
- A virus can only spread from one computer to another by:
  - Sending it over a network as a file or as an email payload.
  - Carrying it on a removable medium.
- Viruses need USER INTERVENTION to spread …



111

Viruses

- Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk.
- Others are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio messages.

112

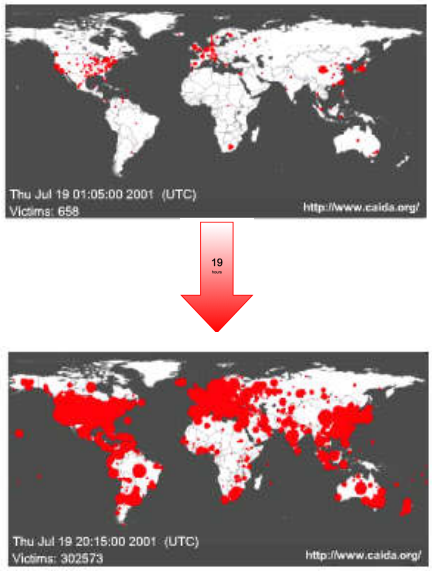
Worms

- Worms are a particularly dangerous type of hostile code.
  - They replicate themselves by independently exploiting vulnerabilities in networks.
  - Worms usually slow down networks.
- Worms DO NOT NEED USER INTERVENTION!
  - Worms do not require user participation and can spread extremely fast over the network.

113

SQL Slammer Worms

- In January 2001, the SQL Slammer Worm slowed down global Internet traffic as a result of DoS.
- Over 250,000 hosts were affected within 30 minutes of its release.
- The worm exploited a buffer overflow bug in Microsoft's SQL Server.
  - A patch for this vulnerability was released in mid-2002, so the servers that were affected were those that did not have the update patch applied.



114

Anatomy of a Worm

- The enabling vulnerability
  - A worm installs itself using an exploit vector on a vulnerable system.
- Propagation mechanism
  - After gaining access to devices, a worm replicates and selects new targets.
- Payload
  - Once the device is infected with a worm, the attacker has access to the host – often as a privileged user.
  - Attackers could use a local exploit to escalate their privilege level to administrator.

115

The year's most-hacked software 2009

- *"Kits that go by names like 'T-IFramer,' 'Liberty Exploit Systems' and 'Elenore' all turned up on underground markets selling for $300 to $500, Kandek says, and allow the attacker to install a Trojan program ready to download whatever malicious software a cybercriminal wishes, from spyware to click-fraud software. All three of those kits exploit three unique Adobe Reader bugs, along with a smaller number of bugs in Internet Explorer, Microsoft Office, Firefox and even Quicktime."*

Excerpt from the article at:

http://www.cbc.ca/technology/story/2009/12/16/f-forbes-adobe-hacked-software.html

116

Trojan Horse

- A Trojan horse is a program that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- Trojan horses may appear to be useful or interesting programs, or at the very least harmless to an unsuspecting user, but are actually harmful when executed.
- Trojan horses are not self-replicating which distinguishes them from viruses and worms.

117

Trojan Horse Classification

- Remote-access Trojan Horse
  - Enables unauthorized remote access
- Data sending Trojan Horse
  - Provides the attacker with sensitive data such as passwords
- Destructive Trojan Horse
  - Corrupts or deletes files
- Proxy Trojan Horse
  - User's computer functions as a proxy server
- FTP Trojan Horse (opens port 21)
  - Security software disabler Trojan Horse (stops anti-virus programs or firewalls from functioning)
- Denial of Service Trojan Horse (slows or halts network activity)

118

Five Phases of a Virus/Worm Attack

- Probe phase:
  - Vulnerable targets are identified using ping scans.
  - Application scans are used to identify operating systems and vulnerable software.
  - Hackers obtain passwords using social engineering, dictionary attack, brute-force, or network sniffing.
- Penetrate phase:
  - Exploit code is transferred to the vulnerable target.
  - Goal is to get the target to execute the exploit code through an attack vector, such as a buffer overflow, ActiveX or Common Gateway Interface (CGI) vulnerabilities, or an email virus.
- Persist phase:
  - After the attack is successfully launched in the memory, the code tries to persist on the target system.
  - Goal is to ensure that the attacker code is running and available to the attacker even if the system reboots.
  - Achieved by modifying system files, making registry changes, and installing new code.
- Propagate phase:
  - The attacker attempts to extend the attack to other targets by looking for vulnerable neighboring machines.
  - Propagation vectors include emailing copies of the attack to other systems, uploading files to other systems using file shares or FTP services, active web connections, and file transfers through Internet Relay Chat.
- Paralyze phase:
  - Actual damage is done to the system.
  - Files can be erased, systems can crash, information can be stolen, and distributed DDoS attacks can be launched.

119

How Do You Mitigate Viruses and Worms?

