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

1.6.2 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.
-

1.6.3 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.

1.6.4 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.

1.6.5 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`

1.7 Malware Threats

1.7.1 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.

1.7.2 APT Concepts

-

1.7.3 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

1.7.4 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.

1.7.5 Fileless Malware Concepts

-

1.7.6 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.

1.7.7 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.

1.8 Sniffing

1.8.1 Sniffing Concepts

-

1.8.2 Sniffing Techniques

- Tools
  - Nikto: A web server and web application 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.

1.8.3 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

1.9 Social Engineering

1.9.1 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.

1.9.2 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.

1.9.3 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

1.9.4 Social Engineering Countermeasures

- Social Engineers Toolkit

1.10 Denial-of-Service

1.10.1 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.

1.10.2 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.

1.10.3 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.

1.11 Session Hijacking

1.11.1 Session Hijacking Concepts

-

1.11.2 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

1.11.3 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

1.11.4 Session Hijacking Tools

- Burp Suite: Burp Suite is a web security testing tool that can hijack session IDs in established sessions. The Sequencer tool in Burp Suite tests the randomness of session tokens. With this tool, an attacker can predict the next possible session ID token and use that to take over a valid session

- 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: Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning. They also analyze the market share of web servers, operating systems, hosting providers and SSL certificate authorities, and other parameters of the Internet. 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

1.11.5 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.

1.12 Evading IDS, Firewalls, and Honeypots

1.12.1 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.
-

1.12.2 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: Zimperium's zIPS™ is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks.
- 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.

1.12.3 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.

1.12.4 Evading Firewalls

- Tools
  - Snort: Snort is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.
  - Suricata: Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing.
  - Bitvise: Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers by encrypting data during transmission. It is ideal for remote administration of Windows servers, for advanced users who wish to access their home machine from work or their work machine from home, and for a wide spectrum of advanced tasks, such as establishing a VPN using the SSH TCP/IP tunneling feature or providing a secure file depository using SFTP.
  - HTTPTunnel: Uses technique of tunneling traffic across TCP port 80 to bypass firewall.
  - Loki: ICMP tunneling is used to execute commands of choice by tunneling them inside the payload of ICMP echo packets.
  - AckCmd: (http://ntsecurity.nu) use ACK tunneling
  - Super Network Tunnel: a two-way HTTP tunneling software that connects two computers utilizeing HTTP-tunnel client and HTTP-tunnel server. It can bypass any firewall to surf the web, use IM applications, games, and so on. Super network tunnel integrates SocksCap function along with bidirectional HTTP tunneling and remote control to simplify the configuration.
  - SecurePipes: SSH tunneling tool
  - Traffic IQ Professional: Traffic IQ Professional is a tool that audits and validates the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines. This tool is generally used by security personnel for assessing, auditing, and testing the behavioral

characteristics of any non-proxy packet-filtering device, which can include application firewalls, IDS, IPS, routers, switches, etc. However, as this tool can generate custom attack traffic, it is extensively employed by attackers to bypass the installed perimeter devices in the target network.

  - Colasoft Packet Builder: Colasoft Packet Builder: Colasoft Packet Builder is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them such that firewalls cannot detect them. They can create custom network packets such as Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet. Security professionals use this tool to check your network's protection against attacks and intruders.

- 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.

1.12.5 Honeypot, IDS, and Firewall Evasion Countermeasures

- Tools:
  - Sebek: catches read() system calls.

1.13 Hacking Web Servers

1.13.1 Web Server Concepts

- Document Root: The document root is one of the root file directories of the web server that stores critical HTML files related to the web pages of a domain name, which will be sent in response to requests.
- Server Root: It is the top-level root directory under the directory tree in which the server's configuration and error, executable, and log files are stored.
- Virtual Hosting: It is a technique of hosting multiple domains or websites on the same server. This technique allows the sharing of resources among various servers.
-
- Virtual Document Tree: A virtual document tree provides storage on a different machine or disk after the original disk becomes full.
- Data Tampering: alters or deletes the data of a web server and replaces the data with malware.
- Web Proxy: A proxy server is located between the web client and web server. Owing to the placement of web proxies, all requests from clients are passed on to the web server through the web proxies. They are used to prevent IP blocking and maintain anonymity
- PHP: application layer and is used to generate dynamic web content.

1.13.2 Web Server Attacks

- Session hijacking attacks:

  - Session fixation
  - Session sidejacking
  - Cross-site scripting
- DNS Hijacking: malicious attack that modifies or overrides a systems TCP/IP settings to redirect it at a rouge DNS server, thereby invalidating the default DNS settings.

1.13.3 Web Server Attack Methodology

- Tools:
  - NCollector Studio: a website mirroring tool used to download content from the web to a local computer. This tool enables users to crawl for specific file types, make any website available for offline browsing, or simply download a website to a local computer.
  - ID Server: A simple internet server identification utility also performs HTTP Server Identification, Non-HTTP Server Identification and Reverse DNS lookup.
  - Open Sez Me: A lookup database for default passwords, credentials and ports.
  - HTTrack: HTTrack is an offline browser utility that is capable of performing website mirroring by downloading a website from the Internet to a local directory, building all the directories recursively, and getting HTML, images, and other files from the server.
  - Nessus: Vulnerability scanner
  - Hydra: Password Cracker

1.13.4 Web Server Attack Countermeasures

- Tools:
  -
  - Mimikatz: Allows attackers to pass Kerberos TGT to other computer and sign in using the victim's ticket. The tool also helps in extracting paintext passwords, hashes, PIN codes, and Kerberos tickets from memory.
  - N-Stalker: N-Stalker is a web application security scanner that searches for vulnerabilities to attacks such as clickjacking, SQL injection, and XSS. It allows spider crawling throughout the application and the creation of web

macros for form authentication. It also provides proxy capabilities for "drive-thru" attacks and identifies components through reverse proxies that distribute different platforms in the same application URL.

  - Immunity Debugger: tool used to write exploits, analyze malware, and reverse engineer binary files.
  - Fortify WebInspect: Webserver security tools
  - Retina CS: Webserver security Tool
  - NetIQ secure configuration manager: Webserver security tool.

