Course Notes

1 Definitions

1.1 Chapter 1: Introduction To Ethical Hacking

1.1.1 Information Security Overview

- Intelligence based warfare: A sensor-based technology that directly corrupts technological systems. "Warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space.
-

1.1.2 Cyber Kill Chain Concepts

- Reconnaissance: An Adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before attacking.
- Installation: Adversary downloads and intalls more malicious software on the target system to maintain access to the target network for an extended period.
- Command and control: The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adverary-controlled servers to communicate and pass data back and forth.
- Weaponization: Adversary selects or creates a tailored deliverable malicious payload (remote access malware weapon) using an exploit and a backdoor to send it to the victim.
-

1.1.3 Hacking and Ethical Hacking Concepts

1.1.4 Information security controls, laws and standards

- SOX Titles:
  - Title 3: Corpoate Responsability, eight sections and mandates that senior executives take individual responsability for the accuracy and completeness of corporate financial reports.

- Title 5: Analyst Conflicts of Intrest: One section that discusses the measures designed to help restore investor confidence in the reporting of securities analyst. Defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.
- Title 6: Commission Resources and Authority: four sections defining practices to restore investor confidence in securities analysts. Defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.
- Title 7: Studies and Reports: five sections, requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings.

1.2 Chapter 2: Footprinting and Reconnaissance

1.2.1 Footprinting Concepts

- Sherlock: To search a vast number of social networking sites for a target username. This tool helps the attacker to locate the target user on various social networking sites along with the complete URL.
- BeRoot: BeRoot is a post-exploitation tool to check for common misconfigurations which can allow an attacker to escalate their privileges.
- OpUtils: SNMP enumeration protocol that helps to monitor, diagnose and trouble shoot the IT resources.
- Sublist3r: Sublist3r is a Python script designed to enumerate the subdomains of websites using OSINT. It enables you to enumerate subdomains across multiple sources at once.
- Passive footprinting: no direct interaction, archived and stored information from publically accessible sources.
  - Finding information through search engines
  - Finding the Top-level Domains (TLDs) and sub-domains of a target network through web services.
  - Collecting information on the target through web services.
  - Performing people search using social networking sites and people search engines.
  - Gathering financial information about the target through financial services.

  - Gathering infrastructure details of the target organization through job sites.
  - Monitoring target using alert services.
- Active footprinting, direct interaction with the target network:
  - Querying published name servers of the target.
  - Extracting metadata of published documents and files.
  - Gathering website information using web spiderin and mirroring tools.
  - Gathering information through email tracking.
  - Performing Whois lookup
  - Extracting DNS Information
  - Performing traceroute analysis
  - Performing social engineering.

1.2.2 Footprinting Methodology

1.2.3 Footprinting Tools and Countermeasures

1.3 Chapter 3: Scanning Networks

1.3.1 Network Scanning Concepts and Tools

1.3.2 Host, Port and Service Discovery

1.3.3 OS Discovery and Scanning Beyond IDS/Firewall

1.4 Chapter 4: Enumeration

1.4.1 Enumeration Concepts

1.4.2 NetBIOS and SNMP Enumeration

- Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems on the internet. Used by ISPs to maintain large routing tables. Utilizes port 179

1.4.3 LDAP, NTP, NFS, and SMTP Enumeration

- LDAP - Lightweight Directory Access Protocol

1.5 Chapter 5: Vulnerability Assessment

1.5.1 Vulnerability Assessment Concepts

- Vulnerability management lifecycle:
  - Risk assessment: All serious uncertanties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws.
  - Remediation: The process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities.
  - Verification: Provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not.
  - Monitoring: Organizations need to perform regular monitoring to maintain system security. Continuous monitoring identifies potential threats and any new vulnerabilities.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
  - Base metric group
    - Exploitability Metrics
      - Attack Vector
      - Attack Complexity
      - Privileges Required
      - User Interaction
      - Scope
    - Impact Metrics
      - Compatibility Impact
      - Integrity Impact
      - Availability impact
      - Scope
- Temporal Metric group

