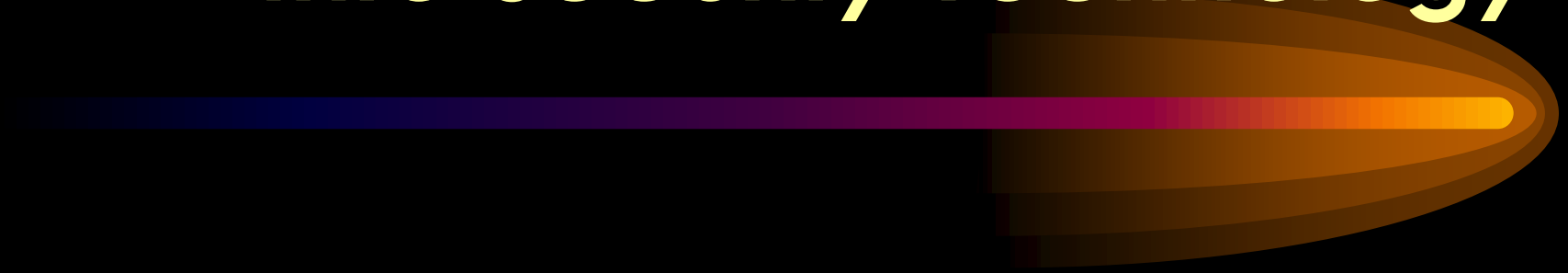
NANYANG POLYTECHNIC

Info Security Technology



Topic 1

Introduction to Information Security

References

- Security+ Guide to Network Security Fundamentals, 4th Edition; Mark Ciampa.
  - Chapter 1: Introduction to Security
  - Chapter 14: Risk Mitigition (Pg 539-550)

Objectives

- Describe Confidentiality, Integrity and Availablity(CIA)
- Describe the challenges of securing information
- Define information security
- Identify the types of attackers
- List the basic steps of an attack
- Describe the five steps in a defense
- Understand how risk can be mitigated through security policies
- Appreciate computer misuse laws and information ethics

Challenges of Securing Information

- No single solution to protect computer and securing information
- Different types of attacks
- Difficult to defend against attacks

2015 Crime types

By Victim Count			
Crime Type	*Victim Count*	*Crime Type*	*Victim Count*
Non-Payment/Non-Delivery	67,375	Lottery/Sweepstakes	5,324
419/Overpayment	30,855	Malware/Scareware	3,294
Identity Theft	21,949	Corporate Data Breach	2,499
Auction	21,510	Ransomware	2,453
Other	19,963	IPR/Copyright and Counterfeit	1,931
Personal Data Breach	19,632	Investment	1,806
Employment	18,758	Crimes Against Children	1,348
Extortion	17,804	Civil Matter	1,148
Credit Card Fraud	17,172	Re-shipping	1,073
Phishing/Vishing/Smishing/Pharming	16,594	Denial of Service	1,020
Advanced Fee	16,445	Virus	971
Harassment/Threats of Violence	14,812	Health Care Related	465
Confidence Fraud/Romance	12,509	Charity	411
No Lead Value	12,187	Terrorism	361
Government Impersonation	11,832	Hacktivist	211
Real Estate/Rental	11,562	Gambling	131
Business Email Compromise	7,837	Criminal Forums	62
Misrepresentation	5,458		

Source : https://pdf.ic3.gov/2015_IC3Report.pdf

Norton Cyber Crime reports

- 2013 Norton Cyber CrimeReport - http://www.slideshare.net/marianmerritt/the-norton-report-2013
- 2015 Mcafee Threat Prediction - http://www.mcafee.com/sg/resources/misc/infographic-threats-predictions-2015.pdf
- 2015 Mcafee Threat report - http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q3-2014.pdf

Cyber Crime stories (Read)

http://us.norton.com/cybercrime-stories/promo

- Cybercrime Stories: Sandra
- Cybercrime Stories: Michelle
- Cybercrime Stories: Koby
- Cybercrime Stories: Steve

Challenges of Securing Information

- There is no simple solution to securing information
- This can be seen through the different types of attacks that users face today
  - As well as the difficulties in defending against these attacks

What Is Information Security?

- What are the assets worth protecting?
- Key assets & Priority of assets?
- Who are your potential enemies?
- How to find weakness in yourselves ?

"If you know others and know yourself, you will not be imperilled in a hundred battles"

Defining Information Security

- Security
  - Steps to protect person or property from harm
    - Harm may be intentional or non intentional
  - Sacrifices convenience for safety
- Information security
  - Guarding digitally-formatted information:
    - That provides value to people and organizations

Different Types of Attacks

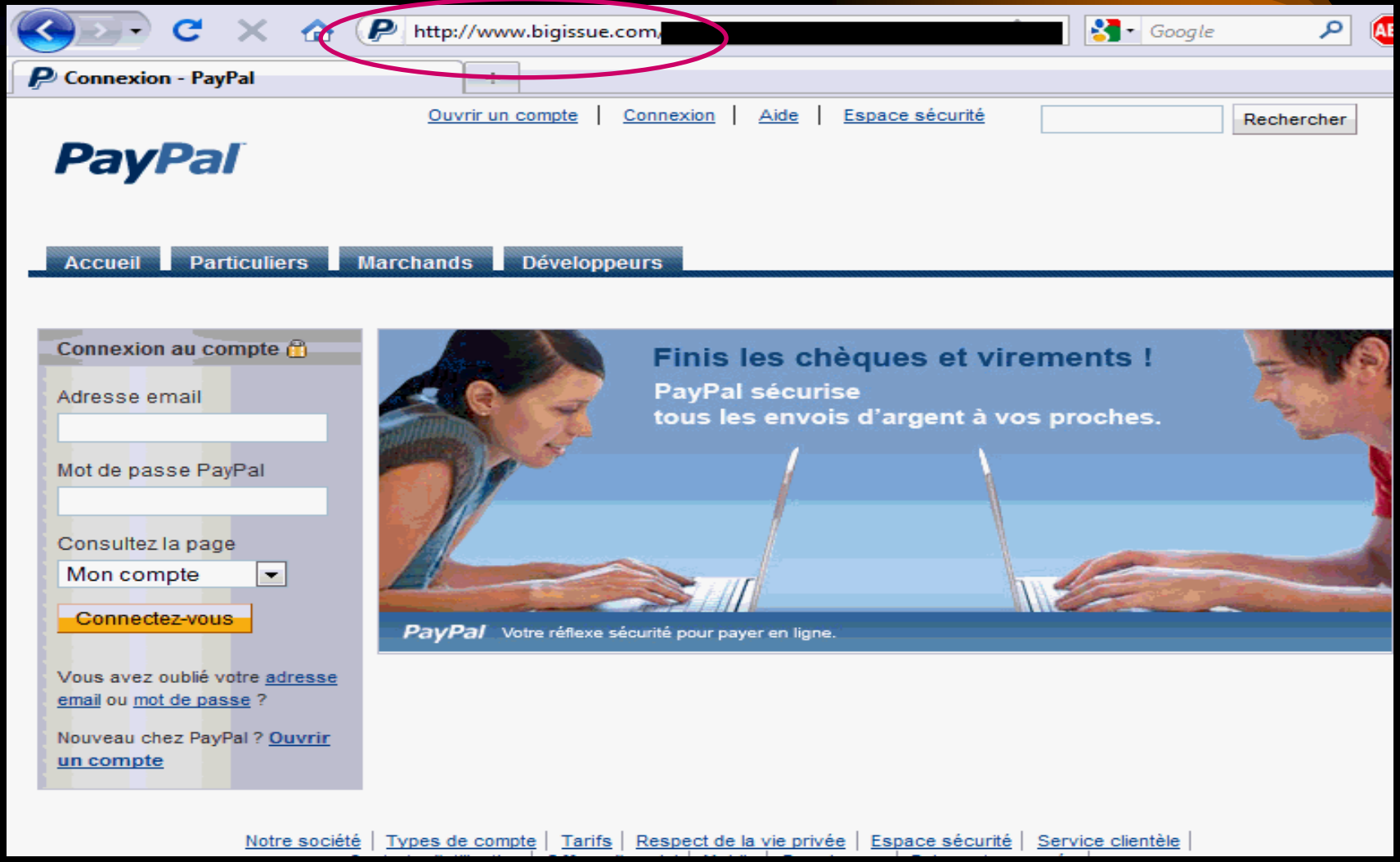
- Booby-trapped Web pages are growing at an increasing rate
- Hacktivism through Anonymous Attack
- Advanced Persistent Threat
- Mobile devices are targeted
- Security statistics: 70% of Singapore Net Users hit by Cybercrime

