Chapter 7

Malware Threats

Theory

Ethical Hacking

Malware

Malware (malicious software) is a type of program that combines malicious code with genuine application to perform unauthorized operations in such a way that it can take control of a system or cause damage.

Types of Malware

1. Trojan
2. Virus
3. Worm
4. Rootkits
5. Spyware
6. Ransomware
7. Adware
8. Backdoor

Trojan

Trojan is a malicious program, bound with a harmless application program or data in such a way that it can help an attacker gain control and cause damage to the targeted machine. Malware tries to steal victims confidential information and sends back to the attacker.

Symptoms of Trojan Attack

- Computer browser is redirected to unknown pages.
- Strange chat boxes appear on computer screen.
- Reversing the functions of the right and left mouse buttons.
- Abnormal activity by the modem, network adapter, or hard drive.
- The account passwords changes.
- The ISP complains to the target that your computer is performing unauthorized network scanning.
- An attacker can gain access to personal information about a target

Trojan Detection

- Scan for suspicious OPEN PORTS
- Scan for suspicious RUNNING PROCESSES
- Scan for suspicious DEVICE DRIVERS INSTALLED
- Scan for suspicious REGISTRY ENTRIES
- Scan for suspicious WINDOWS SERVICES
- Scan for suspicious STARTUP PROGRAMS
- Scan for suspicious NETWORK ACTIVITIES

Checking for Open Ports

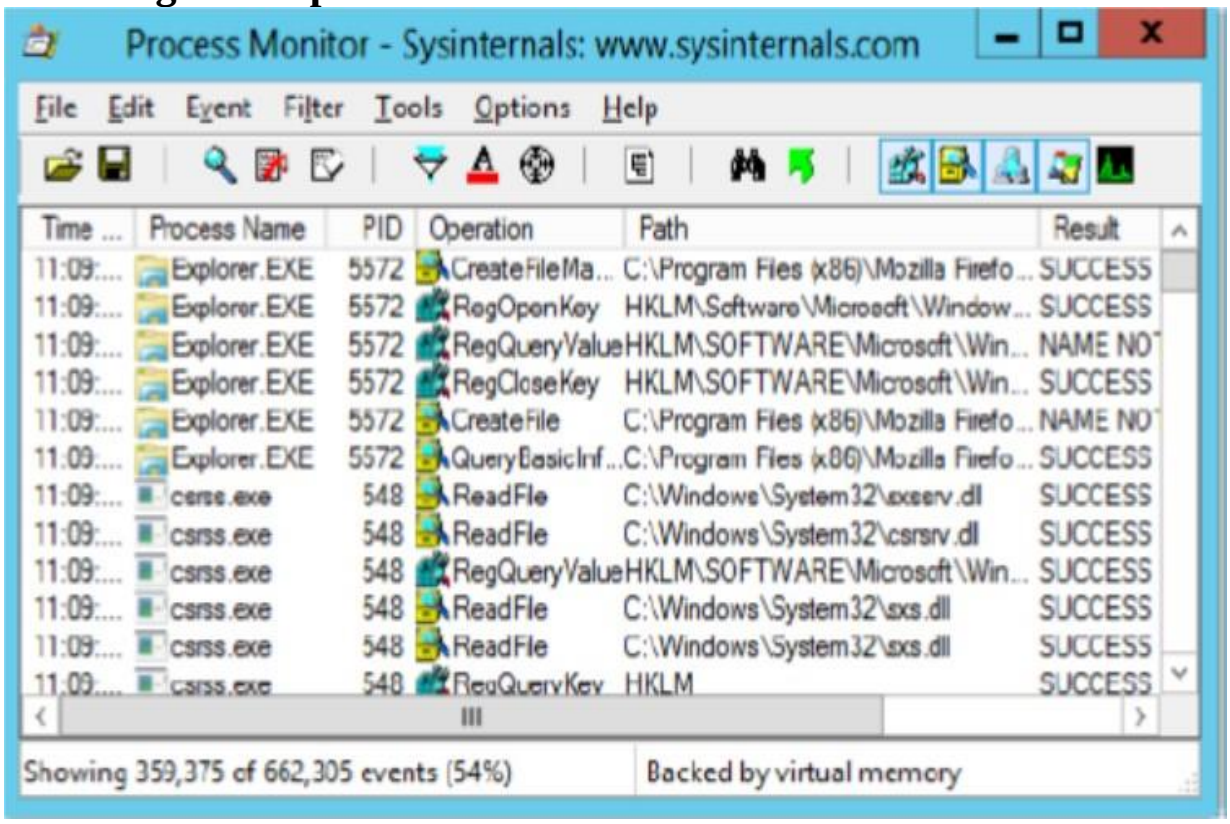
```
G:\Users\SAM>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3790           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8501           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:26143          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49408          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49409          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49410          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49411          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49416          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49417          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49424          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49427          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7337         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50505        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:50425      111.221.29.153:443     ESTABLISHED
  TCP    192.168.1.2:51413      74.125.130.108:993     ESTABLISHED
  TCP    192.168.1.2:52039      216.58.220.5:443       ESTABLISHED
  TCP    192.168.1.2:52042      216.58.220.14:443      ESTABLISHED
  TCP    192.168.1.2:52043      216.58.220.14:443      ESTABLISHED
  TCP    192.168.1.2:52045      216.58.220.1:443       TIME_WAIT
  TCP    192.168.1.2:52055      111.221.29.254:443     ESTABLISHED
```

