Malware

Today's Plan

- 09:00 – 10:00: **MALWARE (William Stallings, Lawrie Brown, *Computer Security Principles and Practice* [Chapter 6], Third edition, Pearson, Australia).**
  - Definition.
  - Propagation methods.
  - Types of payload.

- 10:00 – 10:30: Demo.

- 10:30 – 11:00: Coursework Questions and VMs Sharing.

- 11:00 – 12:00: Lab 7 (Spreading Python Malware using a SSH Linux Connection).

What is Malware?

www.menti.com

Definition and Types

- Malicious Software

- A program that is inserted into a system (usually unsuspectedly) with the intend of compromising the system's requirements.

- Examples?

- Types:
  - Parasitic: Cannot exist independently (virus, logic bombs, backdoors).
  - Independent: Self-contained and can be scheduled to run by OS (worms, bots).

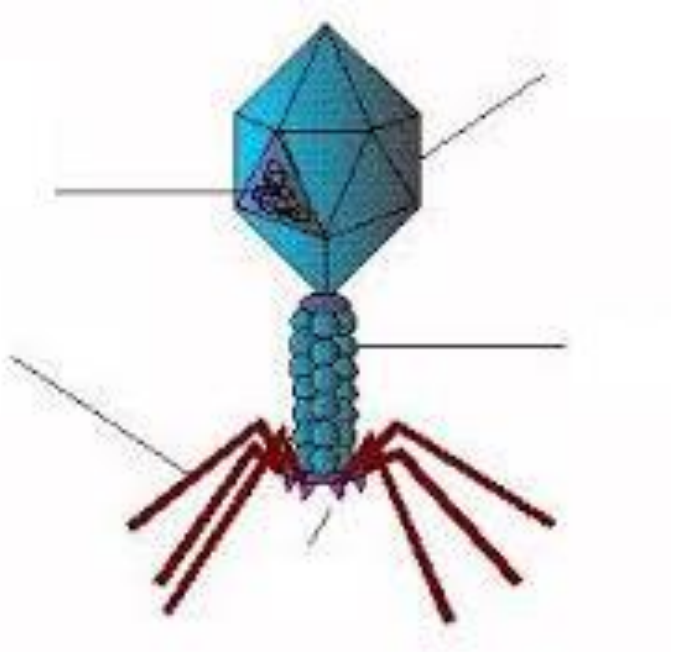
Propagation Mechanisms

Propagation Mechanisms

- Infection of existing files.
  - Viruses
- Exploitation of vulnerabilities.
  - Worms
- Social engineering attacks to bypass security mechanisms.
  - Trojans
- Blended attacks (multiple methods of propagation).
- Advanced Persistent Threats (careful target selection).

Infecting Files (Virus)

- Computer program that can infect other programs by modifying them to include a (possibly evolved) version of itself.
- Components:
  - Infection mechanism
  - Trigger/Logic bomb
  - Payload
- Phases:
  - Dormant
  - Propagation
  - Triggering
  - Execution



Virus Design: Simple

```
program V
1234567;

procedure attach-to-program;
begin
     repeat
          file := get-random-program;
     until first-program-line ≠ 1234567;
     prepend V to file;
end;

procedure execute-payload;
begin
     (* perform payload actions *)
end;

procedure trigger-condition;
begin
     (* return true if trigger condition is true *)
end;

begin (* main action block *)
     attach-to-program;
     if trigger-condition then execute-payload;
     goto original program code;
end;
```

(a) A simple virus

1. Set a marker.
2. Seek for uninfected files.
3. Establish the trigger conditions.
4. Define the payload actions.
5. Main action block.

Easiest way to detect these type of viruses?

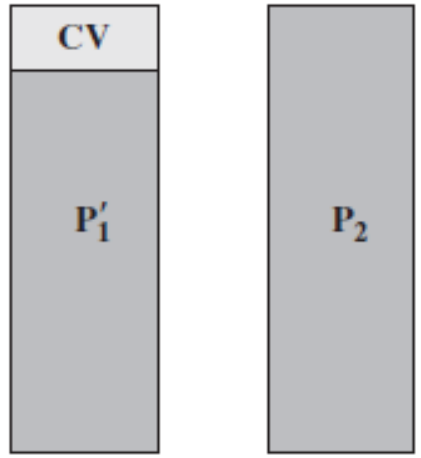
Virus Design: Compressed

- Compress the .exe so that both the infected and uninfected versions are of identical length.

