Module 1: Introduction to Echical Hacking

Essential Terminology

- **Hack Value:** A notion among hackers that something is worth doing or is interesting.
- **Vulnerability:** Existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system.
- **Exploit:** A breach of IT system security through vulnerabilities.
- **Payload:** Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer.
- **Zero-Day Attack:** An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability.
- **Daisy Chaining:** It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information.
- **Doxing:** Publishing personally identifiable information about an individual collected from publicly available databases and social media.
- **Bot:** A "bot" is a software application that can be controlled remotely to execute or automate predefined tasks.

Information Security

The information security is a state of well-being of information and infrastructure in which the possibility of theft, tampering , and disruption of information and services is kept low or tolerable.

Elements of Information Security

CIA triad

- **Confidentiality:** Assurance that the information is accessible only to those authorized to have access.
- **Integrity:** The trustworthiness of data or resource in terms of preventing improper and unauthorized changes.
- **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users.

Other

- **Authenticity:** Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine.

- **Non-Repudiation:** Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

The Security, Functionality, and Usability triangle

Security: Restrictions imposed on accessing the components of the system (restrictions).

Functionality: The set of features provided by the system (features).

Usability: The GUI components used to design the system for ease of use (GUI).

Information Security Attacks and Attack Vectors

- Attacks = Motive (Goal) + Method + Vulnerability
- A motive originates out of the notion that the target system stores or process something valuable and this leads to threat of an attack on the system
- Attackers try various tools and attacks techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Motives behind attacks:

- Disrupting business continuity
- Information theft and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Demanding reputation of the target
- Taking revenge
- Demanding ransom

Top InfoSec Threats

- Cloud Computing Threat
- Advanced Persistent Threats (APT): stealing information from the victim machine without the user being aware of it
- Viruses and Worms
- Ransomware

- Mobile Threats

Top InfoSec vectors:

- Botnet
- Insider Attack
- Phishing
- Web Application Threat
- IoT Threats

InfoSec Threats categories:

- Network Threats (spoofing, sniffing, ...)
- Host Threats (malware, dos, ...)
- Application Threats (auth attacks, SQL injection, ...)

Type of Attacks on a System:

- Operating System Attacks (OS vulnerabilities)
- Misconfiguration Attacks
- Application-Level Attacks (exploit the application)
- Shrink-Wrap Code Attacks (exploit the common vulnerable libraries)

ICT : Information and Communication Technologies

Classification of Attacks

- **Passive Attacks:** Do not tamper with the data and involve intercepting and monirotring network traffice and data flow on the target network. Such as sniffing and eavesdropping.
- **Active Attacks:** Tampter with the data in transit or disrupting the communication or services, such as DoS, MitM, Session Hijacking.
- **Close-in Attacks:** The attacker is in close physical proximity with the target, such as social engineering attack.
- **Insider Attacks:** Using privileged access to violate rules or intentionally cause a threat to…. Such as theft of devices, keyloggers, backdoor…
- **Distribution Attacks:** Attachers tamper with hardware or software prior to installation. Such as modification of software or hardware during production or distribution.

Cyber Kill Chain Methodology

- **Reconnaissance:** Gather data on the target to probe for weak points
- **Weaponization:** Create a deliverable malicious payload using an exploit and a backdoor
- **Delivery:** Send weaponized bundle to the civtim using email, USB, etc.
- **Exploitation:** Exploit a vulnerability by executing code on the victim's systerm
- **Installation:** Install malware on the target system
- **Command and Control:** Create a command and control channel to communicate and pass data back and forth
- **Actions on Objectives:** Perform actions to achieve intended objectives.

Water hole attack: Watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware.

TTPs: Patterns of activities and methods associated with specific threat actors or groups of threat actors.

- **Tactics:** Guidelines that describe the way an attacker performs the attack from beginning to the end.
- **Techniques:** Technical methos used by an attacker to achieve intermediate results during the attack.
- **Procedues:** Organizational approaches that threat actos follow to launch an attack.

Adversary Behavioral Identification

- Internal Reconnaissance
- Use of PowerShell
- Unspecified Proxy Activities
- Use of Command-Line Interface
- HTTP User Agent
- Command and Control Server
- Use of DNS Tuneling
- Use of Web Shell
- Data Staging

Indicators of Compromise (IoCs): Clues, artifacts, and pieces of forensic data found on the network or OS of an organization that…

Hacker Classes:

Black Hats, White Hats, Gray Hats, Suicide Hackers, Script Hiddies, Cyber Terrorists, State-Sponsored Hackers, Hacktivist (Individuals who promote a political agenda by hacking…)

Hacking Phase: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks

- **Reconnaissance:** Passive Reconnaissance and Active Reconnaissance. PR involves acquiring info without directly interacting with the target such as searching public records or news releases, AR involves directly interacting with the target by any means such as telephone calls.
- **Scanning:** Pre-attack phase. Port Scanner, Extract Info.
- **Gaining Access:** The atttacker obtains access to the OS or App on the target. Such as escalating privileges, password cracking, buffer overflow, DoS, Session Hijacking
- **Maintaining Access:** The attacker tries to retain their ownship of the system. Use the compromised system to launch further attacks
- **Clearing Tracks:** Hide malicious acts,overwrite the server, system, and application logs to avoid suspicion.

Information Assurance (IA): Assurance that integrity, availability, confidentiality and authenticity of info…

Defense-in-Depth: A security strategy in which several protection layers are placed throughout an information system. Prevent direct attacks

Risk: Degree of uncertainty or expectation that an adverse event may cause damage to the system.

- **RISK**= Threat x Vulnerabilities x Impact
- **RISK**= Threat x Vulnerabilities x Asset Value
- **Level of Risk**= Consequence x Likelihood
- **Likelihood:** The chance of the risk occurring
- **Consequence:** The severity of a risk event that occurs

Risk Management

Phase:

- **Risk Identification:** Identifies the sources…
- **Risk Assessment:** Assess the organization's risk…
- **Risk Treatment:** Selects and implements appropriate controls…
- **Risk Tracking:** Ensures appropriate controls are implemented…
- **Risk Review:** Evaluate the performance…

Cyber Threat Intelligence (CTI): Collection and analysis of info about threats and adversaries…

- **Types:** Strategic, Tatical, Operational, Taechnical
- **Threat Modeling:** A risk assessment approach
- **Process:** Identify security objectives, application overview, decompose the application, identify threats, identify vulnerbilities.
- **Incident Management:** A set of defined processes to identify, analyze, prioritize, and resolve security incidents…
- **Incident Handling and Response (IH&R):** The process of taking organized and careful steps when reacting to a security incident or cyberattack

PCI DSS (Payment Card Industry Data Security Standard): A proprietary information security standard for org that handle cardholder info….Apply to all entities involved in payment card processing.

ISO/IEC 27001:2013: Specifiy the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization

HIPAA (Health Insurance Portability and Accountability Act):

Electronic Transaction and Code Set Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the standards for enforcing all the **Administration Simplification Rules**

SOX (Sarbanes Oxley Act): Protect investors and the public by increasing the accuracy and reliability of corporate disclosures.

DMCA (The Digital Millennium Copyright Act): A United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization (WIPO)**. Define the legal prohibitions against the…

FISMA (Federal Information Security Management Act): Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operatrions and assets.

GDPR (General Data Protection Regulation): One of the most stringent privacy and security laws globally. Lecy harsh fines against those who violate its pricacy…

DPA (Data Protection Act 2018): Set out the framework for data protection law in the **UK.** Protect individuals concerning the processing of personal data.

Module 2: Footprinting and Reconnaissance

Terminology

- **Footprinting:** collect information about a target network.
- **Passive Footprinting:** collect without direct interaction. Such as search engines, Top-level Domains (TLDs) and sub-domains of a target through web services, social networking sites, competitive intelligence, monitor website traffic of the target
- **Active Footprinting:** collect with direct interaction, such as Harvesting email lists, Whois lookup, extracting DNS info, Traceroute analysis, social engineering, extracting metadata of published documents and files, searching for digital files, querying published name servers of the target
- **Social Network Footprinting:** get information about the target.
- **Website Footprinting:** Information about the target through web pages.

Methods

- Examining the web page's source code
- Examining cookies
- Extracting metadata of web sites
- Monitoring website for updates
- Tracking email
- Email header analysis
- Competitive Intelligence Gathering
- Monitoring website traffic
- Tracking online reputation
- WHOIS
- IP geolocation
- DNS footprinting

Information collected

- Organization Information (phone numbers, employee details, etc...)
- Relations with other companies
- Network Information (Domains, IPs, etc...)
- System Information (OSes, passwords)

Objectives of Footprinting:

- **Know Security Posture**: know the security posture of the target organization
- **Reduce Focus Area**: reduce the attackers focus area to a specific range of IP, network, domain names, etc...
- **Identify Vulnerabilities**: identify vulnerabilities in the target system
- **Draw Network Map**: draw a map or outline the target organization's network infrastructure

Footprinting Methodology

- Search engines
- Web services,
- Social networking sites,
- Website footprinting,
- Emai footprinting,
- DNS footprinting,
- Network footpringting,
- Through social engineering

Google Hacking

Operators (No spaces between the operator and the query):

- **cache:** - Display the web page stored in the google cache
- **link:** - List of web pages that have links to the specified web page
- **related:** - List of web pages that are similar to a specified web page
- **info:** - Presents some information that google has about the particular page
- **site:** - Restrict the results to those websites in the given domain
- **allintitle:** - Restricts the result to those websites with all of the search keywords in the title
- **intitle:** - Restrict the results to documents containing the search keyword in the title
- **allinurl:** - Restrict the results to those with all of the search keywords in the URL
- **inurl:** - Restrict the results to documents containing the search keyword in the URL
- **location:** - Find information for a specific location
- **intext:** - Restrict the results to documents containing the search keyword in the content

Google Hacking Database (GHDB): An authoritative source for querying the ever-widing scope of the Google search engine.

FTP Search Engines: Search for files located on FTP servers that contain valuable info. Such as NAPALM FTP Indexer, Global FTP Search Engine, and FreewareWeb FTP File Search.

IoT Search Engines: Crawl the Internet for IoT devices that are publicly accessible, such as Shodan.

SCADA: Supervisory Control and Data Acquisition

Findding a Company's TLDS and Sub-domains

- Sub-domains provide an insight into **different departments and business units**…
- **Sublist3r** python script can enumerates subdomains across multiple sources at once

Search on Social Networking Sites and People Search Services

- People search services: Such as Intelius (www.intelius.com)
- Gather people and email info from LinkedIn, using **theHarvester**

Determining the OS

- Netcraft, SHODAN, CENSYS

Competitive Intelligence Gathering: The process of idenfifying, gathering, analylzing, verifying, and using info about your competitors from resources. **Non-interfering** and **subtle** in nature

Website Footprinting: The monitoring and analysis of the target org's website for info

Tracking Email Communications: Monitor the delivery of emails

WHOIS: Whois databases are maintained by Regional Internet Registries and contain personal information of domain owner

whois uses TCP port 43.

Example on Linux:

whois danielgorbe.com

DNS footprinting: Reveal info about DNS zone data, including DNS domain names, computer names, IP address, and more.

DNS record types:

A: Points to a host's IP address

MX: Points to a domain's mail server

NS: Points to a host's name server

CNAME: Canonical naming allows aliases to a host

SOA: Indicate authority for domain

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

Example on Linux:

dig danielgorbe.com

Traceroute: Work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover…

Trace the path between you and your target computer.

Examples

On Windows: tracert 216.239.39.10

On Linux: tcptraceroute www.google.com/ traceroute www.google.com **(UDP Traceroute)**

Footprinting Tools

- **Maltego:** Be used to determine the relationships and real world links between people, groups, orgs, websites…
- **Recon-ng:** A web reconnaissance framework with independent modules and database interaction
- **FOCA (Fingerprinting Organizations with Collected Archives):** A tool used mainly to find metatada and hidden info in the document it scans.
- **OSRFramework:** Include applications related to username checking, DNS lookups, info leaks research, deep web search…

- **OSINT Framework:** An open source intelligence gathering framework that is focused on gathering info from free tools or resources.
- **Recon-Dog, BillCipher, theHarvester, Th3Inspector, Raccoon, Orb, PENTMENU**

Countermeasures

- Resctrict the employees' access to …
- Configure web servers to avoid info leakage
- Educate employee to use pseudonyms on blogs, groups…
- Limit amount of info published

Module 3: Scanning Networks

OSI Model

Layer	Name	Example protocols
7	Application layer	HTTP, SNMP
6	Presentation layer	MIME, ASCII
5	Session layer	SOCKS, NetBIOS
4	Transport layer	TCP, UDP
3	Network layer	IP, ICMP
2	Data link layer	MAC, ARP
1	Physical layer	ethernet, Wi-Fi

TCP/IP Model

Layer	Name	Example protocols
4	Application layer	HTTP, SNMP
3	Transport layer	TCP, UDP
2	Internet layer	IP, ICMP
1	Link layer	ARP, MAC

TCP Flags

- **SYN:** Initiates a connection between two hosts to facilitate communication
- **ACK:** Acknowledge the receipt of a packet
- **URG:** Indicates that the data contained in the packet is urgent and should process it immediately
- **PSH:** Instructs the sending system to send all buffered data immediately
- **FIN:** Tells te remote system about the end of the communication. In essence, this gracefully closes the connection
- **RST:** Reset a connection

TCP Session Establishment

- **Three-way Handshake**
- **Step1**: Bill to Sheela: SYN
- **Step2:** Sheela to Bill: SYN+ACK
- **Step3:** Bill to Sheela: ACK

TCP Session Termination

- Bill is the **client**, Sheela is the **server**
- Bill to Sheela: FIN
- Sheela to Bill: ACK
- Bill to Sheela: FIN
- Sheela to Bill: ACK

Scanning Tools

- **Nmap:** Inventory a network. Extract info such as live hosts, open ports, services, types of packet filters/firewalls, OS and its version…
- **Hping2/Hping3:** Command line network scanning and packet crafting tool for the TCP/IP protocol. Can be used for network security auditing, firewall testing, manual path MTU discovery, remote OS fingerprinting…
- **Metasploit:** An open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing.
- **NetScanTools Pro:** Assist attackers in automatically or manually listing IPv4/v6 addresses, hostnames, domain names, and URLs