1.13.5 Patch Management

- Tools:
  -

1.14 Web Applications

1.14.1 Web App Concepts

- Web Application Layers:
  - Client/Presentation Layer: includes all physical devices present on the client side, such as laptops, smartphones, and computers. These devices feature operating systems and compatible browsers, which enable users to send requests for required web applications. The user requests a website by entering a URL in the browser, and the request travels to the web server. The web server then responds to the request and fetches the requested data; the application finally displays this response in the browser in the form of a web page.
  - Business Logic Layer: consists of two layers: the web-server logic layer and the business logic layer. The business logic layer includes the functional logic of the web application, which is implemented using technologies such as .NET, Java, and "middleware". It defines the flow of data, according to which the developer builds the application using programming languages. It stores the application data and integrates legacy applications with the latest functionality of the application.
  - Web-Server Logic Layer: contains various components such as a firewall, an HTTP request parser, a proxy caching server, an authentication and login handler, a resource handler, and a hardware component, e.g., a server. The

firewall offers security to the content, the HTTP request parser handles requests coming from clients and forwards responses to them, and the resource handler is capable of handling multiple requests simultaneously.

  - Database Layer: consists of cloud services, a B2B layer that holds all the commercial transactions, and a database server that supplies an organization's production data in a structured form (e.g., MS SQL Server, MySQL server).

- SOAP Messages: Simple Object Access Protocol. Application communication protocol. Format for sending and recieving messages. Platform independent, based on XML.

- UDDI: Universal Description, Discovery, and Integration (UDDI) is a directory service that lists all the services available.

- WSDL: Web Services Description Language is an XML-based language that describes and traces web services.

- WS-Security: Web Services Security (WS-Security) plays an important role in securing web services. It is an extension of SOAP and aims to maintain the integrity and confidentiality of SOAP messages as well as to authenticate users.

- WS-Policy: WS-Policy is a specification that allows web services to use XML to advertise their policies (on security, quality of service, etc.) and for web service consumers to specify their policy requirements.

- Publish: During this operation, service descriptions are published to allow the requester to discover the services.

- Bind: During this operation, the requester calls and establishes communication with the services during run time, using binding data inside the service descriptions to locate and invoke the services.

- Find: During this operation, the requester tries to obtain the service descriptions. This operation can be processed in two different phases: obtaining the service interface description at development time and obtain the binding and location description calls at run time.

- Service: It is a software module offered by the service provider over the Internet. It communicates with the requesters. At times, it can also serve as a requester, invoking other services in its implementation

1.14.2 Web App Threats

- SQL injection: injection of malicious SQL queries into user input forms.
- LDAP injection involves the injection of malicious LDAP statements.
- Shell injection: the attacker tries to craft an input string to gain shell access to a web server.
- Command Injection: injection of malicious HTML code or command through a web application. In command injection attacks, a hacker alters the content of the web page by using HTML code and by identifying the form fields that lack valid constraints.
- Cross-Site Scripting: In cross-site scripting, attackers bypass client-ID security mechanisms and gain access privileges, and then inject malicious scripts into specific webpages. These malicious scripts can even rewrite HTML website content.
- Sensitive data exposure: caused by flaws in insecure cryptographic storage and information leakage
- Clickjacking:
  - Complete Transparent overlay: In this technique, the trasnparent, legitimate page or tool page is overlaid on the previously designed malicious page. Then, it is loaded into an invisible iframe and the higher z-index is assigned for positioning it on top.
  - Hidden Overlay: Attacker creates an iframe of 1x1 pixels contianing malicious content placed secretly under the mouse cursor. When the user clicks on this cursor, it will be registered on the malicious page although the malicious content is concealed by the cursor.
  - Click Event Dropping: Can completely hide a malicious page behind a legitimate page. It can also be used to set the CSS pointer-events proptery of the top to none. This can cause click events to "drop" through the legitimate masked page and registers only the malicious page.
  - Rapid Content Replacement: In this technique, the targeted controls are covered by opaque overlays that are removed only for a moment for registering a click. An attacker using this technique needs to accurately predict the time taken by the victim to click on the web page.
  - Cropping: Only the selected controls from the transparent page are overlaid. This technique depends on the goal of the attack and may involve masking

buttons with hyperlinks and text labels with false information, changing the button labels with wrong commands, and completely covering the legitimate page with misleading information while exposing only one original button.

- Timing Attacks:
  - Direct Timing Attack: Carried out by measureing the appoximate time taken by the server to process a POST request to deduce the existence of a username.
  - Cross-site Timing Attack: Attackers send crafted request packets to the website using JavaScript.
  - Browser-Based Timing Attack: Attackers take advantage of side-channel leaks of browser to estimate the time taken by the browser to process the requested resources. Attackers can abuse different browser functionalities to launch further attacks such as video parsing attacks and chace storage timing attacks.
  - Cache Storage Timing Attack: The cache API interface (used to load, fetch, and delete any responses) offers complete cache (memory) to the developers. Loading resources in the disk takes some amount of time based on the resource size. If attackers can estimate the time taken by the browser to perform this task, then can measure the corresponding response size.

1.14.3 Web App Hacking Methodology

- Tools:
  - Halberd: Halberd can identify the real IP address of load balancers. When organizations implement load balancers, their real IP address is hidden behind a virtual IP address.
  - WAFW00F: Allows one to identify and fingerprint WAFs protecting a website.
  - Professional Toolset: A DNS interrogation tool that provides information about the locations and types of servers.
- Evade XSS filters: Allows an attacker to inject unusual characters into HTML code to bypass client-side controls.
- Verbose Failure Message: In a typical login system, the user enters two fields, namely username and password. In some cases, an application will ask for additional information. If the user is trying to log in and fails, it implies that at least one field was incorrect. This provides grounds for an attacker to exploit the application.