120

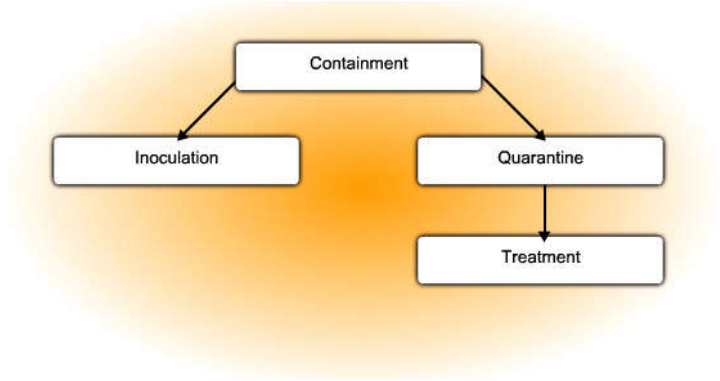
Viruses and Trojan Horses - Mitigation

- The primary means of mitigating virus and Trojan horse attacks is anti-virus software.
  - For total protection, host-based intrusion prevention systems (HIPS), such as Cisco Security Agent should also be deployed.
  - HIPS protects the OS kernel.
- Anti-virus software helps prevent hosts from getting infected and spreading malicious code.
  - However, antivirus software must be used properly.
  - Always update with the latest antivirus .dat and application versions.
  - Consider that it requires much more time to clean up infected computers than it does to maintain up-to-date anti-virus software and anti-virus definitions on the same machines.

121

Mitigating an Active Worm

- Worm attack mitigation requires diligence on the part of system and network administration staff.
- There is a four-phase process to mitigate an active worm attacks.



122

Worms - Mitigation

- Containment Phase:
  - Limit the spread of a worm infection to areas of the network that are already affected.
  - Compartmentalize and segment the network to slow down or stop the worm to prevent currently infected hosts from targeting and infecting other systems.
  - Use both outgoing and incoming ACLs on routers and firewalls at control points within the network.
- Inoculation Phase:
  - Runs parallel to or subsequent to the containment phase.
  - All uninfected systems are patched with the appropriate vendor patch for the vulnerability.
  - The inoculation process further deprives the worm of any available targets.

123

Worms - Mitigation

- Quarantine Phase:
  - Track down and identify infected machines within the contained areas and disconnect, block, or remove them.
  - This isolates these systems appropriately for the Treatment Phase.
- Treatment Phase:
  - Actively infected systems are disinfected of the worm.
  - Terminate the worm process, remove modified files or system settings that the worm introduced, and patch the vulnerability the worm used to exploit the system.
  - In more severe cases, completely reinstalling the system to ensure that the worm and its by products are removed.

124

Example: Mitigating SQL Slammer

- The SQL Slammer worm used UDP port 1434.
  - This port should normally be blocked by a firewall on the perimeter.
  - However, most infections enter internally and therefore, to prevent the spreading of this worm it would be necessary to block this port on all devices throughout the internal network.
- When SQL Slammer was propagating, some organizations could not block UDP port 1434 because it was required to access the SQL Server for legitimate business transactions.
  - Permit only selective access to a small number of clients using SQL Server.

125

Types of Attacks

- There are four categories of attacks:
  - Malicious Code: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - Access Attacks
  - Denial of Service (DoS) Attacks

126

Reconnaissance

- Reconnaissance also known as information gathering is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
  - In most cases, precedes an access or DoS attack.
- Reconnaissance attacks can consist of the following:
  - Internet information queries
  - Ping sweeps
  - Port scans
  - Packet sniffers

127

Internet Information Queries

- DNS queries can reveal information such as who owns a particular domain and what addresses have been assigned to that domain.
  - Use tools such as **whois**, **nslookup**, …

128

Ping Sweeps and Port Scans

- A ping sweep, or ICMP sweep, scans to determine which range of IP addresses map to live hosts.
- A port scan consists of sending a message to each port, one port at a time.
  - Response received indicates whether the port is used and can therefore be probed for weakness.

129

Ping Sweeps and Port Scans

- As legitimate tools, ping sweep and port scan applications run a series of tests against hosts to identify vulnerable services.
- The information is gathered by examining IP addressing and port data from both TCP and UDP ports.

130

Packet Sniffing

- A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
  - Packet sniffers can only work in the same collision domain as the network being attacked.
  - Promiscuous mode is a mode in which the network adapter card sends all packets that are received on the physical network wire to an application for processing.
  - Wireshark is an example of a packet sniffer.

131

Packet Sniffing

- Some network applications (FTP, Telnet, TFTP, SNMP, …) distribute network packets in plaintext.
  - The packets can be processed and understood by packet sniffing applications.
  - Numerous freeware and shareware packet sniffers are available that do not require the user to understand anything about the underlying protocols.

132

Types of Attacks

- There are four categories of attacks:
  - Malicious Code: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - **Access Attacks**
  - Denial of Service (DoS) Attacks

133

Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information for these reasons:
  - Retrieve data
  - Gain access
  - Escalate their access privileges

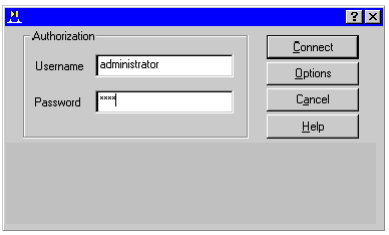
134

Access Attacks

- Access attacks can be performed in a number of different ways, including:
  - Password attacks
  - Trust exploitation
  - Port redirection
  - Man-in-the-middle attacks
  - Buffer overflow

