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.
- Psycological Warfare: Psycological warefare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in battle
- Hacker Warfare: The purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system monitoring, false messaging, and access to data.
- Command and control (C2) Warfare: In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- Economic Warfare:
- Cyberwarfare: involves the use of information systems against the virtual personas of individuals or groups and includes information terrorism, semantic attacks, and simula-warfare?
- Electronic warfare: uses radio-electronic and cryptographic techniques to degrade the communication.
- Integrity: The trustworthiness of data or resources in terms of preventing improper or unauthorized changes.
- Non-Repudiation: A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- Authenticity: Refers to the characteristic of a communication, document, or any

data that ensures the quality of being genuine.

- Availability: Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users.

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

- Security Audit Steps:
    1. Talk to the client and discuss the needs to be addressed during testing.
    2. Prepare and sign NDA documents with the client.
    3. Organize an ethical hacking team and prepare the schedule for testing.
    4. Conduct the test.
    5. Analyze the results of the testing and prepare a report.
    6. Present the findings to the client.

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.

- Threat Intelligence:
  - Strategic threat intelligence: provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions.
  - Operational threat intelligence: Provides contectual information about security events and incidents that help defenders disclose risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way.
  - Technical threat intelligence: it provides rapid distribution and response to threats. For example, a piece of malware used to perform an attack is tactival threat intelligence, wheras the details related to the specific implementation of the malware come under technical threat intelligence.
  - Tactical threat intelligence: Plays a major role in protecting the resources of the organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks.

- Risk Management:
  1. Risk Identification:
  2. Risk Assessment:
  3. Risk treatment:
  4. Risk tracking and review:

- Threat Modeling Process:

1. Identify security objectives:
2. Application overview:
3. Decompose the application:
4. Identify threats:
5. Identify vulnerabilities:

- Machine Learning classification:
  - Dimensionality Reduction: the process of reducing the dimensional (attributes) of data.
  - Classification: Includes completely divided classes. Its main task is to define the test sample to identify its class.
  - Clustering: Clusters divides the data into clusters based on the similarities, regardless of class information.
  - Regression: Used when data classes are not separated, such as when the data is continuous.
- Incident Triage: The identified security incidents are analyzed, validated, categorized, and prioritized.
- Incident recording and assignment: The initial reporting and recording of the incident takes place.
- Containment: helps prevent the spread of infection to other organizational assets and avoid additional damage.
- Recovery: After eliminating the causes for the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery.

1.2 Chapter 2: Footprinting and Reconnaissance

1.2.1 Footprinting Concepts

- Tools:
  - 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.
  - BuzzSumo: Advanced social search engine that displayed shared activity across all major social networks including Twitter, Facebook, LinkdIn, Google Plus, and Pinterest.

- 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

- Tools:
  - TinEye: Reverse image search Attacker use online tools, such as Google Image Search, TinEye reverse image search, Yahoo image search, and Bing image search to perform a reverse image search.
  - Mention: An online reputation tracking tool that helps attackers monitoring the web, social media, forums, and blogs to learn more about the target brand and industry.
  - Intelius: Attackers can use Intelius people search online service to search for people belonging to the target organization.
  - ExoneraTor: Attackers can use deep and dark web searching tools such as Tor Browser, ExoneraTor, and OnionLand Search engine to gather confidential information about the target, such as credit card details, passports information, identification card details, medical records, social media accounts, and Social Security Numbers (SSNs).
  - Spokeo: People search online service
  - Been Verified: People search online service
  - Whitepages: People search online service.
  - Professional Toolset: DNS interrogation tools such as Professional Toolset (https://tools.dnsstuff.com) and DNS Records (https://network-tools.com) enable the user to perform DNS footprinting.
  - Infoga: Infoga is a tool used for gathering email account information from different public sources and it checks if an email was leaked using the haveibeenpwned.com API.
  - Octoparse: Octoparse offers automatic data extraction, as it quickly scrapes web data without coding and turns web pages into structured data.
  - Metagoofil: Metagoofil extracts metadata of public documents (pdf, doc, xls, ppt, docx, pptx, and xlsx) belonging to a target company.
- DNS Record Types:
  - SOA: Indicates the authority for a domain of the target DNS server.
  - A: Points to a host's IP address

  - MX: points to domain's mail server
  - NS: Points to a host's name server.
  - CNAME: Canonical naming allows aliases to a host.
  - SRV: Service records.
  - PTR: Maps IP address to a hostname
  - RP: Responsible person.
  - HINFO: Host information record includes CPU type and OS.
  - TXT: Unstructured text records.

- Whois lookup: query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases and it contains the personal information of domain owners. For each resource, Whois database provides text records with information about the resource itself, and relevant information of assignees, registrants, and administrative information (creation and expiration dates).
  Returns the following information:
  - Domain name details
  - domain name servers
  - NetRange
  - When a domain has been created.
  - Contact details of domain owner.
  - Expiry records
  - Records last updated.

- DNS Lookup reveals information about DNS zone data. including domain names, computer names, IP addresses and more about a particular network.

1.2.3 Footprinting Tools and Countermeasures

- Tools:
  - OSRFramework tools:

    * usufy.py: Checks for a user profile on up to 290 different platforms.
    * mailfy.py: Check for the existence of a given email.
    * searchfy.py: Performs a query on the platforms in OSRFramework.
    * domainfy.py: Check for the existence of domains.
    * phonefy.py: Checks for the existence of a given series of phones.
    * entify.py: Uses regular expressions to extract entities.
- Recon Dog: An all in one tool for all basic information gathering needs. It uses APIs to collect information about the target system.
  Features:
    * Censys: Uses censys.io to gather a massive amount of information about an IP address.
    * NS lookup: Performs name server lookup
    * Port scan: Scans most common TCP ports
    * Detect CMS: Can detect 400+ content management systems
    * Whois lookup: Performs a Whois lookup
    * Detect honeypot: Uses shodan.io to check if the target is a honeypot
    * Find subdomains: Uses findsubdomains.com to find subdomains
    * Reverse IP lookup: Performs a reverse IP lookup to find domains associated with an IP address
    * Detect technologies: Uses wappalyzer.com to detect 1000+ technologies
    * All: Runs all utilities against the target
- FOCA (Fingerprinting Organizations with Collected Archives): Tool used to find metadata and hidden information in the documents it scans.
  Features:
    * Web Search - Searches for hosts and domain names through URLs associated with the main domain. Each link is analyzed to extract information from its new host and domain names.
    * DNS Search - Checks each domain to ascertain the host names configured in NS, MX, and SPF servers to discover the new host and domain names.

* IP Resolution - Resolves each host name by comparison with the DNS to obtain the IP address associated with this server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.

* PTR Scanning - Finds more servers in the same segment of a determined address; IP FOCA executes a PTR log scan.

* Bing IP - Launches FOCA, which is a search process for new domain names associated with that IP address for each IP address discovered.

* Common Names - Perform dictionary attacks against the DNS.

1.3 Chapter 3: Scanning Networks

1.3.1 Network Scanning Concepts and Tools

- Tools:
  - Fing: Mobile app network scanning tool, provides complete network information, such as IP address, MAC address, device vendor, and ISP location.
  - Hping2/Hping3: A command line oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP,UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

1.3.2 Host, Port and Service Discovery

- ICMP Address Mask Ping Scan: This type of ping method is also effective in identifying the active hosts similarly to the ICMP timestamp ping, specifically when the administrator blocks the traditional ICMP Echo ping
- ICMP ECHO Ping Scan: ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.
- ICMP ECHO Ping Sweep: A ping sweep (also known as an ICMP sweep) is a basic network scanning technique that is adopted to determine the range of IP addresses that map to live hosts (computers). Although a single ping will tell the user whether a specified host computer exists on the network, a ping sweep consists

of ICMP ECHO requests sent to multiple hosts. If a specified host is active, it will return an ICMP ECHO reply.

- UDP Ping scan: UDP ping scan is similar to TCP ping scan; however, in the UDP ping scan, Nmap sends UDP packets to the target host.
- UDP Scanning: There is no three-way TCP handshake for UDP scanning. The system does not respond with a message when the port is open. If a UDP packet is sent to a closed port, the system will respond with an ICMP port unreachable message. Spyware, Trojan horses, and other malicious applications use UDP ports
- SCTP INIT Scanning: Attackers send an INIT chunk to the target host, and an INIT+ACK chunk response implies that the port is open, whereas an ABORT Chunk response means that the port is closed. No response from the target or a response of an ICMP unreachable exception indicates that the port is a Filtered port
- SSDP Scanning: The Simple Service Discovery Protocol (SSDP) is a network protocol that works in conjunction with the UPnP to detect plug and play devices. Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks. Attacker may use the UPnP SSDP M-SEARCH information discovery tool to check if the machine is vulnerable to UPnP exploits or not
- List Scanning: This type of scan simply generates and prints a list of IPs/Names without actually pinging them. A reverse DNS resolution is performed to identify the host names

1.3.3 OS Discovery and Scanning Beyond IDS/Firewall

- Active Banner grabbing techniques:
  - TCP Sewuence ability test
  - Port unreachable
- Passive Banner Grabbing techniques:
  - Banner grabbing from error messages
  - Sniffing the network traffic
  - Banner grabbing from page extensions
- Tools:
  - Tails

  - Scany: a network scanner for iPhone and iPad that is used to scan LAN, Wi-Fi networks, websites, open ports, and network devices and can support several networking protocols
  - Psiphon
  - Whonix

1.4 Chapter 4: Enumeration

1.4.1 Enumeration Concepts

- Secure Shell (SSH) is a command-level protocol mainly used for managing various networked devices securely. It is generally used as an alternative protocol to the unsecure Telnet protocol. SSH uses the client/server communication model, and the SSH server, by default, listens to its client on TCP port 22
- File Transfer Protocol: FTP is a connection-oriented protocol used for transferring files over the Internet and private networks. FTP is controlled on TCP port 21, and for data transmission, FTP uses TCP port 20 or some dynamic port numbers depending on the server configuration
- Telnet: The Telnet protocol is used for managing various networked devices remotely. It is an unsecure protocol because it transmits login credentials in the cleartext format. Therefore, it is mostly used in private networks. The Telnet server listens to its clients on port 23. Attackers can take advantage of the Telnet protocol to perform banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks, etc.
- Border Gateway Protocol: BGP is widely used by Internet service providers (ISPs) to maintain huge routing tables and for efficiently processing Internet traffic. BGP routers establish sessions on TCP port 179
- IPSEC IKE: IP Security Internet Key Exchange Protocol is used for establishing Security Association for IPsec Protocol Suite. IKE uses UDP port 500 for establishing security association.
  - Ipsec NAT-T uses port 4500
- Remote mail checking uses port 50 TCP/UDP

1.4.2 NetBIOS and SNMP Enumeration

- Tools:

–

- PsList: Displays the CPU and memory information or thread statistics.

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 information. 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 information. It analysis 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 information 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 SQL Injection

1.15.1 SQL Injection Concpets

- Types of attacks:

- Authorization Bypass: Using this attack, an attacker alters authorization information stored in the database by exploiting an SQL injection vulnerability.
- Compromised Data Integrity: Using this attack, an attacker defaces a web page, inserts malicious content into web pages, or alters the contents of a database.
- Remote Code Execution: Using this attack, an attacker compromises the host OS.
- Compromised Availability of Data: Using this attack, an attacker deletes the database information, delete logs, or audit information stored in a database.