Hping command

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
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`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and timestamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH, and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

Host Discovery Techniques

ARP Ping Scan:

- ARP request proble → ARP response
- NMAP: **-sn -PR** (-sn disables port scan)
- Efficient and accurate than other host discovery techniques
- Automatically handles ARP requests, retransmission, and timeout as its own direction.
- Useful for system discovery, where we may need to scan large address spaces
- Display response time or latency

UDP Ping Scan:

- UDP ping → UDP response
- NMAP: **-sn -PU**
- Behind firewalls with strict TCP filtering, leaving the UDP traffic forgotten

ICMP Ping Scan

- **ICMP ECHO Ping:**
    - Send ICMP ECHO requests to a host.
    - Useful for locating active devices or determining if the ICMP is passing through a firewall.
    - NMAP: **-sn -PE**
- **ICMP ECHO Ping Sweep:**
    - Determine the live hosts from a range of IP address

    - NMAP: **-sn -PE <IP Range>**
    - Tool: Angry IP Scanner
    - Countmeasures: Configure firewalls, IDS/IPS, Evaluate type of ICMP traffic…
- **ICMP Timestamp Ping:**
    - If the administrators block ICMP ECHO pings.
    - NMAP: **-sn -PP**
- **ICMP Address Mask Ping:**
    - If the administrators block ICMP ECHO pings.
    - NMAP: **-sn -PM**

TCP Ping Scan

- **TCP SYN Ping:**
    - Send empty TCP SYN packets, an **ACK response** means active host
    - NMAP: **-sn -PS**
- **TCP ACK Ping:**
    - Send empty TCP ACK packets, an **RST reponse** means active host
    - NMAP: **-sn -PA**

IP Protocol Scan:

- Send various probe packets using different IP protocols, **any response** means active host
- NMAP: **-sn -PO**

Common Ports and Services

- **ftp-data:** 20/tcp, data transfer
- **ftp:** 21/tcp, ftp command
- **ssh:** 22/tcp
- **telnet:** 23/tcp
- **smtp:** 25/tcp
- **domain:** 53/dual
- **sql*net:** 66/dual
- **tftp:** 69/dual, Trivial File Transfer
- **www-http:** 80/dual
- **kerberos:** 88/dual
- **pop3:** 110/tcp
- **nntp:** 119/dual, Usenet Network News Transfer
- **ntp:** 123/tcp, Network Time Protocol
- **netbios-ns:** 137/dual, Netbios Name Service
- **netbios-dgm:** 138/dual, Netbios Datagram Service
- **netbios-ssn:** 139/dual, Netbios Session Service
- **snmp:** 161/dual

- **snmp-trap:** 162/dual

Port Scanning Techniques

TCP Scanning

1: Open TCP Scanning Methods

- **1.1: TCP Connect/Full Open Scan:**
    - Detect when a port is open after completing three-way handshake
    - Establish a full connection and then close it by sending RST packet
    - Do not require superuser privileges
    - **Easily detectable and filterable**
    - OPEN: **three-way handshake and end it with RST packet**
    - CLOSED: **get a RST reponse**
    - NMAP: **-sT**

2: Stealth TCP Scanning Methods

- **2.1: Half-open Scan:**
    - Abruptly reset the TCP connection before the three-way handshake
    - Bypass firewall rules and logging mechanisms, hide themselves
    - OPEN: **two-way handshake, end it with RST packet**
    - CLOSED: get a **RST response**
    - NMAP: **-sS**

- **2.2: Inverse TCP Flag Scan**
    - Send TCP probe packets with a **TCP flag (FIN, URG, PSH)** set or with no flags
    - **No reponse** implies open port, **RST response** means closed port
    - Avoid many IDS and logging system, highly stealthy
    - Pros: **Requiring super-user privileges**
    - Cons: **Not effective against Windows hosts**

        - **2.2.1: XMAS Scan**
            - Send a TCP frame to a remote device with **FIN, URG, and PUSH** flags set
            - Will not work against any current version of MS Windows.
            - Pros: Avoid IDS and TCP three-way handshake
            - Cons: Works on the UNIX platform only

        - NMAP: **-sX**

    - **2.2.2: FIN Scan**

        - A Fin probe with the FIN TCP flag set
        - FIN scanning works only with OS uses an RFC 793-based TCP/IP implementation
        - NMAP: **-sF**

    - **2.2.3: NULL Scan**

        - A NULL probe with no TCP flags set
        - NMAP: **-sN**

    - **2.2.4: Maimon Scan**

        - Similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK
        - NMAP: **-sM**

- **2.3: ACK Flag Probe Scan**

    - Send TCP probe packets set with an ACK flag, and then analyze the header information (TTL and Window field) of received RST packets.
    - Can be used to check the filtering system of a target
    - NMAP: **-sA**
    - Filtered (stateful firewall is present): **No response**
    - Not filtered: **RST response**
    - Pros: Evade most IDS
    - Cons: Slow and can exploit only older OS with vulnerable BSD-derived TCP/IP stracks

        - **2.3.1: TTL-Based Scan**

            - NMAP: **-ttl [time] [target]**
            - Open: **Less than the boundary value**

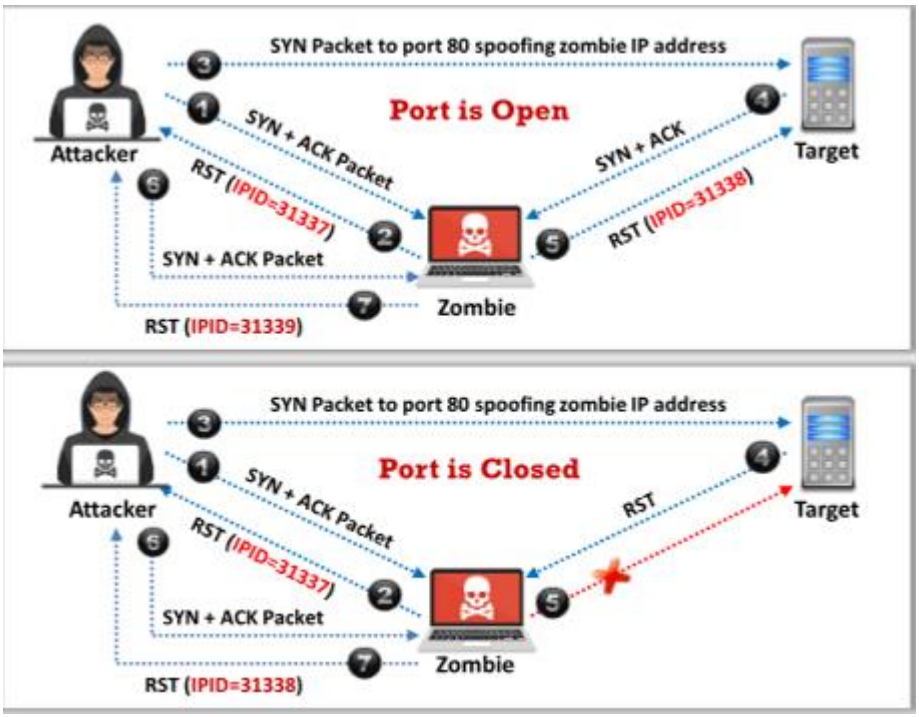
        - **2.3.2: Window Scan**

            - Open: **TCP RST with non-zero window field**
            - Closed: **TCP RST zero window field**
            - NMAP: **-sW**

3: Third Party and Spoofed TCP Scanning Methods

3.1: IDLE/IP ID Header Scan

- Every IP packet on the Internet has a fragment identification number (IPID); an OS increases the IPID for each packet send, thus, probing an IPID gives an attacker the number of packets send after the past probe.



- NMAP: **-sI**

UDP Scanning

1: UDP Scanning

- Open: **No response**
- Closed: **ICMP port unreachable message**
- NMAP: **-sU**
- Pros: Very efficiently on Windows devices
- Cons: Provide port info only.

SCTP Scanning

1: SCTP INIT Scanning

- SCTP: **Stream Control Transport Protocol,** a **reliable message-oriented transport layer protocol**, it is used as an alternative to the TCP/UDP protocol, its characteristics are similar to those of TCP and UDP
- **For-way handshake:**
- Step1: Cliend to Server: **INIT**

- Step2: Server to Client: **INIT-ACK**
- Step3: Client to Server: **COOKIE-ECHO**
- Step4: Server to Client: **COOKIE-ACK**
- Open: Attackers send an **INIT chunk** to the target host, and an **INIT+ACK chunk response** implies open port
- Closed: **ABORT Chunk** response
- Filter: **ICMP unreachable exception**
- NMAP: **-sY**

2: SCTP COOKIE/ECHO Scanning

- Open: Send a **COOKIE ECHO chunk** to the target host, **no response** implies open port
- Closed: **ABORT Chunk**
- Not blocked by non-stateful firewall rulesets
- Only a good IDS will be able to detect SCTP COOKIE ECHO chunk
- NMAP: **-sZ**
- Pros: Not as conspicuous as the INIT scan
- Cons: Cannot differentiate clearly between open and filtered ports, show open/filtered in both cases.

SSDP Scanning

1: SSDP and List Scanning

SSDP: **Simple Service Discovery Protocol**, a network protocol that **works in conjunction with the UPnP to detect plug and play devices**

- Vulnerabilities in UpnP may alllow attackers to launch **Buffer overflow or DoS attacks**
- Attacker may use the **UpnP SSDP M-SEARCH** info discovery tool to check if the machine is vulnerable to UPnP exploits or not.

List Scanning: Generate and print a **list of IPs/Names** without actually pinging them. **A reverse DNS resolution** is performed to identify the host names

- NMAP (List scanning): **-sL**
- Pros: Perform a good sanity check. Detect incorrectly defined IP addresses in the cmd line or in an option file.

Ipv6 Scanning

1: Ipv6 Scanning

- Harvest Ipv6 addresses from network traffic, recorded logs, or Received from: header lines in archived emails.

- NMAP: **-6**

Service Version Discovery

- Help attackers to obtain info about running service and their versions on a target system
- Determine the vulnerability or target system to particular exploits
- NMAP: **-sV**

Counter Port Scanning

- Configure firewall and IDS rules
- Filter all ICMP messages at the firewalls and routers
- Check network configuration, firewall configuration by scanning org's hosts
- Anti-scanning and anti-spoofing

OS Discovery

- **Active banner grabbing:** Specially crafted packets are send to remote OS and the responses are noted. Compare the responses with a database. Responses vary due to different TCP/IP implementation.
- **Passive banner grabbing:** From error messages, sniffing the network traffic, from page extensions, such as **.aspx→ IIS server and Windows platform**

Identify Target System OS

- Look at the **TTL** and **TCP window size** in the IP header of the first packet in a TCP session
- Use packet-sniffing tools such as Wireshark and observe the TTL and windows size fields.

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

- NMAP: **-O**
- Unicornscan: **unicornscan <target ip address>**
- NMAP Script Engine: **nmap –script smb-os-discovery.nse <target IP >**
- IPv6 use several **additional advanced probes specific to IPv6** along with **a separate OS detection engine that is specialized for IPv6**
- IPv6 Fingerprinting: **nmap -6 -O <target IP>**

Banner Grabbing Countermeasures

- Display **false banners** to mislead attackers
- Turn off unnecessary services
- Use **ServerMask** to disable or change banner info
- Hide file extensions to mask web technologies

IDS/Firewall Evasion Techniques

- **Packet Fragmentation:**

  Splitting of a probe packet into several smaller packets

  Not a new method but a modification of the precvious techniques

NMAP: **-f**

- **Source Routing:**

  Send a packet to the intended destination with a partially or competely specified route (without firewall/IDS-configured routers)

- **Source Port Manipulation:**

  Manipulate actual port numbers with common port numbers

  It occurs when a firewall is configured to allow packets from well-known ports such as HTTP, DNS, FTP…

  NMAP: **-g** or **–source-port**

- **IP Address Decoy:**

  Generate or manually specify the IP address of decoys

  The technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and…

  NMAP: **-D RND:10** or **-D decoy1, decoy2, decoy3…**

- **IP Address Spoofing:**

  Change the source IP address

  The reply return to the spoofed address rather than the attacker's

  The attacker modify the address info in the IP packet header and the source address bits field

  Hping3: **Hping3 <targe addresst> -a <spoofed address>**

  Detections of IP Spoofing:

  Direct TTL Probes: Send a packet to the host of a suspented spoofed packet, compare the TTL, **successful when the attacker is in a different subnet from that of the victim**

  IP Identifacation Number: Send a probe, compare IPIDs. **Reliabled even if the attacker is in the same subnet.**

  TCP Flow Control Method: Attackers will not receive SYN-ACK packets from the target, therefore attackers cannot respond to a change in the congestion window size.

When received traffic continues after a window size is exhausted, the packets are most likely spoofed.

Window size field represents the maximum amount of data that the recipient can receive and the maximum amount of data that the sender can transmit without ack. The sender should stop sending data whenever the window size is set to 0.

IP Spoofing Countermeasure

Encryption all the network traffic such as IPsec, TLS, SSH, HTTPS

Use multiple firewalls

Do not reply on IP-based authentication

Use a random **ISN (initial sequence number)**

Ingree Filtering

Egress Filtering

- **Creating Custom Packet:**

  Create custom TCP packets using various packet crafting tools like Colasoft Packet Builder, NetScanTools Pro

  NMAP: **nmap <target address> --data 0xdeadbeef** (Append Custom Binary Data)

  namp <target address> --data-string "Ph34r my l33t skills" (Regular string as payloads)

  nmap <target address> --data-string 5 (Append Random Data)

- **Randomizing Host Order:**

  Scan the number of hosts in random order

  NMAP: **nmap –randomize-hosts <target host>**

- **Send Bad Checksum:**

  Send packets with bad or bogus TCP/UDP checksums

  NAMP: **nmap –badsum <target>**

- **Proxy Server:**

  An application serve as an intermediary for connecting..

  hide the actual source of a scan, evade certain IDS/firewall restrictions

  Mask the actual source of an attack by impersonating the fake source address of the proxy

  Remotely access intranets and other website resources that restrcited

  Interrupt all requests sent by a user and tranmit them to a third destination such that victims can only idenfity the proxy server address

  Chain multiple proxy servers to avoid detection

  Proxy Chaining:

  Step1: User requests a resource from the dest

  Step2: Proxy client at the user's system connects to a proxy server and passes the request to proxy server

  Step3: The proxy server strips the user's id info and passes the request to next proxy server

  Step4: The process is repeated by all the proxy server in the chain

  Step5: At the end, the unencrypted request is passed to the web server

  Proxy Tools: Proxy Switcher, CyberGhost VPN…

- **Anonymizers:**

  Remove all id info from the user;s computer

  Make activity on the Internet untraceable

  Allow you to bypass Internet cernsor

  Why use?