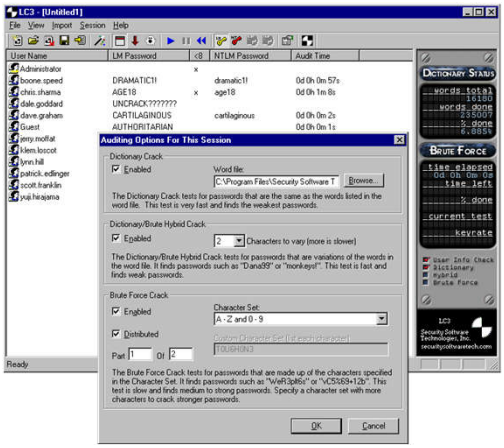
Password Attacks

- Hackers implement password attacks using the following:
  - Brute-force attacks
  - Trojan horse programs
  - IP spoofing
  - Packet sniffers



Password Attack Example

- L0phtCrack ("loft-crack") takes the hashes of passwords and generates the plaintext passwords from them.
- Passwords are compromised using one of two methods:
  - Dictionary cracking
  - Brute-force computation



Trust Exploitation

- Trust exploitation refers to an individual taking advantage of a trust relationship within a network.
- An example of when trust exploitation takes place is when a perimeter network is connected to a corporate network.
  - These network segments often contain DNS, SMTP, and HTTP servers.
  - Because these servers all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems also trust systems that are attached to the same network.

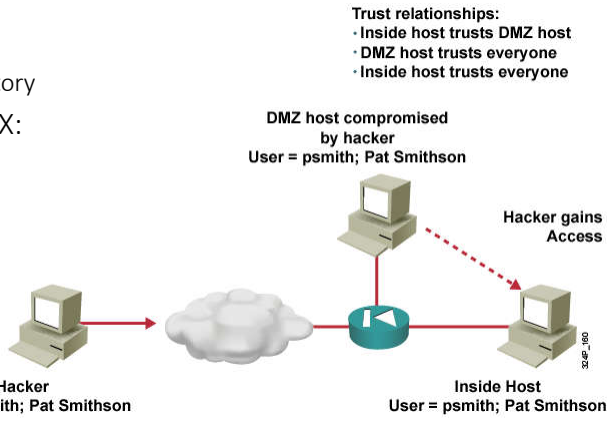
Trust Exploitation

- Another example of trust exploitation is a Demilitarized Zone (DMZ) host that has a trust relationship with an inside host that is connected to the inside firewall interface.
- The inside host trusts the DMZ host.
  - When the DMZ host is compromised, the attacker can leverage that trust relationship to attack the inside host.

139

Trust Exploitation

- A hacker leverages existing trust relationships.
- Several trust models exist:
  - Windows:
    - Domains
    - Active directory
  - Linux and UNIX:
    - NIS
    - NIS+



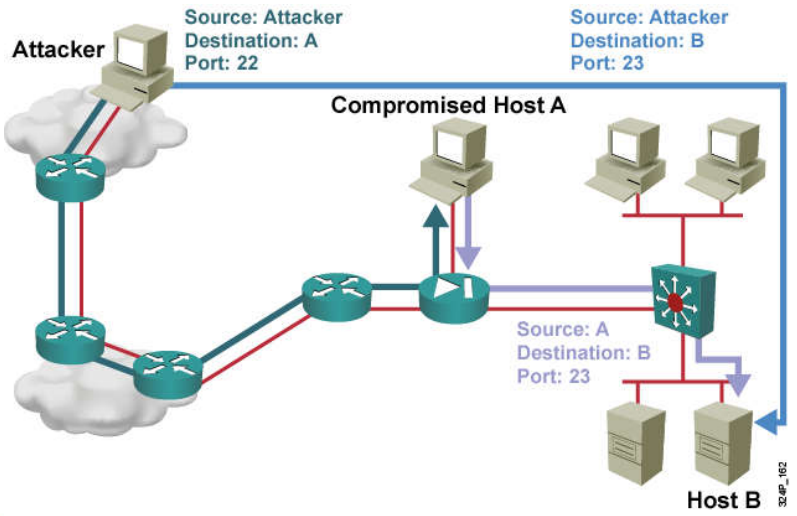
140

Port Redirection

- A port redirection attack is a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise have been dropped.
  - Port redirection bypasses the firewall rule sets by changing the normal source port for a type of network traffic.
  - You can mitigate port redirection by using proper trust models that are network-specific.
  - Assuming a system is under attack, an IPS can help detect a hacker and prevent installation of such utilities on a host.

141

Port Redirection



142

"Man-in-the-Middle" Attacks

- Man-in-the-middle attacks have these purposes:
  - Theft of information
  - Hijacking of an ongoing session to gain access to your internal network resources
  - Traffic analysis to obtain information about your network and network users
  - DoS
  - Corruption of transmitted data
  - Introduction of new information into network sessions
- An example of a man-in-the-middle attack is when someone working for your ISP gains access to all network packets that transfer between your network and any other network.

143

Types of Attacks

- There are four categories of attacks:
  - Malicious Code: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - Access Attacks
  - **Denial of Service (DoS) Attacks**

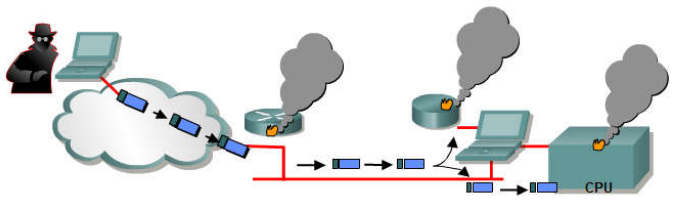
144

Denial of Service Attack (DoS)

- Among the most difficult to completely eliminate because they require so little effort to execute.
- Types of DoS attacks include:
  - Ping of death
  - Smurf Attack
  - TCP SYN flood attack
- Others include packet fragmentation and reassembly, E-mail bombs, CPU hogging, Malicious applets, Misconfiguring routers, the chargen attack, out-of-band attacks such as WinNuke, Land.c, Teardrop.c, and Targa.c.