Booby-trapped Web pages

- Hackers make 57,000 booby-trapped websites weekly: experts
  September 10, 2010

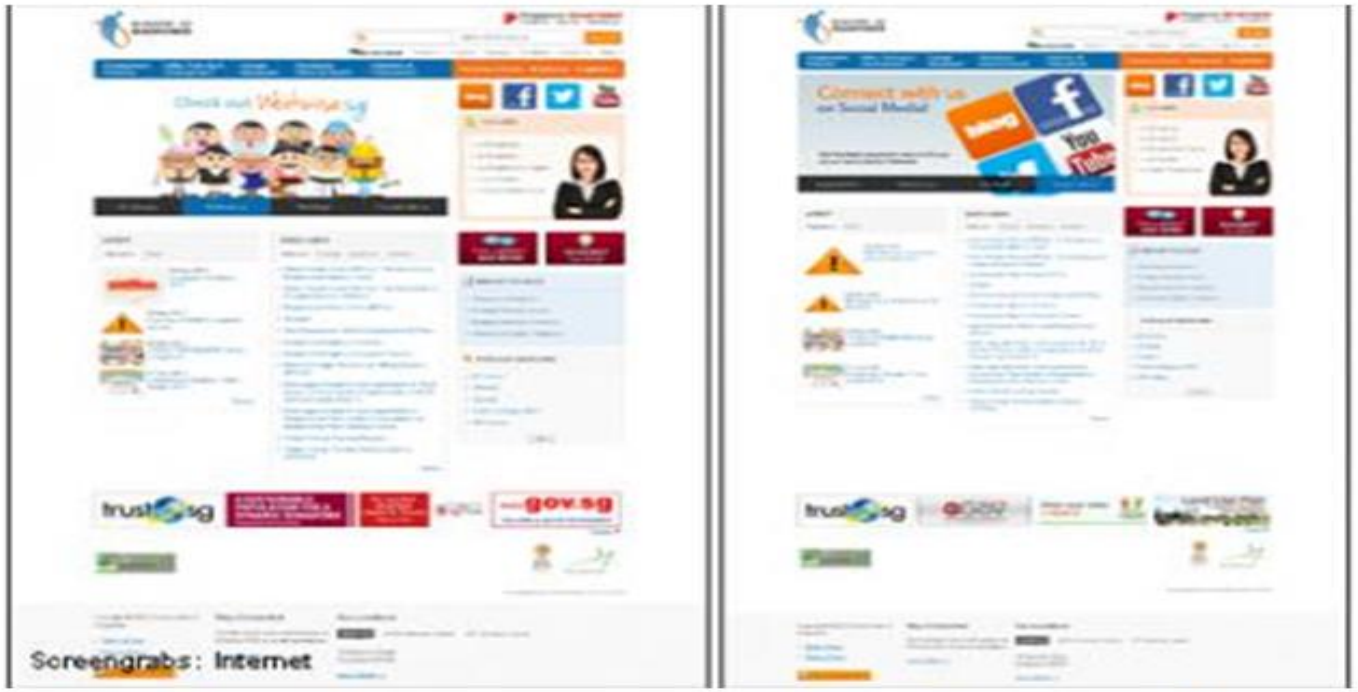
- The online traps are often made to look like versions of legitimate bank, auction, or shopping websites
- The problem is that when you visit a website through email or search engines, it can be difficult for users to know whether it is genuine or not.
- Bogus websites are typically designed to slip viruses onto visitors's computers and trick people into typing in valuable information such as account names or passwords.
- Nearly two-thirds of the trick websites had to do with banks, according to PandaLabs.

Booby-trapped Web pages



Booby-trapped Web pages

MyPaper, Dec 02, 2013: Fake MOM site



On the left: The official corporate website of MOM, on the right: the duplicate website reported on Nov 29. MOM said Sunday that another duplicate has been discovered.

www.mom.gov.sg

www.momgov.sg

https://www.youtube.com/watch?v=FoNTXTyly-

Ransomware

- CryptoLocker, a new "ransomware" virus, began in mid-September 2013, affecting individuals and business owners alike.
- The malware takes hold in a variety of ways: after a user clicks on a link or attachment in a spam email; or through Trojans that pretend to be required programs to view online videos.
- Once installed, CryptoLocker scans a computer's local and network drives, encrypts over 50 different file types, and then demands anywhere from $100-$300 to de-encrypt them.

Ransomware


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/30/2013
3:53 PM
Time left
26 : 16 : 22
Next >>

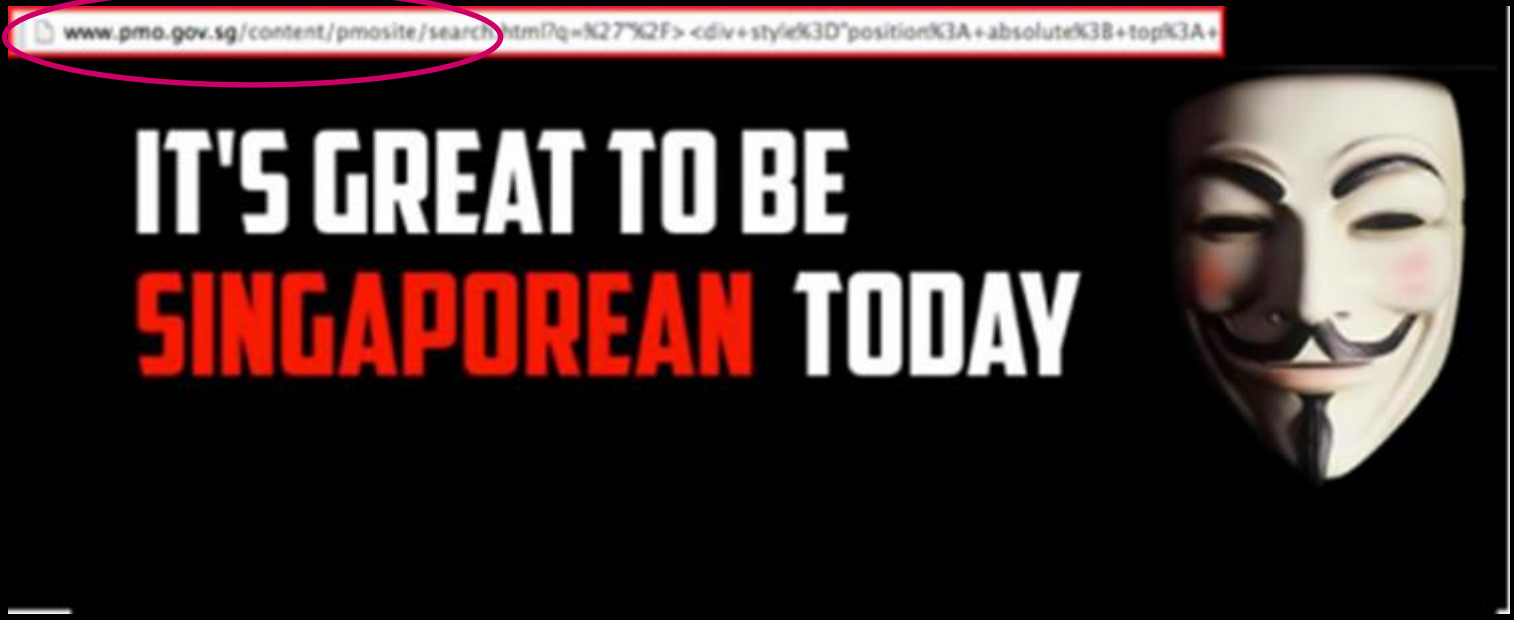
Hacktivism

- Hacktivism is the use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics.
- Anonymous' hacker targets The Straits Times website in protest against licensing rules for news websites on Nov 01, 2013.

