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.
  - AnDOSid: Allows the attacker to simulate a DoS attack (an HTTP POST flood attack) and DDoS attack on a web server from mobile phones.
  - Xplico: extracts application data from captured internet traffic. Is an open source Network Forensic Analysis Tool (NFAT).
  - Akamai: provides DDoS protection for enterprises regularly targeted by DDoS attacks. Akamai Kona Site Defender delivers multi-layerd defense that effectivly protects websites and web applications against the increasing threat, sophistication, and scale of DDoS attacks.
  - Vindicate: A LLMNR/NBNS/mDNS spoofing detection toolkit for network administrators. Security professionals use this tool to detect name service spoofing.

- DNS Poisoning Techniques: sniff DNS traffic of a target network. An attacker can obtain the ID of the DNS request by sniffing and can send a malicious reply to the sender before the actual DNS server.
  - Intranet DNS spoofing: An attacker can perform an intranet DNS spoofing attack on a switched LAN with the help of the ARP poisoning technique. To perform this attack, the attacker must be connected to the LAN and be able to sniff the traffic or packets. An attacker who succeeds in sniffing the ID of the DNS request from the intranet can send a malicious reply to the sender before the actual DNS server.
  - Internet DNS spoofing: Attackers perform Internet DNS spoofing with the help of Trojans when the victim's system connects to the Internet. It is an MITM attack in which the attacker changes the primary DNS entries of the victim's computer.
  - Proxy server DNS poisoning: In the proxy server DNS poisoning technique, the attacker sets up a proxy server on the attacker's system. The attacker also configures a fraudulent DNS and makes its IP address a primary DNS entry in the proxy server.
  - DNS cache poisoning: Attackers target this DNS cache and make changes or add entries to the DNS cache. If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request.

1.9.3 Sniffing Tools and Countermeasures

- Tools
  - Spoof-Me-Now: program to change (spoof) your MAC address.
  - OmniPeek: Network analyzer provides real time visibility and expert analysis of each part of the target network. will analyze, drill down, and fix performance bottlenecks across multiple network segments.
  - DerpNSpoof: DNS poisoning tool that assists in spoofing the DNS query packet of a certian IP address or group of hosts on the network.
  - ike-scan: discovers IKE hosts and can fingerprint them using the retransmission backoff pattern.
  - Nmap: Used to scan networks, has a NSE script that allows you to check if a target on a local Ethernet has its network card in promiscuous mode by doing

the ARP test.

  - FaceNiff: Android app that can sniff and intercept web session profiles over the WiFi connected to the mobile. This app works on rooted Android devices. Whe WiFi connection should be over Open, WEP, WPA-PSK, or WPA2-PSK networks while sniffing the session.

  - shARP: an anti ARP-spoofing application software that uses active and passive scanning methods to detect and remove any ARP-spoofer from the network.

- Sniffing Attacks

  - ARP Spoofing: A method of attacking an Ethernet LAN. When a legitimate user initiates a session with another user in the same layer 2 broadcast domain, the switch broadcasts and ARP request using the recipient's IP address, while the sender waits for the recipient to respond with a MAC address.

  - ARP Poisoning: With the help of ARP poisoning, an attacker can use fake ARP messages to divert all communications between two machines so that all traffic redirects via the attacker's PC.

  - ARP Method: Sends a non-broadcast ARP to all nodes in the network. The node that runs in promiscuous mode on the netwrok will cache the local ARP address. Then it will broadcast a ping message on the network with the local IP address but a different MAC address. In this case, onlt the node that has the MAC address (cached eariler) will be able to respond to your braodcast ping request.

  - Ping method: To detect a sniffer on a network, identify the system on the network running in promiscuous mode. The ping method is useful in detecting a system that runs in promiscuous mode, which in turn helps detect sniffers installed on the network.s

1.10 Social Engineering

1.10.1 Social Engineering Concepts

- Intimidation: refers to an attempt to intimidate a victim into taking several actions by using bullying tactics.

- Scarcity: Implies the state of being scarce. In the context of social engineering, scarcity often implies creating a feeling of urgency in a decision making process.

- Consensus or Social Proof: Refers to the fact that people are usually willing to like

things or do things that other people like or do.