DoS Attacks

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



Resource overloads	Malformed data
• Disk space, bandwidth, buffers, and so on. • Ping floods: smurf, and so on. • Packet storms: UDP bombs, fraggle, and so on.	• Oversized packets: ping of death, and so on. • Overlapping packets: winuke, and so on. • Un-handled data: teardrop, and so on.

Denial-of-Service Facts

- Commonly used against information stores like web sites
- Simple and usually quite effective
- Does not pose a direct threat to sensitive data
- The attacker tries to prevent a service from being used and making that service unavailable to legitimate users
- Attackers typically go for high visibility targets such as the web server, or for infrastructure targets like routers and network links

147

Denial-of-Service Example

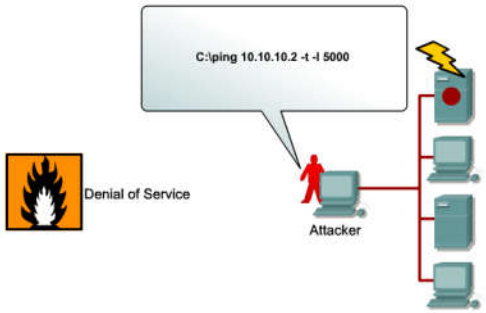
If a mail server is capable of receiving and delivering 10 messages a second, an attacker simply sends 20 messages per second. The legitimate traffic (as well as a lot of the malicious traffic) will get dropped, or the mail server might stop responding entirely.

- This type of an attack may be used as a diversion while another attack is made to actually compromise systems
- In addition, administrators are likely to make mistakes during an attack and possibly change a setting that creates a vulnerability that can be further exploited

148

Types of Denial-of-Service Attacks

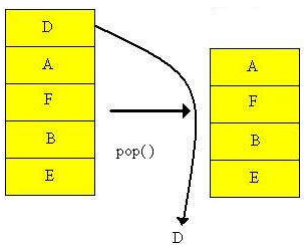
- Buffer Overflow Attacks
- SYN Flood Attack
- Teardrop Attacks
- Smurf Attack
- DNS Attacks
- Email Attacks
- Physical Infrastructure Attacks
- Viruses/Worms



149

DoS - Buffer Overflow Attacks

The most common DoS attack sends more traffic to a device than the program anticipates that someone might send Buffer Overflow.



150

DoS - SYN Flood Attack

- When connection sessions are initiated between a client and server in a network, a very small space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up a session.
- The session-establishing packets include a SYN field that identifies the sequence order.
- To cause this kind of attack, an attacker can send many packets, usually from a spoofed address, thus ensuring that no response is sent.

DoS - Teardrop Attack

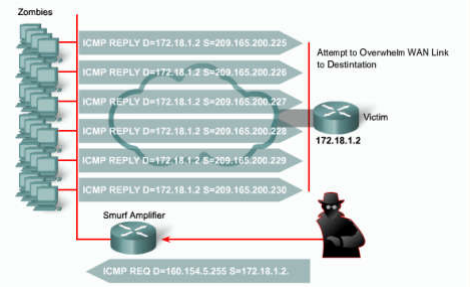
- Exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments.
- The fragmented packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system.
- In the teardrop attack, an attacker's IP puts a confusing value in the second or later fragment. If the receiving operating system cannot cope with such fragmentation, then it can cause the system to crash.

DoS - Smurf Attack

The attacker sends an IP ping request to a network site.

The ping packet requests that it be broadcast to a number of hosts within that local network.

The packet also indicates that the request is from a different site, i.e. the victim site that is to receive the denial of service.



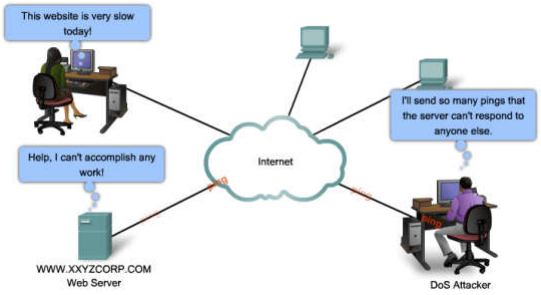
This is called IP Spoofing--the victim site becomes the address of the originating packet.

The result is that lots of ping replies flood back to the victim host. If the flood is big enough then the victim host will no longer be able to receive or process "real" traffic.

153

DoS - DNS Attacks

- A famous DNS attack was a DDoS "ping" attack. The attackers broke into machines on the Internet (popularly called "zombies") and sent streams of forged packets at the 13 DNS root servers via intermediary legitimate machines.



- The goal was to clog the servers, and communication links on the way to the servers, so that useful traffic was gridlocked. The assault is not DNS-specific--the same attack has been used against several popular Web servers in the last few years.