1.15.2 Types of SQL Injection

- Union SQL Injection: In a UNION SQL injection, an attacker combines a forged query with a query requested by the user using a UNION clause.
- Blind/Inferential SQL Injection: In blind SQL injection, an attacker poses a true or false question to the database to determine whether the application is vulnerable to SQL injection.
- Error-based SQL injection: In this type of SQL injection, the attacker forces the database to return error messages in response to his/her inputs. Later, the attacker may analyze the error messages obtained from the underlying database to gather information that can be used for constructing the malicious query.
- In-band SQL injection: In in-band SQL injection, attackers use the same communication channel to perform the attack and retrieve the results.
- Out-of-band SQL Injection: Attacker uses different communication channels to perform the attack and obtain results. Difficult to perform as the attacker needs to communicate with a database server and determine the server features used by a web application.
- tautology-based SQL injection attack, an attacker uses a conditional OR clause in such a way that the condition of the WHERE clause will always be true.
- end-of-line SQL injection, an attacker uses Line comments in specific SQL injection inputs.
- Piggybacked Query: Attacker injects an additional malicious query into the original query.

1.15.3 SQL Injection Methodology

- Database Objects:
  - Oracle:
    - SYS.USER_OBJECTS
    - SYS.TABLES, SYS.USER_TABLES
    - SYS.USER_VIEWS
    - SYS.ALL_TABLES
    - SYS.COLUMNS
    - SYS.USER_OBJECTS
  - MS Access
    - MsysACEs
    - MsysObjects
    - MsysQueries
    - MsysRelationships
  - MySQL:
    - mysql.user
    - mysql.db
    - mysql.tables_priv
  - MSSQL Server:
    - sysobjects
    - syscolumns
    - systypes
    - sysdatabases
  - DB2:
    - syscat.columns
- Functions:

  - LOAD_FILE(): function within MySQL and is used to read and return the contents of a file located within MySQL server.
  - OPENROWSET(): An SQL Server can be linked back to an attacker's DB via OPENROWSET.
  - CONVERT(): Used to convert one data type to another.
  - INTO OUTFILE(): The OUTFILE function within MySQL is often used to run a query and dump the results into a file.
  - CHAR(): attacker can encode a common injection variable present in the input string in an attempt to avoid detection in the signatures of network security measures. Converts hexadecimal values into characters that can easily pass through SQL engine parsing. For MySQL.
  - ASCIISTR(): Oracle function that takes a string (or an expression that resolves to a string), and returns an ASCII version of the string in the cur.
  - CHR(): Oracle function that returns the ASCII character that corresponds to the value passed to it.

- Column Enumeration:
  - MSSQL:
    `SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name`
  - MySQL:
    `show columns from tablename`
  - Oracle: `SELECT * FROM all_tab_columns WHERE table_name='tablename'`
  - DB2:
    SELECT * FROM syscat.columns WHERE tabname='tablename'—

- single and double quotes: In black box testing, single and double quotes are used as the input data to catch instances where the user input is not sanatized.
- Semicolon: In black box penetration testing, a semicolon is used to group two or more SQL statements in the same line.
- Static Code analysis: Main objective is to improve the quality of software products by finding errors in the early stages of the development lifecycle. Code is not executed. Covers structural and statement coverage testing.
- Dynamic code analysis: Checks for functional behavior of the software system,

memory/CPU usage, and overall performance of the system. In dynamic testing code is executed to uncover bugs in the software system. Testing is done in the later stages of the software development lifecycle.

- Variations: Uses the WHERE statement that always evaluates to true, so that any mathematical or string comparison can be used. It is performed by placing characters such as `' or '1'='1'` on any basic injection statement.
- Declare Variables: uses variables that can be used to pass a series of specially crafted SQL statements and bypass the detection mechanism.
- Case Variation: Obfuscate an SQL statement by mixing it with uppercase and lowercase letters.
- Null Byte: Uses the null byte (`%00`) character prior to a string in order to bypass the detection mechanism.

1.15.4 SQL Injection Countermeasures

- Tools:
  - Acunetix Web Vulnerability Scanner provides automated web application security testing with innovative technologies including DeepScan and AcuSensor Technology. Rigorously tests for thousands of web application vulnerabilities including SQL injeciton and XSS.

1.16 Hacking Wireless Networks

1.16.1 Wireless Concepts

- Orthogonal Frequency-division Multiplexing (OFDM): Method of encoding digital data on multiple carrier frequencies.
- Frequency-hopping Spread Spectrum (FHSS): A method of transmitting radio signals by rapidly switching a carrier among many frequency channels.
- Multiple input, multiple output orthogonal frequency-division multiplexing (MIMO-OFDM): An air interface for 4G and 5G broadband wireless communications.
- Direct-sequence Spread Spectrum (DSSS): An original data signal multiplied with a pseudo-random noise spreading the code.
- Shared Key authentication: each wireless station recieves a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication

channels. The following steps illustrate the establishment of connectino in the shared key authentication process

  - Station sends an authentication frame to the AP.
  - The AP sends a challenge text to the station.
  - The station encrypts the challenge text by making use of its configured 64- or 128-bit key, and it sends the encrypted text to the AP.
  - The AP uses its configured WEP key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the AP authenticates the station.
  - The station connects to the network.

- Wireless Standards:
  - 802.11d: Enchanced version of 802.11a and 802.11b. Supports regulatory domains. The particulars of this standard can be set at the media access control (MAC) layer.
  - 802.11e: Used for real-time applications such as voice, VoIP, and video. To ensure that these time-sensitive applications have the network resources they need, 802.11e defines mechanisms to ensure Quality of Service (QoS) to Layer 2 of the reference model, the medium-access layer, or MAC.
  - 802.11i: Improves WLAN security by implementing new encryption protocols such as TKIP and AES. It is a standard for wireless local area networks (WLANs) that provides improved encryption for networks that use the popular 802.11a, 802.11b (which includes Wi-Fi) and 802.11g standards.
  - 802.11n: A revision that enhances the earlier 802.11g standards with multiple-input multiple-output (MIMO) antennas. It works in both the 2.4GHz and 5GHz bands. IEEE industry standard for Wi-Fi wireless local network transportations. Digital Audio Broadcasting (DAB) and Wireless LAN use OFDM.
  - IEEE 802.16: wireless communication standard designed to provide multiple physical layer (PHY) and media access control (MAC) options. It is also known as WiMax. This standard is a specification for fixed broadband wireless metropolitan access networks (MANs) that use point-to-multipoint architecture. It has a range of 1609.34-9656.06 Kilometers (1-6 miles).

1.16.2 Wireless Encryption

- PEEAP: a protocol that encapsulates the EAP within an encrypted and authenticated transport layer security (TLS) tunnel.
- WEP: An encryption algorithm for IEEE 802.11 wireless networks. Uses RC4 encryption with a 40/104-bit key. CRC-32 for integrity checking. Does not provide cryptographic integrity protection.
- CCMP: An encryption protocol used in WPA2 for strong encryption and authentication.
- WPA: RC4 and TKIP encryption algorithms with 128-bit keys. Michael algorithm and CRC-32 for integrity checking. Succeptable to KRACK.
- WPA2: An upgrade to WAP using AES and CCMP for wireless data encryption. Introduces the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, a strong wireless encryption, and counter mode cipher block chaining message authentication code protocol (CCMP). Provides stronger data protection and network access control. Gives a high level of security to Wi-Fi connections, so that only authorized user can access it. 128-bit key, CBC-MAC for integrity checking.
- WPA3: Is a third generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication. Susceptable to Dragonblood vulnerabilities.
- WPA:
- Counter Mode Cipher Block Chaining Message Authentication Protocol (CCMP): an encryption protocol used in WPA2 for stronger encryption and authentication. Uses AES

1.16.3 Wireless Threats

- Confidentiality Attack: Attempt to intercept confidential information sent over wireless associationsm regardless of whether they were sent in clear text or encrypted by Wi-Fi protocols.
- Availability Attacks: Aim at obstructing the delivery of wireless services to legitmiate users, wither by crippling those resources or by denying them access to WLAN resources.

- Authentication Attacks: Steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources.
- Integrity Attacks: Attackers send forged control, management, or data frames over a wireless network to misdirect the wireless devices to perform anothe type of attacks (e.g., DoS).
- Ad hoc associations: An attacker may perform this kind of attack using any Universal Serial Bus (USB) adapter or wireless card. The attacker connects the host to an unsecured client to attack a specific client or to avoid AP security.
- Promiscuous Client: Allows an attacker to transmit target network traffic through a fake AP. It is very similar to the evil-twin threat on wireless networks, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID.
- Client mis-associtaion: The client may intentionally or accidentally connect or associtae with an AP outside of the legitimate network because the WLAN signals travel through the air, walls, and othe obstructions.
- Unauthorized association: A major threat to wireless networks. The prevention of this kind of attack depends on the method or technique that the attacker uses to get associated with a network.

1.16.4 Wireless Hacking Methodology

- Tools:
  - Netcat: A networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by othe programs and scripts. It is also a network debugging and exploration tool.
  - NetStumbler: Used for collecting wireless packets and detecting wireless LANs using 802.11b, 802.11a and 802.11g WLAN standards. Runs on Windows.
  - L0phtCrack: Tool designed to audit passwords and recover applications. Recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks, also checks the strenght of the password.
  - Kismet: An 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system. Identifies networks by passively collecting packets and detecting standard named networks. It detects hidden networks and the presence of non-beaconing networks via traffic.

- Robber: Open-source tool that helps attackers to find executalbes prone to DLL hijacking.
- CommView for WiFi: CommView for Wi-Fi is a wireless network monitor and analyzer for 802.11 a/b/g/n networks. It captures packets to display important information such as the list of APs and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for Wi-Fi can view and examine packets, pinpoint network problems, and troubleshoot software and hardware.
- WiFiFoFum: WiFiFoFum is a wardriving app to locate, display and map found WiFi networks. WiFiFoFum scans for 802.11 Wi-Fi networks and displays information about each including: SSID, MAC, RSSI, channel, and security. WiFiFoFum also allows you to connect to networks you find and log the location using the GPS. KML logs can be emailed.
- BlueScan: BlueScan is a bash script that implements a scanner to detect Bluetooth devices that are within the range of our system. BlueScan works in a non-intrusive way, that is, without establishing a connection with the devices found and without being detected. Superuser privileges are not necessary to execute it.
- WiFish Finder: WiFish Finder is a tool for assessing whether WiFi devices active in the air are vulnerable to 'Wi-Fishing' attacks. Assessment is performed through a combination of passive traffic sniffing and active probing techniques. Most WiFi clients keep a memory of networks (SSIDs) they have connected to in the past. Wi-Fish Finder first builds a list of probed networks and then using a set of clever techniques also determines security setting of each probed network. A client is a fishing target if it is actively seeking to connect to an OPEN or a WEP network.

- WarFlying: Attackers use drones to detect open wireless networks.
- WarWalking: Attackers walk around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.
- WarDriving: Attacker drive around with WiFi enabled laptops installed with a wireless discovery tool to map out open wireless networks.
- WarChalking: Symbols are drawn in public places to advertise open Wi-Fi networks.