Hacktivism

PM Lee warns hackers: 'We will track you down -- even if you think you're anonymous'

www.pmo.gov.sg/content/pmosite/search.html?q=%27%2F><div+style%3D"position%3A+absolute%3B+top%3A+



IDA managing director Jacqueline Poh says the Singapore Government faces millions of attempted cyber intrusions every day.
~The Straits Times, Friday Feb 21, 2014

Singapore short of cybersecurity experts, data analysts

Not enough people want such jobs but Govt stepping up efforts to plug shortage: Yaacob

Published on Dec 12, 2013 7:53 AM

Advanced Persistent Threat

- Advanced persistent threat (APT) usually refers to a group of sophisticated, determined and coordinated attackers that seek to systematically compromise government and commercial computer networks.
- These are highly complex threats that differ from traditional threats in that they are targeted, persistent, evasive and extremely advanced.
- Two well-known examples are Operation Aurora, and Stuxnet.

Stuxnet – "Cyberweapon!"

- 2010 June, Iran nuclear plants using Siemens control systems, under attack.
- 1st worm that spies on and reprograms industrial systems, unusual large file size and take large team & long effort to develop (nation state or large organisation sponsored)
- The primary goal of the attack was to gain access and control the industrial plants by reprogram the programmable logic controllers (PLCs) using first ever PLC rootkit.
- https://www.youtube.com/watch?v=zEjUlbmD9kQ

Stuxnet – "Cyberweapon!"

- 2010 June, Iran nuclear plants using Siemens control systems, under attack.
- 1st worm that spies on and reprograms industrial s and take large team & l state or large c
- T k was to gain access and c reprogram the p ers (PLCs) using first ever P
- https://www.youtube.com/watch?v=zEjUlbmD9kQ

Mobile Devices are targeted

UK bans iPads from Cabinet meetings

Nov 05, 2013

British Cabinet ministers have been banned from bringing their iPads into meetings due to fears of foreign intelligence agencies bugging confidential meetings.

By - 5 HOURS 46 MIN AGO

British Cabinet ministers have been banned from bringing their iPads into meetings due to fears of foreign intelligence agencies bugging confidential meetings.

The securities services fear foreign intelligence agencies have developed the ability to turn mobile devices, such as phones and tablets, into bugs without the owner's knowledge, allowing them to eavesdrop on confidential meetings.

It is feared that China, Russia, Iran and Pakistan have developed the ability of using a Trojan computer virus to turn mobile phones into microphones and transmitters even when they are switched off.

Difficulties in Defending against Attacks

- Increased speed of attacks
  - Attackers can launch attacks against millions of computers within minutes from anywhere in the world
- Greater sophistication of attacks
  - Attack tools vary their behaviour so the same attack appears differently each time.
- Simplicity of attack tools
  - Attacks are no longer limited to highly skilled attackers

Difficulties in Defending against Attacks

- Quicker detection of vulnerabilities
  - Attackers can discover security holes in hardware or software more quickly. **Zero day attack**
- Delays and weak patching
  - Many software products lack a means to distribute security patches in timely fashion.
- Distributed attacks
  - Attackers use thousands of computers in an attack against a single computer or network
- User confusion
  - Users are required to make difficult security decision with little or no instruction

What Is Information Security?

- Before defense is possible, one must understand:
  - What information security is
  - Why it is important
  - Who the attackers are

Defining Information Security

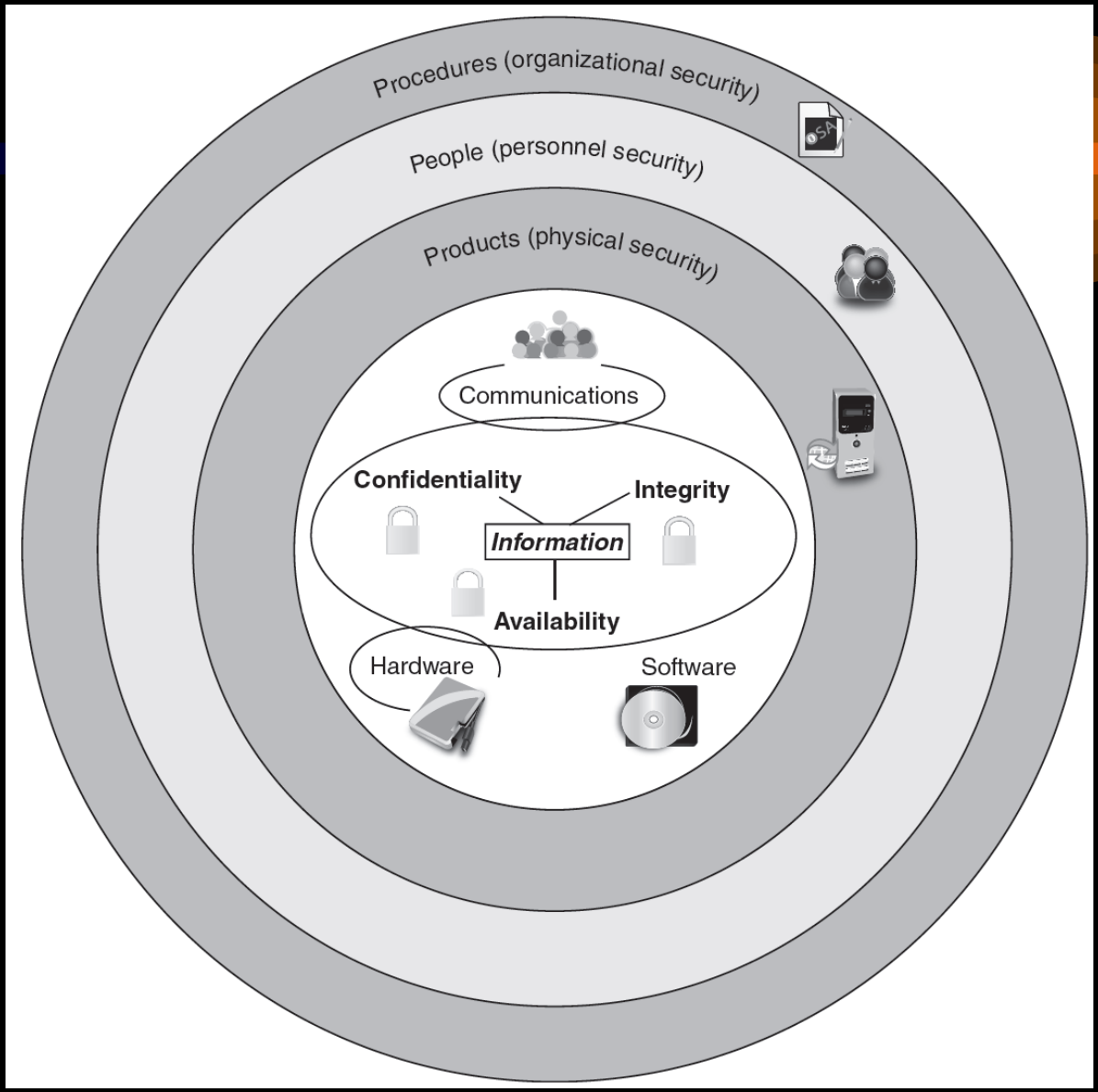
- Security
  - Steps to protect person or property from harm
    - Harm may be intentional or non intentional
    - Sacrifices convenience for safety
- Information security
  - Guard digitally-formatted information
    - Protect information that has value to people and organizations
    - Value comes from the characteristics of the information