154

DoS - Email Attacks

- When using Microsoft Outlook, a script reads your address book and sends a copy of itself to everyone listed there, thus propagating itself around the Internet.
- The script then modifies the computer's registry so that the script runs itself again when restarted.

155

DoS - Physical Infrastructure Attacks

- Someone can just simply snip your cables! Fortunately this can be quickly noticed and dealt with.
- Other physical infrastructure attacks can include recycling systems, affecting power to systems and actual destruction of computers or storage devices.

156

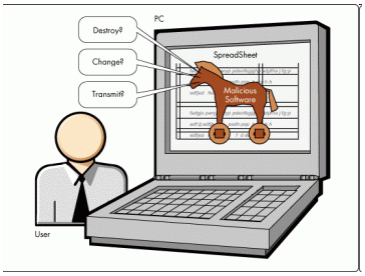
DoS - Viruses/Worms

- Viruses or worms, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus.
- Available bandwidth can become saturated as the virus/worm attempts to replicate itself and find new victims.

157

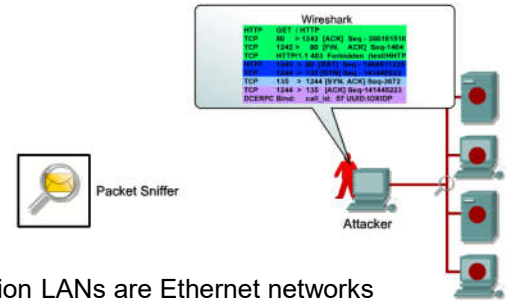
Malicious Code Attacks

- Malicious code attacks refers to viruses, worms, Trojan horses, logic bombs, and other uninvited software
- Damages personal computers, but also attacks systems that are more sophisticated
- Actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems
- Costs can be significant



158

Packet Sniffing Attacks



- Most organization LANs are Ethernet networks
- On Ethernet-based networks, any machine on the network can see the traffic for every machine on that network
- Sniffer programs exploit this characteristic, monitoring all traffic and capturing the first 128 bytes or so of every unencrypted FTP or Telnet session (the part that contains user passwords)

159

Information Leakage Attacks

- Attackers can sometimes get data without having to directly use computers
- Exploit Internet services that are intended to give out information
- Induce these services to reveal extra information or to give it out to unauthorized people
- Many services designed for use on local area networks do not have the security needed for safe use across the Internet
- Thus these services become the means for important information leakage

160

Social Engineering Attacks

- Hacker-speak for tricking a person into revealing some confidential information
- Social Engineering is defined as an attack based on deceiving users or administrators at the target site
- Done to gain illicit access to systems or useful information
- The goals of social engineering are fraud, network intrusion, industrial espionage, identity theft, etc.

161

Ping of death

- Legacy attack that sent an echo request in an IP packet larger than the maximum packet size of 65,535 bytes.
  - Sending a ping of this size can crash the target computer.
- A variant of this attack is to crash a system by sending ICMP fragments, which fill the reassembly buffers of the target.

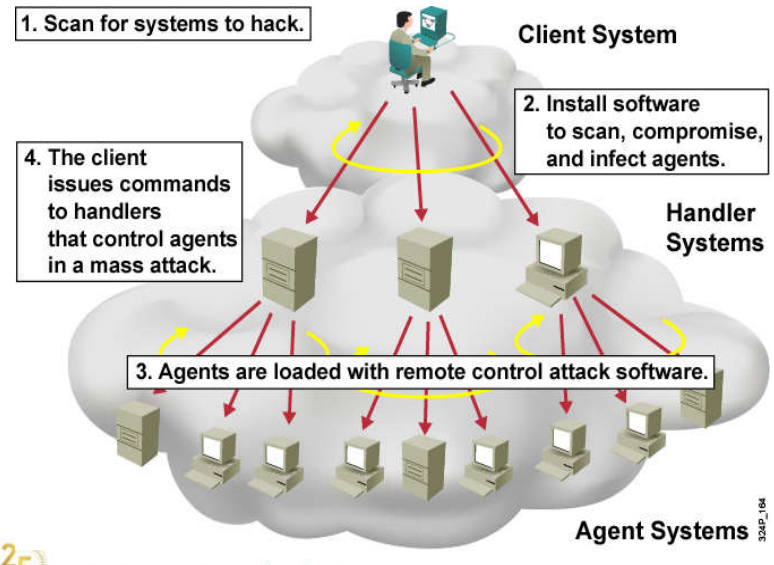
162

DoS and DDoS Attacks and Mitigation

- A DDoS attack and the simpler version of a DoS attack on a server, send extremely large numbers of requests over a network or the Internet.
  - These many requests cause the target server to run well below optimum speeds.
  - Consequently, the attacked server becomes unavailable for legitimate access and use.
  - By overloading system resources, DoS and DDoS attacks crash applications and processes by executing exploits or a combination of exploits.
  - DoS and DDoS attacks are the most publicized form of attack and are among the most difficult to completely eliminate.