- Authority: Implies the right to exercise power in an organization. Attackers take advantage of this by presenting themselves as a person of authority, such as a technician or an executive.
- Steps of a social engineering attack: Research on target company -¿ selecting target -¿ develop relationship -¿ exploit the relationship.

1.10.2 Social Engineering Techniques

- Pop-Up Windows: windows that suddenly pop up while surfing the Internet and ask for user information to login or sign-in.
- Hoax (Letters): Emails or popups that issue warnings to the user about new viruses, Trojans, or worms that may harm the user's system.
- Instant Chat Messenger: Gathering personal information by chatting with a selected user online to get information such as birth dates and maiden names.
- Chain Letters: A chain letter is a message or email offering free gifts, such as money and software, on the condition that the user forward the email to a predetermined number of recipients.
- Pharming: Also known as "phishing without a lure" and performed by using DNS Cache Poisoning or Host File Modification.
- Whaling: Attacker tries to trick the victim into revealing critical corporate and personal information through email or website spoofing.
- Spimming: SPIM (Spamming over instant messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called a Spimmer. Spimmers generally make use of bots to harvest Instan Messaging IDs and forward spam messgaes to them.
- Spear Phising: Sending a specialized message with social engineering content directed at a specific person, or small group.
- Skimming: refers to stealing credit/debit card number by using special storage devices called scimmers or wedges when processing the card.
- Wardriving: Attackers search for unsecured WiFi networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured netowrks, they access any sensitive information stored on the devices of the users on the networks.

- Pretexting: fraudsters may pose as executives from financial institutions, telephone companiesm and so on who rely on "smooth talking" and win the trust of an individual to reveal sensitive information.
- Pharming: an advanced form of phishing in which attackers modify DNS protocol and redirects the connection between the IP address and its target server.

1.10.3 Insider threats and Identity Theft

- Malicious Insider: Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injectin malware into the corporate network.
- Negligent Insider: Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency are more vulnerable to social engineering attcks. A large number of insider attacks result from employee's laxity towards security measures, policies and practices.
- Professional Insider: The most harmful insiders where they use their technical knowledge to identify weaknesses and vulnerabilities of the company's network and sell the confidential information to the competitors or black market bidders.
- Compromised Insider: An outsider compromises insiders having access to critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.
- Tax Identity Theft: This type of identity theft occurs when perpetrator steals the victim's Social Security Number or SSN in order to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing the legitimate tax refunds and results in a loss of funds.
- Identity cloning and concealment: This is a type of identity theft which encompasses all forms of identity theft where the perpetrators attempt to impersonate someone else in order to simply hide their identity. These perpetrators could be illegal immigrants or those hiding from creditors or simply want to become "anonymous" due to some other reasons.
- Synthetic identity theft: This is one of the most sophisticated types of identity theft where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number or SSN and uses it with a combination of fake names, date of birth, address and other details required for creating new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods and services.

- Social identity theft: This is another most common type of identity theft where the perpetrator steals victim's Social Security Number or SSN in order to derive various benefits

1.10.4 Social Engineering Countermeasures

- Social Engineers Toolkit

1.11 Denial-of-Service

1.11.1 DoS/DDoS Concepts

- DoS attakcs have various forms and target various services. The attacks may cause the following:
  - Consumption of resources
  - consumption of bandwidth, disk space, CPU time, or data structures.
  - Actual physical destruction or alteration of network components
  - Destruction of programming and files in a computer system.

1.11.2 DoS/DDoS Attack Techniques and Tools

- Back chaining Propogation: In this technique, the attacker places an attack toolkit on their own system, and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. The attack tools installed on the attacking machine use some special methods to accept a connection from the compromised system and then transfer a file containing the attack tools to it.
- Autonomous Propagation: In autonomous propagation, the attacking host itself transfers the attack toolkit to a newly discovered vulnerable system, exactly at the time it breaks into that system.
- Central Source Propagation: In this technique, the attacker places an attack toolkit on a central source and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. Once the attacker finds a vulnerable machine, they instruct the central source to transfer a copy of the attack toolkit to the newly compromised machine, on which attack tools are automatically installed under management by a scripting mechanism.
- Spyware Propagation: As its name implies, spyware is installed without user knowledge or consent, and this can be accomplished by "piggybacking" the spyware onto other

applications.

