Malwares

- What is Malware?

Any software intentionally designed to cause damage to a computer, server or computer network. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user.

Types of Viruses and Worms 

- **How it works?**
  i. Infection Phase - a virus planted on a target system and replicates itself and attaches to one or more executable files
  ii. Attack phase - the infected file is executed accidentally by the user, or in some way is deployed and activated
- **Virus** - Designed to spread from host to host and has the ability to replicate itself. They cannot reproduce/spread without help. They operate by inserting or attaching itself to a legitimate program or document in order to execute its code.
- **Macro Virus** - Written in a macro language (e.g: VBA) and that is platform independent.
- **Compression Viruses** - Another type of virus that appends itself to executables on the system and compresses them by user's permissions.
- **Stealth Virus** - Hides the modifications it has made; Trick antivirus software; intercepting its requests to the OS and provides false and bogus information.
- **Polymorphic Virus** - Produces varied but operational copies of itself. A polymorphic virus may have no parts that remain identifcal between infections, making it very hard to detect using signatures.
- **Multipart Virus** - Attempts to infect both boot sector and files; generally refers to viruses with multiple infection methods
- **Self-garbling (metamorphic) virus** - Rewrites itself every time it infects a new file.
- **Other Virus Types**

    - **Boot Sector Virus** - known as system virus; moves boot sector to another location and then inserts its code int he original location
    - **Shell Virus** - wraps around an application's code, inserting itself before the application's
    - **Cluster Virus** - modifies directory table entries so every time a file or folder is opened, the virus runs
    - **Encryption Virus** - uses encryption to hide the code from antivirus
    - **Cavity Virus** - overwrite portions of host files as to not increase the actual size of the file; uses null content sections
    - **Sparse Infector Virus** - only infects occasionally (e.g. every 10th time)
    - **File Extension Virus** - changes the file extensions of files to take advantage of most people having them turned off (readme.txt.vbs shows as readme.txt)
- **Virus Makers**
    - Sonic Bat
    - PoisonVirus Maker
    - Sam's Virus Generator
    - JPS Virus Maker
- **Worm** - self-replicating malware that sends itself to other computers without human intervention
    - Usually doesn't infect files - just resides in active memory
    - Often used in botnets
- **Ghost Eye Worm** - hacking tool that uses random messaging on Facebook and other sites to perform a host of malicious efforts.
- **Logic Bomb** - Executes a program when a certain event happens or a date and time arrives.
- **Rootkit** - Set of malicious tools that are loaded on a compromised system through stealthy techniques; Very hard to detect;
- **Ransomware** - malicious software designed to deny access to a computer until a price is paid; usually spread through email
    - **WannaCry** - famous ransomware; within 24 hours had 230,000 victims; exploited unpatched SMB vulnerability
        - **Other Examples**
            - Cryptorbit
            - CryptoLocker
            - CryptoDefense
            - police-themed

- **Trojan horse** - A program that is disguised as another legitimate program with the goal of carrying out malicious activities in the background without user's knowledge.
    - **RAT - Remote Access Trojans** - Malicious programs that run on systems and allow intruders to access and use a system remotely.
- **Immunizer** - Attaches code to a file or application, which would fool a virus into 'thinking' it was already infected. (e.g: like human vaccine).
- **Behavior blocking** - Allowing the suspicious code to execute within the OS and watches its interactions looking for suspicious activities.

> ⚠ - **Viruses needs help/interaction to propagate; Worms self propagates**

Major characteristics of viruses:

1. Infecting other files
2. Alteration of data
3. Transforms itself
4. Corruption of files and data
5. Encrypts itself
6. Self-replication

Stages of Virus Lifecycle:

1. Design
2. Replication
3. Launch
4. Detection
5. Incorporation - A.V. figures out the virus pattern & builds signatures to identify and eliminate the virus
6. Execution of the damage routine - A.V. to the rescue

Malware Basics

- **How is malware distributed?**
    - SEO manipulation
    - Social Engineering / Click-jacking
    - Phishing
    - Malvertising
    - Compromising legitimate sites

    - Drive-by downloads
    - Spam
- **Malware** - software designed to harm or secretly access a computer system without informed consent
    - Most is downloaded from the Internet with or without the user's knowledge
- **Overt Channels** - legitimate communication channels used by programs
- **Covert Channels** - used to transport data in unintended ways
- **Wrappers** - programs that allow you to bind an executable to an innocent file

Basic components of Malware

1. **Crypters** - use a combination of encryption and code manipulation to render malware undetectable to security programs; protects from being scanned or found during analysis.
2. **Downloader** - Used to download additional malware.
3. **Dropper** - Used to install additional malware into the target system.
4. **Exploit** - Malicious code used to execute on a specific vulnerability.
5. **Injector** - Used to expose vulnerable processes in the target system to the exploit.
6. **Obfuscator** - Used to conceal the true purpose of the malware.
7. **Packers** - Used to bundle all of the malware files together into a single executable.
8. **Payload** - Used to take over the target machine.
9. **Malicious Code** - Used to define the abilities of the malware.

Exploit Kits - help deliver exploits and payloads

- Infinity
- Bleeding Life
- Crimepack
- Blackhole Exploit Kit

Trojans 

- Software that appears to perform a desirable function but instead performs malicious activity
    - To hackers, it is a method to gain and maintain access to a system

    - Trojans are means of delivery whereas a backdoor provides the open access
    - Trojans are typically spread through **Social Engineering**.