1.16.5 Bluetooth Hacking

- Protocols:
  - Link management protocol (LMP): Used for control of the radio link between two devices, handling matters such as link establishment, querying device abilities and power control. It is implemented on the controller.
  - OBEX: Object Exchange protocol is used for communicating binary objects between devies. Bluejacking is sending anonymouse message to othe Bluetooth-equipped devices via the OBEX protocol
  - Logical link control and adaptation protocol (L2CAP): L2CAP passes packets to either the Host Controller Interface (HCI) or on a hostless system, directly to the Link Manager/ACL link.
  - Service Discovery Protocol (SDP): Is used to allow devices to discover what services each other support, and what parameters to use to connect to them.
- Non-pairable mode: In the non-pairable mode, a Bluetooth device rejects pairing requests sent by any device.
- Limited discoverable mode: In the limited discoverable mode, the Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions.
- Non-discoverable mode: Setting a Bluetooth device to the non-discoverable mode prevents that device from appearing on the list during a Bluetooth-enabled device search process. However, it remains visible to users and devices that were previously paired with it or know its MAC address.
- Discoverable mode: When Bluetooth devices are in the discoverable mode, they are visible to other Bluetooth-enabled devices. If a device attempts to connect to another, the device attempting to establish the connection must search for a device that is in the discoverable mode; otherwise, the device attempting to initiate the connection will not be able to detect the other device.
- BluePrinting: BluePrinting is a footprinting technique performed by an attacker in order to determine the make, device model, firmware version, etc. of the target Bluetooth-enabled device. Attackers collect such information from remote bluetooth devices and analyze them in an attempt to find out whether the devices are in the range of vulnerability to exploit.
- Bluejacking: Bluejacking is the use of Bluetooth to send messages to users without

the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking does not cause any damage to the receiving device. However, it may be irritating and disruptive to the victims. OBEX protocol.

- Bluebugging: Bluebugging is an attack in which an attacker gains remote access to a target Bluetooth-enabled device without the victim being aware of it. In this attack, an attacker sniffs sensitive information and might perform malicious activities such as intercepting phone calls and messages, forwarding calls and text messages, etc.
- BlueSniff: BlueSniff is a proof of concept code for a Bluetooth wardriving utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.

1.16.6 Wireless Security Tools and Hacking Countermeasures

- Countermeasures to prevent KRACK attacks:
  - Update all the routers and Wi-Fi devices with the latest security patches.
  - Turn on auto updates for all the wireless devices and patch the device firmware.
  - Avoid using public Wi-Fi networks.
  - Browse only secured websites and do not access sensitive resources when the device is connected to an unprotected network.
  - If there are IoT devices, audit the devices and do not connect to insecure Wi-Fi routers.
  - Always enable the HTTPS Everywhere extension.
  - Enable two-factor authentication.
  - Use a VPN to secure information in transit.
- SSID Cloaking: Used to keep default wireless messages from broadcasting the ID to everyone.
- RF Scanning: Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area.

- Wired Side Inputs: Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols.
- AP Scanning: Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface.
- Wireless control system: Provides the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, and set APs in the wireless IPS monitor mode.
- Wireless LAN controller(s): These controllers forward attack information from wireless IPS monitor-mode APs to the MSE and distributes configuration parameters to Aps.
- Mobility services engine: It is the central point of alarm aggregation from all controllers and their respective wireless IPS monitor-mode APs. Alarm information and forensic files are stored on the system for archival.
- Local mode AP: This mode provides wireless service to clients in addition to time-sliced rogue and location scanning.

1.17 Hacking Mobile Platforms

1.17.1 Mobile Platform Attack Vectors

- M1 - Improper Platform Usage: This category covers the misuse of a platform feature or the failure to use platform security controls. It includes Android intents, platform permissions, and the misuse of Touch ID, Keychain, or some other security control that is part of the mobile device's OS
- M3 - Insecure Communication: This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, and so on. Such flaws expose an individual user's data and can lead to account theft.
- M7 - Client Code Quality: This category covers "Security Decisions via Untrusted Inputs" and is one of the less frequently used categories. it is the catch-all for code-level implementation problems in the mobile client, which are distinct from server-side coding mistakes.
- M8 - Code Tampering: This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

1.17.2 Hacking Android OS

- Countermeasures that can help you to protect your Android device and the data stored on it from malicious users.
  - Enable screen lock for your phone.
  - Never root your android device.
  - Download apps only from official Android markets
  - Keep your device updated with Google Android anti-virus software.
  - Do not directly download APKs
  - Update the OS regularly
  - Use a free protector Android apps such as Android Protector, where you can assigne passwords to text messages, mail accounts, and so on.
  - Customize your locked home screen with the user information.
  - Enable encryption in your Android device to enhance its security.
  - Lock your apps that hold private information to prevent other from viewing it, using apps such as AppLock.
  - Enable GPS on your Android device for it to be tracked when lost or stolen.
  - Enable two-step verification on your Android mobile device.
  - Never root your Android device
  - Download apps only from official Android markets
  - Uninstall apps that invade your privacy
  - Encrypt all the Internet traffic through VPN services such as ExpressVPN and VyprVPN for Android.
  - Block all the ads displayed by apps
  - Enable two-step verification on your Android mobile device
  - Disable features such as SmartLock instead of passwords, and auto sign-in functionality.
  - Install password manager apps such as LastPass to manage passwords securely
  - Enable the screen pinning option to securely access Android apps

- Native libraries
  - Open Max AL: Companion API to OpenGL ES but used for multimedia (video and audio) rather than audio only.
  - Libc: Comprises System C libraries
  - FreeType: Meant for rendering fonts.
  - Surface Manager: Meant for display management.
  - SSL: meant for Internet security.
  - Open GL — ES: 2D and 3D graphics library
  - WebKit and Blink: Web browser engine to display HTML content.
  - SQLite: database engine used for data storage purposes.
- Storage:
  - Shared Preferences: Stores private parameters in key values pairs
  - Internal Storage: Private data on the deivce
  - External Storage: Public data on the shared external storage
  - SQLite Databases: Store structed data in a private database.
- Tools:
  - zANTI: android application which allows you to perform various attacks.
  - LOIC Low orbit ion cannon: mobile application that allows the attacker to perform DoS/DDoS attacks on the target IP address.
  - DroidSheep: simple Android tool for web session hacking (sidejacking).
  - TunesGo is an Android tool that has an advanced android root module that recognizes and analyzes your Android device and chooses the appropriate Android root plan for it automatically.
  - Orbot: proxy app that empowers other apps to use the internet more privately. Uses Tor to encrypt internet traffic and then hides it by bouncing through a series of computers around the world.
  - NetCut: Allows attackers to identify the target devices and block the access of Wi-Fi to the victim devices in a network.

- X-Ray: Android vulnerability scanning tool.

1.17.3 Hacking iOS

- Apricot: Web-based mirror operating system for all the latest iPhones
- Spyzie: attackers use various online tools such as Spyzie to hack the target iOS mobile devices. Allows attacker to hack SMS, call logs, app chats, GPS, etc.
- Cydia: Software application for iOS that enables a user to find and install software packages on a jailbroken iPhone.
- Hexxa Plus: a jailbreak repo extractor for iOS 13.2 which allows you to install themes, tweaks, and apps. Compatible with iOS 13, up to 13.2.3.
- xHelper: Android/Trojan.Dropper.xHelper is a variant of Android/Trojan.Dopper. The first noticeable characteristic of xHelper is the use of stolen package names. For Instance, xHelper uses package names starting with "com.muf". This package name is associated with a number of puzzle names found on Google Play, including a puzzle called New2048HD with the package name com.mufc.fireuvw.
- Trident: A sophisticated spyware that exploits vulnerabilities in an iPhone to spy on users. These vulnerabilities allow attackers to jailbreak the target iPhone remotely and install malicious spyware such as Pegasus. Trident is capable of taking complete control of the target mobile device, and it allows attackers to monitor and track all the user activities.
- Gustuff: A type of banking trojan that uses malicious SMS to compromise the security of the target Android mobile device.
- iOS layers:
  - Cocoa Application: This layer contains key frameworks that help in building iOS apps. These frameworks define the appearance of the apps, offer basic app infrastructure, and support key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. Cocoa apps use the AppKit framework.
  - Media: This layer contains the graphics, audio, and video technologies that enable multimedia experiences in apps.
  - Core OS: This layer contains low-level features on which most other technologies are based. Frameworks in this layer are useful when dealing explicitly with security or communicating with an external hardware and networks. The

services provided by this layer are dependent on the Kernel and Device Drivers layer

  - Core Services: This layer contains fundamental system services for apps. The key services are Core Foundation and Foundation frameworks (define the basic types that all apps use). Individual technologies that support features such as social media, iCloud, location, and networking belong to this layer

- untethered jailbreak: If the user turns the device off and back on, the device will start up completely, and the kernel will be patched without the help of a computer - it will be jailbroken after each reboot.
- semi-tethered jailbreak: has the property that if the user turns the device off and back on, the device will start up completely; it will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken addons, the user needs to start the device with the help of the jailbreaking tool.
- iOS jailbreaking tools:
  - Yalu
  - Velonzy
  - TaiG
- Unrevoked: Android Jailbreaking tool.
- Userland Exploit: uses a loophole in the system application. It allows user-level access but does not allow iboot-level access. you cannot secure iOS devices against this exploit, as nothing can cause a recovery mode loop. Only firmware updates can patch these types of vulnerabilities. iBoot Exploit and Bootrom Exploit allow user-level access and also iboot-level access.

1.17.4 Mobile Devices Management

- Tools:
  - XenMobile: Complete Mobile device management software
  - SpyBubble: Geolocation tracking
  - Phonty: Geolocation tracking
  - GadgetTrak: Geolocation tracking

1.17.5 Mobile Security Guidelines and Tools

- Tools:
  - Promon Shield: Promon SHIELD is used to protect mobile apps against repackaging attacks. It detects when an app has been modified (repackaged). Consequently, the original app that has Promon SHIELD™ implemented cannot be executed when repackaged
  - Lookout Personal: Lookout Personal helps to protect your device from security threats, loss, and theft. It is available for Android and iOS devices. It provides mobile security, identity protection, and theft prevention in a single app
  - Apktool: Apktool is used for reverse engineering third-party, closed, binary Android apps. It can decode resources nearly to their original form and rebuild them after making some modifications. It also makes working with an app easier because of the project-like file structure and automation of some repetitive tasks such as building APK, etc
  - FaceNiff: FaceNiff is an Android app that can sniff and intercept web session profiles over a Wi-Fi connection to a mobile.

1.18 IoT and OT Hacking

1.18.1 IoT Concepts

- Layers
  - Internet Layer: A crucial layer as it servers as the main component in carrying out communication between two endpoints, such as device-to-device, device-to-cloud, device-to-gateway, or back-end data sharing.
  - Access Gateway Layer: This layer helps to bridge the gap between two endpoints, such as a device and a client. The initial data handling also takes place in this layer. This layer carries out message routing, message identification, and subscribing.
  - Middleware Layer: This is one of the most critical layers that operates in two-way mode. It is responsible for important functions such as data management, device management, and various issues like data analysis, data aggregation, data filtering, device information discovery, and access control.
  - Edge Technology Layer: This layer consists of all the hardware components, including sensors, radio-frequency identification (RFID) tags, readers, or other

soft sensors, and the device itself.

  - Application Layer: This layer is placed at the top of the stack, is responsible for the delivery of services the the respective users from different sectors like building, industrial, manufacturing, automobile, security, healthcare, etc.

- Communication Protocol:

  - Very Small Aperture Terminal (VSAT): A communication protocol that is used for data transfer using small dish antennas for both broadband and narrowband data.

  - QUIC: Quick UDP Internet Connections (QUICs) are multiplexed connection between IoT devices over the User Datagram Protocol (UDP); they provide security equivalent to SSL/TLS.

  - Near-Field Communication (NFC): NFC is a type of short-range communication that uses magnetic field induction to enable communication between two electronic devices. It is primarily used in contactless mobile payment, social networking, and the indentifiaction of documents or other products.