- Tools:
  - CORE Impact: Finds vulnerabilities in an organization's web server. This tool allows a user to evaluate the security posture of a web server by using the same techniques currently employed by cyber criminals.
  - HULK: Denial of Service tool used to attack web servers by generating unique and obfuscated traffic volumes and its generated traffic also bypasses caching engines and hits the server's direct resource pool.
  - Pupy: cross platform, muli function RAT and post-exploitation tool used for executing applications remotely.
  - NetVisor: Desktop and child monitoring spyware that comes with an unparalleled task recording feature set that in secret records everything employees do on your network.
  - Fritzing: assists attackers in designing electronic diagrams and circuits.
  - Stormwall PRO: Filtering mitigation of all existing types of DDoS attacks on network, transport and session layers as well as application layer for HTTP(S)/Websocket traffic.
  - Suphacap: a Z-Wave sniffer, is a hardware tool used to sniff traffic generated by smart devices connected in the network. It allows attackers to perform real-time monitoring and capturing of packets from all Z-Wave networks.
  - KillerBee: Python based framework and tool set for exploring and exploiting the security of ZigBee and IEEE 802.15.4 netowrk.
- Application-level flood attacks result in the loss of services of a particular network resource. Examples include email, network resources, temporary ceasing of applications and services, and so on. By using this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests. In this type of attack, an attacker tries to exploit the vulnerabilities in application layer protocol or in the application itself to prevent the access of the application to the legitimate user.
  - Flood web applications to legitimate user traffic (GET/POST)
  - Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts.

  - Jam the application database connectino by crafting malicious SQL queries.
  - Slowloris
  - OS Vulnerabilities.

- Protocol Attack: includes SYN floods, fragmented packets, ping of death, smurf DDos, teardrop, land, and other attacks.
- Volume-based attack: UDP floods, ICMP floods, and other spoofed packet floods.

1.11.3 DoS/DDoS Protection Tools and Countermeasures

- Activity profiling: Performed based on the average packet flow rate for network flow, which consists of consecutive packets with similar packt header information.
- Wavelet-Based Signal Analysis: The wavelet analysis technique analyzes network traffic in terms of spectral components. it divides incoming signals into various frequencies and analyzes different frequency components separately.
- Sequential Change-Point Detection: Change-Point detection algorithms isolate changes in network traffic statistics and in the traffic flow rate caused by attacks. Uses cumulative sum algorithms.
- Absorbing the attack: Is a DoS/DDoS countermeasure strategy, in which additional capacity is used to absorb an attack, which requires preplanning and additional resources.
- Cisco IPS Source and reputation filtering: reputation services help in determining if an IP or service is a source of threat.
- Black Hole Filtering: refers to discarded packets at the routing level.
- RFC 3704 Filtering: a basic access control list (ACL) filter, which limits the impact of DDoS attacks by blocking traffic with spoofed addresses.
- DDoS Prevention Offering from ISP or DDoS service: Enable IP Source Gurad (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, preventing a bot from succeeding with spoofed packets.
- Ingress Filtering protects against flooding attacks that originate from valid prefixes (IP addresses).
- Egress filtering scans the headers of IP packets going out of the network.

- TCP intercept: In this mode the router intercepts the SYN packets sent by the clients to the server and matches with an extended access list. If there is a match, then on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software also setablishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept software combines them transparently. Prevents the attempts of fake connection from reaching the server. Acts as a mediator between the server and the client throughout the connection.
- MAC address filtering allows you to define a list of devices and only allows those devices on your network.
- Tools
  - DDoS-Guard: online service to protect against DDoS
  - A10 Thunder TPS: an Appliance that ensures reliable access to key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages.
  - Imperva Incapsula DDoS protection: Quickly miticgates attacks of any size without affecting legitimate traffic or increasing latency.

1.12 Session Hijacking

1.12.1 Session Hijacking Concepts

-

1.12.2 Application Level Session Hijacking

”

- Man in the Middle Attack: A MITM attack is used to intrude into an exiting connection between systems and to intercept messages being transmitted. In this attack, attacks use different techniques and split a TCP connectin into two: client-to-attacker and attacker-to-server connections.
- Fragmentation Attack: These attacks destroy a victim's ability to reassemble fragmented packets by flooding it with TCP or UDP fragments, resulting in reduced performance. The attacker sends a large number of fragmented (1500+ byte) packets to a target web server with a relatively small packet rate.
- Man in the Browser Attack: Similar to a MITM attack. The difference between the

two is that a MITB attack uses a Trojan horse to intercept and mainpulate calls between a browser and its security mechanisms or libraries. An attack positions a previously installed Trojan between the browser and its security mechanism, and the Trojan can modify web pages and transaction content or insert additional transactions. All of the Trojan's activities are invisible to both the user and the web application.