  Privacy and anoymity, Protection against online attacks, Access restricted content, Bypass IDS and firewall rules.

  Censorship Circumvention Tools: Alkasir, Tails

  Anonymizers: Whonix, Psiphon

Network Discovery and Mapping Tools

- Discover a network and produces a comprehensive network diagram.
- Display in-depth connections such as **OSI Layer2 and Layer3** topology data

Module 04 : Enumeration

Concept

- Enumeration: An attacker **creates avtive connections** with a target system and perform **directed queries** to gain more info about the target
- Identify points for a system attack and perform password attacks to...
- Conducted in an **intranet environment**
- Enumerated information:
    - Network resources
    - Network shares
    - Routing tables
    - Audit and service settings
    - SNMP and FQDN (Fully Qualified Domain) details
    - Machine names
    - Users and groups
    - Applications and banners
- Techniques:
    - Extract usernames using **email IDS**
    - Extract info using **default passwords**
    - Brute force **AD**
    - Extract info using **DNS Zone Transfer**
        - Replicate DNS datra across several DNS servers or back up DNS files
        - using **nslookup** and **dig** commands
    - Extract **user groups** from Windows
    - Extract usernames using **SNMP**

Services and Ports to Enumerate

- TCP/UDP 53: DNS Zone Transfer
- TCP/UDP 135: MS RPC Endpoint Mapper
- UDP 137: NBNS (NetBIOS Name Service)
- TCP 139: NetBIOS Session Service (SMB over NetBIOS)

- TCP 445: SMB over TCP (Direct Host)
- UDP 161: SNMP
- TCP/UDP 390: LDAP
- TCP 2049: NFS (Network File System)
- TCP 25: SMTP
- TCP/UDP 162: SNMP Trap
- UDP 500: ISAKMP (Internet Security Association and Key Management Protocol) /IKE (Internet Key Exchange)
- TCP 22: SSH
- TCP 23: Telnet
- TCP 20/21: FTP
- TCP/UDP 5060,5061: SIP (Session Initation Protocol)
- TCP/UDP 3268: Global Catalog Service
- UDP 69: TFTP (Tricial File Transfer Protocol)
- TCP 179: BGP (Border Gateway Protocol)

NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII char string used to identify the network devices over TCP/IP
- Attackers use it to obtain the **list of computers belongs to a domain**, the **list of shares on the individual hosts in the network**, **policies and passwords**
- command: **nbtstat -a <target>** -> obtain the NetBIOS name table of a remote computer
- command: **nbtstat -c** -> obtain the contents of the NetBIOS name cache, table of NetBIOS names, and their resolved IP address
- Tools:
    - **NetBIOS Enumerator:** Help to enumerate details such as NetBIOS names, usernames, domain names, Mac address…
    - **Nmap: nbstat NSE script** allow attackers to retrieve target's NetBIOS names and MAC address
    - NMAP**: nmap -sV-v –script nbstat.nse <target>**

Enumerating User Accounts

- Use **PsTools** suite helps to control and manage remote systems from the command line

Enumerating Shared Resources Using Net View

- It is used to obtain a list of all the **shared resources of a remote host or workgroup**
- command: **net view \\<computername> net view /domain: <domain name>**

SNMP Enumeration

- The process of enumerating user accounts and devices on a target system using SNMP
- Agents are embedded on each network device, manager is on a separate computer
- SNMP holds **two passwords**. **Read community string**, it is public by default and allows for the veiwing of the device configuration. **Read/Write community string**: It is private by default and allows remote editing of configuration
- Attacker extract info about **network resources** (hosts, routers, devices, shares), **network info** (ARP tables, routing tables, traffic)

Management Info Base (MIB)

- A virtual database containing **a formal description of all the network objects** that can be managed using SNMP
- It is hierarchical, each managed object in a MIB is addressed through **OIDs (Object Identifiers)**

SNMP Enumeration Tools

- **Snmpcheck:** Allow one to enumerate the SNMP devices and place the output…
- **SoftPerfectNetworkScanner:** Discover shared folders and retrieve practically any info about the network device via WMI (Windows Management Instrumentation), SNMP, HTTP, and PowerShell

LDAP Enumeration

- **An internet protocol** for accessing distributed directory services

- A client starts a LDAP session by connecting to a **directory system agent (DSA)** on **TCP 389** and then sends an operation request to the DSA
- Transmitted info using **BER (Basic Encoding Rules)**
- Attacker query the LDAP service to gather info, such as **valid usernames, addresses, and departmental details**
- Tools: Softerra LDAP Administrator, LDAP Admin Tool…

NTP and NFS Enumeration

- NTP is designed to **synchronize the clocks** of networked computer, using **UDP 123**
- Attackers query the NTP server to obtain info such as list of connected hosts, clients IP address in a network, their system name, and OS
- Internal IPs can be obtained if the NTP server is in the DMZ
- NTP Enumeration Commands:
    - **ntptrace:** Trace a chain of NTP server back to the primary source
    - **ntpdc:** Monitors operation of the NTP daemon, ntpd
    - **ntpd:** Monitor NTP daemon (ntpd) operations and determines performance
    - **ntpdate:** Collect the number of time samples from several time sources
- NTP Enumeration Tools: PRTG Network Monitor, NMAP, Wireshark, NTP Server Scanner
- NFS enumeration enables attackers to identify the **exported directories, list of clients and their IP address, and the shared data**.
- command: **showmount -e <Target Address>** -> view the list of shared files and dirs
- command: **rpcinfo -p <Target Address> ->** scan the target address for an open NFS port and the NFS services running on it
- NFS Enumeration Tools: RPCScan, SuperEnum

SMTP Enumeration

- Provide **3 built-in-commands**:
    - **VRFY**: Validate users
    - **EXPN**: Show the actual delivery addresses of ailiases and mailling lists
    - **RCPT TP**: Define the recipients of a message
- Attackers can directly interact with SMTP via the **telnet** prompt and collect **a list of valid users** on the SMTP server
- Tools: NetScan Tools Pro, smtp-user-enum

DNS Enumeration Using Zone Transfer

- If the target DNS serverr allow zone transfer, attackers can use this technique to obtain **DNS server names, hostnames, machine names, usernames, IP address, aliases,** etc...
- Tools: **nslookup, dig, and DNSRecon**
- dig command: **dig ns <target domain>**
- nslookup command: **nslookup set querytype=soa (Start of Authority) <target domain>**
- DNSRecon command: **dnsrecon -t axfr -d <target domain>**
- DNS Cache Snooping: A DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.
- **Non-recursive Method** and **Recursive Method**
- **DNSSEC Zone Walking: A DNS enumeration technique** where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured.
- **LDNS** and **DNSRecon,** to exploiot this vulnerability and obtain the network info

IPSec Enumeration

- IPSec uses **ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange)** to secure communication between VPN end points
- NMAP: **nmap -sU -p 500 <target address>** ->perform an Nmap scan for checking the status of ISAKMP over port 500
- **ike-scan -M <target gateway address>**

VoIP Enumeration

- VoIP uses **SIP (Session Initation Protocol)** to enable voice and..
- UDP/TCP ports 2000, 2001, 5000, 5061
- Provide sensitive info such as **VoIP gateway/servers, IP-PBX system, client software, user extensions, IP...**
- This info can be sued to launch VoIP attacks such as **DoS, Session Hijacking, Caller ID spoofing, Evaesdropping, SPIT (Spamming over the Internet Telephone), and VoIP phishing (Vishing)**
- Tool command: **svmap <target network range>**

RPC Enumeration

- Allow clients and servers to communicate in distributed client/server programs

- Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports.
- NMAP: **nmap -sR <Target address>** / **nmap -T4 -A <Target address>**

Unix/Linux User Enumeration

- **rusers:** Display a list of users who are logged on to remote machines or local network machines
- **rwho:** Display a list of users who are logged on to hosts on the local network
- **finger:** Display info about system users, such as login name, real name, terminal name, idle time…

Telnet and SMB Enumeration

- Attackers can access shared info, including the hardware and software info of the target it the Telnet port is found open
- Enable attackers to **exploit identifid vulnerabilities** and perform **brute-force attacks** to gain unauthorized…
- Attacks use SMB enumeration tools, such as **Nmap, SMBMap, enum4linux**, and nullinux, to perform a directed scan on the SMB service running on port 445
- Help attacks to perform **OS banner grabbing** on the garget

FTP and TFTP Enumeration

- FTP transfers data in plain text
- Attacker use Nmap to scan and enumerate open port 21
- Attackers perform TFTP enumeration using **PortQry** and **Nmap**, to extract info such as running TFTP services and files stored on the remote server

BGP Enumeration

- Using Nmap and BGP Toolkit to discover the IPv4 prefixes announced by the **AS (Autonomous System)** number and routing path followed by the target

Enumeration Countermeasures

- ### SNMP
    - Remove the SNMP agent or turn off the SNMP service
    - Change the default community string names
    - Upgrade to SNMP3, which encrypts passwords and meesages

- **DNS**
    - Disable the DNS zone transfer to the untrusted hosts
    - Use premium DNS registration servies
    - Use standard network admin contacts for DNS registrations
    - Ensure the private hosts and their IP are not published in DNS zone files of public DNS servers
- **SMTP**
    - Ignore email messages to unknown recipents
    - Exclude sensitive mail server and local host info in mail responses
    - Disable open relay feature
    - Limit the number of accepted connections from a source to prevent brute-force attacks
- **LDAP**
    - Use SSL or STARTTLS technology to encrypt the traffic
    - Select a username different from your email address and enable account lockout
    - Use NTLM or any basic authentication mechanism to limit access to legitimate users only
- **SMB**
    - Disable SMB procotol on Web and DNS servers
    - Disable SMB protocol on Internet facing servers
    - Disable ports TCP 139 and TCP 445
    - Restrict anomymous access
- **NFS**
    - Implement proper permissions on exported files systems
    - Implement firewall rules to block NFS port 2049
    - Proper configuration of files
    - Log requests to access system files on the NFS server
- **FTP**
    - Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which use SSL)
    - Strong password or a certification-based authentication policy

- Ensure that unrestricted uploading of files on the FTP server is not allowed
- Disabled anomyous FTP accounts
- Restrict access by IP or domain name to the FTP server

Module 05: Vulnerability Analysis

Vulnerability Research

- The process of analyzing protocols, services, and configurations to discover vulnerabilities and design flaws that will expose an OS and its applications to exploit, attack, or miuse.
- Classfied based on severity level and exploit range (local, remote)

Vulnerabilities Assessment

- An in-depth examination of the ability of a system or application, including current security procedures and cointrols, to withstand the exploitation.
- Recognize, measure, and classfy security vulnerabilities in a computer system, network, and communication channels.

Vulnerability Scoring System and Databases

- **CVSS**: Common Vulnerability Scoring System, provide an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- **CVE**: Common Vulnerabilities and Exposures, a publicly available and free-to-use list od dic of standardized identifiers for common…
- **NVD**: National Vulnerability Database, a **US government repository** of standards-based vulnerability management data represented using the **SCAP (Security Content Automation Protocol)**
- **CWE:** Common Weakness Enumeration, **a category system** for software vulnerabilities and weaknesses.

Vulnerability Assessment Life-Cycle

- Identifies assets and create a baseline
- vulnetability scan
- risk assessment
- remediation
- verification
- monitor

Vulnerability Classfication

- Misconfiguration
- Default Installation
- Buffer Overflow
- Unpatched Servers
- Design Flaws
- OS Flaws
- Application Flaws
- Open Services
- Default Passwords

Types of Vulnerability Assessment

- **Active Assessments** : actively sending requests to the live network and examining the the responses. It requires probing the target host.
- **Passive Assessments** : includes packet sniffing to discover vulnerabilities, running services, open ports, and others. It is a process without interfering the target host.
- **External Assessment** : find out vulnerabilities and exploit them from outside.
- **Internal Assessment** : find and exploit vulnerabilities in the internal network.
- **Host-based Assessment…**
- **Network-based Assessment…**
- **Application Assessment…**
- **Database Assessment…**
- **Wireless Network Assessment…**
- **Distributed Assessment…**
- **Credentialed Assessment…**
- **Non-credentialed Assessment…**
- **Manual Assessment…**
- **Automated Asssessment…**

Vulnerability Assessment Solutions

Product based solution vs Service based solution

- **Product based solutions** are deployed within the network. Usually dedicated for internal network.

- **Service based solutions** are third-party solutions which offers security and auditing. This can be host either inside or outside the network. This can be a security risk of being compromised.

Tree-based Assessment vs Inference-based Assessment

- **Tree-based Assessment** is the approach in which auditor follows different strategies for each component of an environment
- **Inference-based Assessment** is the approach to assist depending on the inventory of protocols in an environment

Vulnerability Assessment Tools

- **Qualys Vulnerability Management:** A cloud-based service that offers…
- **Nessus Professional:** An assessment solution for identifying the…
- **GFI LanGuard:** Scan, detect, assesses and retifies security vulnerabilities…
- **OpenVAS:** A framework of several services and tools offering…
- **Nikto:** Web server assessment tool that examines a web server to discover…

Module 06: System Hacking

CHM (CEH Hacking Methodology)

- Footprinting
- Scanning
- Enumeration
- Vulnerability Analysis
- System Hacking
    - Gaining Access
        - Cracking Passwords
        - Vulnerability Exploitation
    - Escalating Priviledges
    - Maintaining Access
        - Executing Applications
        - Hiding Files
    - Clearing Logs
        - Covering Tacks

Microsoft Authentication

- **SAM (Security Accounts Manager) Database**: Store user passwords, or in the AD database in domains. Passwords are **hashed**.
    - It is located at **C: \windows\system32\config\SAM.**
    - **Form:** Username: User ID: LM Hash: NTLM Hash
    - **Example:** Shiela: 1005: NO PASSWORD **********:0CB6948805F797BF2A82807973B89537: : :
    - LM hashes have been **disabled** in newer Windows OS, should be blank in those system
- **NTLM Authentication (NT LAN Manager)**: Using a **challenge/response strategy**.
    - The NTLM authentication protocol types are as follows: **NTLM authentication protocol** and **LM authentication protocol**.
    - There protocols store password in the SAM database using different hashing method.
- **Kerberos Authentication**: Microsoft has upgraded its **default authentication protocol** to Kerberos, providing a stronger authentication for C/S apps than NTLM.
    - It employs the **KDC (Key Distribution Center)**, which is a trusted third party.
    - This consists of **AS (Authentication Server)** and a **TGS (Ticket Granting Server).**

    - It use **tickets** to prove a user's id.