  - Exploit Code maturity
  - Remediation level
  - Report confidence
- Environmental Metric group
  - Confidentiality Requirement
  - Integrity Requirement
  - Availability Requirement
  - modified Base Metrics

1.5.2 Vulnerability Classification and Assessment Types

- Internal Assessment: Involves scrutinizing the internal network to find exploits and vulnerabilities.
- Network-based Assessment: Discover network resources and map the ports and services running to various areas on the network.
- Non-credentialed Assessment: Hacker does not possess any credentials.
- Credentialed Assessment: The ethical hacker possesses the credentials of all machines present in the assessed network.
- Distributed Assessment: employed by organizations with assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications using appropriate synchronization techniques.

1.5.3 Vulnerability Assessment Solutions, Tools and Reports

- Product-Based Solutions: Solutions are installed either on a private or non-routable space or on the internet-addressable portion of an organization's network.
- Tree-Based Assessment: the auditor (parent) selects different strategies for each machine or component (child nodes) of the information system. This approach relies on the administrator to provide a starting piece of intelligence and then to start scanning continuously without incorporating any information found at the time of scanning.

- Service-Based Solutions: Offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network.
- Inference-Based Assessment: Scanning starts by building an inventory of the protocols found on the machine.
- Depth Assessment Tools: Used to discover and identify previously unknown vulnerabilities in a system. Generally tools such as fuzzers, which provide arbitrary input to a system's interface, are used to identify vulnerabilities to an unstable depth.
- Host-Based Vulnerability Assessment Tools: appropriate for servers running various applications, such as the Web, critical files, databases, directories, and remote accesses. These host based scanners can detect high levels of vulnerabilities and provide required information about the fixes (patches)
- Scope assessment tools: Scope assessment tools provide an assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide standard controls and a reporting interface that allows the user to select a suitable scan.
- Application-Layer Vulnerability Assessment Tools: Designed to sever the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose.
- Vulnerability scanning solutions steps:
    1. Locating nodes: locate live hosts in the target network using various scanning techniques.
    2. Performing service and OS discovery: enumerate the open ports and services along with the operating system on the target systems.
    3. Testing for vulnerabilities: test for vulnerabilities on target nodes.
- Tools
    - `theHarvester`: used for open-source intelligence gathering and helps to determine a company's external threat landscape on the Internet. Attackers use this tool to perform enumeration on the LinkdIn social networking site to find employees of the target company along with their job titles.
    - `Qualys VM`: Cloud based service that gives immediate global visibility into where IT systems might be vulnerable to the latest Internet threats and how to

protect them. Helps to continuously identify threats and monitor unexpected changes in a netowrk before they turn into breaches.

  - `Sherlock`: Searches a vast number of social networking sites for a target username.

  - `Octoparse`: Offers automatic data extraction, scrapes web data without coding and turns web pages into structured data. gathers text, links, image urls and html code.

- Report sections

  - Scan information: Provides information such as the name of the scanning tool, its version, and the network ports to be scanned.

  - Target Information: information about the target system's name and address.

  - Results: A complete scanning report containing subtopics such as target, services, vulnerability, classification, and assessment.

  - Target: Includes each host's detailed information and contains the following information:

    * `<Node>` name and address of the host.

    * `<OS>` Operating system

    * `<Date>` Date of the test.

  - Services: Defines the network services by their names and ports.

  - Classification: Allows the system administrator to obtain additional information about the scan, such as its origin.

  - Assessment: provides information regarding the scanner's assessment of discovered vulnerabilities.

1.6 System Hacking

1.6.1 System Hacking Concepts

1.7 Gaining Access (Cracking Passwords and Vulnerability Exploitation)

- Kerberos authentication: Employs a key distribution center (KDC) that consists of an authentication server (AS) and a ticket-granting server (TGS), and uses "tickets" to prove a user's identity.

