EE4758//IM303 COMPUTER/INFORMATION SECURITY
TUTORIAL NO. 3

1. What are the various types of Malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?

- **Malware** is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.
- Common types of malware are viruses, worms, Trojan horses, logic bombs, and back doors.
- Computer viruses are segments of code that induce other programs to perform actions.
- Worms replicate themselves constantly without requiring another program to provide a safe environment for replication.
- Once a trusting user executes a Trojan horse program it will unleash viruses or worms to the local workstation and the network as a whole.

CLASSIFICATION OF MALWARE

CLASSIFIED INTO TWO BROAD CATEGORIES:

based first on how it spreads or propagates to reach the desired targets

then on the actions or payloads it performs once a target is reached

ALSO CLASSIFIED BY

those that need a host program (parasitic code such as viruses)

those that are independent, self-contained programs (worms, trojans, and bots)

malware that does not replicate (trojans and spam e-mail)

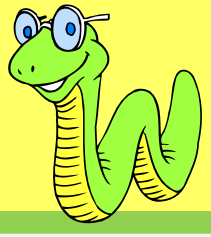
malware that does replicate (viruses and worms)

2. Describe worms and their replication mechanism. Have there been any dangerous worm attacks apart from Morris worm, which was released in 1988?

❑ WORMS

- ❑ Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- ❑ Can use network connections to spread from system to system
- ❑ Spreads through shared media (USB drives, CD, DVD data disks)
- ❑ E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- ❑ Upon activation the worm may replicate and propagate again
- ❑ Usually carries some form of payload
- ❑ First known implementation was done in Xerox Palo Alto Labs in the early 1980s.

WORM REPLICATION



ELECTRONIC MAIL OR INSTANT MESSENGER FACILITY	• worm e-mails a copy of itself to other systems • sends itself as an attachment via an instant message service
FILE SHARING	• creates a copy of itself or infects a file as a virus on removable media
REMOTE EXECUTION CAPABILITY	• worm executes a copy of itself on another system
REMOTE FILE ACCESS OR TRANSFER CAPABILITY	• worm uses a remote file access or transfer service to copy itself from one system to the other
REMOTE LOGIN CAPABILITY	• worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

MORRIS WORM

- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems
  - Attempted to crack local password file to use login/password to logon to other systems
  - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - Exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
  - Sent interpreter a bootstrap program to copy worm over

RECENT WORM ATTACKS

MELISSA	**1998**	e-mail worm first to include virus, worm and Trojan in one package
CODE RED	**JULY 2001**	exploited Microsoft IIS bug, probes random IP addresses, consumes significant Internet capacity when active
CODE RED II	**AUGUST 2001**	also targeted Microsoft IIS, installs a backdoor for access
NIMDA	**SEPTEMBER 2001**	had worm, virus and mobile code characteristics, spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL SLAMMER	**EARLY 2003**	exploited a buffer overflow vulnerability in SQL server, compact and spread rapidly
SOBIG.F	**LATE 2003**	exploited open proxy servers to turn infected machines into spam engines
MYDOOM	**2004**	mass-mailing e-mail worm, installed a backdoor in infected machines
WAREZOV	**2006**	creates executable in system directories, sends itself as an e-mail attachment, can disable security related products
CONFICKER	**NOVEMBER 2008**	exploits a Windows buffer overflow vulnerability, most widespread infection since SQL Slammer
STUXNET	**2010**	restricted rate of spread to reduce chance of detection, targeted industrial control systems
FLAME	**2012**	Similar to STUXNET targeted Iran Nuclear plant and oil facilities

RECENT WORM ATTACKS

CryptoLocker	**SEP 2013**	Cryptolocker encrypts the files on a user's hard drive, then prompts them to pay a ransom in order to receive the decryption key.
Regin	**NOV 2014**	Trojan horse primarily spread via spoofed Web pages. Once downloaded, Regin quietly downloads extensions of itself, making it difficult to be detected via anti-virus signatures

3. Eve installed some spyware software on 1000 USB flash drives and has designed this software to auto load from these drives along with some photos of a famous star. She then painted the logo of a well-known magazine on each one and randomly scattered these flash drives in the parking lots of several large companies in her town. What type of malware attack is this and what vulnerability is she trying to exploit in order to get her malware code past the network firewalls of these companies?

- **Solution:**
- This is a Trojan horse attack, since the users are probably expecting the photos of famous star, given the logo, but are not expecting the spyware.
- Eve is trying to get employees of these companies to insert these USB flash drives in their company computers (inside the firewall) and exploit a vulnerability of having auto-execution enabled, so that the spyware auto loads along with the expected photos.

4. Suppose you want to use an Internet cafe to login to your personal account on a bank web site, but you suspect that the computers in this cafe are infected with software keyloggers. Assuming that you can have both a web browser window and a text editing window open at the same time, describe a scheme that allows you to type in your userID and password so that a keylogger, used in isolation of any screen captures or mouse event captures, would not be able to discover your userID and password.

- **Solution:**
- Open both the web browser, pointing to your bank's login page, and a text editing window to open a new un-named file.
- To enter your userID and password, use your mouse to toggle input between the text editor and the web browser.
- When you are in the browser window type a single character of your userID or password and then click back to the text editor window.
- When you are in the text editor window, type a reasonably long sequence of random characters.

- By toggling back and forth between these two windows you will end up typing in your userID and password, but a keylogger will only see a sequence of random characters with the characters of your userID and password intermixed in such a way as to be hard to detect.
- In fact, you could cycle through all the characters on the keyboard for each character in your userID and password, clicking to the browser just for the appropriate character needed in each cycle and then immediately clicking back to the text editor.
- In this case, a key logger would only see a repeated series of sequences of all the characters on the keyboard.

5. What is the difference between a skilled hacker and an unskilled hacker (other then the lack of skill)? How does protection against each differ?

- An expert hacker is one who develops software scripts and codes to exploit relatively unknown vulnerabilities.
- The expert hacker is usually a master of several programming languages, networking protocols, and operating systems.
- An unskilled hacker is one who uses scripts and code developed by skilled hackers.
- They rarely create or write their own hacks, and are often relatively unskilled in programming languages, networking protocols, and operating systems.
- Protecting against an expert hacker is much more difficult, due in part to the fact that most of the time the expert hacker is using new, undocumented attack code.
- This makes it almost impossible to guard against these attacks at first.
- Conversely, an unskilled hacker generally uses hacking tools that have been made publicly available.
- Therefore, protection against these hacks can be maintained by staying up-to-date on the latest patches and being aware of hacking tools that have been published by expert hackers.

QUIZ

A. What is a computer virus?

i. Any program that is downloaded to your system without your permission

ii. Any program that self-replicates

iii. Any program that causes harm to your system

iv. Any program that can change your Windows Registry

The answer is ii

B. What is spyware?

i. Any software that monitors your system

ii. Only software that logs keystrokes

iii. Any software used to gather intelligence

iv. Only software that monitors what websites you visit

The answer is i

QUIZ

C. When a hacking technique uses persuasion and deception to get a person to provide information to help them compromise security, this is referred to as what?

i. Social engineering
ii. Conning
iii. Human inelegancy
iv. Soft hacking

The answer is i

D. What is malware?

i. Software that has some malicious purpose
ii. Software that is not functioning properly
iii. Software that damages your system
iv. Software that is not properly configured for your system

The answer is i