

Information Security

Cyber security

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objective

- ☞ Understand the key terms of information security

Define cyber crime

- ∞ Crime committed using a computer and the internet to steal data or information.
 - Illegal imports.
 - Malicious programs



26/11/2017

3

Types of cyber crime

- ∞ Categorization of cyber crime
 - The Computer as a Target
 - The computer as a weapon
- ∞ Types of cyber crime
 - Hacking
 - Denial of service attack
 - Virus Dissemination
 - Computer Vandalism
 - Cyber Terrorism
 - Software Piracy

26/11/2017

4

Clean up cost of Cyber-attacks

- **SirCam: 2.3 million computers affected**
 - –Clean-up: \$460 million
 - –Lost productivity: \$757 million
- **Code Red: 1 million computers affected**
 - –Clean-up: \$1.1 billion
 - –Lost productivity: \$1.5 billion
- **Love Bug: 50 variants, 40 million computers affected**
 - –\$8.7 billion for clean-up and lost productivity
- **Nimda**

Virus Profiles

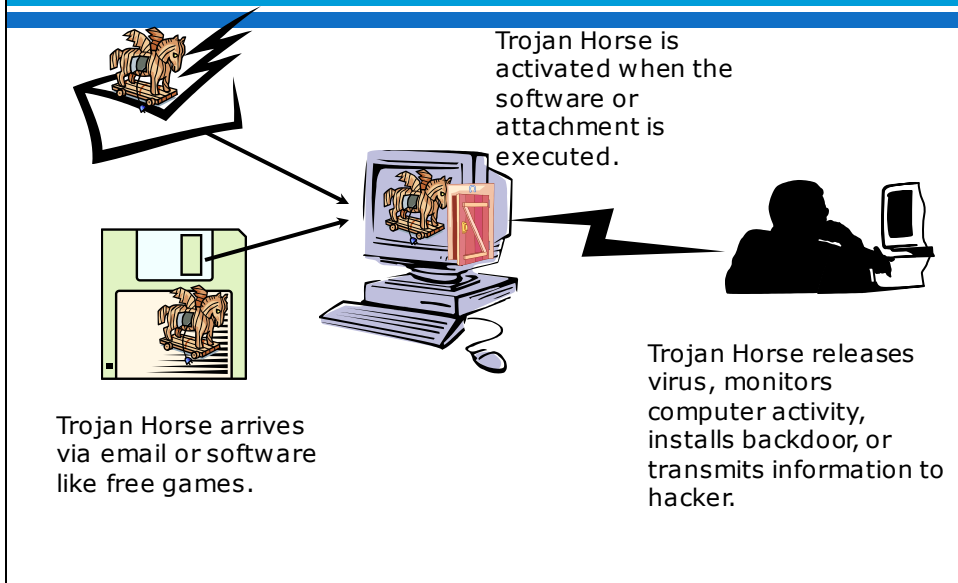
Nimda (note the garbage in the subject)

Sircam (note the "personal" text)
Both emails have executable attachments with the virus payload.

Scan type: Realtime Protection Scan
Event: Virus Found
Virus name: W32/Nimda enc
File: C:\DOCUME~1\mwhitman\LOCALS~1\Temp\Time.00
Location: Quarantine
Computer: VICAPFD
User: mwhitman
Action taken: Clean failed: Quarantine succeeded: Access denied

From: "jaffar idrissa" <toure@prody.net>
To: <mwhitman@hennesaw.edu>
Subject: rianey
Message: Hi! How are you?
I send you this file in order to have your advice
See you later. Thanks
rianey.doc...