- Markov-Chain Attack: Attackers gather a password database and split each password entry into two and three character syllables (2-grams and 3-grams); using these character elements, a new alphabet is developed, which is then matched with the existing password database.
- PRINCE Attack: A **PR**obability **IN**finite **C**hained **E**lements (PRINCE) attack is an advanced version of a combinator attack in which, instead of taking inputs from two different dictionaries, attackers use a single input dictionary to build chains of combined words.
- Combinator Attack: Attacker combines the entries of the first dictionary with those of the second dictionary. The resultant list of entries can be used to produce full names and compound words.
- Fingerprint Attack: The passphrase is broken down into fingerprints consisting of single- and multi- character combinations that a target user might choose as his/her password.
- Spiking: Allows attackers to send crafted TCP or UDP packets to the vulnerable server in order to make it crash.
- Generate shellcode: Attackers use the msfvenom command to generate the shellcode and inject it into the EIP register to gain shell access to the target vulnerable server.
- EIP Register: Extended Instruction Pointer (EIP) register contains the address of the next instruction to be executed.
- Fuzzing: Allows the attacker to send large amounts of data to the target server so that it experiences buffer overflow and overwrites the EIP register.
- Overwrite the EIP register allows attackers to identify whether the EIP register can be controlled and can be overwritten with malicious shellcode.
- Tools
  - Factiva: Global news database and licensed content provider. It is a business information and research tool that gets information from licensed and free sources and provides capabilities such as searching, alerting, dissemination, and business information management.
  - Shodan: Computer search engine that searches the Internet for connected devices (routers, servers, and IoT).
  - SecurityFocus: database of the recently reported security vulnerabilities.

  - Maltego: program that can be used to determine the relationship and real-world links between people, groups, organizations, websites, Internet infrastructure and documents.
  - Infoga: Used for gathering email account information (IP,hostname, country) from different public sources and it checks if the email was leaked using the `haveibeenpwned.com` API.
  - Splint: Can be used to detect common security vulnerabilities including buffer overflows.

- NTLMv2 us a default authentication sceme that performs authentication using a challenge/response strategy. Can be cracked with dictionary or brute force, not rainbow table because NTMLv2 adds a salt value that is exchanged in the messaging, thus it cannot be used in a pass-the-hast attack either.
-

1.7.1 Escalating Privileges

- Meltdown vulnerability - This is found in all the Intel processors and ARM processors deployed by Apple. This vulnerability leads to tricking a process to access out-of-bounds memory by exploiting CPU optimization mechanisms such as speculative execution.
- Dylib hijacking - Allows an attacker to inject a malicious sylib in one of the primary directories and simply load the malicious dylib at runtime.
- Spectre Vulnerability - Found in many modern processors such as AMD, ARM, Intel, Samsung and Qualcomm. Leads to tricking a processor to exploit speculative execution to read restricted data. Modern processors implement speculative execution to predict the future and to complete the execution faster.
- DLL hijacking - Attacker places a malicious DLL in the application directory; the application will execute the malicious DLL in place of the real DLL.
- Application Shimming - Malicious technique on Microsoft Windows in which application shim's are abused to establish persistence, inject DLLs, elevate privileges, and much more. The Microsoft Windows Application Compatibility Framework can be used to create Shim Database (.sdb) files that are typically used to fix software compatibility issued, however they can instead be abused for nefarious purposes.

1.7.2 Maintaining Access (Executing Applications and Hiding Files)

- Rootkits

  - Boot Loader Level Rootkit: Replaces the original bootloader with the one controlled by a remote attacker.
  - Hardware/Firmware Rootkit: Hides in hardware devices or platform firmaware that are not inspected for code integrity.
  - Hypervisor level rootkit: Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine.
  - Library Level Rootkit: Replaced the original system calls with fake ones to hide information about the attacker.
  - Application level rootkit: Operate inside the victims computer by replaceing the standard application files (binaries) with rootkits or by modifying behavior of resent applications with patches, injected malicious code, and so on.
  - Kernel level rootkit: the kernel is the core of the operating system. Kernel level rootkits run in Ring-0 with the highest operating system privileges. These cover backdoors on the computer and are created by writing additional code or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel modules in Linux. Of the kit's code contains mistakes or bugs, kernel-level rootkits affect the stability of the system. These have the same privileges of the operating system; hence they are difficult to detect and intercept or subvery the operatings of operating systems.