Defining Information Security

- Characteristics of information that must be protected by information Security
  - **C**onfidentiality
    - To ensure that unauthorized parties cannot get the information. It prevents sensitive information from reaching the wrong people.
  - **I**ntegrity
    - To ensure that unauthorized parties cannot modify the data. It maintains the consistency, accuracy, and trustworthiness of data.
  - **A**vailability
    - To ensure that information must be available when needed by authorised parties. It prevents service disruptions.

Defining Information Security

- Protections to secure information
  - Authentication
    - To verify user credentials to be sure that they are who they claim to be and not an imposter. One way to authenticate is to use personal password.
  - Authorization
    - To grant permission or ability to access confidential information.
  - Accounting
    - To keep track of user access to information. For example, event log.


Procedures (organizational security)
People (personnel security)
Products (physical security)
Communications
Confidentiality
Integrity
Information
Availability
Hardware
Software

Defining Information Security

- Information Security is achieved through a combination of three entities.
  - Products
    - Form the physical security around the data; may be as basic as door locks or as complex as network security equipment
  - People
    - Those who implement and use security products to protect data.
  - Procedures
    - Plan and policies established by an organisation to ensure the people use the products correctly.

Information Security Terminology

- Asset
  - An item that has a value.
- Threat
  - A event that has the possibility to endanger an asset.
- Threat Agent
  - Person that has the power to carry out a threat.
- Vulnerability
  - A weakness that allows a threat agent to bypass security.
- Exploit
  - An action that take advantage of the vulnerability
- Risk
  - The likelihood that a threat agent will exploit the vulnerability

Information Security Terminology

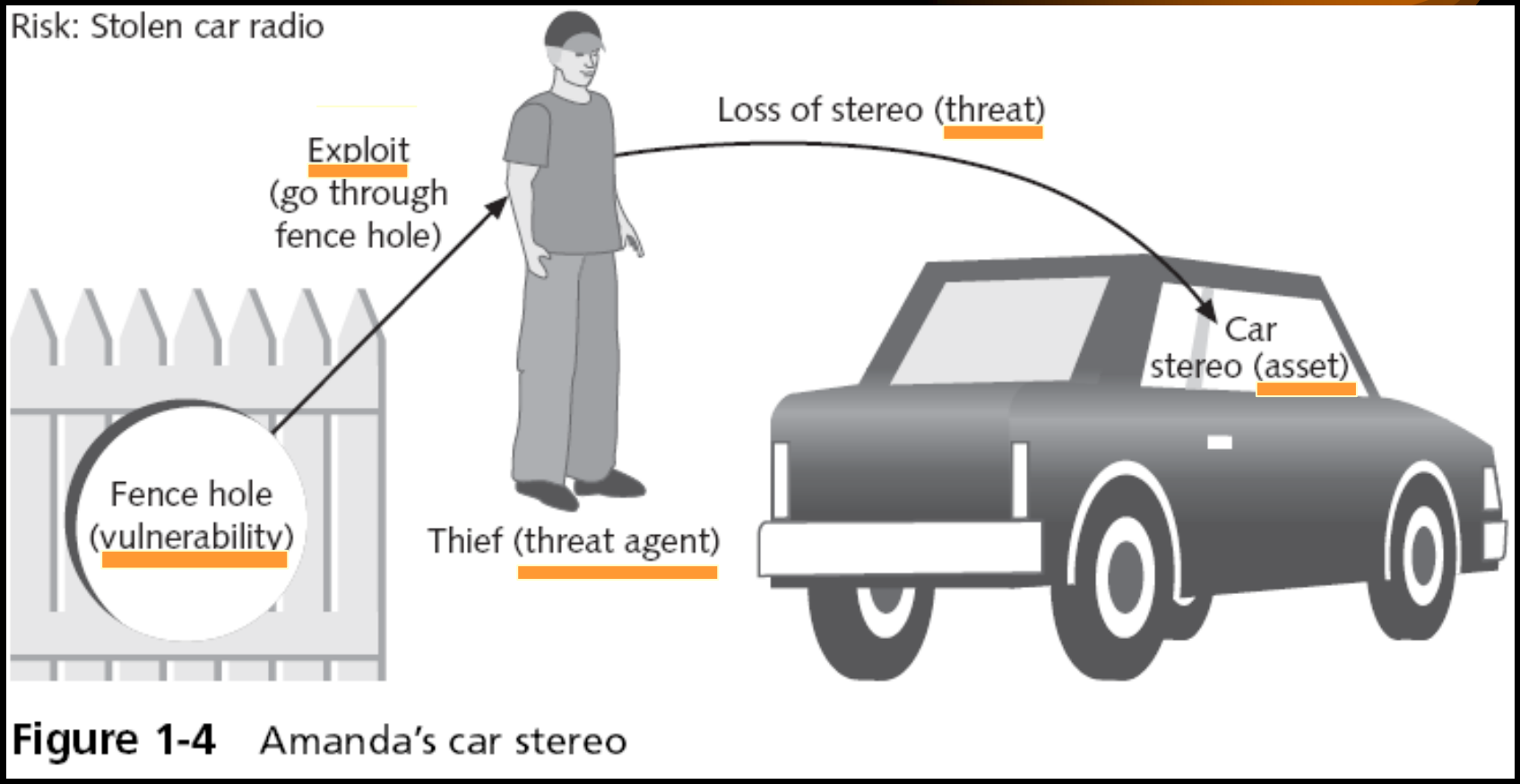


Figure 1-4 Amanda's car stereo

Term: Vulnerability; Exploit; Threat agent; Risk; Threat; Asset

Information Security Terminology

Term	Example in Car Park	Example in Information Security
Asset	Car stereo	Employee database
Threat	Steal stereo from car	Steal data
Threat Agent	Thief	Attacker, virus, flood
Vulnerability	Hole in fence	Software defect
Exploit	Climb through hole in fence	Send virus to unprotected e-mail server
Risk	Purchase car insurance	Regular data backup

The Goals of Information Security

- Prevent data theft
  - The theft of data is one of the largest causes of financial loss due to an attack.
- Prevent identity theft
  - Identity theft involves using someone's personal information to establish bank or credit card accounts
- Maintain Productivity
  - Cleaning up after an attack diverts resources such as time and money away from normal activities
- Counter cyber terrorism
  - Could cripple a nation's electronic and commercial infrastructure. Utility, telecommunications, and financial services companies are considered prime targets of cyber terrorists

Who Are the Attackers?

- Hacker
  - Person who uses computer skills to attack computers.
  - White hat hackers: Goal to expose security flaws; not to steal or corrupt data
  - Black hat hackers: Goal is malicious and destructive
- Script kiddies
  - Want to break into computers to create damage
  - Unskilled users
  - Download automated hacking software (scripts) from Web sites and use it to break into computers
- Computer Spies
  - A person who has been hired to break into a specific computer and steal information
  - Goal: steal information without drawing attention to their actions
  - Spies, like hackers, possess excellent computer skills

Who Are the Attackers?