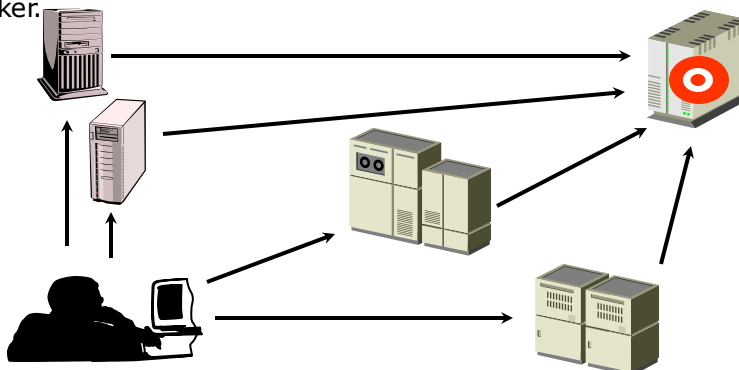
Trojan Horse Attack



Denial of Service Attacks

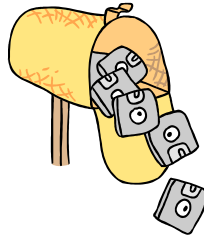
a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

hundreds of computers (known as a zombies) are compromised, loaded with DOS attack software and then remotely activated by the hacker.



Spamming Attacks

- Sending out e-mail messages in bulk. It's electronic "junk mail."
- Spamming can leave the information system vulnerable to overload.
- Less destructive, used extensively for e-marketing purposes.



Safety tips for cyber crime

- Use antivirus software's.
- Insert firewalls.
- Uninstall unnecessary software
- Maintain backup.
- Check security settings.
- Stay anonymous - choose a genderless screen name.
- Never give your full name or address to strangers.
- Learn more about Internet privacy.



Network Security Assessment goal

∞ Network security Assessment: (goal)

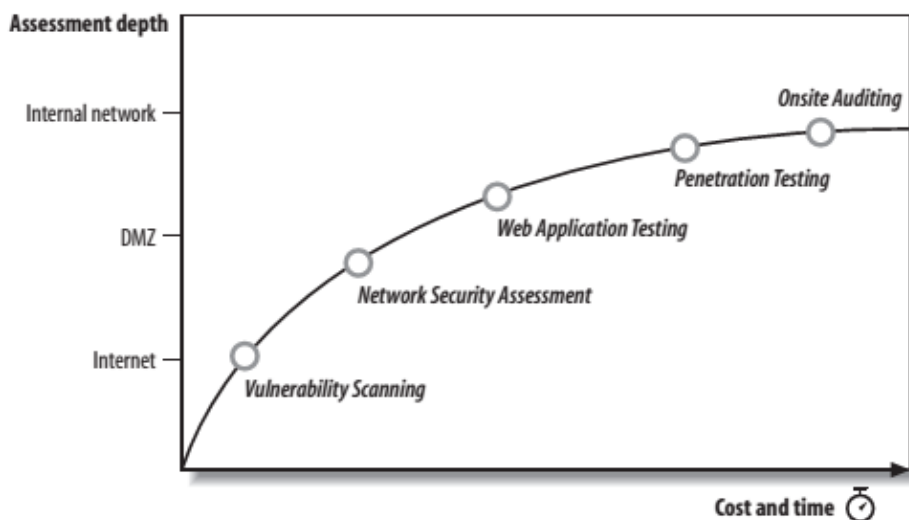
- to identify and categorize your risks.
- is an integral part of any security life cycle
- understand the security techniques of the network, to execute security policy and incident response procedures.
- To protect networks and data from determined attacks,



26/11/2017

11

Security assessment services



Network Security Assessment



Footprinting

- whois,
- dig,
- traceroute,
- nslookup



Scanning Networks

- Nmap
- Nessus
- Commercial Network
- Web Application Testing



Report

26/11/2017

13

Steps of Footprinting

∞ Footprinting generally needs the following steps to ensure proper information retrieval:

1. Collect information about a target: host and network
2. Determine the OS of web server and web application data.
3. Query such as Whois, DNS, network, and organizational
4. Locate existing or potential vulnerabilities or exploits that exist in the current infrastructure
=> helpful to launching later attacks.