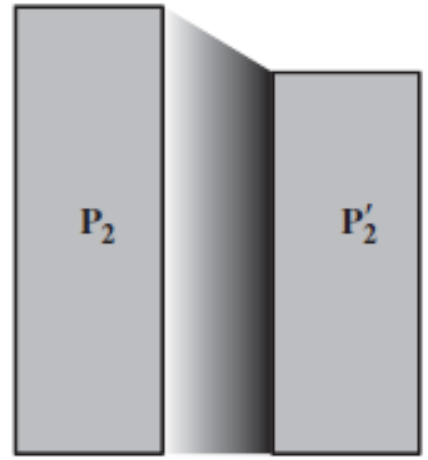
- $t0$: An infected program P_1 is evoked.

```
program CV
1234567;

procedure attach-to-program;
begin
      repeat
            file := get-random-program;
      until first-program-line ≠ 1234567;
      compress file;     (* t1 *)
      prepend CV to file;    (* t2 *)
end;

begin (* main action block *)
      attach-to-program;
      uncompress rest of this file into tempfile;    (* t3 *)
      execute tempfile;    (* t4 *)
end;
```

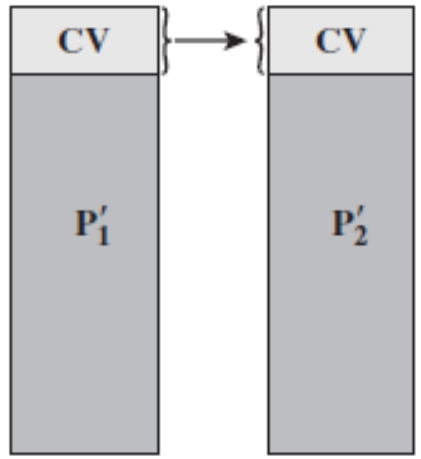
(b) A compression virus



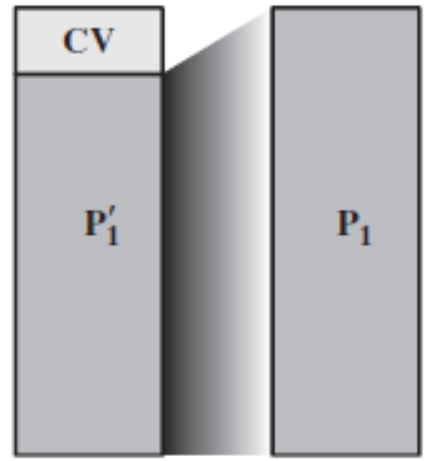
t_0: P_1' is infected version of P_1; P_2 is clean



t_1: P_2 is compressed into P_2'



t_2: CV attaches itself to P_2'



t_3: P_1' is decompressed into the original program P_1

Virus Classification

- By target
  - Boot sector infector
  - File infector
  - Macro virus
  - Multipartite virus
- By concealment strategy
  - Encrypted
  - Stealth
  - Polymorphic
  - Metamorphic

Macro virus

- Platform and hardware independent.
- Infects documents, not executables.
- Easily spread (e-mail).
- Could file access control be used to prevent their propagation?

Vulnerability Exploits (Worms)

- Worm: Self-replicating computer program that (typically) uses a network to send copies of itself to other nodes and does so without any user intervention.
- Means to access a remote system:
  - Email or instant messenger facility.
  - File sharing.
  - Remote execution capability.
  - Remote file access or transfer capability.
  - Remote login capability.

Target Discovery

- **Scanning/Fingerprinting**: Worm searches for other systems to infect.

- Types:
  - Random: Testing random ip addresses.
  - Hit-List: Attacker compiles a list of potentially vulnerable machines (slow).
  - Topological: Uses information contained on an infected machine.
  - Local Subnet: If a worm passes a firewall and infects a host, then looks for targets in the local network.

Rate of Propagation

- Based on classic epidemic models from health sciences:

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

where

$I(t)$ = number of individuals infected as of time t

$S(t)$ = number of susceptible individuals (susceptible to infection but not yet infected) at time t

β = infection rate

N = size of the population, $N = I(t) + S(t)$

Social Engineering (Trojans)

- Tricking users to assist in the compromise of his own system or personal information.

- Widely used thanks to the explosive growth of the Internet and spam e-mail.