- Cookie Poisoning: It is a type of parameter tampering attack in which the attacker modifies the cookie contents to draw unauthorized information about a user and thus perform identity theft.
- Bypass SAML-based SSO: Attackers take advantage of signature misconfigurations, session expiry timeouts, session replays, misdirected SAML messages, etc., to bypass SAML-based SSO authentication.
- Local File Inclusion: LFI vulnerabilities enable attackers to add their own files on a server via a web browser. An LFI vulnerability occurs when an application adds files without proper validation of inputs, thereby enabling the attacker to modify the input and embed path traversal characters
- File Fingerprinting: File fingerprinting is a process of computing the hash value for a given binary code to identify and track data across a network.
- Security Misconfiguration: By exploiting misconfiguration vulnerabilities like unvalidated inputs, parameter/form tampering, improper error handling, insufficient transport layer protection, etc., attackers gain unauthorized access to default accounts, can read unused pages, can read/write unprotected files and directories, etc.
- Hash Stealing: Replaces the value of the Data Source parameter with that of a Rogue Microsoft SQL Server and sets the values of username, data source, and integrated security.
- Port Scanning: Try to connect to different ports by changing the value and seeing the error messages obtained.
- Hijacking Web Credentials: Try to connect to the database using the web application system account instead of a user-provided set of credentials.
- Connection Pool DoS: Attackers examine the connection pooling settings of the target application, construct a large malicious SQL query, and run multiple queries simultaneously to consume all the connections in the connection pool, causing database queries to fail for legitimate users.
- Request Forgery Attack: In a request forgery attack, attackers exploit the trust of a website or web application on a user's browser. The attack works by including a link on a page, which takes the user to an authenticated website.
- Frame Injection: When scripts do not validate their input, attackers inject code through frames. This affects all the browsers and scripts that do not validate untrusted input. These vulnerabilities occur in HTML pages with frames. Another reason for this vulnerability is that web browsers support frame editing.

- Session Fixation: Session fixation helps attackers hijack valid user sessions. They authenticate themselves using a known session ID and then use the known session ID to hijack a user-validated session. Thus, attackers trick users and access a genuine web server using an existing session ID value.
- ActiveX Attacks: Attackers lure victims via email or via a link that is constructed such that the loopholes of remote execution code become accessible, allowing the attackers to obtain access privileges equal to those of authorized users.
- Session prediction: It focuses on predicting session ID values that allow the attacker to bypass the authentication mechanism of an application. By analyzing and understanding the session ID generation process, the attacker can predict a valid session ID value and gain access to the application.
- Session brute-forcing: An attacker brute-forces the session ID of a target user and uses it to log in as a legitimate user and gain access to the application.
- Session poisoning: It allows an attacker to inject malicious content, modify the user's online experience, and obtain unauthorized information.
- Cross-Site Request Forgery: Cross-site request forgery (CSRF), also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page.
- Burp Suite built-in tools:
  - Intercepting proxy for inspecting and modifying traffic between your browser and the target application.
  - Application-aware spider for crawling content and functionality.
  - Sequencer tool for testing the randomness of session tokens.
  - Intruder tool for performing customized attacks to find and exploit unusual vulnerabilities.
- Connection String Parameter Pollution (CSPP) specifically exploits the semicolon delimited database connection strings that are constructed dynamically based on the user inputs from web applications. So, injecting parameters into a connection string using semicolons as a separator is performed for a CSPP attack.

1.14.4 Web API, Webhooks and Web Shell

- Web Service APIs

- SOAP API: SOAP is a web-based communication protocol that enables interactions between applications running on different platforms such as Windows, macOS, Linux, etc., via XML and HTTP. SOAP-based APIs are programmed to generate, recover, modify, and erase different logs such as profiles, credentials, and business leads.
- RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application.
  Features:
  - Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance
  - Uniform Interface: Resources must be specifically and independently recognized via a single URL by employing basic protocol methods such as PUT, POST, GET, and DELETE, and it should be possible to modify a resource
  - Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing
  - Code on Demand: An optional feature where the server can also provide temporary executable code to the client, through which the client's functionality can be customized
- XML-RPC: Extensible Markup Language - Remote Procedure Call (XML-RPC) is a communication protocol that uses a specific XML format to transfer data, whereas SOAP uses proprietary XML to transfer data. It is simpler than SOAP and uses less bandwidth to transfer data.
- JSON-RPC: JavaScript Object Notation - Remote Procedure Call (JSON-RPC) is a communication protocol that serves in the same way as XML-RPC but uses the JSON format instead of XML to transfer data.
- Webhooks: Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as receiving a comment on a post or pushing code to the registry. Webhooks allow applications to update other applications with the latest information

- Parameters

  - response_type: Code used for informing the server which permissions to execute.
  - redirect_uri: URI where the authorization server redirects the user agent when the authorization code is provided.
  - scope: Defines the level of access to the application
  - State: Opaque value used for security implementations. The value is also used for maintinaing the state between requests and callback.
  -

- CSRF on Authorization Response: The attacker performs a CSRF attack to connect a face account on the provider with the victim's account on the client side. This attack exploits a third request related to authorization code grant.
- Attack on 'redirect_uri': While registering, the domain is usually specified by the client and only those "redirect_uri" on the specific domain are permitted. If an attacker can identify vulnerabilities such as XSS on a web page on the client domain, he/she can exploit them to capture authorization code.
- Attack on 'Connect' request: Most sites enable users to access other websites such as LinkdIn, Instagram, and Twitter, via OAuth. An attacker can exploit requests to connect one site to another, i.e., when the user hits the "login with or Connect" button. Then, he or she can gain illegal access to the client-side user/victims account by connecting his/her account to the provider's website.
- Access Token Reusage: OAuth requires access tokens for individual clients. It ensures that these tokens saved on the authorization server are mapped to relevant scopes and time expiry. Access token provided for "clientA" can work for "ClientB". Attackers exploit this feature to perform attacks on clients that allow grants implicitly.
- API security risks:

API	Risks	Solutions
API3	Excessive Data Exposure	▪ Ensure that proper filtering is performed on the server side and not on the client side ▪ Scrutinize the data flow from the endpoint to the client
API7	Security Misconfiguration	▪ Perform hardening process against API continuously ▪ Use scanning tools and human reviews to examine the entire API stack for security misconfigurations
API8	**Injection**	▪ Perform input validation and whitelisting ▪ Implement a parameterized interface for processing inbound API requests ▪ Ensure that the filtering logic limits the number of records returned
API6	Mass Assignment	▪ Do not expose the internal variable or object names as inputs ▪ Ensure whitelisting of all the properties that the client can update

- Fuzzing: Fuzzing: Attackers use the fuzzing technique to repeatedly send some random input to the target API to generate error messages that reveal critical information. To perform fuzzing, attackers use automated scripts that send numerous requests with varying combinations of input parameters. Attackers use tools such as Fuzzapi to perform fuzzing on the target API

- Invalid Input Attacks: In some scenarios, fuzzing is difficult to perform due to its structure. In such cases, attackers will give invalid inputs to the API, such as sending text in place of numbers, sending numbers in place of text, sending a greater number of characters than expected, and sending null characters, etc., to extract sensitive information from unexpected system behavior and error messages. At the same time, attackers also manipulate the HTTP headers and values targeting both API logic and the HTTP protocol.