  - Power-Line Communication (PLC): This is a type of protocol that uses electrical wire to transmit power and data from one endpoint to another. PLC is required for applications in deffernt areas such as home automation, industrial devices, and broadband over power lines (BPL).

  - Constrained Application Protocol (CoAP): A web transfer protocol used to transfer messages between constrained nodes and IoT networks.

  - LWM2M: Lightweight Machine-to-Machine (LWM2M): An application-layer communication protocol used for application-level communication between IoT devices.

  - XMPP: eXtensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication used for IoT devices. This technology is used for developing interoperable devices, applications, and services for the IoT environment.

  - Physical Web: technology used to enable faster and seamless interation with nearby IoT devices. It reveals the list of URLs being broadcast by nearby devices with BLE beacons.

- Contiki: Used in low power wireless devices such as street lighting, sound monitoring systems, etc.

- Edge: Edge computing helps the IoT environment to move computational processing to the edge of the network, allowing smart devices and gateways to perform tasks and services from the cloud end.
- Sensing Technology: Sensors embedded in the devices sense a wide variety of information from their surroundings like temperature, gases, location, working of some industrial machine as well as sensing health data of a patient.
- IoT Gateways: Gateways are used to bridge the gap between the IoT devices (internal network) and the end user (external network) and thus allowing them to connect and communicate with each other. The data collected by the sensors in IoT devices send the collected data to the concerned user or cloud through the gateway.
- Cloud Server/Data storage: the collected data after travelling through the gateway arrives at the cloud, where it is stored and undergoes data analysis. The processed data is then transmitted to the user where he/she takes certain action based on the information recieved by him/her.
- Remote Control using Mobile App: The end user uses remote controls such as mobile phones, tabs, laptops, etc. installed with a mobile app to monitor, control, retrieve data, and take a specific action on IoT devices from a remote location.

1.19 IoT Attacks

- Security issues at IoT layers:
  - Cloud: Improper authentication, no encryption for storage and communications, insecure web interface.
  - Mobile: Insecure API, lack of communication channels encryption, authenticationm lack of storage security.
  - Network: Firewall, improper communications encryption, services, lack of automatic updates.
  - Application: Validation of the inputted string, AuthN, AuthZ, no automatic security updates, default passwords.
- Insecure Data Transfer and Storage: Lack of encryption and access control of data that is in transit or at rest may result in leakage of sensitive information to malicious users.
- Insecure Network Services: Prone to various attacks like buffer overflow attacks,

which cause a denial-of-service scenario, thus leaving the device inaccessible to the user.

- Insecure Ecosystem Interfaces: Web, backend API, mobile, and cloud interfaces outside the devices lead to compromized security of the device and its components.
- Insecure Default settings: Insecure or insufficient device settings restrict the operators from modifying configurations to make the device more secure.
- Device Physical interface vulnerabilities:
  - Firmware extraction
  - User/Admin CLI
  - Privileged escalation
  - Reset to insecure state
  - Removal of storage media
  - Tamper resistance
  - Debug port: UART (Serial), JTAG/SWD
  - Device ID/serial number exposure.
- Device Web Interface Vulnerabilities:
  - Standard set of web application Vulnerabilities:
    * OWASP Web Top 10
    * OWASP ASVS
    * OWASP Testing Guide
  - Credential management vulnerabilities
  - Username enumeration
  - Weak passwords
  - account lockout
  - Known default credentials
  - insecure password recovery mechanism
- Device Firmware Vulnerabilities:

  - Sensitive data exposure (See OWASP Top 10 - A6 Sensitive data exposure):
    * Backdoor accounts
    * Hardcoded credentials
    * Encryption keys
    * Encryption (symmetric, asymmetric)
    * sensitive information
    * sensitive URL disclosure
  - Firmware version display and/or date of last update.
  - Vulnerable services (web, ssh, tftp, etc.)
    * Verify for old software versions and possible attacks (Heartbleed, Shellshock, old PHP versions, etc.)
  - Security-related function API exposure
  - Firmware downgrade possibility
- Network Traffic Vulnerabilities:
  - LAN
  - LAN to internet.
  - Short range
  - Non-standard
  - Wireless (Wi-Fi, Z-wave, XBee, Zigbee, bluetooth, LoRa)
  - Protocol fuzzing.
- Sybil Attack: The attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks.
- Exploitation Kits: The attacker uses malicious scripts to exploit poorly patched vulnerabilities in an IoT device.
- Side-Channel Attack: the attackeer extracts information about encryption keys by observing the emission of signals i.e. "side channels" from IoT devices.
- DNS Rebinding Attack: DNS rebinding is a process of obtaining access to a victim's router using a malicious JavaScript code on a web page.

- Hex Code: A color hex code is a way of specifying color using hexadecimal values. the code itself is a hex triplet, which represents three separate values that specify the levels of the component colors. It is used by programmers to describe locations in memory because it can represent every byte.
- Unicode: Character encoding system to support worldwide interchange, processing, and display of the written texts. This type of code is mostly used in evading IDS.
- Rolling Code: the form of a code from a modern key fob that locks or unlocks the vehicle. Here a code is sent to the vehicle which is defferent for every other use and is only used once, that means if a vehicle receives the same code again it rejects it. This code which locks or unlocks a car or garage is called as Rolling code or Hopping code. it is used in keyless entry systems to prevent replay attacks. An eavesdropper can capture the code transmitted and later use it to unlock the garage or vehicle.
- Polymorphic code: Code that uses a polymorphic engine to mutate while keeping the original algorithm intact. Polymorphic code can also be used to generate encryption algorithms.

1.20 IoT Hacking Methodology

- Phases:
  - Information Gathering
  - Vulnerability Scanning
  - Launching Attacks
  - Gaining Remote Access
  - Maintaining Remote Access
- Tools:
  - MultiPing: find the IP address of any IoT device in the target network.
  - RFCrack: Attackers use RFCrack to obtain the rolling code sent by the victim to unlock a vehicle and later use the same code for unlocking and stealing the vehicle.
  - FCC ID Search: Helps in finding the details and granted certification of devices. FCC ID contains two elements: Grantee ID (initial 3 or 5 characters) and Product ID (Remaining characters).

- IoT Seeker: will scan a network for specific types of IoT devices to detect if they are using the default, factory set credentials.
- Censys: A public search engine and data-processing facility backed by data collected from ongoing Internet-wide scans. Suports full-text searches on protocol banners and queries a wide range of derived fields. It can identify specific vulnerable devices and networks, and generate statistical reports on broad useage patterns and trends.
- RIoT: Vulnerability Scanner: Retina IoT identifies at-risk IoT devices, such as IP cameras, DVRs, printers, and routers. This tool gives an attacker's view of all the IoT devices and their associated vulnerabilities.
- Foren6: uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface. Captures all RPL-related information and identifies abnormal behaviors.
- Zigbee Framework: Attify ZigBee framework consists of a set of tools used to perform ZigBee penetration testing. ZigBee protocol makes use of 16 different channels for all communications. Attackers use Zbstumbler from Attify Zigbee framework to identify the channel used by the target device.
- HackRF One: Attackers use HackRF One to perform attacks such as BlueBorne or AirBorne attacks such as replay, fuzzing, jamming, etc. HackRF One is an advanced hardware and software defined radio with the range of 1MHz to 6GHz. It transmits and receives radio waves in half-duplex mode, so it is easy for attackers to perform attacks using this device.
- Smartpage: Meta search engine
- MetaGer: Meta search engine
- eTools.ch: Meta search engine
- Thingful: Search engine for finding and using open IoT data from around the world. Helps organizations make better decisions with external IoT data.
- beSTORM: smart fuzzer that detects buffer overflow vulnerabilities by automating and documenting the process of delivering corrupted inputs and watching for an unexpected response from the application
- RTL-SDR: hardware is available in the form of a USB dongle that can be used to capture active radio signals in the vicinity (an Internet connection is not mandatory).

  - Universal Radio Hacker (URH): a software of investigating unknown wireless protocols used by various IoT devices.

- firmware analysis steps
  - Obtain firmware
  - Analyze firmware
  - Extract filesystem
  - mount filesystem
  - analyze filesystem content
  - Emulate firmware for dynamic testing

1.21 IoT Countermeasures

- Lack of Secure Update Mechanism:
  - Verify the source and integrity of updates
  - Encrypt communication between endpoints
  - Notify end-users of security updates
- Lack of Physical Hardening:
  - Set unique password for BIOS/firmware
  - Configure device boot order to prevent unauthorized booting
  - Minimize the external ports such as USB ports
- Lack of Device Management:
  - Blacklist malicious devices from suspicious sources.
  - Validate all asset attributes.
  - Secure decommissioning of devices.
- Insecure default settings:
  - Changee the default usernames and passwords.
  - Custom modify the privacy and security settings.
  - Disable remote access to IoT devices when not in use.

- Insecure network services:
  - Close open network ports
  - disable UPnP
  - Review network services for vulnerabilities.
- Insecure Web Interface:
  - Enable default credentials to be changed.
  - Enbale the account lockout mechanism
  - Conduct periodic assessment of web applications
- Insufficient Authentication / Authorization:
  - Implement secure password recovery mechanisms
  - Use strong and complex passwords.
  - Enable two-factor authentication
- Lack of Transport Encryption / Integrity Verification:
  - Encrypt communication between endpoints.
  - Maintain SSL/TLS implementation
  - Not to use proprietary encryption solutions.
- Security Considerations:
  - Mobile: An ideal framework for the mobile interface should include proper authentication mechanism for the user, account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels and the security of the data transmitted over the channel.
  - Gateway: An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. Also, the authentication mechanism for the edge components should be as strong as any other component in the framework. Where ever possible the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

  - Cloud Platform: A secure framework for the cloud component should include encrypted communications, strong authentication credentials, secure web interface, encrypted storage, automatic updates and so on.
  - Edge: Framework consideration for edge would be proper communications and storage encryption, no default credentials, strong passwords, use latest up to date components and so on.

- Tools:
  - DigiCert IoT Security Solution: DigiCert Home and Consumer IoT Security Solutions protect private data and home networks while preventing unauthorized access using PKI-based security solutions for consumer IoT devices.
  - SeaCat.io: SeaCat.io is a security-first SaaS technology to operate IoT products in a reliable, scalable and secure manner. It provides protection to end users, business, and data.
  - Firmalyzer Enterprise: Firmalyzer enables device vendors and security professionals to perform automated security assessment on software that powers IoT devices (firmware) in order to identify configuration and application vulnerabilities. This tool notifies users about the vulnerabilities discovered and assists to mitigate those in a timely manner.

1.22 OT Concepts

- DCS: A Distributed Control System (DCS) is used to control production systems spread within the same gepgraphical location.
- BPCS: Basic Process Control System (BPCS) is responsible for performing process control and monitoring for industrial infrastructure.
- SIS: A safety instrumented System (SIS) is an automated control system designed to safeguard the manufactureing environment in case of any hazardous incident in industry.
- PLC: A programmable logic controller (PLC) is a small solid-state control computer where instructions can be customized to perform a specific task. PLC is a Operational Technology (OT) component.
- SCADA: Supervisory Control and Data Acquisition (SCADA) is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure.