- Hiding data
  - Spread Spectrum Techniques: Communcation signals occupy more bandwidth than required to sent the infomration. The sender increases the band spread by means of code (independent of data), and the reciever uses a synchonized reception with the code to recover the information from the spread spectrum data.
  - Transform Domain Techniques: Hides information in significant parts of the cover image, such as cropping, compression, and some other image processing areas.
  - Substitution Techniques: Attacker tried to encode secret information by substituting the insignificant bits with the secret message.
  - Distortion Techniques: The user implements a sequence of modifications to the cover to obtain a stego-object. The sequence of modifications represents the transformation of a specific message.

- Stego-Attacks
  - Stego-only attack: the steganalyst or attack does not have access to any information except the stego-medium or stego-object. In this attack, the steganalyst must try every possible steganography algorithm and related attack to revoce the hidden information.
  - Chosen-message attack: The steganalyst uses a known message to generate a stego-object by using various steganography tools to find the the steganography algorithm used to hide information.
  - Chosen-stego attack: Takes place when the steganalyst knows both the stego-object and steganography tool or algorithm to hide the message.
  - Chi-square attack: The chi-square method is based on probability analysis to test whether a given stego-object and the original data are the same or not. If the differece between both is nearly zero, then not data are embedded; otherwise, the stego-object includes embedded data inside.

1.7.3 Clearing logs

- Commands
  - `history -c`: useful in clearing the stored history.
  - `export HISTSIZE=0`: This command disables the BASH shell from saving the history by setting the size of the history file to 0.
  - `history-w`: This command only deletes the history of the current shell, wheras the command history of other shells remain unaffected.
  - `shred ~\.bash_history`: This command shreds the history file, making its contents unreadable.
- TCP Parameters: Can be used by the attacker to distribute the payload and to create covert channels. Some of the TCP fields where data can be hidden are:
  - IP Identification field: one character is encapsulated per packet.
  - TCP acknowledgement number: Uses a bounce server that revieves packets from the victim and sends it to an attacker. Here one hidden character is relayed by the bounce server per packet.
  - TCP initial sequence number: does not require an established connection between two systems. Here, one hidden character is encapsulated per SYN

request and Reset packets.

- Clear Online Tracks: Attacker clear online tracks maintained using web history, logs. cookies, cache, downloads, visited time, and other on the target computer, so that victims cannot notice what online activities attackers have performed.
- Programs
  - `Auditpol.exe`: command line utility tool to change Audit Security settings at the category and sub-category levels. Attackers can use AuditPol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.
  - `Clear_Event_Viewer_Logs.bat/clearlogs.exe` utility for wiping the logs of a target system.
  - `SECEVENT.EVT`: Deletes security events
  - `SYSEVENT.EVT`
  - `APPEVENT.EVT`

1.8 Malware Threats

1.8.1 Malware Concepts

- Social Engineering Click-jacking: Inject malware into websites that appear legitimate to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledeg of the user.
- Malvertizing: Embedding malware-laden advertisements in legitimate onlone advertising channels to spread malware on systems of unsuspecting users.
- Black hat search Engine Optimization (SEO): also known as unethical SEO uses agressive SEO tactics such as keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to get higher search engine rankings for malware pages.
- Compromised Legitimate Websites
- Malware Components
  - Downloader: Type of trojan that downloads other malware or malicious code files from the internet on to the PC or device. Attackers usually install downloaders when they first gain access to a system.