- **Types of Trojans:**
    - **Defacement trojan**
    - **Proxy server trojan**
    - **Botnet trojan**
        - Chewbacca
        - Skynet
    - **Remote access trojans**
        - RAT
        - MoSucker
        - Optix Pro
        - Blackhole
    - **E-banking trojans**
        - Zeus
        - Spyeye
    - **IoT Trojans**
    - **Security Software Disable Trojans**
    - **Command Shell Trojan** - Provides a backdoor to connect to through command-line access
        - Netcat
    - **Covert Channel Tunneling Trojan** (CCTT) - a RAT trojan; creates data transfer channels in previously authorized data streams

Infection Process:

1. Creation of a Trojan using Trojan Construction Kit
2. Create a Dropper
    - Used to install additional malware into the target system.
3. Create a Wrapper
    - Wrappers - programs that allow you to bind an executable to an innocent file
4. Propagate the Trojan
5. Execute the Dropper

Trojan Port Numbers:

Trojan Name	TCP Port
Death	2

Trojan Name	TCP Port
Senna Spy	20
Blade Runner, Doly Trojan, Fore, Invisble FTP, WebEx, WinCrash	21
Shaft	22
Executor	80
Hackers Paradise	31,456
TCP Wrappers	421
Ini-Killer	555
Doom, Santaz Back	666
Silencer, WebEx	1001
DolyTrojan	1011
RAT	1095-98
SubSeven	1243
Shiva-Burka	1600
Trojan Cow	2001
Deep Throat	6670-71
Tini	7777
Dumaru.Y	10000
SubSeven 1.0-1.8, MyDoom.B	10080
VooDoo Doll, NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill	12345
Whack a Mole	12361-3
NetBus	17300
Back Orifice	31337,8
SubSeven, PhatBot, AgoBot, Gaobot	65506

> ⚠ - **Its not necessary to know every possible trojan port in the history for the CEH exam, it's good for understanding.**

Trojan Countermeasures

1. Avoid cicking on unusual or suspect email attachments
2. Block unused ports
3. Monitor network traffic
4. Avoid downloading from unstrusted sources
5. Install & updated anti-virus software
6. Scan removable media before use
7. Validate file integrity of all externally sourced software
8. Enable auditing
9. Configure Host-Based firewalls
10. Use IDS

Techniques

- `netstat -an` - shows open ports in numerical order
- `netstat -b` - displays all active connections and the processes using them
- **Process Explorer** - Microsoft tool that shows you everything about running processes
- **Registry Monitoring Tools**
  - SysAnalyzer
  - Tiny Watcher
  - Active Registry Monitor
  - Regshot
- **Msconfig** - Windows program that shows all programs set to start on startup
- **Tripwire** - integrity verifier that can act as a HIDS in protection against trojans
- **SIGVERIF** - build into Windows to verify the integrity of the system
  - Log file can be found at `c:\windows\system32\sigverif.txt`
  - Look for drivers that are not signed

Malware Analysis

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

Types of Malware analysis:

1. **Static (Code Analysis)** - performed by fragmenting the binary file into individual elements that can be analyzed without executing them.
   - File fingerprinting
   - Local & online scanning of elements to see if they match known malware profiles

    - String searching
    - Identifying packers/obfuscators used
    - Identifying the PE's (portable executable) information
    - Identify dependencies
    - Malware disassembly
2. **Dynamic (Behavioral Analysis)** - performed by executing the malware to see what effect it has on the system.
    - System baselining
    - Host integrity monitoring

- **Tools for Disassembling | Debugging | Reverse Engineering:**
    - IDA Pro
    - OllyDdg
    - Ghidra by NSA
- **Sheepdip** - Dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers.

Steps

1. Make sure you have a good test bed
    - Use a VM with NIC in host-only mode and no open shares
2. Analyze the malware on the isolated VM in a static state
    - Tools - binText and UPX help with looking at binary
3. Run the malware and check out processes
    - Use Process Monitor, etc. to look at processes
    - Use NetResident, TCPview or even Wireshark to look at network activity
4. Check and see what files were added, changed, or deleted
    - Tools - IDA Pro, VirusTotal, Anubis, Threat Analyzer

- **Preventing Malware**
    - Make sure you know what is going on in your system
    - Have a good antivirus that is up to date
        - Airgapped - isolated on network

Rootkits

- Software put in place by attacker to obscure system compromise
- Hides processes and files

- Also allows for future access
- **Examples**
  - Horsepill - Linux kernel rootkit inside initrd
  - Grayfish - Windows rootkit that injects in boot record
  - Firefef - multi-component family of malware
  - Azazel
  - Avatar
  - Necurs
  - ZeroAccess
- **Hypervisor level** - rootkits that modify the boot sequence of a host system to load a VM as the host OS
- **Hardware** - hide malware in devices or firmware
- **Boot loader level** - replace boot loader with one controlled by hacker
- **Application level** - directed to replace valid application files with Trojans
- **Kernel level** - attack boot sectors and kernel level replacing kernel code with back-door code; most dangerous
- **Library level** - use system-level calls to hide themselves
- One way to detect rootkits is to map all the files on a system and then boot a system from a clean CD version and compare the two file systems