- Malicious Input Attacks: In the attack discussed above, attackers try to retrieve sensitive information from unexpected system behavior or error messages. A more dangerous attack is where the attackers inject malicious input directly to target both the API and its hosting infrastructure. To perform this attack, attackers employ malicious message parsers using XML.

- Login/Credential Stuffing Attacks: Attackers often target login and validating

systems because attacks on these systems are difficult to detect and stop using typical API security solutions. Attackers perform login attacks or credential stuffing attacks to exploit password reuse across multiple platforms. Most users use the same passwords to access different web services

- API Vulnerabilities:
  - Enumerated Resources:
    - Design flaws can cause serious vulnerability, disclosing information through unauthenticated public API
    - Allows attackers to guess user IDs easily, compromising the security of the user data.
  - RBAC Pivilege Escalation:
    - Privilege escalation is a common vulnerability present in APIs having role-based access control (RBAC) where changes to endpoints are made without proper attention.
    - Allow attackers to gain access to users' sensitive information.
  - No ABAC Validation:
    - No proper attribute-based access control (ABAC) validation allows attackers to gain unauthorized access to API objects or perform actions such as viewing, updating, or deleting.
  - Buisness Logic Flaws:
    - Many APIs come with vulnerabilities in buisness logic.
    - Allows attackers to exploit legitimate workflows for malicious purposes.

1.14.5 Web App Security

- Countermeasures for Watering Hole Attack:
  - Apply software patches regularly to remove any vulnerabilities
  - Monitor network traffic
  - Secure DNS server to prevent attackers from redirecting the site to a new location.
  - Analyze user behavior

  - Inspect popular websites
  - Use browser blug-ins that block HTTP redirects
  - Disable third-party content such as advertizing services, which track user activities.
  - Make sure to hide online activities with a VPN and enable the browser's private browsing feature.
  - Make sure to run the web browser in a virtual environment to limit access to local system.

- Countermeasures against command injection flaws are:
  - Perform input validation
  - Escape dangerous characters
  - Use language-specific libraries that avoid problems due to shell commands
  - Perform input and output encoding
  - Use a safe API that avoids use of the interpreter entirely
  - Structure requests so that all supplied parameters are treated as data rather than potentially executable content
  - Use parameterized SQL queries
  - Use modular shell disassociation from the kernel
  - Use built-in library functions and avoid calling OS commands directly

- countermeasures to defend broken authentication and session management attacks include:
  - Use SSL for all authenticated parts of the application
  - Verify whether all the users' identities and credentials are stored in a hashed form
  - Never submit session data as part of a GET, POST
  - Apply pass phrasing with at least five random words
  - Limit the login attempts and lock the account for a specific period after a certain number of failed attempts

  - Use a secure platform session manager to generate long random session identifiers for secure session development
  - Make sure to check weak passwords against a list of the top bad passwords
- Countermeasures to defend against broken access control:
  - Perform access control checks before redirecting the authorized user to the requested resource
  - Avoid using insecure IDs to prevent the attacker from guessing them
  - Implement a session timeout mechanism
  - Limit file permissions to authorized users to avoid misuse
  - Avoid client-side caching mechanisms
  - Remove session tokens on the server side on user logout
  - Ensure that minimum privileges are assigned to users to perform only essential actions
  - Enforce access control mechanisms once and re-use them throughout the application
- Cookies flagged as secure are only transmitted over HTTPS
- Fuzz testing: Web application Fuzz testing (fuzzing) is a black box testing method. It is quality checking and assurance technique used to identify coding errors and security loopholes in web applications. Huge amounts of random data called "fuzz" is generated by the fuzz testing tools (fuzzers) and used against the target web application to discover vulnerabilities that can be exploited by various attacks.
  - Mutation-based: current data samples create new test data and the new test data again mutates to generate further random data. This type of testin starts with a valid sample and keeps mutating until the target is reached.
  - Protocol-Based: protocol fuzzer send forged packets to the target application that is to be tested
  - Generation-Based

1.15 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.

1.16 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.

1.17 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.

1.18 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

1.19 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.
    *

1.20 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.

2 Review Questions

2.1 Scanning

- In the SYN scan; Nmap will send a SYN message to the target. What is the response if the port is open or closed?
  1. Open: A SYN/ACK packet
  2. Closed A RST packet
  3. Filtered: No response given
- Active banner grabbing techniques used by an attacker to determine the OS running on a remote target system.
  - TCP Sequence ability test
  - Port Unreachable
- Passive banner grabbing techniques:
  - Banner grabbing from error messages
  - Sniffing the network traffic
  - Banner grabbing from page extensions
- Countermeasures to prevent information disclosure through banner grabbing
  - **Display false banners to mislead or deceive attackers.**
  - Turn off unnecessary services on the network host to limit information disclosure.

- Disabling open relay feature protect from SMTP enumeration.
- Disabling the DNS zone transfers to untrusted hosts protect from DNS enumeration
- Restricting anonymous access through RestrictNullSessAccess parameter from the Windows Registry protects from SMB enumeration.

2.2 Chapter 4: Enumeration

2.2.1 Enumeration Concepts

1. Which of the following enumeration techniques does an attacker take advantage of different error messages generated during the service authentication process?
    - **Brute-force Active Directory**
    - Extract usernames using SNMP: attackers guess read-only or read-write community strings by using SNMP API to extract usernames.
    - Extract usernames using email IDs: emails contain a username and a domain name.
    - Extract information using default passwords

2.3 Chapter 5: System Hacking

2.3.1 Escalating Privaleges

- A pen tester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pen tester pivot using Metasploit?
    - Create a route statement in the meterpreter.

2.3.2 Maintaining Access

2.4 Sniffing

2.4.1 Sniffing Concepts

- Which of the following OSI layers do sniffers operate and perform an initial compromize?
    - Data link layer: the second layer of the OSI model. Data packets are encoded and decoded into bits. OSI layers are designed to work independently of each other; thus if a sniffer sniffs data in the data link layer, the upper OSI layers will not be aware of the sniffing.