NTLM Authentication Process:

- Include three methods of challenge-response authentication: LM, NTLMv1, and NTLMv2
- The client and server negotiate an authentication protocol, accomplished through **SSP (Security Support Provider)**

Kerberos Authentication

- A network authentication protocol provides strong authentication for C/S applications through **secret-key** cryptography
- Both the server and the user verify each other's id.
- Messages sent through this protocol are protected against **replay** attacks and **evaesdropping.**

Types of Password Attacks

- **Non-Electronic Attacks:** Do not need technical knowledge to crack the password
    - Shoulder Surfing
    - Social Engineering
    - Dumpster Diving
- **Active Online Attacks:** Perform password cracking by directly communicating with the victim's machine
    - Trojan/Spyware/Keyloggers
    - Dictionary Attack, Brute-Force Attack, Rule-based Attack
    - **LLMNR (Link-Local Multicast Name Resolution)/NBT-NS (NetBIOS Name Service)** poisoning
    - Password Guessing
    - Internal Monologue Attack
    - Cracking Kerberos Passwords
- **Passive Online Attacks:** Without communicating with the authorizing party
    - Wire sniffing
    - MITM attack
    - Replay attack
- **Offline Attacks:** Copy password file and try to crack password on ones own system at a different location
    - Rainbow Table Attack: **Time-memory tradeoff**
    - DNA (Distributed Network Attack)

Password Recovery Tools

- Elcomsoft Distributed Password Recovery:
- Hashcat:

Tools to extract password hashes

- **pwdump7:** Extract LM and NTLM password hashes from SAM database
- **Mimikatz**:

Password-Cracking Tools:

- L0phtCrack: Audit passwords and recover applications
- ophcrack: Windows password cracker based on rainbow tables.
- RainbowCrack: Crack hashes with rainbow tables. Use time-memory tradeoff algorithm to crack hashes,
- John the Ripper

Defend against LLMNR/NBT-NS Poisoning

- Disable LMBNR
- Disable NBT-NS

Tools to detect LLMNR/NBT-NS poisoning

- Vincidate
- got-responded

Vulnerability Exploitation: Involve the execution of multiple complex, interrelated steps to gain access to a remote system.

- identify the vulnerability
- Determine the risk associated with the vulnerability
- Determine the capability of the vulnerability
- Develop the exploit
- Select the method for delivering -local or remote
- Generate and deliver the payload
- Gain remote access

Buffer Overflow

- **Stack-Based Buffer Overflow:** Used for static memory allocation and stores the variables in LIFO (last-in first-out) order.
    - **Five types of registers:**
    - **EBP:** Extended Base Pointer, also known as StackBase, stores the address of the first data element stored onto the stack.
    - **ESP:** Extended Stack Pointer stores the address of the next data element to be stored onto the stack
    - **EIP:** Extended Instruction Pointer stores the address of the next instruction ot be excuted.
    - **ESI:** Extended Source Index maintains the source index for various string operations.
    - **EDI:** Extended Destination Index maintains the destination index for various string operations
- **Heap-Based Buffer Overflow:** Heap memory is dynamically allocated at runtime during the execution of the program and it stores program data. It occurs when a block of memory is allocated to a heap, and data is written without any bounds checking. It leads to overwriting dynamic object pointers, heap headers, heap-based data, virtual function table, etc.

Windows Buffer Overflow Expoitation

- **Perform spiking:** It allows attackers to send crafted TCP or UDP packets to the vulnerable server in order to make it crash. Help attackers to identify buffer overlflow vulnerabilities in the target applications
- **Perform fuzzing:** Use fuzzing to send **large amount of data** so that it experiences buffer overflow and overwrites the EIP. Help in identifying the number of bytes required to crash the target server. Help in determining the exact **location of the EIP**, which further helps in injecting malicious shellcode
- **Identify the offset:** Use the Metasploit framework **pattern_create** and **pattern_offset** ruby tools to identify the offset and exact location where EIP is being overwritten.
- **Overwrite the EIP register:** Allow attackers to identify whether the EIP can be controlled and can be overwritten with malicious shellcode
- **Identify bad characters:** Identify bad characters that may cause issues
- **Identify the right module:** Identify the right module of the vulnerable server that lacks memory protection.
- **Generate shellcode:** Use msfvenom command to generate the shellcode and inject it into the EIP to gain all access to…
- **Gain root access**

Buffer Overflow Detection Tools

- **OllyDbg:** Traces stack frames and program execution, and it logs arguments of known functions.

Defend against Buffer Overflow

- Develop program by following secure coding practices and guidelines
- Use **ASLR (address space layout randomization)** technique
- Validate arguments and minimize code that require root priviledges.
- Employ DEP (Data Execution Prevention) to mark memory regions as non-executable
- …

Escalating Privileges: The second stage of system hacking

- An attacker performs this that take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access…
- **Horizontal Priviledge Escalation:** Acquire the same priviledges that have already been granted, by assuming the id of another user with the same priviledges
- **Vertical Priviledge Escalation:** Gain higher priviledge that those existing

Privilege Escalation Using DLL Hijacking

- Most windows app don't use the **fully qualified path** when locading an external DLL lib. Instead, they search the dir, from which they have been loaded
- If attackers can place **a milicious DLL in the app dir**, it will be executed in place of the real DLL
- Attackers use tools such as **Robber** and **PowerSploit** to detect hijackable DLLs and perform DLL hijacking on the target system
- Robber: An open-source tool that helps attackers to **find executable prone to DLL hijacking**

Privilege Escalation by Exploiting Vulnerabilities

- Exploit software vulnerabilities by taking advantage of programming flaws in a program, service, or within the OS software or kernel, to execute malicious code
- Attackers search for an exploit based on the OS and software app on exploit sites such as **SecurityFocus** and **Exploit Database**

Privilege Escalation Using Dylib Hijacking

- In OS X, when applications **load an external dylib**, the loader searches for the dylib in multiple dirs
- **Dylib Hijack Scanner** helps attackers to detect dylibs that are vulnerable to hijacking attack
- Attackers use tools such as **DylibHijack** to perform dylib hjjacking on the target system

Using Spectre and Meltdown Vulnerabilities

- Spectre and Meltdown are vulnerabilities found in the **design of modern processor chips** from AMD, ARM, and Intel
- **The performance and CPU optimizations** in the processor, such as branch prediction, out of order execution, caching, and speculative execution, lead to these vulnerabilities
- Attacker exploit these vulnerabilities to gain unauthorized access and **steal critical system info such as credentials** and **secret keys** stored in the application's memory, to escalate privileges.
- **Spectre Vulnerability:** Read adjacent memory locations of a process and access info for which he is not authorized. An attacker can even read the kernel memory or perform a web-based attack using JS
- **Meltdown Vulnerability:** Escalate privileges by forcing an unpriviledge process to read other adjacent memory locations such as kernel memory and physical memory. This lead to revealing critical system info such as credentials, private keys, etc.

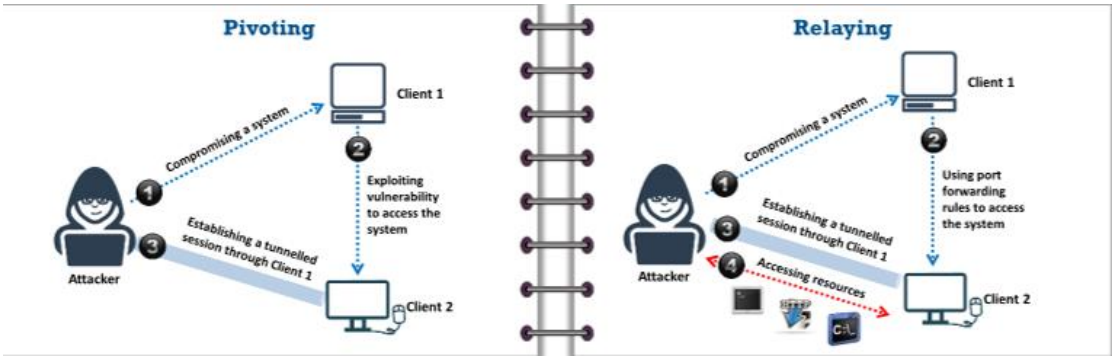
Privilege Escalation Using Named Pipe Impersonation

- In the Windows OS, named pipe provide **legitimate communication** between running processes. Attackers often exploit this technique to escalate privileges on the victim's system to those of a user account **having higher access privilege**
- Attackers use tools such as Metaslpoit to perform named pipe impersonation
- Attackers use Metasploit commands such as getsystem to gain administrative-level privileges and extract password hashes of the admin/user accounts

Privilege Escation by Exploiting Misconfigured Services

- **Unquoted Service Paths:** In windows, the system attempts to find the location of the **executable file** to launch the service when starting a service. The executable path is **enclosed in quotation marks “”**. so that the system can easily locate the application binary. Attackers exploit services with unquoted paths running under **SYSTEM privileges** to elevate their privileges.
- **Service Object Permissions:** Misconfigured service permissions may allow an attacker to modify or **reconfigure the attributes** associated with that service. By exploiting such services, attackers can even **add new users** to the local admin group and then hijack trhe new account to elevate their privilege.
- **Unattended Installs:** Unattended install details such as **configuration settings** used during the installation process are stored in Unattend.xml file. Attackers exploit info stored in Unattend.xml to escalate privileges. It is stored in one of the following locations: **C:\Windows\panther\, C:\Windows\Panther\Unattend\, C:\Windowd\System32\, C:\Windows\System32\sysprep**

Pivoting and Relaying to Hack External Machines

- Use pivoting technique to compromise a system, gain remote shell access on it, and futher **bypass the firewall to pivot via the compromised system** to **access other vulnerable systems** in the network
- Use relaying technique to access resources present on other system via the compromised system such a way that the requests to access the resources are coming from the initially compromised system.
- 

Other Privilege Escalation Techniques

- Access Token Manipulation
- Application Shimming

- Filesystem Permission Weakness
- Path Interception
- Scheduled Task
- Launch Daemon
- Plist Modification
- Setuid and Setgid
- Web Shell
- Abusing Sudo Rights
- Abusing SUID and SGID Permissions
- Kernel Exploits

Privilege Escalation Tools

- **BeRoot:** A post-exploitation tool to check common misconfiguration to find a way to sacalate privileges.
- **Linpostexp:** Obtain detailed info on the kernel, which can be used to escalate privileges on the target system

How to Defend Against Privilege Escalation

- Restrict the interactive logon privileges
- Run users and apps with lowest privileges
- Implement MFA and authorization
- Run services as unprivileges accounts
- Use encryption to protect sensitive data
- .....

Defend against DLL and Dylib Hijacking

- **Dependency Walker:** Detect many common app problems such as missing modules…
- **Dylib Hijack Scanner:** A simple utlity that will scan your computer for app that are…

Defeng Spectre and Meltdown Vulnerabilities

- **InSpect:** Examines and disclose any windows system's hardware and software vulnerabilities to…
- **Spectre & Meltdown Checker:** A shell script to tell if your system is vulnerable again …

Executing Application

- When attackers execute malicious apps it is called **owning** the system
- The attacker executes malicious programs remotely in the victim's machine to gather info.., gain unauthorized access…, crack the password,…
- Malicious Program that attackers execute on target: Keyloggers, spyware, backdoors, crackers

Remote Code Execution Techniques

- Exploitation for Client Execution
- Scheduled Task
- Service Execution
- WMI (Windows Management Instrumentation)
- WinRM (Windows Remote Management)
- Tools for Executing Applications**:** **Remote Exec** remotely installs applications, executes programs/scripts, and updates files and folders on Windows system throughout the network

Keyloggers

- **Spyrix Keylogger FREE:** Used for remote monitoring on your pc that includes recording of keystrokes, passwords, and screenshots.
- Anti-Keyloggers: **Zemana AntiLogger**

Spyware

- A stealthy program that records the user's interaction with the computer and…
- Hide its process, file and other…
- It is like a Trojan horse, which is usually bundled as a hidden component of a…
- **Spytech SpyAgent, Power Spy**
- **Anti-Spyware:** SUPERAnti Spyware

RootKits

- Programs that hide their presence as well as attacker's malicious activities, granting them full access to…
- Replace certain OS calls and utilities with their own modified versions of those routines…

- Comprises of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.
- **Types:**
    - **Hypervisor Level Rootkit:** Act as a hypervisor and modifies the boot sequence of the computer system to load the host OS as a virtual machine
    - **Hardware/Firmware Rootkit:** Hide in hardware devices or platform fireware that we are not inspected for **code integrity**
    - **Kernel Level Rootkit:** Adds malicious code or replaces the **original OS** kernel and **device driver codes**
    - **Boot Loader Level Rootkit:** Replace the original **boot loader** with the one controlled by a remote attacker
    - **Application Level/User Mode Rootkit:** Replace regular **application binaries** with a fake Trojan or modifies the behavior of exeisting applications by injecting mailicous code
    - **Library Level Rootkit:** Repleace the original system calls with fake ones to **hide info** about the attacker
- **System hooking** is the process of changing and replacing the original function pointer with a pointer provided by the rootkit in stealth mode.
- **DKOM (Direct Kernal object manipulation):** Locate and manipulate the system process in kernel memory structures and patch it.
- **Popular Rootkits:** Lojax and Scranos
    - **Lojax:** A type of **UEFI (Unified Extensible Firmware Interface) rootkit** that injects malware into the system and is automatically executed whenever the system starts up. Exploit UEFI that **acts as an interface** between the OS and the fireware
    - **Scranos:** A windows kernel rootkit that runs inside the windows OS and provide an effective mechanism, **hidden storage**, and mailicious command execution while remaining invisible. It injects its malicous code into the boot record which handles the launching of Windows at each step
    - **Horse Pill:** A linux kernel reootkil that resides inside the **initrd,** which it uses to infect the system and deceives the system owner with the use of container primitives.
    - **Necurs:** Contain backdoor functionality allowing remote ccess and control of the infected computer. Monitor and filter network activity and have been observed so send spam and install rogue security software.
- **Steps for detecting Rootkits by examining the filesystem**
    - Run “dir /s /b /ah” and “dir /s /b /a-h” inside the potentially infected OS and save the results
    - Boot into a clean CD, run “dir /s /b /ah” and “dir /s /b /a-h” on the same drive and save the results
    - Run a latest version of **WinMerge** on the two sets of results to detect file-hidhing ghostware