163

DDoS Attack Example



164

DDoS Attack Risks

- DDoS attack risks include:
  - Downtime and productivity loss
  - Revenue loss from sales and support services
  - Lost customer loyalty
  - Theft of information
  - Extortion
  - Stock price manipulation
  - Malicious competition

165

Distributed Denial of Service Attack (DoS)

- DDoS attacks are designed to saturate network links with spurious data which can overwhelm a link causing legitimate traffic to be dropped.
  - DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale.
  - Typically hundreds or thousands of attack points attempt to overwhelm a target.
- Examples of DDoS attacks include the following:
  - Tribe Flood Network (TFN)
  - Stacheldraht

166

Reconnaissance Attacks - Countermeasures

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping.
- Using encryption that meets the data security needs of the organization without imposing an excessive burden on the system resources or the users.
- Using switched networks.

167

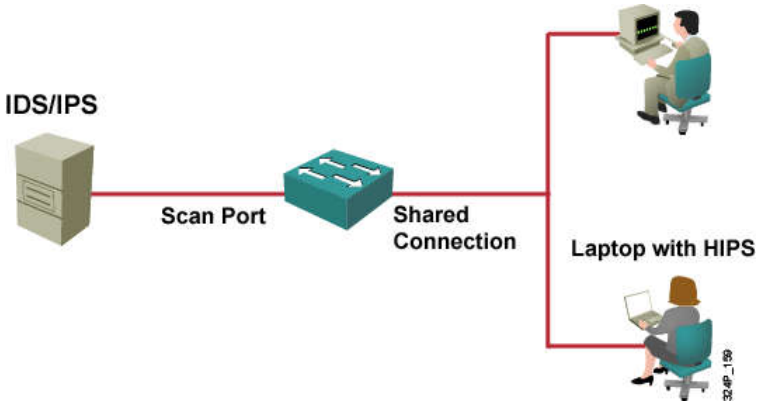
Port Scan and Ping Sweep Mitigation

- Port scanning and ping sweeping is not a crime and there is no way to stop these scans and sweeps when a computer is connected to the Internet.
  - There are ways to prevent damage to the system.
- Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers.
  - When these services are turned off, network diagnostic data is lost.

168

Ping Sweeps and Port Scans Mitigation

- Can't be prevented without compromising network capabilities.
  - However, damage can be mitigated using intrusion prevention systems (IPS) at network and host levels.



169

Packet Sniffer Mitigation

- Authentication
  - Strong authentication is a first line for defense.
- Cryptography
  - If a communication channel is cryptographically secure, the only data a packet sniffer detects is cipher text.
- Anti-sniffer tools
  - Antisniffer tools detect changes in the response time of hosts to determine whether the hosts are processing more traffic than their own traffic loads would indicate.
- Switched infrastructure
  - A switched infrastructure obviously does not eliminate the threat of packet sniffers but can greatly reduce the sniffers' effectiveness.

170

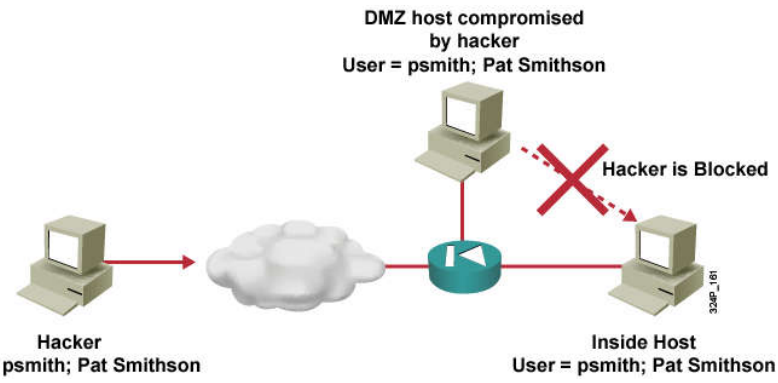
Password Attack Mitigation

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

171

Trust Exploitation Attack Mitigation

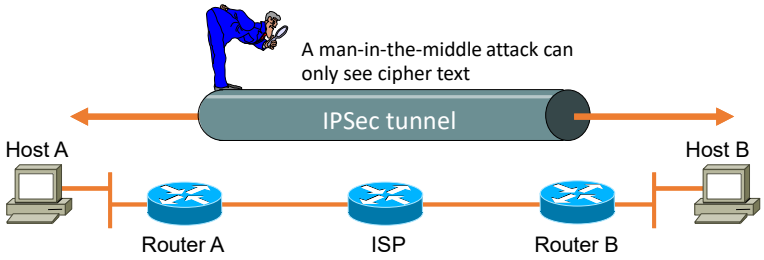
- Trust levels within a network should be tightly restrained by ensuring that systems inside a firewall never absolutely trust systems outside the firewall.



172

Man-in-the-Middle Mitigation

- Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography (encryption).



173

DoS and DDoS Attack Mitigation

- Anti-DoS features on routers and firewalls:
  - Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack.
  - These features often involve limits on the amount of half-open TCP connections that a system allows at any given time.
- Anti-spoof features on routers and firewalls:
  - Proper configuration of anti-spoof features on your routers and firewalls can reduce your risk of attack.
  - These features include an appropriate filtering with access lists, unicast reverse path forwarding that looks up the routing table to identify spoofed packets, disabling of source route options, and others.

174

DoS and DDoS Attack Mitigation

- Traffic rate limiting at the ISP level:
  - An organization can implement traffic rate limiting with its Service Provider.

175

IP Spoofing Attack Mitigation

- The threat of IP spoofing can be reduced, but not eliminated, using these measures:
  - Access control configuration
  - Encryption
  - RFC 3704 filtering
- Additional authentication requirement that does not use IP address-based authentication; examples are:
  - Cryptographic (recommended)
  - Strong, two-factor, one-time passwords

176

10 Best Practices

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.