- Which of the following techniques is also a type of netowkr protocol used for PNAC that is used to defend against MAC address spoofing and to enforce access control at the point where a user joins a network.
  - **Implementation of IEEE 802.1X Suites**: This is a type of network protocol for port-based Network Access control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network.
  - DCHP Snooping Binding Table: DHCP snooping process filters untrusted DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, CLAN number, and interface information to correspond with untrusted interfaces of a switch. It acts as a firewall between untrusted hosts and DHCP servers. It also helps in differentiating between trusted and untrusted interfaces.
  - Dynamic ARP Inspection: The system checks the IP-MAC address binding for each ARP packet in a network. While performing a DAI, the system will automatically drop invalid IP-MAC address binding.
  - IP Source Guard: IP source gurad is a security feature in switches that restricts the IP traffic on untrusted layer 2 ports by filtering traffic based on the DHCP snooping binding database. It prevents spoofing attacks when the attacker tries to spoof or use the IP address of another host.
- Which of the following Cisco switch port configuration commands is used to enter a secure MAC address for the interface and the maximum number of secure MAC addresses?
  - `switchport port-security mac-address mac_address`: Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addreses.
  - `switchport port-security limit rate invalid-source-max`: sets the rate limit for bad packets.
  - `switchport port-security maximum value`: Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072; the default is 1.
  - `switchport port-security mac-address sticky` Enables sticky learning on the interface.
- Which of the following techniques enables devices to detect the existence of unidirectional links and disable the affected interfaces in the network, in addition to causing STP

topology loops.

  - **UDLD (Unidirectional Link Detection)**: def in question
  - BPDU Guard: BPDU guard must be enabled on the ports that should never recieve a BPDU from their connected devices. This is used to avoid the transimission of BPDUs on PortFast-enabled ports. This feature helps in preventing potential bridging loops in the network.
  - Root Guard: Protects the root bridge and ensures that it remains as the root in the STP topology. It forces the interfaces to become the designaged ports (forwarding ports) to prevent the nearby switches from becoming root switches.
  - Loop Guard: Loop guard improves the stability of the network by preventing it against the bridging loops. it is generally used to protect against a malformed switch.

- Which of the following IPv4 DHCP packet fields inculdes random number chosen by a client to associate request messages and their responses between the client and server?
  - Opcode: 1 octet, contains the message opcode that represents the message type: opcode "1" represents messages sent by the client, while "2" represents responses sent by the server.
  - **Transaction ID (XID)**: 4 Octets, a random number is chosen by the client to associate the request messages and their responses between a client and a server.
  - Flags: 2 octets, Flags set by the client; For example, if the client cannot recieve unicast IP datagrams, then the broadcast flag is set.
  - Server Name (SNAME): 64 octets, Optional server hostname.

- Which of the following IOS global commands verifies the DHCP snooping configuration?
  - `show ip dhcp spoofing`: Verifies the configuration.
  - `ip dhcp snooping`: Enables DHCP snooping globally.
  - `ip dhcp snooping trust`: Configures the interface as trusted or untrusted.
  - `no ip dhcp snooping information option`: To disable the insertion and the removal of the option-82 field, use the no ip dhcp snooping information option in global configuration command.

- In which of the following attacks does an attacker send spoofed router advertisement messages so that all the data packets travel through thri system to collect valuble information and launch MITM and DoS attacks?
  - **IRDP Spoofing**: An attacker can use this to send spoofed router advertisement messages so that all the data packets travel through the attacker;s system. Thus, the attacker can sniff the traffic and collect valuble information from the data packets. Attackers can use IRDP spoofing to launch MITM, DoS and passive sniffing attacks.
  - MAC Spoofing: in this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then, the attacker spoofs a MAC address with the MAC address of the legitimate client. If the spoofing is successful, then the attacker can recieve all the traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of someone on the network.
  - ARP Spoofing Attack: ARP spoofing is 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 an ARP request using the recipient's IP address, while the sender waits for the recipient to respond with a MAC address. An attacker eavesdropping on this unprotected layer 2 broadcast domain can respond to the broadcast ARP request and replies to the sender by spoofing the intended recipient's IP address.
  - STP Attack: If an attacker has access to two switches, he/she introduces a rogue switch in the network with a priority lower than any other switch in the network. This makes the rogue switch the root bridge, thus allowing the attacker to sniff all the traffic flowing in the network.
- In one of the following techniques, an attacker must be connected to a LAN to sniff packets, and on successful sniffing, they 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.
  - DNS Cache poisoning: DNS cache poisoning refers to altering or adding forged

DNS records in the DNS resolver cache so that a DNS query is redirected to a malicious site. The DNS system uses cache memory to hold the recently resolved domain names.

  - 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. The attacker changes the proxy server settings of the victim with the help of a Trojan. The proxy serves as a primary DNS and redirects the victim's traffic to the fake website, where the attacker can sniff the confidential information of the victim and then redirect the request to the real website.

  - Internet DNS Spoofing: Internet DNS poisoning is also known as remote DNS poisoning. Attackers can perform DNS spoofing attacks on a single victim or on multiple victims anywhere in the world. To perform this attack, the attacker sets up a rogue DNS server with a static IP address.

- Which of the following is not a mitigation technique against MAC address spoofing?

  - **DNS security (DNSSEC)**: Implement Domain Name System Security Extension to prevent DNS spoofing attacks.

  -

2.4.2 Sniffing Tools and countermeasures

- What is the correct pcap filter to capture all transmission control protocol (TCP) traffic going to or from host 192.168.0.125 on port 25?

  - tcp.port == 25 and ip.addr == 192.168.0.125

2.5 Social Engineering

2.5.1 Social Engineering Concepts

- Mat, a software engineer, received an email from his colleague John, stating that project files were missing from his system and asking Mat to send them to his personal email. Mat was suspicious and called John on his personal number. To his surprise, John replied that he has never written an email recently to Mat.
  Which of the following types of attacks was Mat subjected to?

  - **Intimidation**

2.5.2 Social Engineering Techniques

- A consultant is hired to do a physical penetration test at a large financial company. On the first day of his assessment, the consultant goes to the company's building dressed as an electrician and waits in the lobby for an employee to pass through the main access gate, and then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

  – **Tailgating** implies access to enter into the building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as when a polite user opens and then holds the door for those following. An attacker wears a fake badge and attempts to enter a secured area by closely following an authorized person through a door requiring key access. He/she can then try to get into restricted areas by pretending to be an authorized person.

2.6 Denial-of-Service

2.6.1 DoS/DDoS Concepts

2.6.2 DoS/DDoS Attack Techniques and Tools

- When a client's computer is infected with malicious software which connects to the remote computer to receive commands, the remote computer is called _____.