- Client-side Attack: Target vulnerabilities in client applications that interact with a malicious server or process malicious data. Depending on the nature of vulnerabilities, an attacker can exploit an application by sending an email with a malicious ling or otherwise tricking a user into visiting a malicious website.

- XXS: enables attackers to inject malicious client-side scripts into web pages viewed by other users.

- Trojans: can change the proxy settings in the user's browser to send all sessions through an attacker's machine.

- Malicious JavaScript Codes: An attacker can embed in a web page a malicious script that does not generate any warning but captures session tokens in the background and sends them to the attacker.

- Session donation Attack: An attacker donates his/her own session identifier (SID) to the target user. The attacker first obtains a valid SID by logging into a service and later feeds the same SID to the target user. This SID links a target user back to the attacker's account page without any information to the victim.

- Proxy servers: An attacker lures the victim to click on a bogus link, which looks legitimate but redirects the user to the attackers server. The attacker forwards the request to the legitimate server on behalf of the victim and servers as a proxy for the entire transaction. The attacker then captures the session's information during the interaction of the legitimate server and user.

- CRIME Atatck: Compression Ratio Info-Leak Made Easy (CRIME) is a client side attack that exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS. Attackers hijack the session by decrypting secret session cookies. The authentication information obtained from the session cookies is used to establish a new session with the web application.

- Forbidden attack: Type of MITM used to hijack HTTPS sessions. It exploits the reuse of cryptographic nonce during the TLS handshake. After hijacking the GTTPS session, the attacker inject malicious code and forged content that prompts the victim to disclose sensitive information, such as bank account numbers,

passwords, and social security numbers.

- Session replay attack: An attacker captures the authentication token of a user by listening to a conversation between the user and the server and reiterates the authentication request to the server with the captured authentication token to gain unauthorized access to the server.

- Application Level Hijacking: gaining control over HTTP's user session by obtaining the session IDs.

- Network Level hijacking: interception of packets during transmission in a TCP and UDP session between a server and client communication. attacks transport an internet level protocols

1.12.3 Network Level Session Hijacking

- IP Spoofing: Source routed packets: useful in gaining unauthorized access to a computer with the help of a truseted host's IP address. This type of hijacking allows attackers to create their own acceptable packets to insert into the TCP session. First, the attacker spoofs the trusted host's IP address so that the server managing a session with the host accepts the packets from the attacker. The packets are source routed, so the sender specifies the path for packets from the source to the destination IP. Using this source-routing technique, attackers can fool the server into thinking that it is communicating with the user.

- Blind Hijacking: A hacker can inject malicious data or commands into the intercepted communications in a TCP session, even if the victim disables source routing. Here, an attacker correctly guesses the next ISN of a computer attempting to establish a connection; the attacker sends malicious data or a command, such as password setting to allow access from another location on the network, but the attacker can never see the response. To be able to see the response, a MITM attack works much better.

- TCP/IP hijacking: an attacker intercepts an established connection between two communicating parties using spoofed packets, and then pretends to be one of them. In this approach, the attacker uses spoofed packets to redirect the TCP traffic to his/her own machine. Once this is successful, the victim's connection hangs and the attacker is able to communicate with the host's machine on behalf of the victim.