- Insiders
  - Employees, contractors, and business partners
  - 48 percent of breaches attributed to insiders
  - An employee might want to show the company a weakness in their security
  - Disgruntled employees may be intent on retaliating against the company
  - Industrial espionage, Blackmailing
- Cybercriminals
  - Network of attackers, identity thieves, spammers, financial fraudsters
  - More highly motivated, less risk-averse, better funded, and more tenacious than hackers
  - Cybercriminals have a more focused goal that can be summed up in a single word: *money*

Who Are the Attackers?

- Cyberterrorists
  - Their motivation may be defined as ideology, or attacking for the sake of their principles or beliefs
  - Attack networks and computer infrastructures to cause panic among citizens.

Goals of a cyberattack:

- To deface electronic information and spread misinformation and propaganda
- To deny service to legitimate computer users
- To commit unauthorized intrusions into systems and networks that result in critical infrastructure outages and corruption of vital data

Steps of an Attack

- The five steps that make up an attack
  - Probe for information
  - Penetrate any defenses
  - Modify security settings
  - Circulate to other systems
  - Paralyze networks and devices

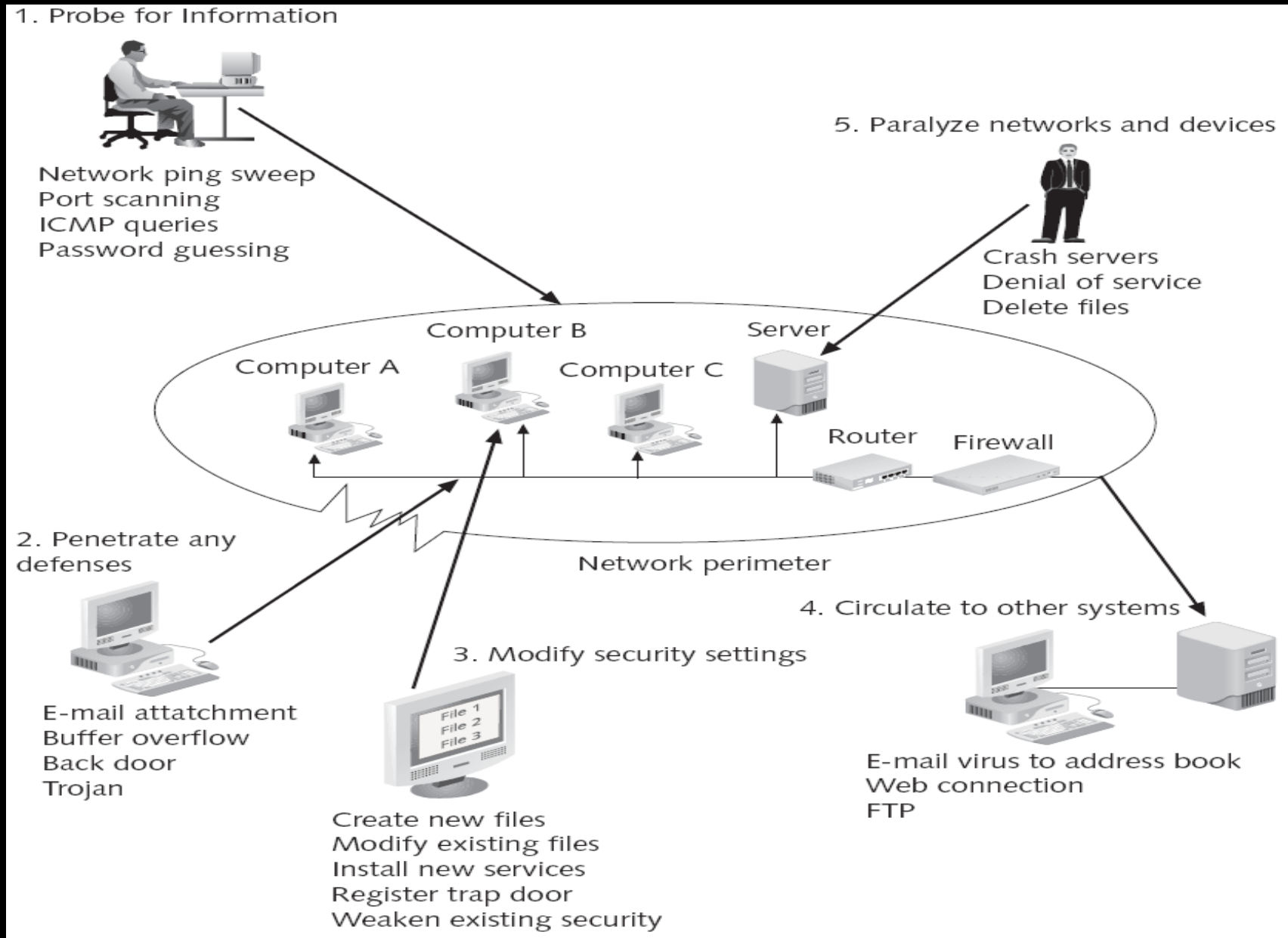
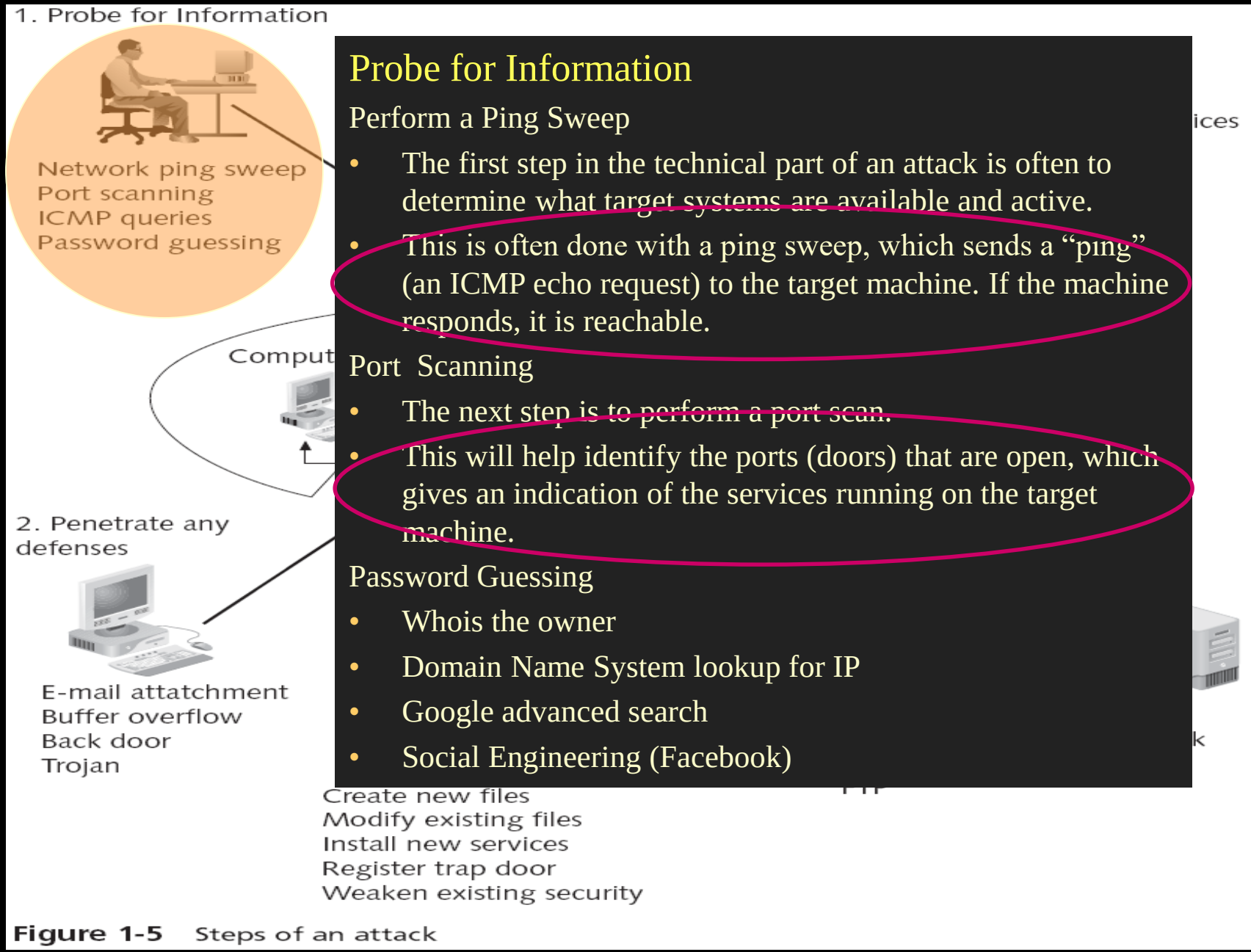