177

10 Best Practices

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.
   - http://www.networkworld.com/news/2010/091610-social-networks.html?source=NWWNLE_nlt_daily_pm_2010-09-16
   - http://searchsecurity.techtarget.com/news/1519804/Phishing-attacks-target-users-of-Facebook-other-social-networks?asrc=EM_NLN_12420860&track=NL-102&ad=784799&
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.

178

ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

6. Thinking Like a Hacker

179

Know Thine Enemy

- "If you know yourself but not your enemy, for every victory gained you will also suffer a defeat."
  - Sun Tzu – The Art of War
- Before learning how to defend against attacks, you need to know how a potential attacker operates.

180

Hacking a Network

- The goal of any hacker is to compromise the intended target or application.
- Hackers begin with little or no information about the intended target.
- Their approach is always careful and methodical—never rushed and never reckless.
- The seven-step process outlined on the next slide is a good representation of the method that hackers use – and a starting point for an analysis of how to defeat it.

181

Seven Steps to Hacking a Network

- Step 1 — Perform footprint analysis (reconnaissance).
- Step 2 — Detail the information.
- Step 3 — Manipulate users to gain access.
- Step 4 — Escalate privileges.
- Step 5 — Gather additional passwords and secrets.
- Step 6 — Install back doors.
- Step 7 — Leverage the compromised system.

182

Step 1 - Footprint Analysis (Reconnaissance)

- Gain knowledge of acquisitions using Web pages, phone books, company brochures, subsidiaries, etc.
- Use commands to develop a more detailed footprint:
  - **nslookup** command to reconcile domain names against IP addresses of the company's servers and devices.
  - **traceroute** command to help build topology.
- Use program and utilities:
  - **WHOIS** queries (http://www.who.is/)
  - Port scanning to find open ports and operating systems installed on hosts.
  - **Nmap**: Network Mapper (Nmap) is a free open source utility for network exploration or security auditing.

183

How to Defeat Footprinting

- Keep all sensitive data off-line (business plans, formulas, and proprietary documents).
- Minimize the amount of information on your public website.
- Examine your own website for insecurities.
- Run a ping sweep on your network.
- Familiarize yourself with one or more of the five Regional Internet Registries – such as ARIN for North America – to determine network blocks.

184

Step 2 - Detail the Information

- Find your server applications and versions:
  - What are your web, FTP, and mail server versions?
  - Listen to TCP and UDP ports and send random data to each.
  - Cross-reference information to vulnerability databases to look for potential exploits.
- Exploit selected TCP ports, for example:
  - Windows NT, 2000, and XP file sharing using SMB protocol which uses TCP port 445.
  - In Windows NT, SMB runs on top of NetBT using ports 137, 138 (UDP), and 139 (TCP).

185

Software Tools

- A great deal of hacker tools are available:
  - Netcat: Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol.
  - Microsoft EPDump and Remote Procedure Call (RPC) Dump: These tools provide information about Microsoft RPC services on a server:
    - The Microsoft EPDump application shows what is running and waiting on dynamically assigned ports.
    - The RPC Dump (rpcdump.exe) application is a command-line tool that queries RPC endpoints for status and other information on RPC.
  - GetMAC: This application provides a quick way to find the MAC (Ethernet) layer address and binding order for a computer running Microsoft Windows 2000 locally or across a network.
  - Software development kits (SDKs): SDKs provide hackers with the basic tools that they need to learn more about systems.

186

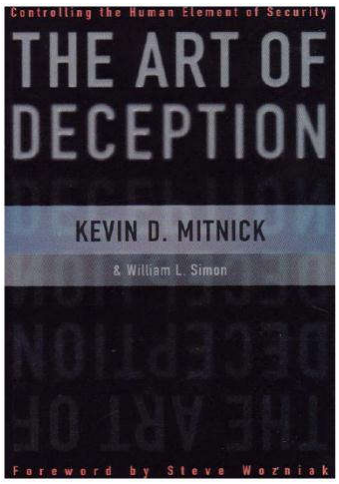
Step 3 - Manipulate Users to Gain Access

- Even with the most sophisticated security in place, a company is still vulnerable because of securities weakest link: People!
- The first thing that hackers need is a password and there are two ways to get that password:
  - Social engineering
  - Password cracking attacks

187

Step 3 - Manipulate Users to Gain Access

- Social engineering is a way to manipulate people inside the network to provide the information needed to access the network.
  - A computer is not required!!
  - Social engineering by telephone
  - Dumpster diving
  - Reverse social engineering
- Recommended reading:
  - "The Art of Deception: Controlling the Human Element of Security"
  - Mitnik, KD and Simon, WL; Wiley; New Ed edition



188

Social Engineering Example #1

- Call in the middle of the night:
  - 'Hi this is _____ from Bell. I'm very sorry to wake you up but we've noticed some very unusual activity on your Bell calling card and we're wondering if you're using it to call Baghdad, Iraq for the last 6 hours?'
  - 'Well, we have a call that's actually still active right now and it's now well over $2,000 worth of charges. I'll terminate that call right now but unfortunately you are responsible for the charges made on your card.'
  - 'Look I sympathize with you and can see that you've been victimized here, but if I get rid of that charge I can loose my job.'
  - 'Okay … but you'll have to confirm some details first. What is your full name and address?'
  - 'Can you confirm the Bell calling card number?'
  - 'Finally, please confirm your PIN number?'
  - 'Great. Everything matches. I'll get rid of that charge for you.'
  - 'You're welcome and thank you for being a Bell Canada client.'