26/11/2017

14

Footprinting Tools

- ⌘ Whois
- ⌘ NSLookup,
- ⌘ Search engines,
- ⌘ Social Networking Site
- ⌘ ARIN
- ⌘ Neo Trace
- ⌘ VisualRoute Trace
- ⌘ SmartWhois
- ⌘ eMailTrackerPro
- ⌘ Website watcher
- ⌘ Google Earth
- ⌘ GEO Spider
- ⌘ HTTrack Web Copier
- ⌘ E-mail Spider

26/11/2017

15

Objectives of Scanning

- ⌘ To detect the live systems running on the network
- ⌘ To discover which ports are active/running
- ⌘ To discover the operating system running on the target system (fingerprinting)
- ⌘ To discover the services running/listening on the target system
- ⌘ To discover the IP address of the target system



26/11/2017

Types of Scanning

Port Scanning

- A series of messages sent by someone attempting to break into a computer to learn about the computer's network services



Network Scanning

- A procedure for identifying active hosts on a network



Vulnerability Scanning

- The automated process of proactively identifying vulnerabilities of computing systems present in a network

26/11/2017

17

Checking for Live Systems

- Some common ways to perform these types of scans are:

- **Pinging (ICMP Scanning)**

- Port scanning



26/11/2017

18

Pinging

- ∞ it is found out which hosts are up in a network by pinging them all
- ∞ It can be run parallel so that it can run fast
- ∞ It can also be helpful to tweak the ping timeout value with the `-t` option
- ∞ Tools:
 - Ping <target> [option]
 - Angry IP: for Windows
 - Hping2
 - Ping Sweep
 -



26/11/2017

19

Checking for open ports

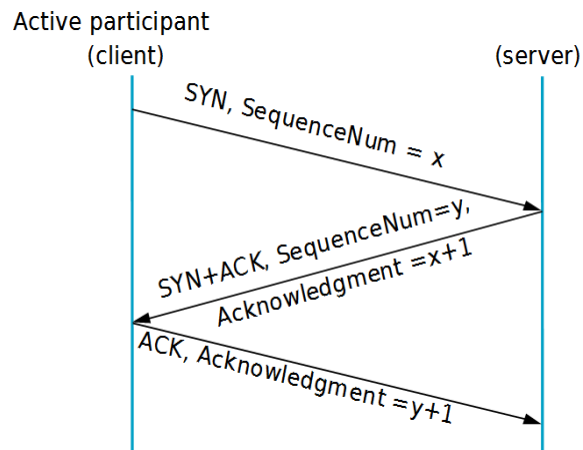
- ∞ Three Way Handshake, TCP flags
- ∞ Types of Scans
 - Full Open Scan
 - Stealth Scan, or Half-open Scan
 - Xmas Tree Scan
 - FIN Scan
 - NULL Scan
 - ACK Scanning
 - UDP Scanning