Figure 1-5 Steps of an attack



Probe for Information

Perform a Ping Sweep

- The first step in the technical part of an attack is often to determine what target systems are available and active.
- This is often done with a ping sweep, which sends a "ping" (an ICMP echo request) to the target machine. If the machine responds, it is reachable.

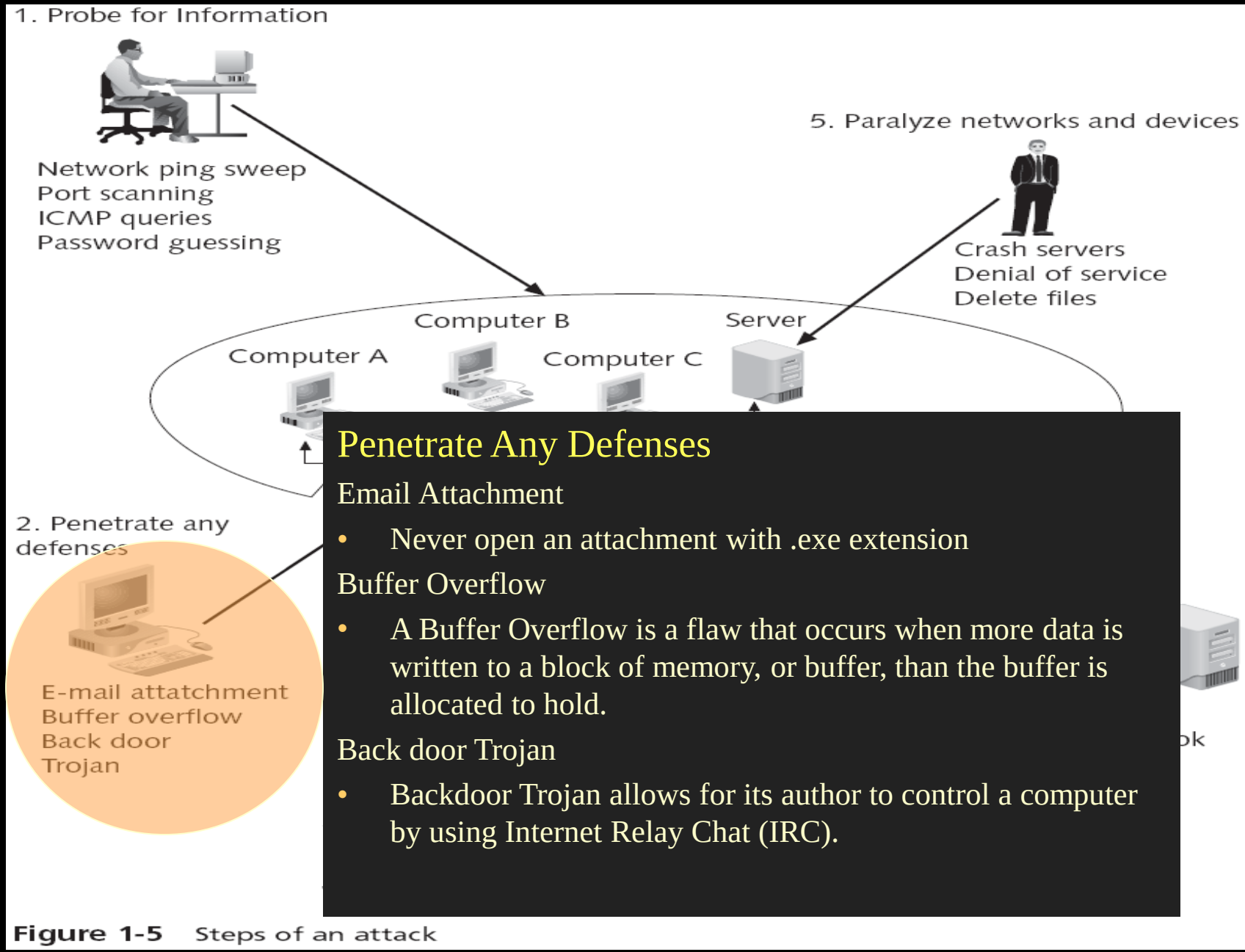
Port Scanning

- The next step is to perform a port scan.
- This will help identify the ports (doors) that are open, which gives an indication of the services running on the target machine.

Password Guessing

- Whois the owner
- Domain Name System lookup for IP
- Google advanced search
- Social Engineering (Facebook)