  – Answer is C&C, which will instruct the Bot what to do. When a client's computer is infected with malicious software which connects to the remote computer to receive commands, the remote computer is called C&C. Bot and Botnet respectively represent infected computer and network of the infected computers managed by C&C and server is not used in this terminology.

- The DDoS tool used by anonymous in the so-called Operation Payback is called _____.

  – LOIC is the first version of the tool and it was used in Operation Payback. HOIC is the second version of the tool with some additional features, and it was used in the Operation Megaupload. BanglaDos and Dereil do not have direct connection with anonymous group.

2.6.3 DoS/DDoS Protection Tools and Countermeasures

- What is the DoS/DDoS countermeasure strategy to at least keep the critical services functional?

  - Degrading services: During an attack, if it is not possible to keep all the services functioning, then it is a good idea to keep at least the critical services functional. To do this, first, identify the critical services and then customize the network, systems, and application designs to cut down on the noncritical services. This may help you to keep the critical services functional.

- Ivan works as security consultant at "Ask Us Intl." One of his clients is under a large-scale volume-based DDoS attack, and they have to decide how to deal with the issue. They have some DDoS appliances that are currently not configured. They also have a good communication channel with providers, and some of the providers have fast network connections. In an ideal scenario, what would be the best option to deal with this attack. Bear in mind that this is a volume-based DDoS attack with at least 1 000 000 bots sending the traffic from the entire globe!

  - The answer is "Absorb the attack," since this is a really large volume of traffic, and using additional capacity (DDoS appliances that are currently not configured) to absorb the attack. Most of the other options are not practically feasible. Blocking the traffic at the provider level is a viable option, but in this case, since the attack cannot be easily filtered (Since the traffic coming from the entire globe), this is not an apt solution. Filtering the traffic at the provider level is the same thing as blocking the traffic at the provider level, so this is not a correct answer and filtering the traffic at the company's Internet facing routers option will not work because the traffic is already there, and in this case, it is impossible to do anything at the client's site.

- John's company is facing a DDoS attack. While analyzing the attack, John has learned that the attack is originating from the entire globe, and filtering the traffic at the Internet Service Provider's (ISP) level is an impossible task to do. After a while, John has observed that his personal computer at home was also compromised similar to that of the company's computers. He observed that his computer is sending large amounts of UDP data directed toward his company's public IPs.

  John takes his personal computer to work and starts a forensic investigation. Two hours later, he earns crucial information: the infected computer is connecting to the C&C server, and unfortunately, the communication between C&C and the infected computer is encrypted. Therefore, John intentionally lets the infection spread to another machine in his company's secure network, where he can observe and record all the traffic between the Bot software and the Botnet. After thorough analysis he discovered an interesting thing that the initial process of infection downloaded the malware from an FTP server which consists of username and password in cleartext format. John connects to the FTP Server and finds the Botnet software including

the C&C on it, with username and password for C&C in configuration file. What can John do with this information?

  - The correct answer is "neutralize handlers," because with admin's access to C&C John can stop the attack, disable the C&C software, and/or change the password to stop the DDoS attack on his company's network. Deflect the attack and mitigate the attack are not the correct answers because in both these cases, he is literally stopping the attack. Protect secondary victims is not the correct answer because secondary victims are still infected.

- After successfully stopping the attack against his network, and informing the CERT about the Botnet and new password which he used to stop the attack and kick off the attackers from C&C, John starts to analyze all the data collected during the incident and creating the so-called "Lessons learned" document. What is John doing?

  - John is trying the postattack forensics in order to learn how to fight this type of attacks in the future. John is not trying to neutralize the handlers because this requires some type of access to C&C, which was already done, and he is not trying to prevent potential attacks and protect secondary victims—this was already done in previous steps.

2.7 Session Hijacking

2.7.1 Session Hijacking Concepts

-

2.7.2 Application Level Session Hijacking

"

-

2.7.3 Network Level Session Hijacking

- In order to hijack TCP traffic, an attacker has to understand the next sequence and the acknowledge number that the remote computer expects. Explain how the sequence and acknowledgment numbers are incremented during the 3-way handshake process.

  - During the 3-way handshake, sequence and acknowledgment numbers are (relatively) incremented by one. After that acknowledge number will be incremented for the size of the packet received.

- Maira wants to establish a connection with a server using the three-way handshake. As a first step she sends a packet to the server with the SYN flag set. In the second step, as a response for SYN, she receives packet with a flag set.

  Which flag does she receive from the server?

  - In the second step, the server sends a response to her with the SYN + ACK flag and an ISN (Initial Sequence Number) for the server. In the third step, Maira sets the ACK flag acknowledging the receipt of the packet and increments the sequence number by 1.

2.7.4 Session Hijacking Tools

- Marin was using sslstrip tool for many yearsagainst most of the websites, like Gmail, Facebook, Twitter, etc. He was supposed to give a demo on internet (in)security and wanted to show a demo where he can intercept 302 redirects between his machine and Gmail server. But unfortunately it does not work anymore. He tried the same on Facebook and Twitter and the result was the same. He then tried to do it on the company OWA (Outlook Web Access) deployment and it worked! He now wants to use it against Gmail in his demo because CISO thinks that security through obscurity is a best way to a secure system (obviously BAD CISO) and demonstrating something like that on company live system is not allowed. How can Marin use sslstrip or similar tool to strip S from HTTP?

  - HSTS protection is basically the cookie that the website issues to the web browser, when user visits the website for the first time. It's long term cookie, which means that it will not expire. If the cookie is set - web browser prevents visiting the website over HTTP connection. So, by using sslstrip+ with dnsspoof module, one can effectively combat the protection if the user NEVER visited this website before. That's why he has to use IE in InPrivate browsing mode because it will not read the HSTS cookie. This is NOT the case with Firefox or Chrome though! SslstripHSTS tool does not exist.

2.7.5 Session Hijacking Countermeasures

- Which of the following countermeasures should be followed to defend against session hijacking?

  - Use HTTP Public Key Pinning (HPKP) to allow users to authenticate web servers

- Which of the following techniques mitigates the risk of ARP spoofing and other session hijacking attacks caused when using a hub network?

- **Switch Netowrk**: Mitigates the risk of ARP spoofing and other session hijacking attacks.