189

Social Engineering Example #2

- The facilitator of a live Computer Security Institute neatly illustrated the vulnerability of help desks when he "dialed up" a phone company, got transferred around, and reached the help desk:
  - 'Who's the supervisor on duty tonight?'
  - 'Let me talk to _____.' (he's transferred)
  - 'Hi _____, this is _____ from security in the IT center. Having a bad day?'
  - 'No, why?...Your systems are down.'
    - Response: 'my systems aren't down, we're running fine.'
  - 'Hmmm … Really? Do me a favor then and sign off and on again.'
  - 'We didn't even show a blip, we show no change. Sign off again.'
  - 'There's something funny going on here. I'm going to have to sign on with your ID to figure out what's happening. Let me have your user ID and password.'

190

Other Social Engineering Examples

- A confused and befuddled person will call a clerk and meekly request a password change.
- People identifying themselves as executives, will telephone a new system administrator and demand access to their account IMMEDIATELY!
- Somebody will call and confidently instruct a computer operator to type in a few lines of instruction at the console.
- At an airport, somebody will look over a shoulder, 'shoulder surfing,' (sometimes even using binoculars or camcorders) as telephone credit card numbers or ATM PINs are keyed.

191

Common Social Engineering Methods

- Posing as a fellow employee, as an employee of a vendor, partner company, or law enforcement, as someone in authority, as a new employee requesting help, as a vendor or systems manufacturer calling to offer a system patch or update.
- Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help.
- Sending free software or patch for victim to install.
- Sending a virus or Trojan Horse as an email attachment.
- Using a false pop-up window asking user to log in again or sign on with password.
- Leaving a USB stick, or CD around the workplace with malicious software on it.
- Using insider lingo and terminology to gain trust.
- Offering a prize for registering at a Web site with username and password.
- Dropping a document or file at company mail room for intra-office delivery.
- Modifying fax machine heading to appear to come from an internal location.
- Asking receptionist to receive then forward a fax.
- Asking for a file to be transferred to an apparently internal location.
- Getting a voice mailbox set up so call backs perceive attacker as internal.
- Pretending to be from remote office and asking for email access locally.

192

Warning Signs of an Attack

- Refusal to give call back number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of non compliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

193

Password Cracking

- Hackers use many tools and techniques to crack passwords:
  - Word lists
  - Brute force
  - Hybrids
  - The yellow Post-It stuck on the side of the monitor, or in top of desk drawer
- Password cracking attacks any application or service that accepts user authentication, including those listed here:
  - NetBIOS over TCP (TCP 139)
  - Direct host (TCP 445)
  - FTP (TCP 21)
  - Telnet (TCP 23)
  - SNMP (UDP 161)
  - PPTP (TCP 1723)
  - Terminal services (TCP 3389)

194

Step 4 - Escalate Privileges

- After securing a password for a user account and user-level privileges to a host, hackers attempt to escalate their privileges.
- The hacker will review all the information he or she can see on the host:
  - Files containing user names and passwords
  - Registry keys containing application or user passwords
  - Any available documentation (for example, e-mail)
- If the host cannot be seen by the hacker, the hacker may launch a Trojan application such as W32/QAZ to provide it.

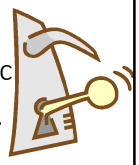
195

Step 5 – Gather Passwords and Secrets

- Hackers target:
  - The local security accounts manager database
  - The active directory of a domain controller
- Hackers can use legitimate tools including pwdump and lsadump applications.
- Hackers gain administrative access to all computers by cross-referencing user names and password combinations.

196

Step 6 - Install Back Doors and Port Redirectors



- Back doors:
  - Provide a way back into the system if the front door is loc
  - The way into the system that is not likely to be detected.
- Back doors may use reverse trafficking:
  - Example: Code Red which used TCP port 80 to instruct unpatched web servers to execute a TFTP connection from the server.
- Port redirectors:
  - Port redirectors can help bypass port filters, routers, and firewalls and may even be encrypted over an SSL tunnel to evade intrusion detection devices.

197

Step 7 - Leverage the Compromised System

- Back doors and port redirectors let hackers attack other systems in the network.
- Reverse trafficking lets hackers bypass security mechanisms.
- Trojans let hackers execute commands undetected.
- Scanning and exploiting the network can be automated.
- The hacker remains behind the cover of a valid administrator account.
- The whole seven-step process is repeated as the hacker continues to penetrate the network.

198

Best Practices to Defeat Hackers

- Keep patches up to date.
- Shut down unnecessary services and ports.
- Use strong passwords and change them often.
- Control physical access to systems.
- Avoid unnecessary web page inputs.
  - Some websites allow users to enter usernames and passwords.
  - A hacker can enter more than just a username and programmers should limit input characters and not accept invalid characters (| ; < >).
- Perform system backups and test them on a regular basis.
- Educate users about social engineering.
- Encrypt and password-protect sensitive data.
- Use appropriate security hardware and software.
- Develop a written security policy for the company.

199

200