  - Crypters: software that encrypts the original binary code of the .exe file. Crypters hide viruses, spyware, keyloggers, Remote Access Trojans (RATs), and others to make them undetectable to anti-viruses.
  - Obfuscator: Obfuscation means to make code harder to understand or read, generally for privacy or security concerns. Converts a straightforward program into one that works the same way but is much harder to understand. It is a program to conceal the malicious code of malware via various techniques, thus making it hard for security mechanisms to detect or remove it.
  - Payload: Part of the malware that performs desired activity when activated.

1.8.2 APT Concepts

-

1.8.3 Trojan Concepts

- Ports for trojans:
  - Port 80: Necurs, NetWire, Ismdoor, Poison Ivy, Executer, Codered, APT 18, APT 19, APT 32, BBSRAT, Calisto, Carbanak, Carbon, Comnie, Empire, FIN7, InvisiMole, Lazarus Group, MirageFox, Mis-Type, Misdat, Mivast, MoonWind, Night Dragon, POWERSTATS, RedLeaves, S-Type, Threat Group-3390, UBoatRAT.
  - Port 20/22/80/442: Emotet
  - Port 8080: Zeus, APT 37, Comnie, EvilGrab, FELIXROOT, FIN7, HTTPBrowser, Lazarus Group, Magic Hound, OceanSalt, S-Type, Shamoon, TYPEFRAME, Volgmer.
  - Port 11000: Senna Spy
- Banking trojan - steals credentials before they are encrypted by the system and sends them to the attacker.
  - TAN Grapper: Transaction Authentication Number (TAN) is a single-use password for authenticating online banking transactions. Banking trojans intercept valid TANs entered by users and replace them with random numbers. Subsiquently, the attacker misuses the intercepted TAN with the target's login details.
  - HTML Injection: Trojan creates fake form fields on e-banking pages, therby enabling the attacker to collect the target's account details, credit card number,

date of birth, etc. The attacker can use this information to impersonate the target and compromise his/her account.

  - Form Grabber: Type of malware that captures a target's sensitive data such as IDs and passwords, from a web browser form or page. It is an advanced method for collecting the target's Internet banking infomration. It analyses POST requests and responses to the victims browser. it compromises the scramble pad authentication and intercepts the scramble pad input as the user enters his/her Customer Number and Personal Access Code.

  - Covert Credential Grabber: This malware remains dormant until the user performs an online financial transaction. It works covertly to replicate itself on the computer and edits the registry entries each time the computer is started. The trojan also searches the cookie files that had been stored on the computer while browsing financial websites. Once the user attempts to make an online transaction, the Trojan covertly steals the login credentials and transmits them to the hacker.

- Covert Channel: methods attackers use to hide data in an undetectable protocol. Rely on tunneling, which enables one protocol to transmit ofver the other. Any process or a bit of data can be a covert channel. Attackers can use covert channels to install backdoors on the target machine.

- Asymmetric routing: Routing technique where packets flowing through TCP connections travel through different routes to different directions.

- Tools:

  - Trojan.Gen: generic detection for many individual but varied Trojans for which specific definitions have not been created.

  - Senna Spy Trojan Generator: Trojan that comer hidden in malicious programs. Once you install the source program, the trojan attempts to gain 'root' access without knowledge.

  - Win32.Trojan.BAT: System destructive trojan program. It will crash the system by deleting files.

  - DarkHorse Trojan Maker: Used to create user-specific trojans by selecting from various options.

- Trojans

  - Mirai: a self-propagating botnet that infects poorly protected internet devices

(IoT). Uses Telnet port 23 or 2323 to find devices that are using their factory default username and password. Mirai is used to coordinate and mount a DDoS attack against a chosen victim.