- Purdue Model:
  - Level 0 (physiacl process): In this level, the actual physical process is defined, and the product is manufactured.
    - BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 62443, ISA SP100, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7 Communications, WiMax.
  - Level 1 (basic controls/intelligent devices): Analyzation and alteration of the physical process can be done at this level. The operations in basic control include "start motors", "open valves", "move actuators", etc.
    - BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 62443, ISA SP100, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7 Communications, WiMax.
  - Level 2 (Control Systems/Area Supervisory Controls): Supervising, monitoring, and controlling the physical process is carried out at this level.
    - Level 2 uses protocols such as 6LoWPAN, DNP3, DNS/DNSSEC, FTE, HART-IP, IEC 60870-5-101/104, SOAP.
  - Level 3 (Operational Systems/Site Operations): In this level, the production management, individual plant monitoring, and control functions are defined.
  - Level 4
    - DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi.
  - Level 5
    - DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi.
- ISA/IEC 62443: Provides a flexible framework for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems.
- ICCP (IEC 60870-6): ICCP (inter-control center communications protocol) (IEC 68070) provides a set of standards and protocols for covering ICS or SCADA communication in power system automation.
- IEC 61850: A common protocol that enables interoperability and communications between the IEDs at electrical substations.
- HSCP: Hybrid SCP (Secure Copy Protocol): is developed for transmitting larger file sizes at high speed on long-distance and wideband infrastructure.

1.23 OT Hacking Methodology and Countermeasures

- Tools:
  - CRITIFENCE: Online tool that allows attackers to discover the default credentials of a device or product simply by entering the device name or manufacturer name
  - GRASSMARLIN: Open source tool that passively maps and visually displays an ICS/SCADA network topology, while safely conducting device discovery, accounting and reporting on these critical cyber-physical systems.
  - SCADA Shutdown tool: An ICS testing and automation tool that allows attackers to fuzz, scan, and run remote commands on ICSs, SCADA networks and controllers.
  - Gqrx: An SDR implemented with the help of the GNU Radio and Qt GUI tool. Attackers use hardware devices such as FunCube dongles, Airspy, HackRF, and RTL-SDR along with Gqrx SDR, to analyze the spectrum.

1.24 Cloud Computing

1.24.1 Cloud Computing Concepts

- Cloud Deployment Models:
  - Public Cloud: In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet. Therefore, he is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform, IBM Bluemix).
  - Multi Cloud: It is a dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals. The multi cloud uses multiple computing and storage services from different cloud vendors. It distributes cloud assets, software, applications, etc. across various cloud-hosting environments.
  - Community Cloud: It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on- or off-premises and governed by the participated

organizations or by a third-party managed service provider (e.g., Optum Health Cloud, Salesforce Health Cloud).

  - Hybrid Cloud: It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but are bound together to offer the benefits of multiple deployment models. In this model, the organization makes available and manages some resources in-house and provides other resources externally (e.g., Microsoft Azure, Zymr, Parangat, Logicalis).

  - Private Cloud: Internal or Corporate Cloud is a cloud infrastructure that a single organization operates solely. The organization can implement the private cloud within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data.

- Cloud Storage Layers:

  - Front-end layer: accessed by the end user where it provides APIs for the management of data storage.

  - Middleware Layer: Performs several functions such as data de-duplication and replication of data.

  - Back-end layer: Where the hardware is implemented.

  - Application Layer: Is a cloud security control layer that includes software development lifecycle, binary analysis, scanners, web app firewalls, transactional sec, etc.

  -

- NIST Cloud Deployment Actors:

  - Cloud Carrier: Acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices.

  - Cloud Auditor: A party that performs an independent examination of cloud service controls to express an opinion thereon. Audits verify adherence to standards through a review of the objective evidence.

  - Cloud Consumer: A person or organization that maintains a business relationship with the cloud services providers (CSPs) and utilizes the cloud computing services.

  - Cloud Provider: A person or organization who acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to interested parties via network access.

- Infrastructure-as-a-service (IaaS): This cloud computing service enables subscribers to use on-demand fundamental IT resources, such as computing power, virtualization, data storage, and network. This service provides virtual machines and other abstracted hardware and operating systems (OSs), which may be controlled through a service application programming interface (API). As cloud service providers are responsible for managing the underlying cloud computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, GoGrid, Microsoft OneDrive, Rackspace).

- Platform-as-a-Service (PaaS): This type of cloud computing service allows for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations. This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications (e.g., Google App Engine, Salesforce, Microsoft Azure). Advantages of writing applications in the PaaS environment include dynamic scalability, automated backups, and other platform services, without the need to explicitly code for them.

- Software-as-a-Service (SaaS): This cloud computing service offers application software to subscribers on-demand over the Internet. The provider charges for the service on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users (e.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, and Freshbooks).

- Identity-as-a-Service (IDaaS): This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services. It provides services such as Single-Sign-On (SSO), Multi-Factor-Authentication (MFA), Identity Governance and Administration (IGA), access management, and intelligence collection. These services allow subscribers to access sensitive data more securely both on and off-premises (e.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, Okta).

- Anything-as-a-service (XaaS): also known as everything-as-a-service. Includes all the other types of cloud services.

- service Intermediation: Improves a given function by a specific capability and provides value-added services to cloud consumers.

- Service aggregation: Combines and integrates multiple services into one or more new services.
- Service Arbitrage: It is like service aggregation but without the fixing of the aggregated services (the cloud broker can choose services from multiple agencies).
- Distributed Storage: A characteristic of cloud computing that offers better scalability, availability, and reliability of data. However, cloud distributed storage can potentially raise security and compliance concerns.
- Automated Management: By minimizing user involvement, cloud automation speeds up the process and reduces labor costs and the possibility of human error.
- Measured Service: Cloud system employ the "pay-per-use" metering method. Subscribers pay for cloud services by monthly subscription or according to the usage of resources such as storage levels, processing power, and bandwidth. Cloud service providers monitor, control, report, and charge consumption of resources by customers with complete transparency.
- Virtualization Technology: Enables the rapid scaling of resources in a way that non-virtualized environments cannot achieve.
- Broad network access: Cloud resources are available over the network and accessed through standard procedures via a wide variety of platforms, including laptops, mobile phones, and personal digital assistants (PDAs).
- Rapid Elasticity: The cloud offers instant provisioning of capabilities to rapidly scale up or down, according to demand. To the consumers, the resources available for provisioning seem to be unlimited and can be purchased in any quantity at any point in time.
- Resource Pooling: Cloud service provider pools all the resources together to server multiple customers in the multi-tenant environment, with phtsical and virtual resources dynamically assigned and reassigned on demand by the consumer of the cloud.

1.24.2 Container Technology and Serverless Computing

- Container Technology Tiers:
  - Tier-1: Developer machines - image creation, testing and accreditation.
  - Tier-2: Testing and accreditation systems - Verification and validation of image contents, signing images and sending them to the registries.

  - Tier-3: Registries - Storing images and disseminating images to the orchestrators based on requests.
  - Tier-4: Orchestrators - Transforming image into containers and deploying containers to hosts.
  - Tier-5: Hosts - Operating and managing containers as instructed by the orchestrator.

- Container network model:
  - Sandbox: Comprises the container network stack configuration for the management of container interfaces, routing tables, and domain name system (DNS) settings.
  - Endpoint: To maintain application portability, an endpoint is connected to a network and is abstracted away from the application, so that services can implement different network drives.
  - Network Drivers: The network fucntions through the implementation of Docker network drivers. These drivers are pluggable so that multiple network drivers can be used concurrently on the same network. There are two types of CNM network drivers: namely native and remote network drivers.
  - IPAM Drivers: IP address management (IPAM) drivers assign default subnet and IP addresses to the endpoints and networks if they are not assigned.
  - Container Orchestration: an automated process of managing the lifecycles of software containers and their dynamic environments. It is used for scheduling and distributing the work of individual containers for microservices-based applications spread across multiple clusters.
  - Bridge: A component of docker native network drivers. A bridge driver is used to create a Linux bridge on the host that is managed by the Docker.
  - Network: A network is an interconnected collection of endpoints. Endpoints that do not have network connection cannot communicate over the network.

- Docker netowrk drivers:
  - Contiv: Open-source network plugin introduced by Cisco for building security and infrastructure policies for multi-tenant microservices deployments.
  - Weave: Network plugin that is used to build a virtual network for connecting Docker containers spread across multiple clouds.

  - Kuryr: A network plugin that implements the Docker libnetwork remote driver by using Neutron, an OpenStack networking service, and also includes a IPAM driver.
  - MACVLAN: used to create a network connection between container interfaces and the parent host interface or sub-interfaces using the Linux MACVLAN bridge mode. It is a native network driver of a Docker engine.
  - Host: By using a host driver, a container implements the host networking stack.
  - Overlay: An overlay driver is used to enable container communication over the physical network infrastructure.
  - None: A none driver implements its own networking stack and is isolated completely from the host networking stack.
- Domain Snipping: Involves registering an elapsed domain name
- Microservices: Monolithic applications are broken down into cloud-hosted sub-applications called microservices that work together, each performing a unique task. As each microservice is packaged into the Docker container along with the required libraries, frameworks, and configuration files, microservices belonging to a single application can be developed and managed using multiple platforms.
- Docker Engine Components:
  - Client CLI: the command line interface used to communicate with the daemon and where various Docker commands are initiated.
  - Rest API: allows the communication and assignment of tasks to the daemon.
  - Server: It is a persistent back-end process, also known as a daemon process (dockerd command).
  - Docker Swarm: The Docker engine supports the swarm mode that allows managing multiple Docker engines within the Docker platform. Docker CLI is used for creating a swarm, deploying an application to the swarm, and handling its activity or behavior.
  - Docker daemon: (dockerd) processes API requests and handles various Docker objects, such as containers, volumes, images, and networks.
  - Docker images: Used to store and deploy containters. They are read-only binary templates with instructions for container creation.

  - Docker registries: Locations where images are stored and pulled, and can be either private or public. Docker Cloud and Docker Hub are two popular public registries. Docker Hub is a predefined location of Docker images, which can be used by all users.
  - Docker Client: The primary interface through which users communicate with Docker. When commands such as docker run are initiated, the client passes related commands to dockerd, which then executes them. Docker commands use the Docker API for communication.

- Docker Objects:
  - Images: Used to store and deploy containers. They are read-only binary templates with instructions for container creation.
  - Services: Services enable users to extend the number of containers across daemons, and together they serve as a swarm with several managers and workers. Each swarm member is a daemon, and all these daemons can interact with each other using Docker API.
  - Networking: is a channel through which all isolated containers communicate.
  - Volumes: A storage where persisting data created by Docker and used by Docker containers are stored.

- Kubernetes Architecture:
  - Kube-proxy: A network proxy service that also runs on every worker node. This service maintains the network rules that enable network conncetion to the pods.
  - Etcd cluster: A distributed and consistent key-value storage where Kubernetes cluster data, service discovery details, API objects, etc. are stored. It is a master node component.
  - Container Runtime: A software designed to run the containers. Kubernetes supports various container runtimes, such as Docker, rktlet, containerd, and cri-o.
  - Kubelet: Kubelet is an important service agent that runs on each node and ensures containers running in a pod. It also ensures pods and containers are healthy and running as expected. Kubelet does not handle containers that are not generated by Kubernetes.

- Tools:

- Microsoft Azure Functions:
- Knative
- Red Hat OpenShift
- Portainer

1.24.3 Cloud Computing Threats

- DNS Poisoning: Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system.
- Cybersquatting: Involves conducting phishing scams by registering a domain name that is similar to a CSP.
- Domain Hijacking: Involves stealing a CSP domain name.
- Domain Snipping: Involves registering an elapsed domain name.
- Isolation failure: Multi-tenancy and shared resources are the characteristics of cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation among different tenants is lacking. Because of isolation failure, attackers try to control operations of other cloud customers to gain illegal access to the data.
- Privilege Escalation: A mistake in the access allocation system causes a customer, third party, or employee to get more access rights than needed.
- Illegal Access to the cloud: Attackers can exploit weak authentication and authorization to get illegal access, thereby compromising confidential and critical data stored in the cloud.
- Supply Chain Failure: A disruption in the chain may lead to loss of data privacy and integrity, unavailability of services, violation of SLA, economic and reputational losses resulting in failure to meet customer demand, and cascading failure.
- Abuse and Nefarious Use of Cloud services: Presence of weak registration systems in the cloud-computing environment gives rise to this threat. Attackers create anonymous access to cloud services and perpetrate various attacks such as password and critical cracking, building rainbow tables, CAPTCHA-solving farms, launching dynamic attack points, hosting exploits on cloud platforms, hosting malicious data, Botnet command or control, DDoS, etc.