- Anti-Rootkits: **GMER** is an application that detects and removes rootkits by scanning processes, threads, modules, services…

NTFS Data Steam

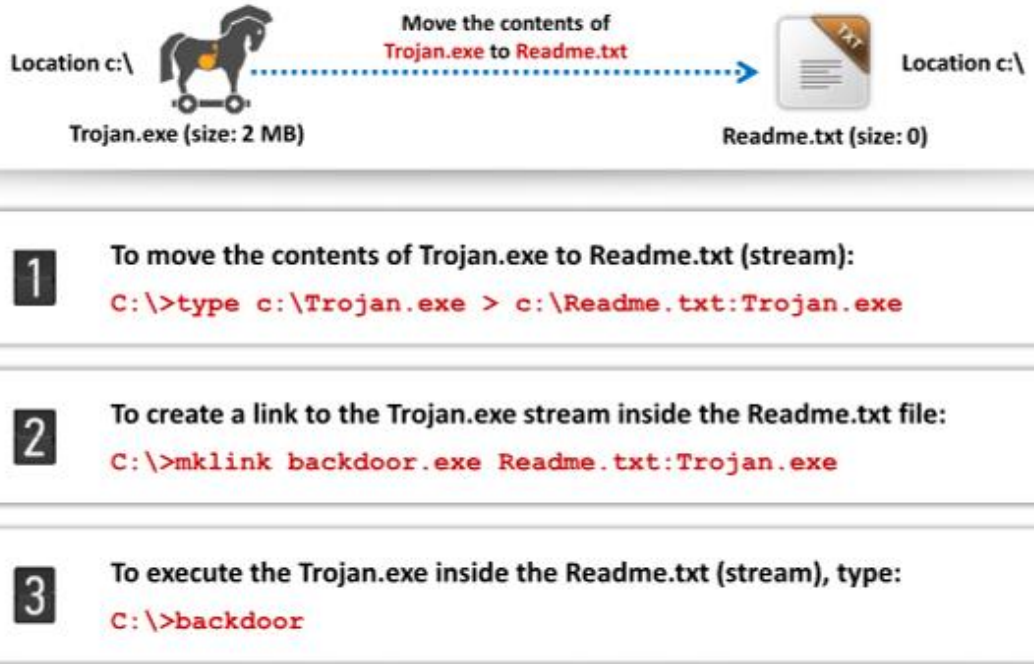
- **NTFS ADS (Alternate Data Stream)** is a windows hidden stream, which contains metadata for the file, such as attributes, word count, author name and access…
- ADS can **fork data into exisiting files** without changing or altering their functionality, size, or display to file browsing ultities
- ADS allow an attacker to **inject malicious code** to files on accessible system and execute them without being detected by the user
- **Steps:**

Notepad is stream compliant application

Step 1	Launch `c:\>notepad myfile.txt:lion.txt` Click 'Yes' to create the new file, enter some data and Save the file
Step 2	Launch `c:\>notepad myfile.txt:tiger.txt` Click 'Yes' to create the new file, enter some data and Save the file
Step 3	View the file size of `myfile.txt` (It should be zero)

Step 4	To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:
	`notepad myfile.txt:lion.txt`
	`notepad myfile.txt:tiger.txt`

- **NTFS Steam Manipulation**



- **Defend against NTFS Streams:**
  - Move the suspected files to FAT partition
  - Use a third-party integrity checker such as Tripewire File Integrity Manager to maintain the integrity…
  - Use programs such as Stream Detector, LADS, or ADS Detector to detect streams
  - Enable real-time antivirus scanning to…
  - Use up-to-data antivirus software…
- **Detectors: Stream Armor** discovers hidden ADS and cleans them completely

Steganography

- **Whitespace Steganography:** Use the **SNOW** tool to hide the message
- **Image Steg:** The info is hidden in image files of different formats such as PNG, JPG, BMP. Image steg tools replace redundant bits of imaga data with the message…Techniques includes **Least Significant Bit Insertion, Masking and Filtering, Algorithms and Transformation**.
- **Image Steg Tools:** OpenStego has function of data hiding and watermarking.
- **Document Steg:** Include the addition of white space and tabs at end of the lines.
- **Document Steg Tool:** StegoStick
- **Video Steg:** DCT (Discrete Cosine Tranorm) manipulation is used to add secret data at the time of the transformation process of the video.
- **Video Steg Tool:** OmniHide Pro
- **Audio Steg:** Omfp can be hidden in an audio file using LSB or using frequencies that are inaudible to the human ear. Some of the audio steg methods are echo

data hiding, spread spectrum method, LSB coding ,tone insertion, phase encoding, etc.

- **Audio Steg Tool:** DeepSound
- **Folder Steg:** Files are hidden and encrypted within a folder and do not appear to normal windows applications, including windows explorer.
- **Folder Steg Tool:** GiliSoft File Lock Pro
- **Spam/Email Steg:** Spam emails help to communicate secretly by embedding the secret messages in some way and hiding the embedded ddata in the spam emails.
- **Spam Steg Tool:** Spam Mimic
- **Mobile Steg Tool:** Steg Master, Stegais

Steganalysis

- The art of discovering and redering covert messages using steg.
- Detect hidden messages embedded in images,txt...
- Challenges
    - Suspect info stream may or may not have encoded hidden data
    - Efficient and accurate detection of hidden content within digital images is difficult
    - The message could be encrypted before being inserted..
    - May have irrelevant data or noise encoded into them
- Steganalysis Methods/Attacks on Steg
    - **Steg-only:** Only the stego object is available for analysis
    - **Known-Stego:** Have access to the stego algorithm and both the cover medium and steg-object
    - **Known-Message:** Have access to the hidden message and the stego object
    - **Known-Cover:** Compare the stego-object and the cover medium to identify the hidden message
    - **Chosen-message:** Generate stego objects from a known message using specific stego tools in order to identify the stego algorithm
    - **Chosen-stego:** Have access to the stego-object and stego algorithm
    - **Chi-square:** Perform probability analysis to test whether the setgo object and original data are the same or not
    - **Distinguishing Statistical:** The attacker analyzes the embedded algorithm used to detect distinguishing statistical changes along with the length of the embedded data
    - **Blind Classifier:** A blind detector is fed with the original or unmodified data to learn the resemblance of original data from multiple perspectives
- Detect Stego

    - **Text file:** The alteration are made to the character positions to hide the data. The alterations are detected by looking for the text patterns or disburbances, language used, and an unusual amount of blank spaces
    - **Image file:** Determine changes in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data. The statistical analysis method is used
    - **Audio file:** Statistical analysis method is used as it involves LSB modification. The inaudible frequencies can be scanned for hidden info. Any odd distortions and patterns show the existence.
    - **Video file:** A combination of methods in image and autio files
- Detection tools: **zsteg**

Covering Tracks:

- Disable Auditing
    - Tools: Audipol
- Clearing Logs
    - Tools: Clear_Event_Viewer_Logs.bat
- Manipulateing Logs
    - For windows: Start->Control Panel->System and security->Administrative Tools->Event viewer
    - For Linux: /var/log/messages
- Covering BASH Shell Tracks:
    - more ~/.bash_history
- Covering Tracks on the Network/OS
    - Using Reverse HTTP Shells
    - Using Reverse ICMP Tunnels
    - Using DNS Tunneling
    - Using TCP Parameters
    - For Windows: ADS
    - For UNIX: Append a dot in front of a file name.
- Deleting Files
    - **Cipher.exe** is an in-built windows command-line tool that can be used to securely detele data by overwriting it to avoid their recovery in the future
- Disabling Windows Functionality
    - **Disable the Last Access Timestamp: fsuti**l is a ultility in windows used to set the **NTFS** volume behabior parameter, DisableLastAccess which controls…
    - **Disable Windows Hibernation:** Use the registry editor or powercfg command
    - **Disable Windows Thunmnail Cache**
    - **Disable Windows Prefetch Feature**
- Tools: CCleaner

Defend against Covering Tracks

- Activate logging functionality on all critical systems
- Conduct a periodic audit on IT system to ensure…
- Ensure new event do not overwrite old entries
- Configure appropriate and minimal permissions necessary…
- Maintain a separate logging server on the DMZ to store…
- Update and patch regularly
- …

Module 07: Malware Threats

Common Techniques Attackers Use to Distribute Malware on the Web

- **Black hat Search Engine Optimization (SEO):** Ranking malware **pages highly** in search results
- **Social Engineered Click-jacking:** Tricking users into **clicking on innocent-looking** webpages
- **Spear-phishing Sites:** Mimicking legitimate institutions in an attemp to **steal login credentials**
- **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites
- **Compromised Legitimate Websites:** Hosting embedded malware that spreads to unsuspecting vistors
- **Drive-by Downloads:** Exploiting flaws in browser software to install malware just by visiting a web page.
- **Spam Emails:** Attaching the malware to emails and tricking victims to click the attchment.

Components of Malware

- **Crypter**
- **Downloader**
- **Dropper:** A type of Trojan that covertly install other malware files on to the system
- **Injector:** A program that injects its code into other vulnerable running processes and…
- **Exploit**
- **Obfuscator:** A program that conceals its code and intended purpose via various tevchniques
- **Packer:** A program that allows all files to bundle together into a single executable file via compression to bypass security software detection
- **Payload**
- **Malicious Code:** It can take the forms of Java Applets, ActiveX Controls, Browser Plug-ins, Pushed Content

APT (Advanced Persistent Threats)

- Defined as a **type of network attack**, when an attacker gains unauthorized access to a target network and remains undetected for a long period of time
- **Obtain sensitive info** rather than sobotaging the org and its network
- **Lifecycle:** Preparation->Initial Intrusion->Expansion->Persistence->Search and Exfiltration->Cleanup

Trojan

- Get activated when a user perform certain **predefined** actions
- Create a **covert communication** channel between..

Infect Systems Using a Trojan

- Create a new Trojan packet:
    - Trojan Horse construction kits help attacker…
    - Tools in these kits can be dangerous and can backfire if not properly executed
    - DarkHorse Trojan Virus Maker creates user-specified Trojans
- Employ a **dropper** or **downloader** to install the malicious code on the target system
    - **Droppers:** Used to camouflage the malware payloads. Consist of one or more types of malware features. **Emotet dropper** and **Dridex dropper** are some of the famous droppers
    - **Downloads:** A program that can download and install harmful program. Do not carry malware of itself, so it could pass through the AV scanner. **Godzilla Downloader** and **Trojan.Downloader** are some of the famous downlaoders.
- Employ a **wrapper** to bind the Trojan to a legitimate file
    - Bind a Trojan executable with genuine looking .EXE applications.
    - When the user runs the wrapped .EXE, it first installs the Trojan in the background and then runs the wrapping application
    - **Tools:** IExpress Wizard, Elite Wrap
- Employ a **crypter to encrypt** the Trojan
    - A software used to **hide virus, keyloggers** or **tools**. Not easily get detected by AV
    - BitCrypter can be used to encrypt and **compress 32bit executable** and **.NET** apps
    - **Tools:** SwayzCryptor, AegisCrypter
- **Propagate the Trojan** by various methods

    - Use covert channels to **deploy and hide malicious trojans in an undetected protocol**
    - Covert channels operate on **a tunneling method** to evade firewalls
    - Attackers can **create covert channels** using Tools such as **Ghost Tunnel, ELECTRICFISH -A North Korean tunneling tool**
    - **Evade AV:**
        - Break the trojan file into multiple pieces and zip them.
        - Write own Trojan and embed it into an app.
        - Change the syntax. Change the content of the trojan using hex editor and change the checksum and encrypt the file.
        - Never use downloaded trojan
- **Deploy the Trojan on the victim's machine** by executing dropper or downloader on the target machine
    - Deploy a trojan through **emails, covert channels, proxy servers, USB/flash Drives**
    - **Covert Channels** are method used to deploy and hide malicious trojans in an undetectable protocol, they rely on **tunneling**.
- Execute the **damage routine**

Exploit Kits

- An exploit kit or crimeware toolkit is a platform to **deliver explolits and payloads** such as trojans, spyware…
- Come with **pre-written** exploit codes and can be easily used by an attacker
- RIG Explit Kit: RIG EK was used by attackers for distributing…

Stage of Virus Lifecycle

- Design
- Replication
- Launch
- Detection
- Incorporation
- Execution of the damage routine

Type of virus

- 1. System or Boot Sector Virus

- 2. File Virus
- 3. Multipartite Virus
- 4. Macro Virus
- 5. Cluster Virus
- 6. Stealth/Tunneling Virus
- 7. Encryption Virus
- 8. Sparse Infector Virus
- 9. Polymorphic Virus
  10. Metamorphic Virus
- 11. Overwriting File or Cavity Virus
- 12. Companion Virus/Camouflage Virus
- 13. Shell Virus
- 14. File Extension Virus
- 15. FAT Virus
- 16. Logic Bomb Virus
- 17. Web Scripting Virus
- 18. Email Virus
- 19. Armored Virus
- 20. Add-on Virus
- 21. Intrusive Virus
- 22. Direct Action or Transient Virus
- 23. Terminate and Stay Resident Virus (TSR) System

Randomware:

- Dharma
- eCh0raix
- SamSam

Infect Systems Using a Virus

- Creating a Virus
- Propagating and Deploying a Virus
    - Virus Hoaxes
    - Fake Antivirus

Computer Worms

- Mailicous programs that independently replicate, execute, and spread across the network connections, comsuming available computing resources without human interaction.
- Differences from a virus:

Virus	Worm
A virus infects a system by inserting itself into a file or executable program	A worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter the content of files or change the location of files in the system	Typically, a worm does not modify any stored programs; it only exploits the CPU and memory
It alters the way a computer system operates without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot spread to other computers unless an infected file is replicated and sent to the other computers	A worm can replicate itself and spread using IRC, Outlook, or other applicable mailing programs after installation in a system
A virus spreads at a uniform rate, as programmed	A worm spreads more rapidly than a virus
Viruses are difficult to remove from infected machines	Compared with a virus, a worm can be removed easily from a system

- Worm Makers: Internet Worm Maker Thing

Fileless Malware

- Also known as non-malware, **infects legitimate software, applications**, and other protocols
- Leverage vulnerabilities to infect the system
- Reside in the system's RAM, **injecting malicious code** into the running processes.
- Reason for using it:
    - Stealthy in nature
    - **Living-off-the-land:** Exploit default system tools
    - **Trustworthy:** Uses tools that are frequently used and trusted
- Taxonomy:
    - Type1: No file activity performed
    - Type2: No files written on disk, but some files used indirectly
    - Type3: File required to achieve fileless persistence
- How does Fileless malware work
    - **Point of Entry:**
        - Memory Exploits
        - Malicious Document
    - **Code Execution:**

        - Code injection
        - Script-Based
    - **Persistence:** Registry, WMI, Scheduled Task
    - **Achieving Objectives:** Recon, Credential Harvesting, Data Exfiltration, Cyber Espionage
- Launching Fileless Malware
    - **Memory Exploits:** Inject a malicious payload into the RAM, exploit different Win APIs.
    - **Malicious Document:** Trick users into downloading a file consisting of malicious macro code.
    - **Script-Based:** Allow attackers to communicate and infect the applications or OS without being traced
    - **Exploiting System Admin Tools:** Exploit system admin tools such as Certutil, WMIC, and Regsvr32 to launch fileless infections. Exploit cmd tools such as **Regsvr32**, and **runddl32** to run malicious DLLs.
    - **Through Phishing:** Use social engineering techniques. Fileless malware exploits vulnerabilities in system tools to load and run malicious payloads to compromise the sensitive info stored in the process memory.
- Main Persistence with Fileless Techniques
    - **Do not use disk files** to spread its infection or main persistence
    - Adopt unique methods such as **developing load points** to restart infecteted payload
    - Save the malicious payload **inside the registry t**hat hold data for configuration, application files, and settings, which executes itself with evetry restart
- **Fileless Malware:** Divergent is a type of fileless malware that **depends mostly on the registry** for the….It also employs a key in the register to **maintain persistence** and exploits PowerShell to inject itself on to the other processes.
- **Obfuscation Techniques:**
    - Insert characters
    - Insert Parentheses
    - Insert caret symbol
    - Insert double quotes
    - Using custom environment variables
    - Using pre-assigned environment variables

Sheep Dip Computer

- Refer to the analysis of suspect files, incoming messages, etc…

- Is installed with port monitors, files monitor…Connect to a network only under strictly controlled conditions

Antivirus Sensor Systems

- A collection of computer software that detects and analyzes **malicious code threats** such as viruses, worms, and trojans.
- They are used along with **sheep dig computer.**

Malware Analysis

- A process of **reverse engineering** a specific piece of malware to determine the origin…
- **Static Malware Analysis:** Also known as **code analysis without executing** it.
    - **File fingerprinting:** Hash
    - **Local and online malware scanning:** AV software, VirusTotal
    - **Perform string search:** Embedded strings of readble text, using **BinText**
    - **Identify packing/obfuscation methods: PEid tool**
    - **Finding the PE info:** Metadata of PE files, PE explorer
    - **Identify file dependencies:** Dependency Walker
    - **Malware disassembly:** IDA, OllyDbg
- **Dynamic Malware Analysis: Behabioral analysis** involves executing the malware code
    - Require a safe environment such as **virtual machines** and **sandboxes**
    - **System Baseline**: Take a snapshot of the system, compare
    - **Host Integrity Monitoring:**
        - **Port:** netstat, TCPView
        - **Process:** Process Monitor
        - **Registry:** jv16 PowerTools
        - **Service:** Windows Service Monitoring Tools
        - **Startup:** Autoruns for Windows, **C:\ ProgramData\Microsoft \Windows\Start Menu\Programs\Startup**
        - **Event Logs:** Splunk is a SIEM (Security Information and Event Management) tools that…
        - **Installation:** Mirebusoft Install Monitor
        - **File and Folders:** PA File Sight
        - **Drivers:** DriverView, **run->msinfo32->Software Environment->System Drivers**

    - **Network traffic:** SolarWinds NetFlow Traffic Analyzer
    - **DNS/Resolution:** DNSQuerySniffer
    - **API Calls:** API Monitor

Virus Detection Methods

- **Scanning**
- **Integrity Checking**
- **Interception:** Monitor the OS requests written to the disk
- **Code Emulation:** effective in dealing with encrypted and polymorphic virus
- **Heuristic Analysis:** can be static or dynamic

Emotet

- A banking Trojan which can function both as a trojan by itself or as the downloader and dropper of other banking trojans
- It is a **polymorphic malware** as it can change its own identifiable feartures to evade **signature-based** detection

Countermeasures against Fileless Malware

- Disable PDF readers to automatically run JS
- Disable macros and use only digitally signed trusted macros
- Tools: AlienBault USM Anywhere, McAfee End Points Security

Module 8: Sniffing

Packet Sniffing

- Turn the NIC of a system to promiscuous mode.
- Two types of Ethernet environments, sniffers work differently in each
    - **Shared Ethnernet**
    - **Switched Ethernet**
- Sniffing is possible using the following methods
    - **ARP Spoofing:** ARP is stateless, a machine can send an ARP reply even without asking for it and it can accept such a reply.
    - **MAC Flooding:** Siwtches have limited memory, once the memory is fully consumed, the switch will enter **fail-open** mode, it starts acting as a hub by broadcasting packets to all the ports on the switch.
- Passive Sniffing:
- Sniffing through a hub, wherein the traffic is sent to all ports.
    - It involves moniroting packets sent by others without sending any additional data packets in the network traffic
    - All hosts on the network can see all the traffic in a network that uses hub.
    - Hub is mostly replaced with switches
- Active Sniffing:
    - Sniff a switch-based networkf
    - Inject ARP into the network to flood the switch's CAM table
    - Techniques:
        - **MAC flooding,**
        - **DHCP attacks,**
        - **DNS poisoning,**
        - **Switch port stealing**
        - **ARP poisoning,**
        - **Spoofing attack**
- Hack the network using sniffer
    - Connect laptop to a switch port
    - Run discovery tool to learn about network topology
    - Identify a victim's machine
    - Poison the victim's machine by using ARP spoofing
    - Destine for the victim's machine is redirected of the attacker
    - Extract passwords and…

- Protocols vulnerable to sniffing
    - **Telnet and Rlogin:** keystrokes including usernames and pass are in clear text
    - **IMAP (Internet Message Access Protocol):** clear text
    - **HTTP:** clear text
    - **SMTP** and **NNTP (Network News Transfer Protocol):** clear text
    - **POP:** clear text
    - **FTP:** clear text
- Sniffing in the **Data Link Layer** of the OSI model
    - Networking layer are designed to work independently of each other, if a sniffer sniffs data in the data link layer, the upper layers will not be aware of the sniffing

Hardware Protocol Analyzers

- A piece of equipment that **captures signals** without altering the traffic in a cable segment
- It can be used to monitor network usage and identify **malicious network traffic**
- It captures a data packet, decode it, and analyzes its content based on certain **predetermined rules**
- It allows the attacker to see individual **data bytes** of each packet passing through the cable

SPAN (Switched Port Analyzer) Port

- A port that is configured to receive a copy of every packet that passes through a switch
- **Cisco** switch feature, also known as **port mirroring**

Wiretapping

- The process of monitoring of **telephone** and **Internet** conversations by a third party
- Attackers connect a **listening device** to the circuit carrying info between two phones or hosts on the Internet
- It allow an attacker to **monitor, intercept, access**, and **record info** contained in a data flow in a communication system
- **Active Wiretapping:** Monitor, record, alter, and inject data into the …

- **Passive Wiretapping:** Only monitor and record the traffic and collects knowledge regarding the data it contains

MAC address/CAM Table

- Each switch has a fixed-size dynamic Content Addressable Memory (CAM) table
- MAC Address: **3 bytes OUI (Organizationally Unique Identifier)**+**3bytes NIC specific**
- When a CAM Table is full:
    - Additional APP request traffic floods every port on the switch
    - Change the behavior of the switch to reset to its learning mode, broadcasting on every port like a hub
    - This attack will also fill the CAM tables of adjacent switches
- **MAC Flooding:** Flooding of the CAM table with fake MAC address and IP pairs until it is full
- **macof:** A unix/linux tool that is a part of the dsniff collection. Send random source MAC and IP. Floow siwtch's CAM table.

Switch Port Stealing

- Use MAC Flooding to sniff the packet
- Flood the switch with forged ARP packets with the target MAC as the source and his own MAC as destination
- A **race condition** of the attacker's flooded packets and the target host's packets occurs, thus the switch must change its MAC, binding constantly between two different ports
- If the attacker is faster, he will direct packets intended for the target toward his ports.
- The attacker now manages to steal the target' switch port and sends ARP requests to the stolen switch port to discover the target host's IP
- When the attacker gets an ARP reply, the target host's switch port bindin has been restored, and the attacker can now sniff the packets sent toward targeted host.

Defend against MAC Attacks

- Configuring Post Security on Cisco Switch
- Only 1 MAC address allowed on the switch port
- Port security can be used to **restrict inbound traffic** from only a selected set of MAC addresses and limit MAC flooding attack

DHCP

- DHCP Server maintains TCP/IP configuration info
- DHCP Attack: An active sniffing technique used to steal and manipulate sensitive data.
- **DHCP Starvation Attack:** This is a **DoS** attack on the DHCP servers where the attacker broadcasts forget DHCP requests and tries to lease all the DHCP addresses available
- **DHCP Starvation Attack Tools:** Yersinia, Hyenae
- **Rogue DHCP Server Attack:** A rouge DHCP server responds to DHCP request with fake IP addresses resulting in compromised network access. Work in conjunction with the **DHCP starvation attack.**
- Defend against DHCP starvation and Rogue Server Attacks:
    - **Enable port security** to defend against DHCP starvation attacks
    - **Enable DHCP snooping**, allowing the switch accept a DHCP transaction directed from a trusted port

ARP

- A stateless protocol used for resolving IP to MAC address
- ARP Spoofing
- Threats of ARP Poisoning:
    - Packet sniffing
    - Session hijacking
    - VoIP call tapping
    - Manipulating data
    - MitM attack
    - Data interception
    - Connection hijacking
    - Connection Resetting
    - Stealing Password
    - DoS Attack
- ARP Poisoning Tools: **arpspoof, Ettercap,BetterCAP**
- Defend against ARP Poisoning: Implement **Dynamic ARP Inspection** using HDCP snooping binding table
- ARP Spoofing detection tool: XArp

MAC Spoofing/Duplicating

- MAC duplication attack is launched by sniffing a network for MAC of clients who are actively associated with a switch port and re-using one of those addresses
- MAC duplication can be used to bypass wireless access points' MAC filtering
- Tools: Technitium MAC Address Changer, SMAC

IRDP (ICMP Router Discovery Protocol) Spoofing

- A routing protocol that allows a host to discover the IP of active routers on their subnet by listening to router advbertsement and soliciting messages on their network
- The attacker sends a spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
- Allow attackers to sniff the traffic and collect valuabnle info from the packets
- Launch MiTM, DoS, and passive sniffing attacks

VLAN Hopping

- A technique used to target network resource present on a VLAN
- Can be performed by using two primary methods, **Switch Spoofing** and **Double Tagging**
- Attackers perform VLAN hopping attacks to steal sensitive info, install malicious codes or programs, spread virus….
- **Switch Spoofing:** Attackers connect a rouge switch onto the network by tricking a legitimate switch and thereby creating a trunk link between them.
- **Douvle Tagging:** Add and modify tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network

STP Attack

- Attackers connect a **rouge switch** into the network to change the operations of the **STP protocol** and sniff all the network traffic
- Attackers configures the rouge switch such that its priority is less than that of any other switch in the network, which makes it the root bridge, thus allowing the attackers to sniff all the traffic flowing in the network
- **STP**: Spanning Tree protocol ensures that the traffic follows an optimized path to enhance network performance

Defend Against MAC Spoofing

- **DHCP Snooping Binding Table,**
- **Dynamic ARP inspection**
- **IP Source guard**
- **Encryption**
- **Retrieval of MAC Address**
- **Implementation of IEEE 802.1X Suites**
- **AAA (Authentication, Authorization, Accounting)**

Defend Against VLAN Hopping

- **Defend against Switch Spoofing**
    - Configure the ports as access ports and ensure all access ports are configured not to negotiate trunks
    - Ensure all trunks ports are configured not to negotiate trunks
- **Defend against Double Tagging**
    - Ensure that each access port is assigned with VLAN except the default VLAN (VLAN 1)
    - Ensure that the native VLANs on all trunk ports are changed to an unused VLAN ID
    - Ensure that the native VLANs on all trunk ports are explicitly tagged

Defend against STP attacks

- **BPDU (Bridge Protocol Data Protocol) Guard:** Avoid the transmission of BPDUs on PortFast-enabled ports. Help in preventing potential bridging loops in the network
- **Loop Guard:** Protect the root bridge and ensures that it remains as the root in the STP topology, prevent nearby switches from being root switches
- **Root Guard:** Prevent it against the bridging loops, used to protect against a malfunctioned switch.
- **UDLD (Unidirectional Link Detection):** Enable devices to detect the existence of unidirectional links and further disable the affected interfaces in the network. There unidirectional links in the network can cause STP topology loops