- UDP hijacking

- RST Hijacking

1.12.4 Session Hijacking Tools

- Burp Suite: inspect and modify traffic between
- Vega: a free and open-source web security scanner and web security testing platform for testing the security of web applications. Vega helps you to find and validate SQL injection, XXS, inadvertently disclosed sensitive information and other vulnerabilities.
- PortQry: Reports the port status of TCP and UDP ports on a selected target. Attackers can use PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.
- DroidSheep: Used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the WiFi network and uses it to access a website as an authorized user. A DroidSheep user can easily observe the activities of authorized users on websites. It can also hijack social accounts by obtaining the session ID.
- ShellPhish: A phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkdIn. Also displays to victim system's public IP address, browser information, hostname, geolocation, and other information.
- Netcraft: The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Toolbar provides updated information about sites that users visit regularly and blocks dangerous sites
- OhPhish: OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees Apility.io: Apility.io is an anti-abuse API that helps security professionals to know if the IP address, domain, or email of a user is blacklisted. It is a collection of various tools delivered "as a service" to help security professionals, product managers, IT shops, enterprises, and start-ups to acquire more details about their potential visitors, users, customers, and threat actors.
- FaceNiff: FaceNiff is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user's mobile device is connected to. Although FaceNiff can hijack sessions only when the WiFi network does not use the Extensible Authentication Protocol (EAP), it works on any private network, including open, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-pre-shared

key (WPA-PSK), and WPA2-PSK networks.

- sslstrip: Sslstrip tool is exploiting user behavior and if a user does not type https:// in front of the link, and the website has redirection from HTTP to HTTPS, it will intercept HTTP 302 redirection and send the user exactly what the user asked for, i.e. HTTPsite

1.12.5 Session Hijacking Countermeasures

- Tools:
  - AlienVault USM
  - Fiddler: Used for security testing of web applications such as decrypting HTTPS traffic, and manipulating requests using man-in-th-middle decrpytion technique.
  - BetterCAP: ARP poisoning
  - MITMf: ARP poisoning
  - Cain an Abel: ARP poisoning.
- IPsec: used to secure VPN sessions
- IPsec Components:
  - IPsec Driver: Software that performs protocol-level functions required to encrypt and decrypt packets.
  - Internet Key Exchange (IKE): A protocol that produces security keys for IPsec and other protocols.
  - Internet Security Association and Key Management Protocol (ISAKMP): Software that allows two computers to communicate by encrypting the data exchanged between them.
  - Oakley: A protocol that uses Diffie-Hellman algorithm to create a master key and a key that is specific to each session in IPsec data transfer.
  - IPsec Policy Agent:
- IPsec architecture:
  - Authentication Header (AH): Offers integrity and data origin authentication, with optional anti-replay featues.

  - Encapsulating Security payload (ESP): Offers all the services offered by AH as well as confidentiality.
  - IPsec Domain of Interpretation (DOI): Defines the payload formats, types of exchange, and naming conventions for security information such as cryptographic algorithms or security policies. IPsec DOI instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.
  - IPsec Policies: useful in providing network security. Defines when and how to secure data, as well as security methods to use at different levels in the network. One can configure IPsec policies to meet the security requirements of a system, domain, site, organizational unit and so on.

- HTTP Strict Transport Security (HSTS): a web security policy that protects HTTPS websites against MITM attacks. The HSTS policy helps web servers force web browsers to interact with them using HTTPS. With the HSTS policy, all insecure HTTP connections are automatically converted into HTTPS connections. This policy ensures that all the communication between a web server and a web browser is encrypted and that all responses that are delivered and recieved originate from an authenticated server.

- HTTP Public Key Pinning (HPKP): A trust on first use (TOFU) technique used in an HTTP header that allows a web client to associate a specific public key certificate with a prticular server to minimize the risk of MITM attacks based on fraudulent certificates. In TLS sessions, to verify the authenticity of a servers public key, the public key is enclosed in an X.509 digital certificate, which is signed by a certificate authority (CA).

- WEP/WPA Encryption: Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) are wireless protocols that are intended to protect the traffic that is sent and received by users over a wireless network. The implementation of these protocols can thwart the attempts of unwanted users to connect to the network. A weak encryption mechanism enables attackers to brute force credentials and enter the target network to perform an MITM attack.

- Token Binding: When a user logs into a web application, a cookie with a session ID, called a token, is generated. The user utilizes this random token to send requests to the server and access resources. An attacker can impersonate the user and hijack the connection by capturing and reusing a valid session ID. Token binding protects client-server communication against session hijacking attacks. The client creates a public-private key pair for every connection to a remote server.

1.13 Evading IDS, Firewalls, and Honeypots

1.13.1 IDS, IPS, Firewall and Honeypot Concepts

- Signature Recognition: also known as misuse detection, tries to identify events that indicate an abuse of a system or network resource. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision.