- Insecure Interface and APIs: Attackers exploit user defined policies, reusable passwords/tokens, insufficient input-data validation.
- Data Breach/Loss: Attackers gain illegal access to the data and misuse or modify the data.
- Insufficient Due Diligence: Ignorance of CSP's cloud environment poses risks in operational responsibilities such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.
- Session Hijacking Using Session Riding: Attackers exploit websites by engaging in cross-site request forgeries to transmit unauthorized commands. In session riding, attackers "ride" an active computer session by sending an email or tricking users to visit a malicious web page, during login, to an actual target site. When users click the malicious link, the website executes the request as if the user had already authenticated it. Commands used include modifying or deleting user data, performing online transactions, resetting passwords, and others.
- Wrapping Attack: It is performed during the translation of SOAP messages in the TLS layer, where attackers duplicate the body of the message and send it to the server as a legitimate user.
- DNS Attack: The attacker performs DNS attacks to obtain authentication credentials from Internet users.
- Side Channel Attack: The attacker compromises the cloud by placing a malicious virtual machine near a target cloud server and then launches a side channel attack.
- Data remanence: Side channel attack
- Timing attack: side channel attack
- Acoustic cryptanalysis: side channel attack

1.24.4 Cloud Hacking

- Tools:
  - DumpsterDiver: autoamted tool to identify potential secret leaks and hardcoded passwords in cloud services.
- rabbit_lambda: An example lambda function that responds to user-delete events by creating more copies of the deleted user.

- cli_lambda: Lambda function that acts as an AWS cli proxy and does not require credentials.
- backdoor_created_roles_lambda: Lambda function that adds a trust relationship to each newly created role.
- backdoor_created_users_lambda: Lambda function that adda an access key to each newly created user.

1.24.5 Cloud Security

- Cloud Security Control Layer:
  - Tools:
    * Pacu: Open source AWS exploitation framework for enumerating and hijacking IAM roles.
    * Alcide Advisor: As Kubernetes is a de facto container deployment and management tool, its workloads need to be regularly monitored and secured with appropriate security implementations. Security professionals use tools, such as Kube-bench, Alcide Advisor, and StackRox, to secure the Kubernetes environment.
    * CloudGoat AWS: CloudGoat is Rhino Security Labs' "Vulnerable by Design" AWS deployment tool. It allows you to hone your cloud cybersecurity skills by creating and completing several "capture-the-flag" style scenarios
  - Application Layer: To harden the application layer, establish the policies that match the industry adoption security standards; e.g., OWASP for a web application. It should meet and comply with appropriate regulatory and business requirements. Application layer controls include software development lifecycle, binary analysis, scanners, web app firewalls, transactional sec, etc.
  - Information Layer: Develop and document an information security management program, which includes administrative, technical, and physical safeguards to protect information against unauthorized access, modification, or deletion. Some of the information layer security controls include data loss prevention (DLP), content monitoring and filtering, database activity monitoring, encryption, etc.
  - Management Layer: This layer covers the cloud security administrative tasks, which can facilitate continued, uninterrupted, and effective services of the cloud. Cloud consumers should look for the policies mentioned above to

avail better services. Some of the management layer security controls include governance-risk-compliance (GRC), IAM, VA/VM, patch management, configuration management, monitoring, etc.

- Network Layer: It deals with various measures and policies adopted by a network administrator to monitor and prevent illegal access, misuse, modification, or denial of network-accessible resources. Additional network layer security controls include network intrusion prevention/detection services, firewalls, deep packet inspection, anti-DDoS, quality of service (QoS), DNSSEC, and OAuth.
- Trusted Computing: Trust computing defines a secured computational environment that implements internal control, auditability, and maintenance to ensure the availability and integrity of cloud operations. Hardware and software RoT & API are a few security controls for trusted computing.
- Computation and Storage: CSPs must establish policies and procedures for data storage and retention and implement appropriate backup mechanisms to ensure availability and continuity of services that meet with statutory, regulatory, contractual, or business requirements and compliance. Host-based firewalls, host-based intrusion detection/prevention systems, integrity and file/log management, encryption, and masking are some security controls in computation and storage.
- Physical Layer: This layer includes security measures for cloud infrastructure, data centers, and physical resources. Security entities that come under this perimeter are physical plant security, fences, walls, barriers, guards, gates, electronic surveillance, CCTV, physical authentication mechanisms, security patrols, etc.
- Cloud Load Balancing: The process of distributing workloads and computing resources in a cloud computing environment. Load balancing allows enterprises to manage application or workload demands by allocating resources among multiple computers, networks, or servers. Cloud load balancing involves hosting the distribution of workload traffic and demands that reside over the internet.
- Detective Controls: Controls detect and react appropriately to the incidents that happen. For example, employing IDSs, IPSs, and so on helps to detect attacks on cloud systems.
- Deterrent Controls: These controls reduce attacks on the cloud system. Example: Warning sign on the fence or property to inform adverse consequences for potential attackers if they proceed to attack

- Preventive Controls: These controls strengthen the system against incidents, probably by minimizing or eliminating vulnerabilities. Example: Strong authentication mechanism to prevent unauthorized use of cloud systems.
- Corrective controls: These controls minimize the consequences of an incident, probably by limiting the damage. Example: Restoring system backups.

1.25 Cryptography

1.25.1 Cryptography Concepts

- Tools:
  - BCTextEncoder: The BCTextEncoder utility simplifies the encoding and decoding of text data. It compresses, encrypts, and converts plaintext data into text format, which the user can then copy to the clipboard or save as a text file. It uses public key encryption methods as well as password-based encryption. Furthermore, it uses strong and approved symmetric and public-key algorithms for data encryption.
  - Hash Droid: The Hash Droid utility helps to calculate a hash from a given text or a file stored on the device. In this application, the available hash functions are Adler-32, CRC-32, Haval-128, MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger, and Whirlpool
  - MD5 Calculator: MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with large files (e.g., several gigabytes in size). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 Calculator can be used to check the integrity of a file.
  - HashMyFiles: HashMyFiles is a utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in the system. It allows you to copy the MD5/SHA1 hash list to the clipboard or save it in a text/html/xml file. You can launch HashMyFiles from the context menu of Windows Explorer and display the MD5/SHA1 hashes of the selected files or folders.
- Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow. The third party can use or allow others to use the encryption keys under certain predefined circumstances.

1.25.2 Encryption algorithms

- Substitution Cipher: User replaces units of plain text with ciphertext according to a regular system. The units may be single letters, pairs of letters, or combinations of them, and so on.
- Block Cipher: Deterministic algorithms operating on a block (a group of bits) of fixed size with an unvarying transformation specified
- Transposition cipher: Here letters in plaintext are rearranged according to a regular system to produce the ciphertext. For example, "CRYPTOGRAPHY" when encrypted becomes "AOYCRGPTYRHP"
- Stream cipher: Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorndom cipher digit stream). Here, the user applies the key to each bit, one at a time. Examples include RC4, SEAL, etc.
- Camellia: Camellia is a symmetric-key block cipher having either 18 rounds (for 128-bit keys) or 24 rounds (for 256-bit keys). It is a Feistel cipher with a block size of 128 bits and a key size of 128, 192, and 256 bits. Camellia uses four 8x8-bit S-boxes that perform affine transformations and logical operations. A logical transformation layer FL-function or its inverse is applied every six rounds
- TEA: The tiny encryption algorithm (TEA) was created by David Wheeler and Roger Needham, and it was publicly presented for the first time in 1994. It is a simple algorithm, easy to implement in code. It is a Feistel cipher that uses 64 rounds
- GOST Block Cipher: The GOST (Government Standard) block cipher, also called Magma, is a symmetric-key block cipher having a 32-round Feistel network working on 64-bit blocks with a 256-bit key length. It consists of an S-box that can be kept secret and it contains around 354 bits of secret information. GOST is a simple encryption algorithm, where the round function 32-bit subkey modulo 232 is added and put in the layer of S-boxes and the rotate left shift operation is used for shifting 11 bits, thereby providing the output of the round function.
- Serpent: Serpent is a symmetric-key block cipher that was a finalist in the AES contest. This algorithm was designed by Ross Anderson, Eli Biham, and Lars Knudsen. It uses a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits. It can be integrated into software or hardware programs without any restrictions. Serpent involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit

- HSM: Hardware security module (HSM) is an additional external security device that is used in a system for crypto-processing and can be used for managing, generating, and securely storing cryptographic keys.
- TPM: Trusted platform module (TPM) is a crypto-processor or chip that is present on the motherboard that can securely store the enctyption keys, and it can perform many cryptographic operations.
- Elliptic Curve Cryptography (ECC): ECC is a modern public-key cryptography developed to avoid larger cryptographic key usage. The asymmetric cryptosystem depends on number theory and mathematical elliptic curves (algebraic structure) to generate short, quick, and robust cryptographic keys. RSA is an incumbent public-key algorithm, but its key size is large. The speed of the encryption always depends on the key size: a smaller key length allows faster encryption. To minimize the key size, elliptic curve cryptography has been proposed as a replacement for the RSA algorithm
- Quantum Cryptography: In quantum cryptography, the data are encrypted by a sequence of photons that have a spinning trait while traveling from one end to another end. These photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash. Here, vertical and backslash spins imply "ones," while horizontal and forward slash spins imply "zeros."
- Homomorphic Encryption: Homomorphic encryption differs from conventional encryption mechanisms, where math operations are performed to encrypt the plaintext. Homographic encryption allows users to secure and leave their data in an encrypted format even while it is being processed or manipulated. In this technique, encryption and decryption are performed by the same key holder
- Hardware-based Encryption: Hardware-based encryption is a technique that uses computer hardware for assisting or replacing the software when the data encryption process is being performed. Devices that offer encryption techniques can be considered as hardware-based encryption devices.
- MD5 is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. MD5 can be used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.
- MD6: It uses a Merkle-tree-like structure to allow for large-scale parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attacks.

- SHA-2: SHA2 is a family of two similar hash functions with different block sizes, namely SHA-256, which uses 32-bit words, and SHA-512, which uses 64-bit words. The truncated versions of each standard are SHA-224 and SHA-384.
- SHA-3: SHA-3 uses sponge construction in which message blocks are XORed into the initial bits of the state, which the algorithm then invertibly permutes. It supports the same hash lengths as SHA-2 but differs in its internal structure considerably from the rest of the SHA family.
- HMAC: Hash-based message authentication code (HMAC) is a type of message authentication code (MAC) that uses a cryptographic key along with a cryptographic hash function. It is widely used to verify the integrity of data and authentication of a message. This algorithm includes an embedded hash function such as SHA-1 or MD5. The strength of HMAC depends on the embedded hash function, key size, and size of the hash output.
- RIPEMD-160: RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. There exist 128-, 256-, and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. These algorithms replace the original RIPEMD, which was found to have a collision issue. They do not follow any standard security policies or guidelines.
- Diffie-Hellman (DH) groups allows two parties to establish a shared key over an insecure channel. It was developed and published by Whitfield Diffie and Martin Hellman in 1976. Actually, it was independently developed a few years earlier by Malcolm J. Williamson of the British Intelligence Service, but it was classified. There are multiple Diffie-Hellman groups:
  - Diffie-Hellman group 1—768 bit group
  - Diffie-Hellman group 2 —1024 bit group
  - Diffie-Hellman group 5—1536 bit group
  - Diffie-Hellman group 14—2048 bit group
  - Diffie-Hellman group 19—256 bit elliptic curve
  - Diffie-Hellman group 20—384 bit elliptic curve group

1.25.3 Public Key Infrastructure (PKI)

- Validation Authority (VA): Stores certificates (with their public keys)

- Certificate authority (CA): Issues and verifies digital certificates.
- Registration Authority (RA): Acts as the verifier for the certificate authority.
- End user: Requests, manages, and uses certificates.