  - Netwire: type of RAT
  - Theef: type of RAT
  - Kedi RAT: type of RAT

1.8.4 Virus and Worm Concepts

- Virus lifecycle Stages
  - Replication: Virus replicates for a period within the target system and then spreads itself.
  - Launch: Virus is activated when the user performs specific actions such as running an infected program.
  - Detection: Virus is identified as a threat infecting the target system.
  - Execution of the damage routine: User installs antivirus updates and eliminate the virus threats.
- Types of viruses
  - Sparse infector virus: infect less often and try to minimize their probability of discovery. Only infect on a certain condition or those files whose lengths fall within a narrow range.
  - Metamorphic Viruses: Programmed such that they rewrite themselves completely each time they infect a new exe.
  - Cavity Viruses: Some programs have empty spaces in them. Cavity viruses, or space fillers, overwrite a part of the host file with a constant (usually nulls), without increasing the length of the file while preserving its functionality. Maintaining a constant file size when infecting allows the vius to avoid detection.
  - Polymorphic Viruses: Infect a file with an encrypted copy of a polymorphic code already decoded by a decryption module. Polymorphic viruses modify their code for each replication to avoid detection.
  - Tunneling Viruses: Tries to hide from antivirus by actively altering and corrupting the service call interrupts while running. The virus code replaces the requests

to perform operations with respect to these service call interrupts. They state false information to hide their presence from antivirus programs.

- Macro Viruses: Infect Microsoft Word or similar applications by automatically performing a sequence of actions after triggering an application. Mose macro viruses are written using the macro language Visual Basic or Applications (VBA), and they infect templates or convert infected documents into template files while maintaining their appearance of common document files.
- File Viruses: Infect files executed or interpreted in the system, such as COM, EXE, SYS, OVL, OBJ, PRG, MNU, and BAT files. File viruses can be direct-action (non-resident) or memory-resident-viruses.
- System or Boot Sector Viruses: Most common targets for a virus are the system sectors, which include the mastor boot record (MBR) and the DOS boot record system sectors. An OS executes code in these areas while booting. Every disk has some sort of system sector. MBRs are the most virus prone zones because if the MBR is corrupted, all data will be lost. The DOS boot sector also executes during system booting. This is a crucial point of attack for viruses.

1.8.5 Fileless Malware Concepts

-

1.8.6 Malware Analysis

- DLLs
  - `Kernel32.dll`: Core functionality, such as access and manipulation of memory, files, and hardware.
  - `Advapi32.dll`: Provides access to advanced core Windows components such as the Service Manager and Registry.
  - `WSock32.dll` and `Ws2_32.dll`: Networking DLLs that help connect to a network or perform network-related tasks.
  - `Ntdll.dll`: Interface to the Windows kernel.
- Tools
  - Resource Hacker: A resource editor for 32 and 64 bit Windows applications. Both a resource compiler (for .rc files), and a decompiler - enabling viewing

and editing of resources in executables (.exe; .dll; .src; etc.) and compiled resource libraries (.res, .mui).

  - Ghirda: Software reverse engineering (SRE) framework created and maintained by the National Security Agency Reserach Directorate. Framework includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows macOS, and Linux. Capabilities include disassembly, assembly, decompilation, graphine, and scripting, along with hundreds of other features.
  - Hakiri: Monitors Ruby apps for dependency and code security vulnerabilities.
  - Synk: Platform developers choose to build cloud native applications securly.
  - BinText: small text extractor utility that can extract text from any kind of file and includes the ability to find plain ASCII text, Unicode (double byte ANSI) text and Resource strings, providing useful information for each item in the optional 'advanced' view mode.
  - UPX (Ultimate Pakcer for Executables): FOSS exe packer supporting a number of file formats from different operating systems.
  - ASPack: Advanced exe packer created to compress Win32 exe files and to protect them against non-professional reverse engineering.
  - PE Explorer: Allows you to open, view and edit a variety of different 32-bit Windows exe file types (PE files) ranging from common (EXE, DLL, ActiveX) to less familiar types (SCR {Screensavers}, CPL {Control panel applets}), SYS, MSSTYLES, BPL, DPL, and more.

- Malware Encryption
  - SamSam: uses RSA-2048 asymmetric encryption technique
  - WannaCry: Uses a combination of the RSA and AES algorithms to encrypt files
  - Dharma: Encrypts files using an AES 256 algorithm. the AES key is also encrypted with an RSA 1024.
  - Cerber: uses RC4 and RSA algorithms for encryption.