26/11/2017

20

Three Way Handshake

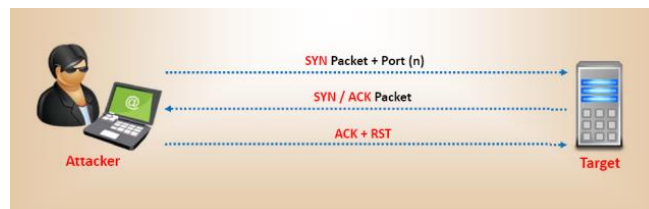


26/11/2017

21

Full Open Scan

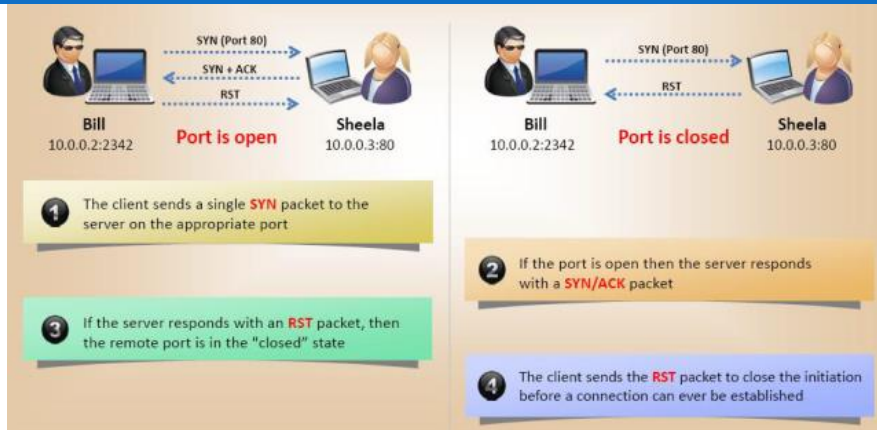
- ∞ the systems involved initiated and completed the three-way handshake.
- ∞ The advantage
 - you have positive feedback that the host is up and the connection is complete.
- ∞ Downside (disadvantage):
 - since you complete the three-way handshake you have confirmed that you as the scanning party are there.



26/11/2017

22

Stealth Scan, or Half-open Scan



- it does not open a full TCP connection
- The key advantage is that fewer sites log this scan

26/11/2017

23

Xmas Tree Scan

- Having all the flags set creates an illogical or illegal combination, and the receiving system has to determine what to do:
 - Drop (old sys)
 - Respond: port is open
 - RST packet: port is closed
- NMAP: **NMAP -sX -v <target IP>**



FIN Scan

- ∞ The attacker sends frames to the victim with the FIN flag set.
- ∞ The victim's response depends on whether the port is open or closed.
 - if an FIN is sent to an open port there is no response,
 - but if the port is closed the victim returns an RST.
- ∞ NMAP: **NMAP -sF <target IP address>**



Null Scan

- ∞ The attacker sends frames to the victim with no flag set.
- ∞ The victim's response depends on whether the port is open or closed:
 - if an FIN is sent to an open port there is no response,
 - if the port is closed the victim returns an RST
- ∞ NMAP: **NMAP -sN <target IP address>**



Scanning Tools

- ∞ Nmap
- ∞ IPsec
- ∞ NetScan
- ∞ SuperScan
- ∞ IPScanner
- ∞ MegaPing
- ∞ Global Network Inventory Scanner
- ∞ Net Tools Suite Pack
- ∞ Floppy Scan

26/11/2017

27

Nmap: Scan Methods

- ∞ Some of the scan methods used by Nmap:
 - Xmas tree: The attacker checks for TCP services by sending "Xmas-tree" packets
 - SYN Stealth: It is referred to as "half open" scanning, as a full TCP connection is not opened
 - Null Scan: It's an advanced scan that may be able to pass through firewalls unmolested
 - Windows scan: It is similar to the ACK scan and can also detect open ports
 - ACK Scan: Used to map out firewall rule set

26/11/2017

28

Nmap: Scan Methods

- ∞ -sT (TcpConnect)
- ∞ -sS (SYN scan)
- ∞ -sF (Fin Scan)
- ∞ -sX (Xmas Scan)
- ∞ -sN (Null Scan)
- ∞ -sP (Ping Scan)
- ∞ -sU (UDP scans)
- ∞ -sO (Protocol Scan)
- ∞ -sI (Idle Scan)
- ∞ -sA (Ack Scan)
- ∞ -sW (Window Scan)
- ∞ -sR (RPC scan)
- ∞ -sL (List/Dns Scan)
- ∞ -P0 (don't ping)
- ∞ -PT (TCP ping)
- ∞ -PS (SYN ping)
- ∞ -PI (ICMP ping)
- ∞ -PB (= PT + PI)
- ∞ -PP (ICMP timestamp)
- ∞ -PM (ICMP netmask)

26/11/2017

29

Practice

- ∞ Install and configure tools to assess network security
 - Footprinting
 - Scan ports using Nmap

26/11/2017

30