Trojan Horses

- (Apparently) useful program containing hidden code.
- Gain access to sensitive data.
- What is the difference with respect to Virus/Worm?

Types of Trojans

1. Continuing to perform the function of the original program and performing a separate malicious activity.

2. Continuing to perform the function of the original program but modifying the function to perform malicious activity.

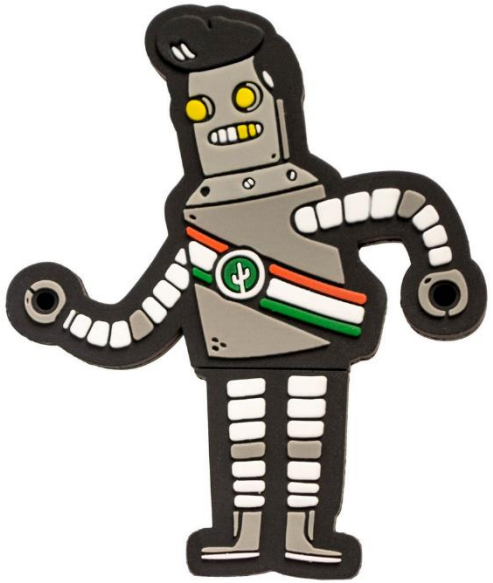
3. Performing a malicious function that completely replaces the function of the original program.

Types of Payload

Types of Malicious Payload

- Data destruction:
  - Chernobyl virus (1998).
- Data kidnapping (ransomware):
  - WannaCry
- Real-world damage:
  - STUXNET
- Logic bombs:
  - Alter or delete data.
  - Cause a machine halt.
  - Other damage.

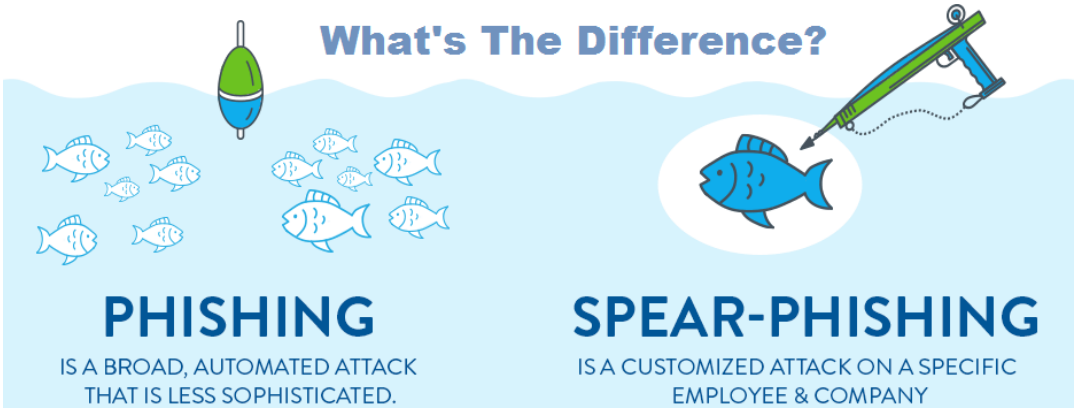
Bots/Zombies



- Malware subverts the computational and network resources of the infected system for use by the attacker (botnet).
- Uses:
  - Distributed denial of service (DDoS) attack.
  - Spamming.
  - Sniffing traffic.
  - Keylogging.
  - Spreading new malware.
  - Installing add-ons ad browser helper objects (BHOs).
  - Attacking the Internet Relay Chat (IRC) network.
  - Manipulating online polls/games.

Information Theft

- Payloads where the malware gathers data.
- Most common target: Username/Password.
- Keylogger:
  - Capture keystrokes on the infected machine.
  - Filtering to receive only important strokes.
- Spyware:
  - Monitors activity.
- Phishing:
  - Mimic a website to obtain data.
  - Spear-phishing: Tailor-made e-mail which increases the chance to fall in the attack.



Stealthing

- Maintain a persistent and undetectable presence on the machine.

- Purpose: Create a backdoor/trapdoor (mechanism that bypasses a normal security check).

- Backdoor/trapdoors are common in SW practice (i.e. debug, maintenance).