Figure 1-5 Steps of an attack



Penetrate Any Defenses

Email Attachment

- Never open an attachment with .exe extension

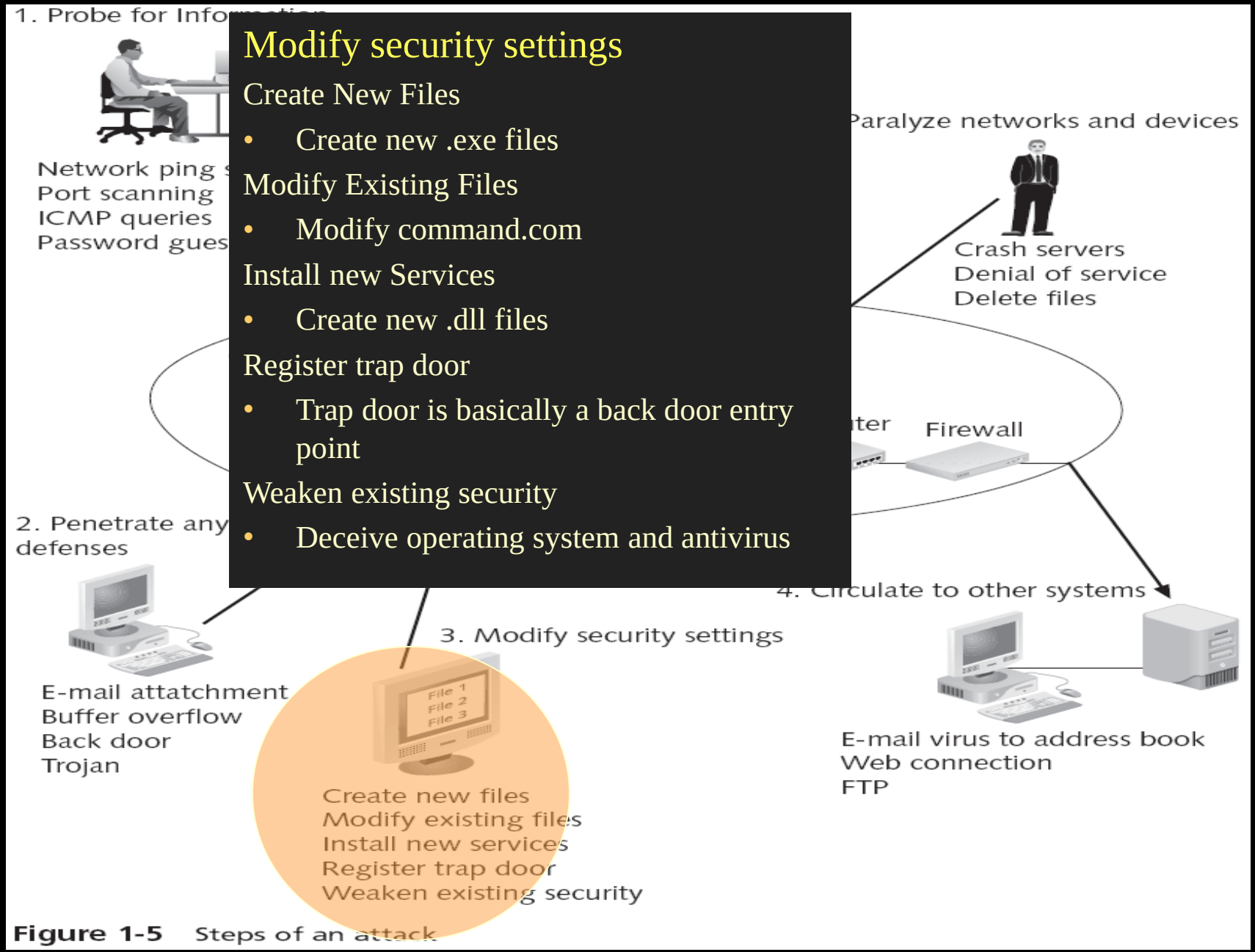
Buffer Overflow

- A Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

Back door Trojan

- Backdoor Trojan allows for its author to control a computer by using Internet Relay Chat (IRC).

Figure 1-5 Steps of an attack



Modify security settings

Create New Files

- Create new .exe files

Modify Existing Files

- Modify command.com

Install new Services

- Create new .dll files

Register trap door

- Trap door is basically a back door entry point

Weaken existing security

- Deceive operating system and antivirus

Figure 1-5 Steps of an attack

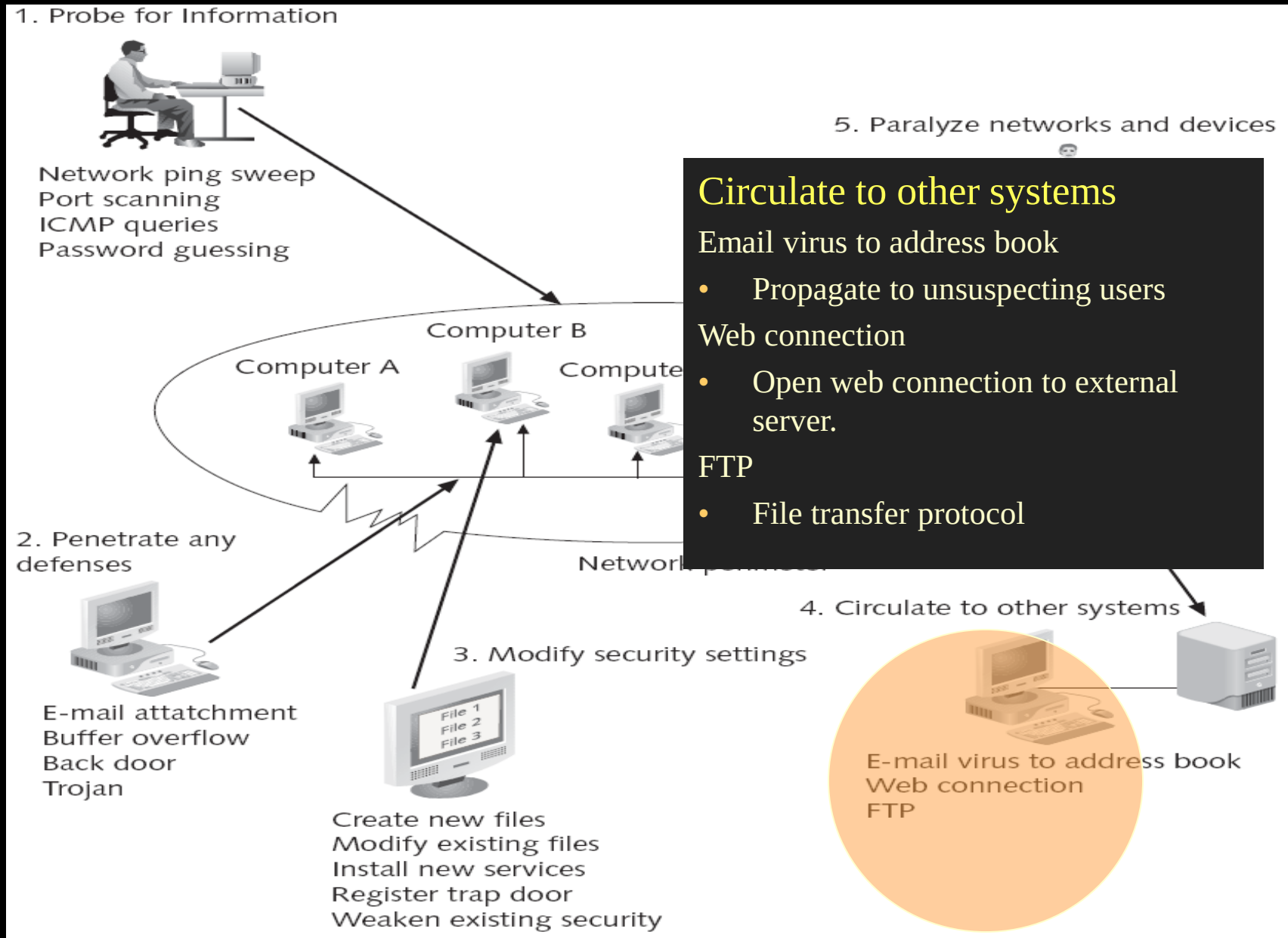
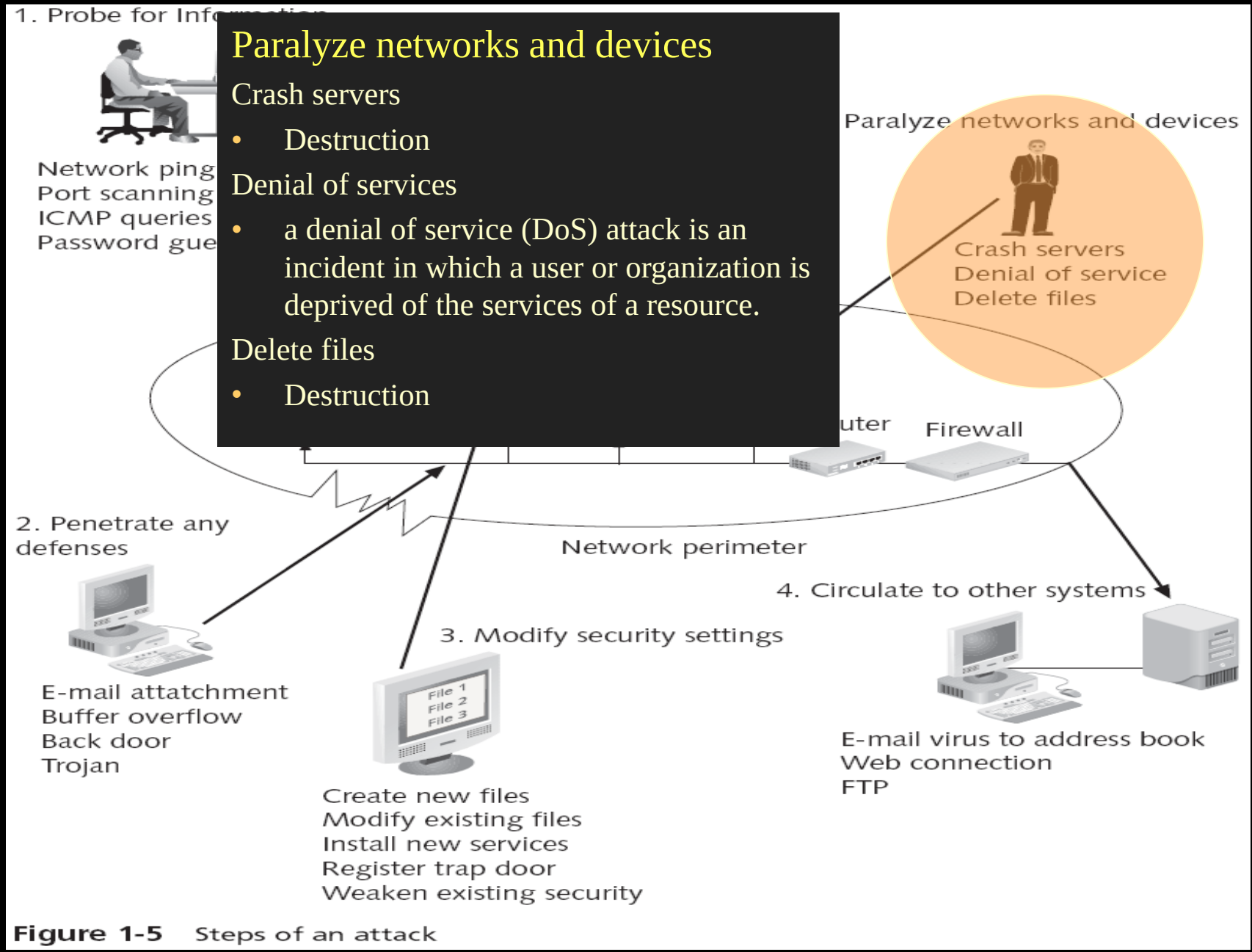