1.25.4 Email and Disk Encryption

-

1.25.5 Cryptanalysis

- Ciphertext-only Attack: Ciphertext-only is less effective but much more likely for the attacker. The attacker only has access to a collection of ciphertexts. This is much more likely than known plaintext but is also the most difficult. The attack is completely successful if the corresponding plaintexts (or even better, the key) can be deduced.
- Chosen-plaintext Attack: A chosen plaintext attack is a highly effective type of cryptanalysis attack. In this attack, the attacker obtains the ciphertexts corresponding to a set of plaintexts of his/her own choosing. This allows the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key.
- Known-plaintext Attack: In this attack, the only information available to the attacker is some plaintext blocks along with the corresponding ciphertext and algorithm used to encrypt and decrypt the text. Using this information, the key used to generate the ciphertext is deduced so as to decipher other messages.
- Adaptive Chosen-plaintext Attack: In this type of attack, an attacker has complete access to the plaintext message including its encryption, and he/she can also modify the content of the message by making a series of interactive queries, choosing subsequent plaintext blocks based on the information from the previous encryption queries and functions.
- Differential Cryptanalysis: Differential cryptanalysis is a form of cryptanalysis applicable to symmetric-key algorithms. It was invented by Eli Biham and Adi Shamir. Essentially, it is the examination of differences in input and how that affects the resultant difference in the output. It originally worked only with chosen plaintext. It can also work with known plaintext and ciphertext
- Linear Cryptanalysis: Linear cryptanalysis is based on finding affine approximations to the action of a cipher. It is commonly used on block ciphers. This technique was invented by Mitsarue Matsui. It is a known plaintext attack and uses a linear

approximation to describe the behavior of the block cipher. Given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained

- Integral Cryptanalysis: Integral cryptanalysis was first described by Lars Knudsen. This attack is particularly useful against block ciphers based on substitution-permutation networks as an extension of differential cryptanalysis. The differential analysis looks at pairs of inputs that differ in only one bit position, with all other bits being identical.

- Frequency Analysis: Frequency analysis is a code breaking methodology which isthe study of the frequency of letters or groups of letters in a ciphertext. Frequency analysis of letters and words is another method used to crack ciphers. It works on the principle that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies

- Meet-in-the-Middle Attack: A meet-in-the-middle attack is the best attack method for cryptographic algorithms using multiple keys for encryption. This attack reduces the number of brute-force permutations required to decode text encrypted by more than one key. A meet-in-the-middle attack uses space-time trade-off; it is also a type of birthday attack because it exploits the mathematics behind the birthday paradox, and the attack consumes less time than an exhaustive attack. It is called a meet-in-the-middle attack because it works by encrypting from one end and decrypting from the other end, thereby meeting "in the middle." In the meet-in-the-middle attack, the attacker uses a known plaintext message and has access to both the plaintext as well as the respective encrypted text. It takes less time than an exhaustive attack and is used by attackers for forging signatures, even on digital signatures that use the multiple-encryption scheme.

- Hash Collision Attack: A hash collision attack is performed by finding two different input messages that result in the same hash output. For example, in a hash collision attack, "hash(a1) = hash(a2)", where a1 and a2 represent some random messages. Since the algorithm itself randomly selects these messages, attackers have no role in the content of these messages

- Side-Channel Attack: A side-channel attack is a physical attack performed on a cryptographic device/cryptosystem to gain sensitive information. Cryptography is generally part of the hardware or software that runs on physical devices

- DUHK Attack: Don't Use Hard-Coded Keys (DUHK) is a cryptographic vulnerability that allows attackers to obtain encryption keys used to secure VPNs and web sessions. This attack mainly affects any hardware/software using the ANSI X9.31

Random Number Generator (RNG). Pseudorandom number generators (PRNGs) generate random sequences of bits based on the initial secret value, called seed, and the current state. The PRNG algorithm generates cryptographic keys that are used to establish a secure communication channel over the VPN.

- Cryptool Project:
  - Cryptool 1 (CT1): It is written in C++ and is a Windows program. It supports classical and modern cryptographic algorithms (encryption and decryption, key generation, secure passwords, authentication, secure protocols, etc.). It is used to perform cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)
  - CrypTool 2 (CT2): It supports visual programming GUI and execution of cascades of cryptographic procedures. It runs under Windows.
  - JCrypTool (JCT): It allows comprehensive cryptographic experimentation on Linux, MAC OS X, and Windows. It also allows users to develop and extend its platform in various ways with their own crypto plug-ins.
  - CrypTool-Online (CTO): It runs in a browser and provides a variety of encryption methods and analysis tools.
- rubber hose attack: attackers extract cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture. Generally, people under pressure cannot maintain security, and they reveal secret or hidden information. Attackers torture the concerned person to reveal secret keys or passwords used to encrypt the information.
- Related key attack: The related-key attack is similar to the chosen plaintext attack, except that the attacker can obtain ciphertexts encrypted under two different keys. This is actually a very useful attack if one can obtain the plaintext and matching ciphertext. The attack requires that the differing keys be closely related, for example, in a wireless environment where subsequent keys might be derived from previous keys. Then, while the keys are different, they are close. Much like the ciphertext-only attack, this one is most likely to yield a partial break.

1.26 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.

1.27 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. This technique allows an attacker to access the victim's contact list, emails, text messages, photos, videos, business data, and so on stored on the device.
  - 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.

1.28 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.

1.29 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

1.30 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.
    *

1.31 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 Chapter 1: Introduction to Ethical Hacking

2.1.1 Information Security Overview

- Which of the following techniques does an attacker use to snoop on the communication between users or devices and record private information to launch passive attacks?
  - Eavesdropping
- Which element of information security does Authentication Header (AH) not address?
  - Confidentiality
    AH will digitally sign packets. That will allow the company to guarantee integrity, authenticity, and non-repudiation. The use of work folders will allow employees to gain access to data, even when the network connection fails. Direct access is used when connecting to the hosted network, not the cloud-based file servers.

2.1.2 Cyber Kill Chain Concepts

- Methodology:
  - Reconnaissance: An adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before attacking.
  - Weaponization: The 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.

- Delivery: Send weaponized bundle to the victim using email, USB, etc.
- Exploitation: Exploit a vulnerability by executing code on the victim's system.
- Installation: The adversary downloads and installs more malicious software on the target system to maintain access to the target netowrk for an extended period.
- Command and Control: The adversary creates a command and control channel, which establishes two-way communication between the victim's machine and adversary-controlled server to communicate and pass data back and forth. Actions on Objectives: Perform actions to achieve intended objectives/goals.

2.1.3 Hacking and Ethical Hacking Concepts

•

2.1.4 Information Security Controls, Laws and Standards

- Which of the following countries' cyber laws include the Patents (Amendment) Act, 1999; Trademarks Act, 1999; and The Copyright Act, 1957?
  - **India: The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957**
  - USA: The Lanham (Trademark) act (15 USC SS 1051 - 1127)
  - China: Copyright Law of the People's Republic of China (Amendments on October 27, 2001)
  - UK: The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002.
- If the final set of security controls does not eliminate all the risk in a system, what could be done next?
  - If the residual risk is low enough, it can be accepted.

2.2 Chapter 2: Footprinting and Reconnaisance

2.2.1 Footprinting Concepts

- What type of information is gathered by an attacker through Whois database analysis and tracerouting?

  - DNS records and related information

- A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching the bank employees time in and out, searching the bank's job postings (paying special attention to IT-related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

  - Passive information gathering

2.2.2 Footprinting Methodology

- Which of the following activities of an organization on social networking sites helps an attacker footprint or collect information regarding the type of business handled by the organization?

  - Background checks to hire employees.

- Which of the following Google search queries allows an attacker to identify the FTP servers of the target organization and identify sensitive directories on FTP?

  - type:mil inurl:ftp ext:pdf — ps

- Google search queires for VoIP footprinting:

  - `intitle:"Login Page" intext:"Phone Adapter Configuration Utility"`: Pages containing login portals

  - `inurl:/voice/advanced/ intitle: Linksys SPA configuration`: Find the Linksys VoIP router configuration.

  - `intitle:"D-Link VoIP Router" "Welcome"`: Pages containing D-Link login portals.

  - `intitle:asterisk.management.portal web-access`: Looks for the Asterisk management portal.

  - `intitle:"SPA504G Configuration"`: finds Cisco SPA504G Configuration Utility for IP phones.

  - `intitle:"Sipura.SPA.Configuration" -.pdf`: Finds configuration pages for online VoIP devices.

  - `inurl:8080 intitle:"login" intext:"UserLogin" "English"`: VoIP login portals.

  - `inurl:"NetworkConfiguration" cisco`: extract Cisco phone details.

- In website footprinting, which of the following information is aquired by the attacker when the examine the cookies set by the server?
  - Software in use and its behavior.

- Which of the following Google dorks is used by an attacker to find Cisco VPN client passwords?
  - `"[main]" "enc_GroupPwd=" ext:txt`

2.3 Chapter 3: Scanning Networks

2.3.1 Network Scanning Concepts and Tools

- Which of the following hping commands is used by an attacker to collect the initial sequence number?
  - `hping3 192.168.1.103 -Q -p 139 -s` Collects all of the TCP sequence numbers generated by the target host.
  - ACK scan on port 80: `hping3 -A 10.0.0.25 -p 80`
  - UDP scan on port 80: `hping3 -2 10.0.0.25 -p 80`
  - Firewalls and Timestamps: `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp` guesses the timestamp update frequency and uptime of the target host.
  - perform FIN, PUSH, and URG scans on port 80 on the target host. `hping3 -F -P -U 10.0.0`

- If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?
  - Hping

2.3.2 Host, Port and Service Discovery

- Which of the following ping methods is effective in identifying active hosts similar to the ICMP timestamp ping, specifically when the administrator blocks the conventional ICMP ECHO ping?
  - ICMP address mask ping sweep

- A hacker is attempting to check for all the systems alive in the network by performing a ping sweep. Which NMAP switch would the hacker use?
  - -sn (no port scan): This option tells Nmap not to do a port scan after host discovery and only print out the available hosts that responded to the host discovery probes. Often called a ping sweep.
- Which of the following scanning techniques is used by an attacker to check whether a machine is vulnerable to UPnP exploits?
  - SSDP scanning
- While performing a UDP scan of a subnetm you receive and ICMP reply of Code 3/Type 3 for all the pings you have sent out. What is the most likely cause of this?
  - UDP port is closed
  - If the port is open the target accepts the packet and does not send and response.
  - If no response is recieved the port is either open or filtered.
- You are performing a port scan with Nmap. You are in a hurry and conducting the scans at the fastest possible speed. What type of scan should you run to get very reliable results?
  - Connect scan.
- Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?
  - NMAP -PN -A -O -sS 192.168.2.0/24

2.3.3 OS Discovery and Scanning Beyond IDS/Firewall

- Which of the following is the active banner grabbing technique used by an attacker to determine the OS running on a remote target system?
  - TCP sequence ability test.