- Which of the following techniques protects the client-server communication against session hijacking attacks by creating a public-private key pair for every connection to a remote server?
  - Token Binding

2.8 Evading IDS, Firewalls, and Honeypots

2.8.1 IDS, IPS, Firewall and Honeypot Concepts

- Which of the following attributes in a packet can be used to check whether the packet originated from an unreliable zone?
  - Source IP address

- What is the main advantage that a network-based IDS/IPS system has over a host-based solution?
  - They do not use host system resources. Host-based intrusion detection systems (IDSes) protect just that: the host or endpoint. This includes workstations, servers, mobile devices and the like. Host-based IDSes are not just one of the last layers of defense, but they're also one of the best security controls because they can be fine-tuned to the specific workstation, application, user role or workflows required. A network-based IDS often sits on the ingress or egress point(s) of the network to monitor what's coming and going. Given that a network-based IDS sits further out on the network, so it doesn't use any host system resources and it may not provide enough granular protection to keep everything in check – especially for network traffic that's protected by SSL, TLS or SSH.

- Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?
  - They must be Dual-homed. Dual-homed devices have two interfaces; a public interface that directly connected to the Internet and a private interface connected to the Intranet. It is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function. The bastion host is an example of dual-homed system 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 attack. Traffic entering or leaving the network passes through the firewall.

- Which of the following descriptions is true about a static NAT?
  - A static NAT uses a one-to-one mapping.
- Jamie needs to keep data safe in a large datacenter, which is in desperate need of a firewall replacement for the end of life firewall. The director has asked Jamie to select and deploy an appropriate firewall for the existing datacenter. The director indicates that the amount of throughput will increase over the next few years and this firewall will need to keep up with the demand while other security systems do their part with the passing data. What firewall will Jamie use to meet the requirements?
  - Performance is the key focus of the question; therefore, the test taker will have to focus on the real need of the most enterprise businesses and not get distracted by other slower firewall types. Packet filtering firewall may seem old school to less experienced test takers and they may immediately choose other options. Packet filtering firewalls are best performing of the choices.
- When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the source IP address and destination IP address are the same. However, no alerts have been sent via email or logged in the IDS. Which type of an alert is this?
  - False Negative
- When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrato's computer to update the router configuration. What type of an alert is this?
  - False Positive
- At which two traffic layers do most commercial IDSes generate signatures? (Select Two)
  - According to New 'semantics-aware' IDS reduces false positives (https://searchsecurity.techta https://www.sanfoundry.com/computer-networks-questions-answers-entrance-exams/, and https://searchsecurity.techtarget.com/quiz/Quiz-IDS-IPS, the most commercial IDSes generate signatures at the network and transport layers.

2.8.2 IDS, IPS, Firewall, and Honeypot Solutions

- When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following:
  - Continues to evaluate the packet until all rules are checked

2.8.3 Evading IDS

- How many bit checksum is used by the TCP protocol for error checking of the header and data and to ensure that communication is reliable?
  - 16-bitwa
- An attacker hides the shellcode by encrypting it with an unknown encryption algorithm and by including the decryption code as part of the attack packet. He encodes the payload and then places a decoder before the payload. Identify the type of attack executed by attacker.
  - Polymorphic Shellcode

2.8.4 Evading Firewalls

- Which of the following attack techniques is used by an attacker to exploit the vulnerabilities that occur while processing the input parameters of end users and the server responses in a web application?
  - XSS attack
- Which of the following techniques is used by attackers for collecting information about remote networks behind firewalls, where the TTL value is used to determine ACL gateway filters and map networks by analyzing the IP packet response?
  - Firewalking
- Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
  - TCP port 21—no response
  - TCP port 22—no response
  - TCP port 23—Time-to-live exceeded
  - The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.

- Which feature of Secure Pipes tool open application communication ports to remote servers without opening those ports to public networks?
  - Local forwards open application communication ports to remote servers without opening those ports to public networks. It brings the security of VPN communication to clients and servers on an ad hoc basis without the configuration and management hassle.

2.8.5 Honeypot, IDS, and Firewall Evasion Countermeasures

- In what way do the attackers identify the presence of layer 7 tar pits?
  - By looking at the latency of the response from the service.
- Which of the following methods is NOT a countermeasure to defend against IDS evasions?
  - Never define the DNS server for client resolver in routers
- Which of the following countermeasures can be employed to defend against firewall evasion?
  - Following are some of the countermeasures to defend against firewall Evasion:
    * By default, disable all FTP connections to or from the network
    * Set the firewall rule set to deny all traffic and enable only the services required.
    * Specify the source and destination IP addresses as well as the ports.
    * Notify the security policy administrator about firewall changes and document them
    * Monitor user access to firewalls and control who can modify the firewall configuration
    * Take regular backups of the firewall rule set and configuration files
    * Configure a remote syslog server and adopt strict measures to protect it from malicious users.
    * Schedule regular firewall security audits.
    * The firewall should be configured such that the IP address of an intruder should be filtered out.

2.9 Hacking Web Servers

2.9.1 Web Server Concepts

- Which of the following types of damage is caused when attackers access sensitive data such as financial records, future plans, and the source code of a program?
  - Data Theft

2.9.2 Web Server Attacks

- In which of the following attack types does an attacker exploit the trust of an authenticated user to pass malicious code or commands to a web server?
  - Cross-site request forgery
- In which of the following attacks does an attacker attempt to access sensitive information by intercepting and altering communications between an end user and a web server?
  - Man-in-the-Middle attack.
- If an attacker compromises a DNS server and changes the DNS settings so that all the requests coming to the target webserver are redirected to his/her own malicious server, then which attack did he perform?
  - DNS server hijacking

2.9.3 Web Server Attack Methodology

- Which of the following tools is not used to perform webserver information gathering?
  - Among the options, Nmap, Netcraft and Whois are the tools used to perform footprinting of webservers, whereas **Wireshark** is a network sniffing tool.
- Which of the following command does an attacker use to enumerate common web applications?
  - `nmap --script http-enum -p80 <host>`
- Atatcker use GET and CONNECT requests to use vulnerable web servers as which of the following?
  - Sometimes, web servers are configured to perform functions such as forwarding or reverse HTTP proxy. Web servers with these functions enabled are employed by the attackers to perform following attacks:

    * Attacking third-party systems on internet
    * Connecting to arbitrary hosts on the organization's internal network
    * Connecting back to other services running on the proxy host itself

    Attackers use GET and CONNECT requests to use vulnerable web servers as proxies to connect and obtain information from target systems through these proxy web servers.