- EXE file sections
  - `.rdata`: Contains the import and export information as well as other read-only data used by the program.

- `.data`: Contains the program's global data, which the system can access from anywhere.
- `.rsrc`: Consists of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support.
- `.text`: Contains instructions and program code that the cpu executes.

- Monitoring
  - Startup Programms monitoring is used to detect suspicious startup programs and processes.
  - Registry Monitoring is used to examing the changes made to the system's registry by malware.
  - Process monitoring is used to scan for malicious processes.
  - Windows services monitoring traces malicious services initiated by the malware. Since malware employs rootkit techniques to manipulate `HKEY_LOCAL_MACHINE\System\Curr` registry keys to hide its processes, windows service monitoring can be used to identify such manipulations.

1.8.7 Malware Countermeasures

- Tools:
  - AlienVault USM Anywhere: A fileless malware detection tool that provides a unified platform for threat detection, incident response, and compliance management. It centralizes security monitoring of networks and devices in the cloud, on premis, and at remote locations, helping to detect threats anywhere.
  - GFI LanGuard: patch management software scans the network and installs and manages security and non-security patches.
  - Sonar Lite: Used to troubleshoot network connetivity, domain resolution issues or find out registration information for any domain.
  - Monit: M/Monit can monitor and manage distributed computer systems, conduct automatic maintenance and repair, and execute meaningful casual actions in error situations.
  - ClamWin: Free antivirus program for Windows.
  - DriverView: Displays the list of all device drivers loaded on the system. Gives additional information about the driver as well.

- Malware:
  - ZeuS: Also known as Zbot, a powerful banking trojan that explicitly attempts to steal confidential infomration like system information, online credentials, banking details, etc. Zeus is spread through drive-by-downloads and phishing schemes.

1.9 Sniffing

1.9.1 Sniffing Concepts

-

1.9.2 Sniffing Techniques

- Tools
  - Nikto: A web server assessment tool that examines a web server to discover potential problems and security vulnerabilities.
  - dsniff: a collection of tools for netowrk auditing and penetration testing and can also be used to perform ARP poisoning.
  - OpenVAS: a framework of several services and tools offering a comprehensive and powerful vulnerability scaning and vulnerability management solution
  - Nexpose: Vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation.

1.10 General / Unsorted

- CIA Triad:
  - Confidentiality: unauthorized access to information.
  - Integrity: Trustworthiness of data
  - Availability: accessible when required
  - (Other) Non-repudiation: Sender of a message cannot deny having sent the message, same for receiver.
  - (Other) Authenticity: quality of being genuine
- OSI model - Open System Interconnection model

- Local Area Network (LAN): Computer network that connects two or more computers within a limited area.
- Virtual Local Area Network (VLAN): Broadcast domain that is divided in a computer network at the data link layer (OSI layer 2).
- Wide Area Network (WAN): Covers larger area than a LAN, typically involves telecommunication circuits for a special purpose, ie: banking network. Nodes are more than 10 miles apart.
- Time to live (TTL): time period a message can live on the network before it is discarded. (8-bits). Number of seconds or number of hops?
- User Datagram Protocol (UDP): light weight communication protocol that gives no assurance of delivery. If the application receives out of order packets they are destroyed rather than worrying about reordering them.
- Transmission Control Protocol (TCP):
- Internet of Things (IoT): Devices with embedded software and network access.
- Malware: software created to harm or infiltrate a computer system without the owners consent.
  - Virus: Create copies of themselves in other programs and activate from a trigger event.
  - Worm
  - Spyware
  - Trojan
- Information Security Policy: set of rules sanction by an organization to ensure that user of networks abide by the prescriptions regarding the security of data stored within the boundaries of the organization.
- Event: Something that happens that is detectable
- Incident: an event that violates policy.
- Certificate Authority: Organization that issues digital certificates.
- Vulnerability Scanner: Computer program designed to assess computer systems, network or applications for known weaknesses.