DNS Poisoning

- Result in the substitution of a false IP address at the DNS level

- Posible using **Intranet DNS spoofing, Internet DNS spoofing, Proxy Server DNS poisoning, DNS Cache poisoning**
- **Intranet DNS Spoofing:** Work well against switches with ARP Poison Routing.
- **Internet DNS Spoofing:** Infect victim's machine with a trojan and changes his DNS ip address to that of the attacker's
- **Proxy Server DNS Poisoning:** Change victim's proxy server setting in IE to that…
- **DNS Cache Poisoning:** Altering or adding forged DNS records into the DNS resolver cache.
- **Tools:** DerpNSpoof, Ettercap, DNS Spoof
- **Countermeasure:**
    - Iplement **DNSSEC (Domain Name System Security Extension)**
    - Use a SSL for securing the traffic
    - Resolve all DNS queries to a local DNS server
    - Block DNS requests being sent to ecternal servers
    - Configure a firewall to restrict ecternal DNS lookups
    - Implement IDS
    - Configure the DNS resolver to use a new random source port for each outgoing query
    - Restrict the DNS recusing service, to authorized users
    - Use NXDOMAIN (DNS Non-existent Domain) the Limiting

Sniffing Tools

- **Wireshark**
- Filters in Wireshark
    - Display Filtering by Protocol Example: Type the protocol in the filter box: arp, http, tcp, udp, dns, ip
    - Monitoring the Specific Ports
        - tcp.port==23
        - ip.addr==192.168.1.100 machine
        - ip.addr==192.168.1.100 && tcp.port=23
    - Filtering by Multiple IP Addresses
        - ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
    - Filtering by IP Address
        - ip.addr == 10.0.0.4
    - Other Filters
        - ip.dst == 10.0.1.50 && frame.pkt_len > 400

        - ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
        - ip.src==205.153.63.30 or ip.dst==205.153.63.30
- Additional Filters

- **OmniPeek:** Display a google map
- **SteelCentral Packet Analyzer:** Provide a graphical console for high-speed packet analysis

Countermeasure against Sniffing

- **Restrict physical access** to network media
- Use **end-to-end encryption**
- Permanently add the **MAC address of the gateway** to the ARP cache
- Use **static IP and ARP table**s to prevent attackers from adding spoofed ARP entries
- Turn of **network identification broadcasts**
- Use **IPv6**
- Use **encrypted sessions**, **SSH** instead of **Telnet**, **SCP (Secure Copy)** instead of **FTP**, SSL for email
- Https instead of HTTP
- Switch instead of a hub
- SFTP instead of FTP
- PGP, S/MIME, VPN, IPSec, SSL/TLS, SSH and OPTs
- WPA, WPA2
- Retrieve the MAC directly from NIC instead of OS
- Detect promiscuous mode
- Use ACL to allow access to only a fixed range of trusted IP

Sniffing Detection Techniques

- Check the devices running in promiscuous mode
- Run IDS
- Run Network Tools
- **Ping Method:** Send a ping request to the suspect machine with its IP and an incorrect MAC. If **do not reject**,…
- **DNS Method:** A machine generating **reverse DNS lookup** traffic is suspious. Increase in network traffic can be an indication of the presence of a sniffer on the network.
- **ARP Method:** Only the machine in the promiscuous mode **caches the ARP info**. A machine in the promiscuous mode responds to the **ping message** as it has the correct info about the host sending the ping request in its cache, the rest of the machines will send an ARP probe to identify the source of the ping request.
- **Promiscuous Detection Tools:** Nmap's NSE script, NetScan Tools PRO

Module 9: Social Engineering

Concept

- The art of convincing people to reveal confidential info

Phase of a Social Engineering Attack

- Research the Target Company
- Select a Target
- Develop a Relationship
- Exploit the Relationship

Social Engineering Techniques

- **Human-based Social Engineering:**
    - Sensitive info is gathered by **interaction**
    - Techniques:
        - **Impersonation:** Pretend to be someone legitimate or an authorized person
        - **Vishing:** An impersonation technique in which the attacker tricks individuals to reveal…using voice technology such as VoIP, telephone system.
        - **Eavesdropping**
        - **Shoulder surfing**
        - **Dumpster diving**
        - **Reverse social engineering:** The attacker presents him as an authority and the target seeks his advice before or after offering the info that the attacker needs
        - **Piggybacking:** An authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door
        - **Tailgating:** Wear a fake ID badge, enter a secured area by closely following an authorized person through a door that requires key access
        - **Diversion theft**: Trick a person responsible for making a genuine delivery into delivering the consignmnet to a location other than the intended location

            - **Honey trap:** Attacker target a person online, pretending to be an attrative person. They then begin a fake online relationship to obtain…
            - **Baiting:** Attackers offer end users sth alluring in exchange for important info such as…A physical device such as USB flash drive containing malicious files is left in a location where people can easily find it.
            - **Quid Pro Quo:** Call numerous random numbers within a company, claiming to be from technical support. Offer their service to end users in exchange for confidential info
            - **Elicitation:** Extract info from the victim by engaging him in normal and disarming conversations. Based on the victim's interests, attackers much work to taraget their elicitation approach to extract the relevant info.
- **Computer-based Social Engineering**
    - Sensitive info is gathered with the **help of computer**
    - Techniques:
        - **Phishing:**
            - **Spear Phishing:** A targeted phishing attack aimed at **specific individuals** within an org.
            - **Whaling:** Target **high profile executives** like CEO.
            - **Pharming:** Redirect **web traffic** to a fraudulent website by installing a malware on a personal computer. Also known as "phishing without a lure", and perform by using **DNS Cache Poisoning** or **Host File Modification**
            - **Spimming:** Exploit Instant Message platform to flood spam. Atttackers uses bots to harvest Instant Message Ids and spread spam
        - **Hoax Letters:** Emails that issue warnings to the user about new malware that may harm the user's system
        - **Chain letters:** Emails that offer free gifts that the user forwards the mail to a specificied number of people
        - **Pop-up windows attacks:** Windows that suddenly pop up while surfing the Internet and ask for user info to login.
        - **Spam mail**
        - **Scareware:** Malware tricks users into visiting malware infested websites, or downloading potentially malicious software
        - **Instant chat messenger**
    - Phishing Tools: **ShellPhish**
- **Mobile-based Social Engineering**

    - Sensitive info is gatherted with the **help of mobile apps**
    - Techniques
        - Publishing malicious apps
        - Using fake security apps
        - Repacking legitimate apps
        - Sms phishing

Insider Threats/Attacks

- Using privileged access to intentionally violate rules or cause threat to the org's info.
- Can be performed by a privileged user, disgruntled employee, terminated employee, accident-prone employee, third party, undertained staff, etc
- Types:
    - Malicious Insider:
    - Negligent Insider
    - Professional Insider
    - Compromised Insider

Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by empoyees.
- Password policies, Physical Security Policies, Defense Strategy
- Train invididuals on security policies
- Implement proper access privileges
- Presence of proper incidence response time
- Availability of resources only to authorized users
- Scrutinize info
- Background check and proper termination process
- anti-virus/phishing defense
- MFA
- Adopt documented change management
- Ensure software is regulary updated
- Detect Insider Threats
    - Insider risk controls
    - deterrence controls
    - detection controls

- Insider Threat Countermeasures
    - Separation and rotation of duties
    - Least privileges
    - Controlled access
    - Logging and auditing
    - Employee monitoring
    - Legal policies
    - Archive critical data
    - Employee training on cyber security
    - Employee background verification
    - Periodic risk assessment
    - Privileged users monitoring
    - Credentials deactivation for terminated employees
- Detect phishing emails
    - It seems to be from a bank, company, or social networking site and has a generic greeting
    - It seems to be from a person listed in your email address book
    - It has an urgent tone or makes a veiled threat ・It may contain grammatical or spelling mistakes
    - It includes links to spoofed websites
    - It may contain offers that seem to be too good to be true
    - It includes official-looking logos and other information taken from legitimate websites
    - It may contain a malicious attachment
- Anti-Phishing Toolbar: **Netcraft, Phish Tank**

Social Engineering Tools

- SET (Social Engineerint Toolkit)

Audit Organization’s Security for Phishing Attacks:

- Tools: **OhPhish**, **a web-based** protal to test…

Module 10: Denial of Service

Basic Categories of DoS/DDOS Attack Vector

- Volumetric Attacks:
    - Consume the bandwidth of a target network or service.
    - The magnitude of attack is measured in **bits-per-second (bps)**
    - Types of bandwidth depletion attacks
        - **Flood attacks**: Zombies send large volumes of traffic to the victim's system to exhaust the bandwidth of these systems
        - **Amplification attacks:** The attacker or zombies transfer messages to a boradcast IP address. This method amplifies malicious traffic that consumes the bandwidth of the victim's system
    - Techniques:
        - UDP flood attack
        - ICMP flood attack
        - Ping of Death attack
        - Smurf attack
        - Pulse wave attack
        - Zero-day attack
        - Malformed IP packet flood attack
        - Spoofed IP packet flood attack
- Protocol Attacks
    - Consume other types of resources like **connection state tables** present in network infrastructure component such as **load-balander, firewalls, and application servers**
    - The magnitude of attack is measured in **packets-per-second (pps)**
    - Techniques:
        - Syn flood attack
        - Fragmentation attack
        - Spoofed session flood attack
        - ACK flood attack
        - RST attack
        - TCP state exhaustion attack
        - TCP connection flood attack
- Application Layer Attacks
    - Consume the resources or services of an application, thereby making the application unavailable to other legitimate users
    - The magnitude of attack is measured in requests-per-second (rps)
    - Techniques:
        - HTTP GET/POST attack

        - Slowloris attack
        - UDP application layer flood attack

DoS/DDoS Attack Techniques

- **UDP flood attack**
    - An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a larget src IP range
    - The flooding of UDP packets causes the server to repeatedly check for **non-existent applications** at the ports
    - Legitimate apps are inaccessible by the system and give an error reply with an ICMP "Destination Unreachable" packet
- **ICMP flood attack**
    - A type of attack in which attackers send large volumes of **IMCP echo request packets** to a victim system directly or through relection networks
    - To protect against this attack, set a threshold limit that invokes an ICMP attack protection feature when exceeded
- **PoD (Ping of Death) attack**
    - An attacker tries to crash,destabilize, of freeze the targeted system or service by sending malformed or oversized packets using a simple ping command
    - Ex: Send a packet which has a size of 65538 bytes
- **Smurf attack**
    - Spoof the source IP address with the victim's IP address and sends a large number of ICMP echo request packets to an IP broadcast network
    - Cause all the hosts on the broadcast network to respond to the received ICMP echo request.
- **Pulse wave attack**
    - Attackers send a **highly repetitive periodic train of packets as pulses** to the target victim every 10 minutes, and each specific attack session can last for a few hours to days.
    - A single pulse (300 Gbps or more) is sufficient to ccrowd a network pipe
- **Zero-day attack**
    - This attack is delivered before the DDoS vulnerabilities of a system have been patched of effective defensive mechanisms are implemented
- **SYN flood attack**
    - Send a large number of SYN requests with fake source IP addresses to the target
    - Take advantage of a flaw in the implementation of the TCP three-way-handshake in most hosts
    - When server receives the SYN request, it must keep track of the partially opened connection is a listen queue for at least **75 seconds.**
    - Countermeasures: Poper packet filtering

- **Fragmentation attack**
    - Stop a victim from being able to re-assemble fragmented packets by flooding the traget system with TCP or UDP fragments. Attackers send a larger number of fragmented packets to a target web server with a relatively small packet rate
    - Ressembling and inspecting these large fragmented packets cinsumes excessive resources. Morever, the content in the packet fragments will be randomized by the attacker, which in turn makes the process consume more resources
- **ACK flood attack**
- **TCP state exhaustion attack**
- **Spoofed session flood attack**
    - Attackers **create fake or spoofed TCP sessions** by carring multiple **SYN, ACK,** and **RST or FIN packets**
    - Attackers employ this attack to bypass firewalls and perform DDoS attacks against target network, exhausting its network resources
    - Multiple SYN-ACK Spoofed Session Flood Attack: Create a fake session with **multiple SYN and muiltiple ACK packets** along with **one or more RST or FIN packets**
    - Multiple ACK Spoofed Session Flood Attack: Attackers create a fake session by **completely skipping the SYN packets** and using only multiple ACK packets along with **one or more RST or FIN packets**
- **HTTPS GET/POST attack**
    - HTTP GET attack: Use a time-delayed HTTP header to maintain HTTP connection and exhauste web server resources
    - HTTP POST attack: Send HTTP requests with complete headers but with incomplete message bodies to the target, prompting the server to wait for the rest of the message body,
- **Slowloris attack**
    - Send partial HTTP requests to the target
    - Upon receiving the partial HTTP requests, the target opens multiple open connections and keeps waiting for the request to complete
    - These requests will not be complete, and the target server's maximum concurrent connection pool will be exhausted, and additional connection attemps will be denied.
- **UDP application layer flood attack**
    - SSDP
    - NTP
    - VoIP
    - TFTP
    - RPC
    - ...
- Multi-vector attack

    - Use **combinations** of vollumetric, protocol, and application-layer attacks to disable the target
- **Peer-to-peer attack**
    - Attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
    - Exploits flaws found in the network using the DC++ (Direct Connect) protocol, which is used for sharing all types of files between instant messaging clients
    - Attacks launch massive DoS and compromise websites.
- **Permanent DoS (PDoS) attack**
    - **Phlashing:** Permanent DoS, also known as plashing, refers to attacks that cause ireversible damage to system hardware
    - **Sabotage:** Unlike other DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware
    - **Bricking a system:** This attack is carried out using a method known as bricking a system. Using this method, attackers send fraudulent hardware updates to the victims
- **Distributed relection DoS (DRDoS) attack**
    - Also known as a spoofed attack, involves the **use of multiple imtermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
    - Launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn **reflect the attack traffic to the target,**
    - Adv: The primary target seems to be directly attacked by the secondary victim rather than the actual attacker. Multiple intermediary victim servers are used, which results in an increase in attack bandwidth
    - **Countermeasure:** Turn off the CHARGEN (Character Generator Protocol) service to stop this attack method.

Botnets

- Software apps that **run automated tasks** over the Internet and perform simple repetitive tasks.
- A huge network of compromised systems and can be used for launching DoS

Scanning methods for finding vulnerable machines

- **Random Scanning:** The infected machine probes IP addresses randomly from the target network IP range and checks for vulnerabilities
- **Hit-list scanning:** First collects a list of potentially vulnerable machines and then scans them to find vulnerable machines

- **Topological Scanning:** Use information obtained from an infected machine to find new vulnerable machines
- **Local Subnet Scanning:** The infected machine looks for new vulnerable machines in its own local network
- **Permutation Scanning:** Use a pseudorandom permutation list of IP addresses to find new vulnerable machines

How Does Malicious Code Propagate?