- Protocol Anomaly Detection: Protocol anomaly detection depends on the anomalies specific to a protocol. It identifies particular flaws between how vendors deploy the TCP/IP protocol. Protocols designs according to RFC specifications, which dictate standard handshakes to permit universal communication. The protocol anomaly detector can identify new attacks.

- Anomaly Detection: Anomaly detection, or "not-use detection," differs from the signature-recognition model. Anomaly detection consists of a database of anomalies. An anomaly can be detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system. Creating a model of normal use is the most challenging task in creating an anomaly detector.

- Obfuscating: Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using the Unicode character, an attacker could encode attack packets that the IDS would not recognize, but an IIS web server would decode.

- Bastion Host: The bastion host is designed for defending the network against attacks. It acts as a mediator between inside and outside networks. A bastion host is a computer system designed and configured to protect network resources from attacks. Traffic entering or leaving the network passes through the firewall

- File System Intrusion: By observing system files, the presence of an intrusion can be identified. System files record the activities of the system.

  - If you find new, unknown files / programs on youe system. Unexplained modification in file size are also an indication of an attack.

  - You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.

  - Missing files are also a sign of a probable intrusion/attack.

- Network Intrusions: general indications of network intrusions include the following
  - A sudden increas in bandwidth consumption
  - repeated probes of the available services on your machine.
  - connection requests from IPs other than those in the network range, which imply that an unauthorized user (intruder) is attempting to connect to the network.
  - Repeated login attempts from remote hosts.
  - A sudden influx of log data, which could indicate attempts at DoS attakcs, bandwidth consumption, and DDoS attacks.
- System Intrusions:
  - sudden changes in logs such as short or incomplete logs.
  - Unusually slow system performance.
  - Missing logs or logs with incorrect permissions or ownership.
  - Unusual graphic displays or text messages.
  - Gaps in system accounting.
- Signature recognition: is an IDS intrusion detection method, also known as misuse detection, tries to identify events that indicate an abuse of a system or network resource.
- Honeynet: Very effective in determining the entire capabilities of adversaries and is mostly deployed in an isolated virutal environment along with a combination of vulnerable servers?
- Packet information:
  - Direction: Used to check whether the packet is entering or leaving the private network.
  - Interface: Used to check whether the packet is coming from an unreliable zone.
  - TCP flag bits: Used to check whether the packet has SYN, ACK, or other bits set for the connection to be made.

  - Source IP address: Userd to check whether the packet is coming from a valid source. The information about the source IP address can be found from the IP header of the packet.

- Circuit-level gateway firewall: The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model

- Stateful Multilayer Instection firewall: They filter packets at the network layer, to determine whether session packets are legitimate, and evaluate the contents of packets at the application layer. With the use of stateful packet filtering, you can overcome the limitation of packet firewalls that can only filter on IP address, port, protocol, and so on. This multilayer firewall can perform deep packet inspection.

- Application-level Firewall: Application-based proxy firewalls concentrate on the application layer rather than just the packets. The need for application-level firewall arises when huge amount of voice, video, and collaborative traffic are accessed at data-link layer and network layer utilized for unauthorized access to internal and external networks. Useful to filter specific commands such as `http:post`

- Packet filtering firewall: A packet filtering firewall investigates each individual packet passing through it and makes a decision whether to pass the packet or drop it. It works at the Internet protocol (IP) layer of the TCP/IP model. Packet filter–based firewalls concentrate on individual packets, analyze their header information, and determine which way they need to be directed.

-

1.13.2 IDS, IPS, Firewall, and Honeypot Solutions

- Wifiphisher: A rouge AP framework for conducting Red Team Engagements or WiFi security testing. Using Wifiphisher, penetration testers can easily achieve an MITM position against wireless clients by performing targeted WiFi association attacks.

- Reaver: designed to be a robust and practical tool against WiFi Protected Setup (WPS) registrar PINs in roder to recover WPA/WPA2 passphrases, and it has been tested against a wide variety of APs and WPS implementations.

- Wifi Inspector: Allows you to find all the devices connected to the network (via both wired and WiFi connections, including consoles, TVs, PCs, tablets, and phones); it gives relevant data such as the IP addresses, manufacturer names, and MAC addresses of connected devices. It also allows you to save a list of known devices with a custom name and finds intruders in a short period.