- Uniform Resource Locator (URL): reference to a web resource. Is a specific type of URI.
- Uniform Resource Identifier (URI): Unique sequence of characters that identifies a logical or physical resource used by web technologies. the `http://` part of the url.
- DNS Zone transfer: Used to duplicate or make copies of DNS data across a number of DNS servers or to back up DNS files.
- Open-source intelligence: to describe identifying information about a target using freely available sources.
- Defence in breadth: planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle.
- Defence in depth (DiD): Information security approach in which a series of security mechanisms and controls are layered throughout a computer network.
- Lawful Interception: Process of legally intercepting communications betwen two or more parties for surveillance on telecommunications, VoIP, data, and multiservice networks.
- Internet Zones
  - Internet (uncontrolled zone): outside the boundary of your organization.
  - Internet DMZ (controlled zone): Internet-facing controlled zone that contains components in which clients may directly communicate with. Usually buffered by two firewalls one from internet to DMZ and one from DMZ to the internal network.
  - Production network (restricted zone): A restricted zone supports functions to which access must be strictly controlled; direct access from an uncontrolled network should not be permitted. In a large enterprise, several network zones might be designated as restricted. As with an internet DMZ, a restricted zone is typically bounded by one or more firewalls that filter incoming and outgoing traffic.
  - Intranet (controlled zone): is not heavily restricted in use, but an appropriate span of control is in place to assure that network traffic does not compromise the operation of critical business functions.
  - Management network (secured zone): In a secured zone, access is tightly controlled and available to only to a small number of authorized users. Access

to one area of the zone does not necessarily apply to another area of the zone.

1.11 Attacks

- SQL Injection:
  - In-band SQL Injection: Attacker uses the same communication channel to launch the attack and gather results. (error-based and union-based SQL injection).
- Bluetooth
  - Bluesnarfing: Theft of information from a target device using a bluetooth connection.
  - Bluejacking: Transmission of data to a target device using a bluetooth connection.
- Operating System Attacks
- Application-Level Attacks
- Shrink Wrap Code Attacks
- Misconfiguration Attacks
- DHCP starvation attack: Broadcasting DHCP requests with spoofed MAC addresses to expend the available address pool, denying access to new users.
- MAC flooding attack: Attacker floods the switch MAC table to push legitimate MAC addresses out of the switch. This causes significant amounts of frames to be broadcasted to all ports.

1.12 Organizations

- Open Web Application Security Project (OWASP): International non-profit organization focused on web application security.
- Federal Risk and Authorization Management Program (FedRAMP): Cloud computing regulatory effort, government-wide, delivers systemized approach to security assessment, authorization, and continuous monitoring of cloud products and services.

1.13 Cloud computing

- Platform as a service (PaaS): Third-party provider delivers hardware and software tools to users over the internet. PaaS frees developers from having to install in-house

hardware and software to develop or run a new application.

- Infrastructure as a Service (IaaS):
- Hardware as a Service (HaaS):
- Software as a Service (SaaS):
- Models:
  - Private
  - Public
  - Community: Infrastructure is shared by several organizations, usually with the same policy and compliance considerations.
  - Hybrid

1.14 Cryptography

- Ciphers
  - Symmetric Ciphers: Single key is used for encryption and decryption
    - Data Encryption Standard (DES): Symmetric-key block cipher with key size of 56-bits
    - Triple Data Encryption Algorithm (3DES, TDES, TDEA): Applies the DES algorithm 3 times to each data block. Key length of $56 \times 3 = 168$ bits when 3 independent keys are used, or 112 when two keys are independent.
  - Asymmetric Ciphers (Public key cryptography): One key can encrypt and one key can decrypt.
    -

1.15 Registers

- EIP - Extended Instruction Pointer stores the address of the next instruction to be executed.
- ESP - Stack pointer, contains the address of the next element to be stored onto the stack.
- EBP - Extended Base pointer (StackBase), contains the address of the bottom (first element) of the stack frame.

- EDI - Destination Index, used with string instruction.
- ESI - Source Index, used with string instruction.