- Which of the following types of payload modules in the Metasploit framework is self-contained and completely stand-alone?
  - Singles

2.9.4 Web Server Attack Countermeasures

- Which of the following guidelines should be followed by application developers to defend against HTTP response-splitting attacks?
  - Parse all user inputs or other forms of encoding before using them in HTTP headers
- Which of the following is NOT a best approach to protect your firm against web server attacks?
  - Allow remote registry Administration.
  - To defend web servers and provide security, you must remove unnecessary ISAPI filters from the web server, apply restricted ACLs, secure the SAM (stand-alone servers only), and block the remote registry administration.
- Choose an ICANN accredited registrar and encourage them to set registrar-lock on the domain name in order to avoid which attack?
  - DNS hijacking attack
- Which on of the following techniques defends servers against blind response forgery?
  - UDP source port randomization technique defends servers against blind response forgery. Limit the number of simultaneous recursive queries and increase the times-to-live (TTL) of legitimate records. Following are some of the methods to defend against HTTP response-splitting and web cache poisoning: Server Admin: Use latest web server software Regularly update/patch OS and web server Run web vulnerability scanner Application Developers: Restrict web

application access to unique IPs Disallow carriage return (`%0d or \r`) and line feed (`%0a or \n`) characters Comply to RFC 2616 specifications for HTTP/1.1

2.9.5 Patch Management

- Which of the following is true for automated patch management process?
  - In an automated patch management process, detect -¿ assess -¿ acquire -¿ test -¿ deploy -¿ maintain is the process that is followed

2.10 Web Applications

2.10.1 Web App Concepts

-

2.10.2 Web App Threats

- Which of the following is a security risk due to the incorrect implementation of applications, allowing attackers to compromise passwords, keys, session tokens, and exploit user identity?
  - Broken authentication
- In which of the following types of injection attacks does an attacker exploit vulnerable form inputs, inject HTML code into a webpage, and change the website appearance?
  - HTML injection
- Which of the following security misconfigurations supports weak algorithms and uses expired or invalid certificates, resulting in data exposure and account theft?
  - Insufficient transport layer protection
- Which of the following attacks allows an attacker to encode portions of the attack with Unicode, UTF-8, Base64, or URL encoding to hide their attacks and avoid detection?
  - Obduscation Application
- Which of the following is a timing attack performed by measuring the approximate time taken by a server to process a POST request so that the existence of a username can be deduced?
  - Direct Timing Attack

- Which of the following is an application security threat that occurs when an application includes untrusted data in a new web page without proper validation or escaping or when an application updates an existing web page with user-supplied data?
  - Cross-site scripting (XSS)
- Which of the following attacks exploits vulnerabilities in dynamically generated webpages, which enables malicious attackers to inject client-side scripts into webpages viewed by other users?
  - Cross-site scripting
- During a penetration test, a tester finds that the web application being analyzed is vulnerable to XSS. Which of the following conditions must be met to exploit this vulnerability?
  - The session cookies do not have the HttpOnly flag set.
- An attacker has been successfully modifying the purchase price of items purchased on the company's website. The security administrators verify the webserver and Oracle database have not been compromised directly. They have also verified the intrusion detection system (IDS) logs and found no attacks that could have caused this. What is the most likely way the attacker has been able to modify the purchase price?
  - By changing hidden form values
- Which of the following conditions must be given to allow a tester to exploit a cross-site request forgery (CSRF) vulnerable web application?
  - The web application should not use random tokens.

2.10.3 Web App Hacking Methodology

- Which of the following HTTP service port numbers is used for connecting to a remote network server system?
  - **384: Remote network Server System**
  - 80: World Wide Web standard port
  - 81: Alternate WWW
  - 88: Kerberos

- Which of the followings techniques is used by an attacker to enumerate usernames from a target web application?
  - Verbose failure message
- Which of the following attacks is possible when an attacker executes .bat or .cmd files and changes the values by superimposing one or more operating-system commands through the request?
  - Parsing Attack
- Which of the following automatically discover hidden content and functionality by parsing HTML form and client-side JavaScript requests and responses?
  - Web Spiders
- An attacker wants to exploit a webpage. From which of the following points does he start his attack process?
  - Identify entry points for user input
    The first step in analyzing a web app is to check for the application entry point, which can later serve as a gateway for attacks. One of the entry points includes the front-end web app that intercepts HTTP requests. Other web app entry points are user interfaces provided by webpages, service interfaces provided by web services, serviced components, and .NET remoting components. Attackers should review the generated HTTP request to identify the user input entry points.

2.10.4 Web API, Webhooks and Web Shell

- Some of the best practices for securing webhooks are as follows:
  - Use rate limiting on webhook calls in the web server to control the incoming and outgoing traffic
  - Compare the request timestamp X-Cld-Timestamp of the webhook with the current timestamp to prevent timing attacks
  - Validate the X-OP-Timestamp within the threshold of the current time
  - Ensure that the event processing is idempotent to prevent event receipts replication
  - Ensure that the webhook code responds with 200 OK (success) instead of 4xx or 5xx statuses in case of errors to ensure that the webhooks are not

deactivated

  - Ensure that the webhook URL supports the HTTP HEAD method to retrieve meta-information without transferring the entire content

  - Use threaded requests to send multiple requests at the same time and to update data in the API rapidly

  - Make sure that the tokens are stored against the store_hash and not against the user data

2.10.5 Web App Security

- While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

  - Data validation is performed to ensure that the data is strongly typed, correct syntax, within length boundaries, contains only permitted characters, or that numbers are correctly signed and within range boundaries. So, while performing data validation of web content, a security technician is required to validate web content input for type, length, and range.

2.11 General

- Where does Microsoft Windows store authentication credentials and passwords?

  1. `C:\windows\system32\config`

- What netstat command will you use if you want to display all connections and listening ports, with addresses and port numbers in numerical form?

  1. `netstat -an`

- What type of rootkit uses system-level calls to hide their existence?

  1. Library Level rootkit (user-level), replaces or modifies the functionality of system calls to the operating system.

-

Issue	Solution	Notest
Telnet, rlogin	Secure Shell (SSH) or openSSH	Sends encrypted data and ma
Any remote connection	Virtual Private Network (VPN)	Implementing encrypting VPN
Server message Block (SMB)	SMB Signing	Improves the security of the S
Hub Network	Switch network	Mitigates the risk of ARP spo