2.4 Chapter 4: Enumeration

2.4.1 Enumeration Concepts

-

2.4.2 NetBIOS and SNMP Enumeration

•

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.

2.5 Chapter 4: Enumeration

2.5.1 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

2.6 Chapter 5: System Hacking

2.6.1 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.

2.6.2 Maintaining Access

2.7 Sniffing

2.7.1 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.
  -

2.7.2 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

2.8 Social Engineering

2.8.1 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**

2.8.2 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.

2.9 Denial-of-Service

2.9.1 DoS/DDoS Concepts

2.9.2 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.

2.9.3 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.

2.10 Session Hijacking

2.10.1 Session Hijacking Concepts

-

2.10.2 Application Level Session Hijacking

"

-

2.10.3 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.

2.10.4 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.

2.10.5 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

2.11 Evading IDS, Firewalls, and Honeypots

2.11.1 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.

2.11.2 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

2.11.3 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

2.11.4 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.

2.11.5 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.

2.12 Hacking Web Servers

2.12.1 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

2.12.2 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

2.12.3 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

2.12.4 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

2.12.5 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

2.13 Web Applications

2.13.1 Web App Concepts

-

2.13.2 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.

2.13.3 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.

2.13.4 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

2.13.5 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.

2.14 SQL Injection

2.14.1 SQL Injection Concpets

- Which of the following system table does MS SQL Server database use to store metadata? Hackers can use this system table to acquire database schema information to further compromise the database.
  - sysobjects: contains a row for every object that has been created in the database, including stored procedures, views, and user tables.
- Which of the following methods carries the requested data to the webserver as part of the message body?
  - HTTP POST
- Which of the following is the most effective technique in identifying vulnerabilities or flaws in the web page code?
  - Code analysis

2.14.2 Types of SQL Injection

- What is the main difference between a "Normal" SQL injection and a "Blind" SQL injection vulnerability?
  - The vulnerable application does not display errors with information about the injection results to the attacker.
- In blined SQLi, attacker can steal data by asking a series of true or false questions through SQL statements. Select all the correct types of blind SQL injections.
  - Time Delay

- Boolean exploitation.

- Which of the following SQL queries is an example of a heavy query used in SQL injection?

  - The following query in Oracle takes a huge amount of time to execute:
    `SELECT count(*) FROM all_users A, all_users B, all_users C`

  - If an attacker injects a malicious parameter to the above query to perform a time-based SQL injection without using functions, then it takes the following form:
    `1 AND 1 < SELECT count(*) FROM all_users A, all_users B, all_users C`

  - The final resultant query takes the form:
    `SELECT * FROM products WHERE id=1 AND 1 < SELECT count(*) FROM all_users A,`

2.14.3 SQL Injection Methodology

- Which of the following countermeasures allows developers to protect PL/SQL code from SQL injection attacks?

  - Make use of bind parameters in dynamic SQL

2.14.4 SQL Injection Countermeasures

- Which of the following practices makes web applications vulnerable to SQL injection attacks?

  - Database server running OS commands.

- Which of the following commands has to be disabled to prevent exploitation at the OS level?

  - The xp_cmdshell option is an SQL server configuration option that enables system administrators to control whether the xp_cmdshell extended stored procedure can be executed on a system. Disable commands such as xp_cmdshell, as they can affect the OS of the system.

- Which of the following is a Snort rule that is used to detect and block an SQL injection attack?

  - Many of the common attacks use specific type of code sequences or commands that allow attackers to gain an unauthorized access to the target's system and data. These commands and code sequences allow a user to write Snort rules that aim to detect SQL injection attacks.

- Expression that can be blocked by Snort:
  - `/(%27)|(\')|(\-\-)|(\%23)|(#)/ix`
  - `/exec(\s|\+)+(s|x)p\w+/ix`
  - `/((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`
  - `alert tcp $EXTERNAL_NET and -> $HTTP_SERVERS $HTTP_PORTS`

2.15 Hacking Wireless Networks

2.15.1 Wireless Concepts

- In LAN-to-LAN Wireless Network, the APs provide wireless connectivity to local computers, and computers on different networks that can be interconnected?
  - True
- In which of the following processes do the station and access point use the same WEP key to provide authentication, which means that this key should be enabled and configured manually on both the access point and the client?
  - WEP encryption

2.15.2 Wireless Encryption

-

2.15.3 Wireless Threats

-

2.15.4 Wireless Hacking Methodology

-

2.15.5 Bluetooth Hacking

-

2.15.6 Wireless Security Tools and Hacking Countermeasures

-

2.16 Hacking Mobile Platforms

2.16.1 Mobile Platform Attack Vectors

- Which of the following categories of mobile risk covers "Security Decisions via Untrusted Inputs" and is one of the less frequently used categories?
  - Client Code Quality
- OWASP Top 10 Mobile Risk?
  1. Improper platform usage
  2. Insecure data storage
  3. Insecure communication
  4. Insecure authentication
  5. Insufficient cryptography
  6. Insecure authorization
  7. Client code quality
  8. Code tampering
  9. Reverse engineering
  10. Extraneous functionality

2.16.2 Hacking Android OS

-

2.16.3 Hacking iOS

- Which of the following statements is not true for securing iOS devices?
  - Jailbreak detection has to be enabled all the time in any iOS device. Disabling Jailbreaking detection in the device cannot secure the device from jailbreaking and once if jailbreaking has been performed on the device, the device can be prone to installation of applications from any untrusted sources and can also lead to various attacks that can cause data theft.

2.16.4 Mobile Devices Management

- Which of the following is the correct BYOD security guideline that an employee should follow to secure sensitive personal or corporate information stored on a mobile device?
  - Do not allow Jailbroken or rooted devices.
- Which of the following is not a feature of Mobile Device Management Software?
  - Sharing confidential data among devices and networks

2.16.5 Mobile Security Guidelines and Tools

-

2.17 IoT Attacks

2.18 IoT Countermeasures

- Which of the following practices helps security professionals in defending against IoT hacking?
  - Monitor traffic on port 48101
- Which of the following is a security consideration for the gateway component of IoT architecture?
  -

2.19 OT Concepts

- In which of the following attacks does an attacker use techniques such as timing analysis and power analysis to obtain critical information from a target industrial system?
  - Side-Channel Attack

2.20 OT Hacking Methodology and Countermeasures

- Nmap commands used by attackers to enumerate open ports and services of ICS/SCADA systems:
  - Identifying HMI systems: `nmap -Pn -sT -p 46824 <TargetIP>`
  - Scanning Siemens SIMATIC S7 PLCs: `nmap -Pn -sT -p 102 --script s7-info <Target`

- Scanning Ethernet/IP Devices: `nmap -Pn -sU 44818 --script enip-info <TargetIP>`
- Scanning Niagara Fox Devices: `nmap -Pn -sT -p 1911,4911 --script fox-info <Targe`

2.21 Cloud Computing

2.21.1 Cloud Computing Concepts

•

2.21.2 Container Technology and Serverless Computing

- Which of the following is the property of container technology that makes it less secure than vitual machines?

Virtual Machines	Conta
Heavyweight	Lightweight a
Run on independent operating systems	Share a single host
Hardware-based virtualization	OS-based vi
Slower provisioning	Scalable and real-
Limited performance	Native per
Completely isolated, making it more secure	Process-level isolatio
Created and launched in minutes	created and laun

2.21.3 Cloud Computing Threats

- In one of the following OWASP cloud security risks, unsecured data in transit are susceptible to eavesdropping and interception attacks. Which is this risk?
  - Service and data integration
- Which of the following is not a legitimate cloud computing attack?
  - Port scanning is correct because it is not an attack. It is used in information gathering. DoS/privilege escalation/MiTM are legitimate attacks because they are generally performed with malice so as to cause damage or steal information from an organization.

2.21.4 Cloud Hacking

- Which of the following information can be enumerated when an attacker runs the command

```
ps -ef | grep apiserver
```

in Kubernetes etcd?

- Location of the etcd server and PKI information

- Which of the following is the docker command used by an attacker to create a container from an image to exploit the docker remote api?

  - Get an image of Alpine Linux:
    `docker -H <Remote IP:Port> pull alpine`

  - Create a container from the image using the following command:
    `docker -H <Remote IP:Port> run -t -d alpine`

  - Run the ls command inside the container to retrieve files stored on the Docker host:
    `docker -H <Remote IP:Port> exec modest_goldstine ls`

  - Use Nmap to scan the host's internal network to identify running services:
    `docker -H <docker host> run --network=host --rm marsmensch/nmap -ox <IP Rang`

  - Retrieve MySQL database credentials?
    `/`

  - Steps to exploit misconfigured AWS S3 buckets:

    1. Identify S3 buckets
    2. Setup the AWS command-line interface
    3. Extract access keys
    4. Configure aws-cli
    5. Identify vulnerable S3 buckets
    6. Exploit S3 buckets

  - Steps to exploit AWS docker containers.

    1. Abuse AWS credentials
    2. Pull the target Docker image
    3. Create a backdoor image
    4. Push the backdoor Docker image

- In which of the following techniques does an attacker use lambda functions such as rabbit_lambda, cli_lambda, and backdoor_created_users_lambda to install a backdoor to AWS infrastructure

- Manipulating access keys.

2.21.5 Cloud Security

- Best practices for securing Docker environment:
  - Enable read-only mode on filesystems and volumes by setting the `--read-onlyflag`.
  - Limit resources such as memory, CPU, the maximum number of file descriptors, the maximum number of processes, and restarts to prevent DoS attacks.
  - Avoid exposing the Docker daemon socket because it is the basic entry point for the Docker API.
  - Always run Docker images with `--security-opt=no-new-privileges` to prevent privilege escalation attacks using setuid or setgid binaries.
  - Only use trusted Docker images because Docker images created by malicious users may be injected with backdoors. Regularly patch host OS and Docker with the latest security updates.
  - Use tools such as InSpec and DevSec to detect Docker vulnerabilities.
- Best practices for securing the Kubernetes environment:
  - Use the copy-then-rename method for log rotation to ensure that logs are not lost when restarting the kubelet.
  - Use kube-apiserver instances that maintain CRLs to check the presented certificates.
  - Use offensive security certified professional stapling to check the revocation status of certificates.
  - Use single encoding format for all configuration tasks because it supports centralized validation. Ensure proper validation of file contents and their path at every stage of processing. Avoid using legacy SSH tunnels because they do not perform proper validation of server IP addresses. Use secure TLS by default in development and production configurations to reduce vulnerabilities owing to misconfiguration.

2.22 Cryptography

2.22.1 Cryptography Concepts

-

2.22.2 Encryption algorithms

- Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?
  - 1025 bit key

2.22.3 Public Key Infrastructure (PKI)

-

2.22.4 Email and Disk Encryption

-

2.22.5 Cryptanalysis

- Mitigation techniques for side-channel-attacks include the following:
  - Use differential power analysis (DPA) proof protocols with delimited side-channel leakage characteristics and update the keys before the leakage accumulation is significant
  - Use fixed-time algorithms (i.e., no data-dependent delays)
  - Mask and blind algorithms using random nonces
  - Implement differential matching techniques to minimize net data-dependent leakage from logic-level transitions
  - Pre-charge registers and busses to remove leakage signatures from predictable data transitions
  - Add amplitude or temporal noise to reduce the attacker's signal-to-noise ratio

2.23 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