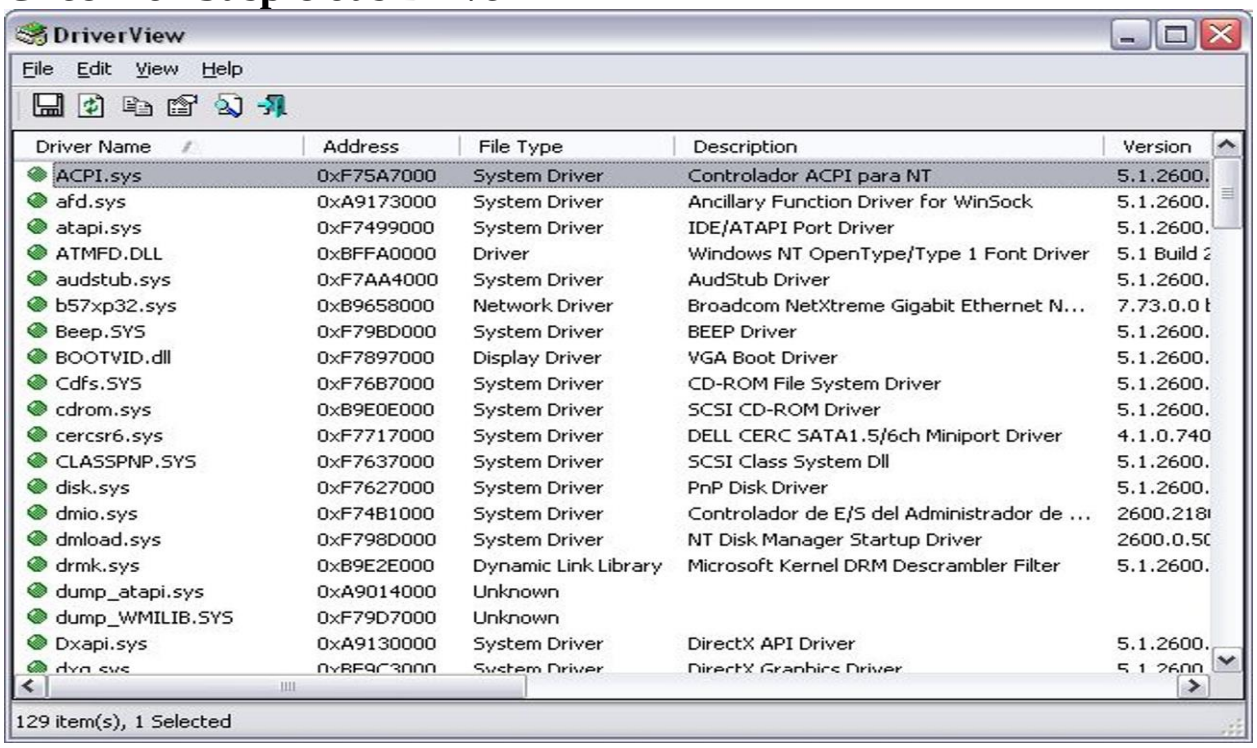
By using the netstat tool to check for open ports, the connection established ports

Checking for suspicious Processes



By using the process monitor tool, we verify for suspicious processes

Check for Suspicious Driver



By using the Driver view tool to check for the Suspicious drivers in the system

Virus

VIRUS stands for Vital Information Resource Under Seize. The virus can self-replicate by producing a copy of itself and attaching to another program, computer boot sector or a document.

Creating a Virus using Batch file programming or bash commands

Batch file programming can be used to automate several jobs in windows operating system, which means the repetitive tasks can be written in a file by the administrators to simplify the job just by running the file instead of executing command separately.

Shell scripting performs the similar job in Linux environment to automate the execution of simple commands. Hackers take advantage of batch or shell scripting knowledge to create dangerous viruses which can destroy data on a victim machine or can consume all the PC resources to make the PC either crash or slow down.

Worms

Worms are malicious programs that replicate and spread across the network connections independently without human restrictions to infect computers.

Rootkit

Rootkit is a malicious program that has the ability to hide its presence from the user (victim) and perform malicious activities to grant full access of the infected computer to the attacker.

Spyware

Spyware is a program that records user interaction with the computer, without their knowledge and sends them to the remote attackers over the internet. Spyware hides its process, files, and other objects to avoid detection and removal.

Ransomware

Ransomware is a malware that can restrict access to computer system files and folders and demands an online ransom payment to the malware creator to remove the restrictions.

Adware

Adware is designed to display unwanted advertisements on the browser which redirects users search requests to malicious web pages that forces them to download malware on to their computers. Adware can also be used to collect users search habits.

Backdoor

A backdoor is a piece of code executed on victim computer system by an attacker to bypass standard authentication and maintain secure unauthorized access to remote desktop.

Countermeasures

- Do not download email attachments received from unknown senders.
- Block unnecessary ports running vulnerable services.
- Avoid downloading and executing applications from untrusted sources.
- Restrict permissions within the desktop environment to prevent malicious applications installation.
- Run host-based antivirus, firewall, and intrusion detection software.
- Manage local workstation file integrity through checksums, auditing, and port scanning.