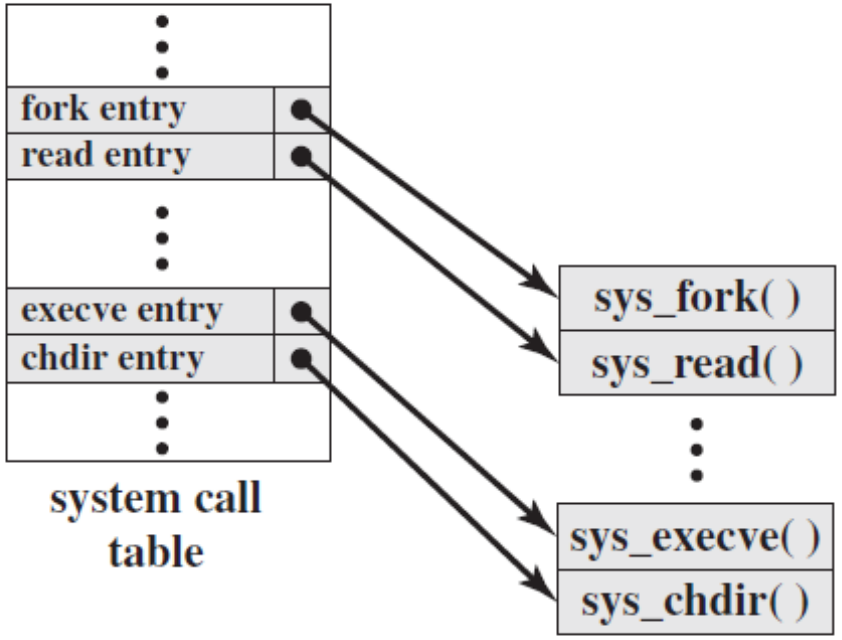
Rootkit

- Set of tools/programs installed to maintain covert access and used after attacker has broken into a system (gained unauthorised root privileges).
- Types:
  - Persistent.
  - Memory-based.
  - User mode.
  - Kernel mode.
  - Virtual machine based.
  - External mode.

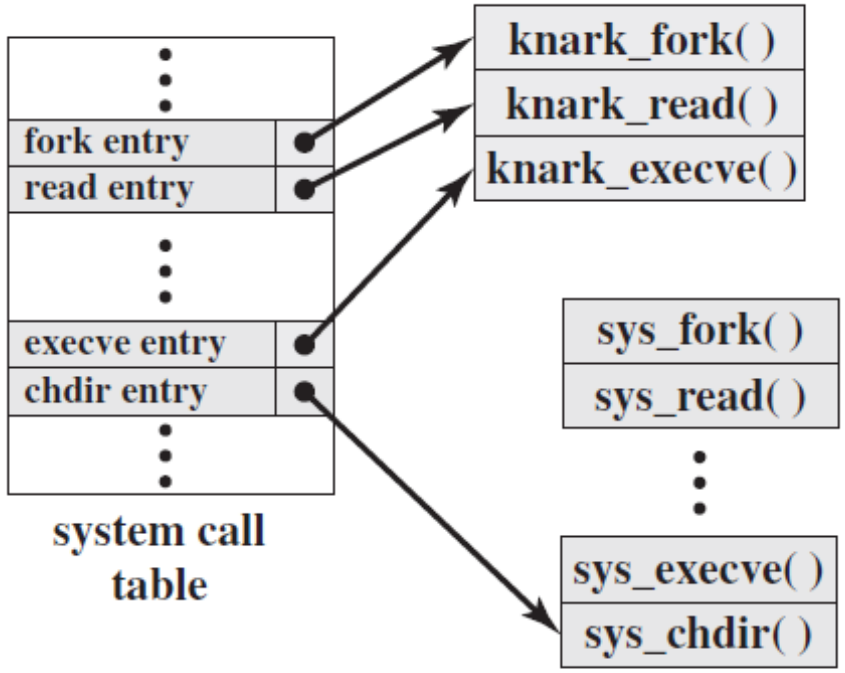
Kernel Mode Rootkit

- Implementation of system calls in Linux.
- Each system call is assigned a unique *syscall number.*
- When a user-mode process executes a system call, process refers to it by the number.
- Kernel maintains a system call table with one entry per routine (i.e. a pointer).
- How to change system calls?
  - Modify system call table targets.
  - Modify the system call table (e.g. knark).
  - Redirect the system call table.

Kernel Mode Rootkit Attack (knark)



(a) Normal kernel memory layout



(b) After knark install

Demo

Lab 7: Spreading Python Malware using a SSH Linux Connection