Figure 1-5 Steps of an attack



Paralyze networks and devices

Crash servers

- Destruction

Denial of services

- a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource.

Delete files

- Destruction

Figure 1-5 Steps of an attack

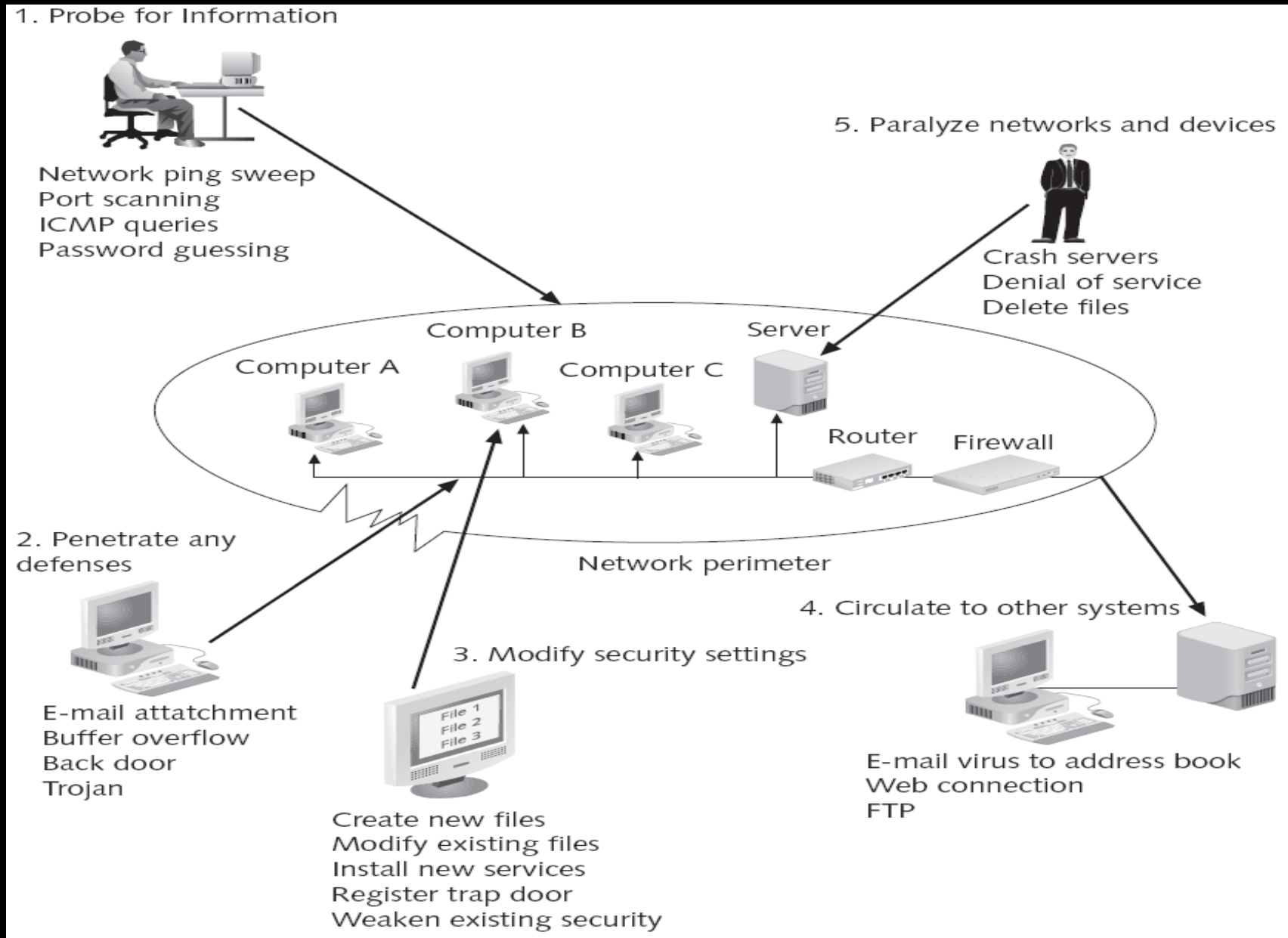


Figure 1-5 Steps of an attack

Defenses against Attacks

- Layering
  - A layered approach creates a barrier of multiple defenses.
  - If one layer is penetrated, several more layers must be breached.
- Limiting
  - Limiting access to information reduces the threat against it
  - Only those who must use data should have access to it
- Diversity
  - A diversity of defence that complements the various layers of security
  - If attackers penetrate one layer, they cannot use the same techniques to break through all other layers

Layering Example:
Norton Internet Security suite, which provides antivirus, firewall, anti-spam, parental controls

Limiting Example:
Separate the duties between two or more persons.

Diversity Example:
a variety of network equipment made by different vendors.

Defenses against Attacks

- Obscurity
  - Hiding information can be an important way to protect information
  - An attacker who knows that information can more easily determine the weaknesses of the system to attack it
- Simplicity
  - As much as possible, a secure system should be simple for those on the inside to understand and use
  - Complex security schemes are often compromised to make them easier for trusted users to work with.

Obscurity Example:
Admin moves a service from its default port to a more obscure port.

Simplicity Example:
Use one security guard instead of having all staff carries a key to a building

Class activity

- Work in a team (students)
- Identify a secured system and apply C.I.A security on the system.
- Deliverables
  - Describe the secured system.
  - Apply C.I.A on the system.
  - Is the secured system safe ? What other additional security may be included to enhanced the system?