- WIBR+: application for testing the security of WPA/WPA2 PSK WiFi networks. It discovers weak passwords. WIBR+ supports queuing, custom dictionaries, a brute-force generator, and advanced monitoring.
- NetPatch firewall is a full-featured advanced android noroot firewall. It can be used to fully control over mobile device network. With NetPatch firewall, you can create network rules based on APP, IP address, domain name, and so on. This firewall is designed to save mobile device's network traffic and battery consumption, and improve network security and protect privacy.
- Comodo Firewall
- Glasswire
- TinyWall
- PeerBlock
- SPECTER: SPECTER is a honeypot. It automatically investigates attackers while they are still trying to break in. It provides massive amounts of decoy content, and it generates decoy programs that cannot leave hidden marks on the attacker's computer. Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to change regularly without user interaction.
- Vanguard Enforcer:
- zIPS:
- ZoneAlarm PRO FIREWALL 2019: ZoneAlarm PRO Firewall blocks attackers and intruders from accessing your system. It monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection. It prevents identity theft by guarding your data. It even erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Also, it filters out an annoying and potentially dangerous email.

1.13.3 Evading IDS

- Invalid RST Packets: The TCP uses 16-bit checksums for error checking of the header and data and to ensure that communication is reliable. It adds a checksum to every transmitted segment that is checked at the receiving end. When a checksum differs from the checksum expected by the receiving host, the TCP drops the packet at the receiver's end. The TCP also uses an RST packet to end two-way

communications. Attackers can use this feature to elude detection by sending RST packets with an invalid checksum.

- Fragmentation attack: Fragmentation can be used as an attack vector when fragmentation timeouts vary between the IDS and the host. Through the process of fragmenting and reassembling, attackers can send malicious packets over the network to exploit and attack systems.

- Obfuscating: It is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode

- Insertion Attack: Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets (i.e., the system may not accept the packet addressed to it). An IDS blindly trusts and accepts a packet that an end system rejects. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. If the IDS reads an invalid packet, it gets confused. An attacker exploits this condition and inserts data into the IDS.

- Flooding: an IDS evasion technique used by an attacker to send a huge amount of unnecessary traffic to produce noise or fake traffic. If the IDS does not analyze the noise traffic, the true attack traffic goes undetected.

- Overlapping fragments:

- Encryption:

- Polymorphic shellcode: an attacker use an existing buffer-overflow exploit and set the "return" memory address on the overflowed stack to the entrance point of the decryption code.

- Session Splicing: Attacker splits the attack traffic into an excessive number of packets sudh that no single packet triggers the IDS.

1.13.4 Evading Firewalls

- Firewalking is a method of collecting information about remote netowrks behind firewalls. It is a technique that uses TTL values to determine gateway ACL filters and map networks by analyzing the IP packet response.

- Banner Grabbing: A simple method of fingerprinting that helps in detecting the vendor of a firewall and the firmware version. It identifies the service running on

the system. Attackers use banner grabbing to fingerprint services and thus discover the services running on firewall.

- IP address spoofing: a hijacking technique in which an attacker masquerades as a trusted host to conceal his identity, spoof a website, hijack browsers, or gain unauthorized access to a network. In IP spoofing, the attacker creates IP packets by using a forged IP address and gains access to the system or network without authorization.

- Tiny fragments: Attackers create tiny fragments of outgoing packets, forcing some of the TCP packet's header information to go into the next fragment. The IDS filter rules that specify patterns will not match with the fragmented packets owing to the broken header information. The attack will succeed if the filtering router examines

- ACK Tunneling method: Allows tunneling a backdoor application with TCP packets with the ACK bit set. The ACK bit is used to acknowledge the reciept of a packet. Some firewalls do not check packets with the ACK bit set because ACK bits are supposed to be used in response to legitimate traffic.

- source routing: using this technique, the sender of the packet designates the route (partially or entirely) that a packet should take through the network such that the designated route should bypass the firewall node. Thus the attack can evade firewall restrictions.

- Anonymizer: Anonymizer's VPN routes all traffic through an encrypted tunnel directly from your laptop to secure and harden servers and networks. It then masks the real IP address to ensure complete and continuous anonymity for all online activities.

1.13.5 Honeypot, IDS, and Firewall Evasion Countermeasures

-

1.14 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.

1.15 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.

1.16 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.

1.17 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

1.18 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.
    -

1.19 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.