- **Central Source Propagation:** Place an attack toolkit on the central source, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system
- **Back-chaining Propagation:** Place an attack toolkit on his own system, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system
- **Autonomous Propagation:** Host itself transfers the attack toolkit to the newly discovered vulnerable system at the exact time that it breaks into that system

DDos Case Study: DDoS attack on github

- The world's largest DDoS attack ever recorded
- Take place on Wed,28 Feb 2018
- Make github's service unavailable for 4 min
- An amplification attack using a Memcached-based approach that peaked at 1.35Tbps

Tools

- **HOIC (High Orbit Ion Cannon):** Carry out a DDoS to attack any IP with a user selected port and a user selected protocol
- **LOIC (Low Orbit Ion Cannon):** Can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests wit hthe intention of disrupting the service of a particular host

Detection Techniques

- Based on identifying and discriminating illegitimate traffic increases and flash events from legitmate packet traffic
- **Activity Profiling:** Based on the average packet rate for a network flow
- **Sequential Change-Point Detection:** Use Cusum (Cumulative Sum) algorithm to identify and locate DoS attacks. Can also be used to identify the typical scanning activities of network worms

- **Wavelet-Based Signal Analysis:** Describe an input signal in terms of spectral components. Analyzing each spectral window's energy determines the presence of anomalies. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise.

DoS Countermeasure Strategies

- Absorbing the Attack
- Degrading Service
- Shutting Down the Services
- Countermeasures:
    - Protect Secondary victims
    - Detect and neutralize handlers
    - Prevent potential attacks
        - Egress filtering
        - Ingress filtering
        - TCP intercept
        - Rate limiting
    - Deflect attacks:
        - Set up honeypots
        - Tool: **KFSenso**r acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans.
    - Mitigate attacks
        - **Load Balancing**
        - **Throttling:** Set routers to access a server with a logic that throttles incoming traffic levels to be safe for the server. Help in preventing damage to servers by controlling DoS traffic. Help router manage heavy incoming traffic. Filter legitimate user traffic from fake DDoS attack traffic
        - **Drop requests**
    - Post-attack forensics
        - Traffic Pattern Analysis
        - Packet Traceback
        - Zombie Zapper Tool
        - Event Log Analysis

Techniques to Defend against Botnets

- **RFC 3704 Filtering:** Limit the impack by denying traffic with spoofed address.
- **Cisco IPS Source IP Reputation Filtering:** Help in determining if an IP or a service is a source of threat. Cisco IPS regularly updates its database with known threats such as botnets…

- **Black Hole Filtering:** Refer to a network node where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient.
- **DDoS Prevention Offerings from ISP of DDoS Service:** Enable IP Source Guard or similar features in other routers to filter traffic based on the DHCP snooping binding database or…

Advanced DDoS Protection Appliances

- FortiDDoS-1200B
- DDoS Protector
- Terabit DDoS Protection System
- A10 Thunder TPS
- Tools: Imperva Incapsula DDoS Protection
- Services: Akamai DDoS Protection

Module 11: Session Hijacking

Concept

- An attack in which an attacker seizes control of **a valid TCP communication session** between two computers
- As most authentication only occur at the **start of a TCP session**, allowing the attacker…
- Attackers can sniff all the traffic from the established TCP sessions and perform identify theft, info theft, traud, etc.
- Steal a valid session ID and use it to authenticate himself

Why is Session Hijacking Successful

- Absence of account lockout for **invalid session IDs**
- Weak **session-ID generation algorithm** or small session IDs
- **Insecure handling** of session IDs
- Indefinite **session timeout**
- Most computeres using **TCP/IP are vulnerable**
- Most countermeasures do not work without encryption

Process

- Sniff
- Monitor
- Session Desynchronization
- Session ID prediction
- Command Injection

Types of Session Hijacking

- **Passive:** The attacker hijacks a session but sits back, watches, and records all the traffic.
- **Active:** The attacker finds an active session and seizes control of it.

Session Hijacking in OSI Model

- **Network Level Hijacking:** Can be defined as the interception of packets during the transmission between a client and the server in a TCP or UDP session

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

Application Level Session Hijacking

- A session is stolen or a valid session taoken is predicted **to gain unauthorized access** to the web server
- A session token can be compromised in various ways
    - **Session sniffing:** Use a sniffer to capture a valid session token or session ID
    - **Predictable session token:** Predict session IDs generated by weak algorithms and impersonate a website user.
    - **MITM attack**
    - **Man-in-the-browser attack:** Use a trojan horse to intercept the calss between the browser and its security mechanisms or libs
    - **XSS:** Inject malicious client-side scripts into the web pages…
    - **CSRF:** Exploit the victim's active session with a trusted site to perform malicious activities
    - **Session replay attack:** Use the authentication token to replay the request
    - **Session fixation attack:** Attackers provide a valid SID to a victim and lure him to authenticate using that SID.
    - **CRIME (Compression Ratio Info-Leak Made Easy) attack:** A client-side attack that exploit the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS.
    - **Forbidden attack:** A type of MITM. Exploit the reuse of cryptographic nonce during the TLS handshake
    - **Session donation attack:** An attacker donates his own SID to the target user.

Network Level Session Hijacking

- Rely on hijacking transport and Internet Protocols used by web applications in the application layer
- **Blind hijacking:** Inject malicious data or cmds into the intercepted communications in the TCP session even if the source-routing is disabled. But **the attacker cannot see the response**
- **UDP hijacking:** Attackers send **forged server reply** to a civtim's UDP request before the intended server replies to it.
- **TCP/IP hijacking:** Use spoofed packets to seize control of a connection. The attacker must be be on the same network as the victim.
- **RST hijacking:** Inject an authentic-looing RST packet using a spoofed source address and predict the ack number. An attacker can reset a victim's connection if it uses an accurate ack num

- **MITM: Packet sniffer:** Change the **default gateway** of the client's gateway and attempt to reroute packets. The packets between the C and S are routed through the hijacker's host using **Forged ICMP** and **ARP Spoofing**.
- **IP spoofing: Source routed packets:** Spoof the host's IP so that the server managing a session with the host accepts the packets from the attacker.

Session Hijacking Tools:

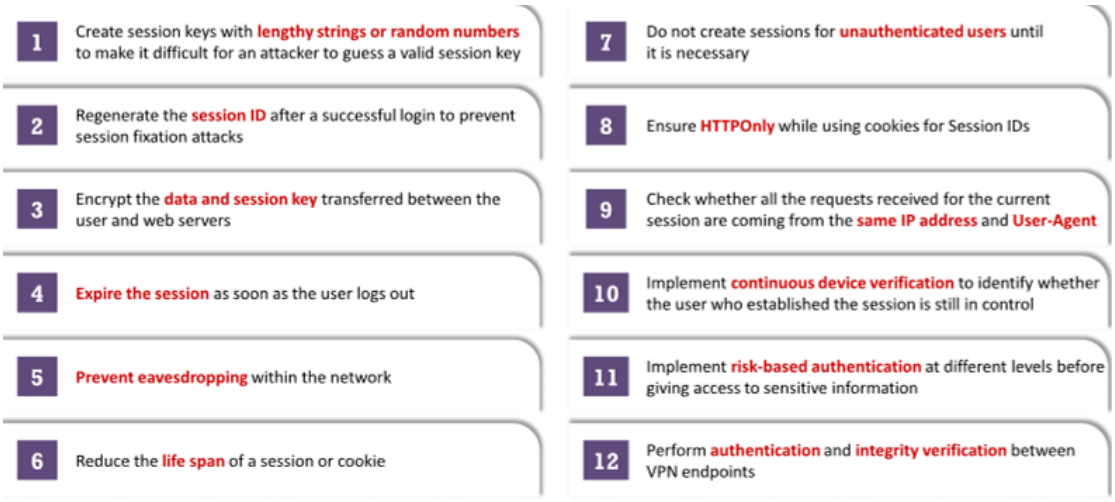
- Burpsuite
- OWASP ZAP
- bettercap
- ssltrip

Countermeasures

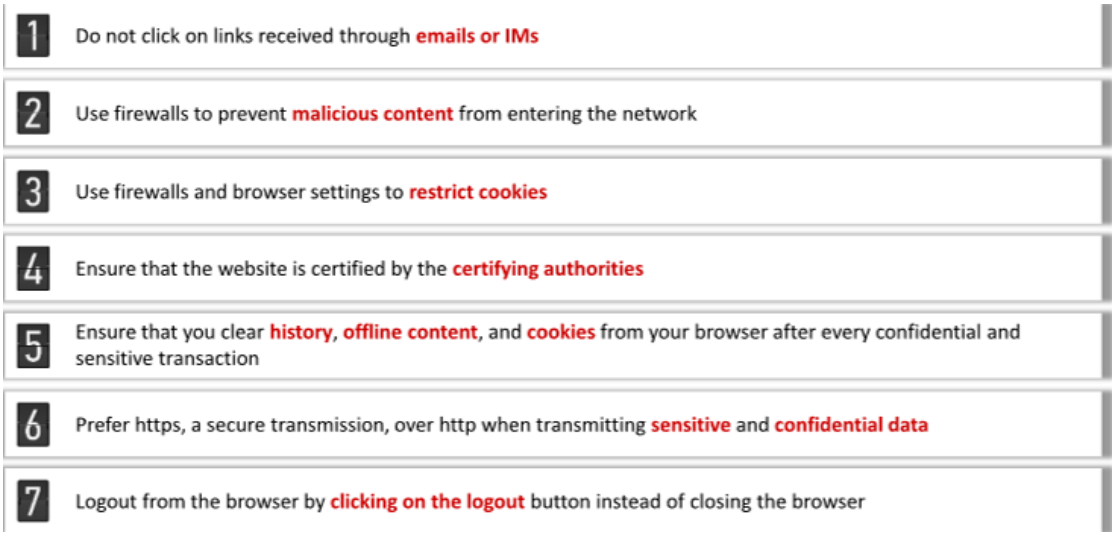
- Detection Method
    - Manual Method
        - Using packet sniffing software
    - Automatic Method
        - IDS
        - IPS

- Protect against Session Hijacking

- Web Dev Guielines to Prevent Session Hijacking



- Web User Guidelines to Prevent Session Hijacking



- Detection Tools
  - AlienVault USM
  - Wireshark
- Approaches Causing Vulnerability to Session Hijacking and Their Preventative Solutions
  - Telnet, rlogin -> OpenSSH or ssh
  - FTP -> SFTP, AS2, MFT, FTPS
  - HTTP -> SSL or TLS
  - IP -> IPsec
  - Any remote connection -> VPN
  - SMB -> SMB signing
  - Hub Network -> Switch Network
- Approaches to Prevent Session Hijacking
  - **HSTS (HTTP StrictTransport Security):** A **web security policy** that protects HTTPs against MITM. Allow web server to **enforce web browsers** to interact with it using HTTPS

    - **Token Binding:** When a user logs on a web app, it generates a cookie with an **SID**, called **token**.
    - **HPKP (HTTP Public Key Pinning):** A **TOFU (Trust on First Use)** technique used in an HTTP header. Allow a web client to **associate a specific public key certificate** with a particular server to minimize the risk of MITM
- Approaches to Prevent MITM Attacks
    - WEP/WPA Encryption
    - VPN
    - TFA
- **IPSec**
    - A protocol suite developed by the IETF for **securing IP communication** by **authenticating and encrypting** each IP packet of a session.
    - Deployed widely to implement **VPNs** and for **remote user access** through dial-up connection to pricate networks
    - **Components:**
        - **IPsec Driver:** Software that performs protocol-level functions required to encrypt and decrypt packets
        - **IKE (Internet Key Exchange):** An protocol that produces security keys for IPsec and other protocols
        - **ISAKMP (Internet Securtity Association Key Management Protocol):** Software that allows two computers to communicate by encrypting the data exchanged between them
        - **Oakley:** A protocol that uses the **Diffie-Hellman algorithm** to create a master key and a key that is specific to each session in IPsec data transfer
        - **IPsec Policy Agent:** A service included in Windows OS that enforces IPsec policies for all the network communications initiated from that system
    - **Benefits**
        - Network-level peer authentication
        - Data origin authentication
        - Data integrity
        - Date confidentiality
        - Replay protection
    - Modes of IPsec
        - **Transport Mode:** Also ESP, encrypts only the **payload** of the IP packet, leaving the header untouched.
        - Tunnel Mode: Also AH, encrypt **both the payload and header**. More secure than the transport mode.
    - IPsec Architecture:
        - **AH (Authentication Header):** Offer **integrity** and data origin authentication, with optional anti-replay features.

        - **ESP (Encapsulating Security Payload):** Offer all the services offered by AH as well as **confidentiality**
        - **DOI (IPsec Domain of Interpretation):** Define the payload formats, types of exchange, and naming conventions for security info such as cryptographic algorighms or security policies
        - **ISAKMP (Internet Security Association and Key Management Protocol):** A key protocol in the IPsec architecture that establishes the required security for various communications over the Internet, such as gov, private, and com communications.
        - **Policy:** Define when and how to secue data, as well as security methods to use at differnet level in the network.
- Session Hijacing Prevention Tools:
    - CxSAST
    - Fiddler

Module 12: Evading IDS, Firewalls, and Honeypots

IDS:

- Also referred to as a packet sniffer, which intercepts packets traveling via various communication media and protocols
- Check traffic for signatures that match known intrusion patterns and signals an alaram when a match is found
- Placed outside/inside the firewall
- How an IDS detects an Intrusion?
    - **Signature Recongnition:** Misuse detection, tries to identify events that indicate an abuse of a system or network resource.
    - **Anomaly Detection:** Not-use detection, base on the fixed behaviroal characteristics of the users and components in a computer system
    - **Protocol Anomaly Detection:** Models are built to explore anomalies in the way in which vendors deploy the TCP/IP specification
- **Types of IDS**
    - **Network-Based IDS:** Consist of a black box that is placed on the network in a promiscuous mode, listening for patterns indicative of an instrusion.
    - **Host-Based IDS:** Usually include auditing for events that occur on a specific host
- **Types of IDS Alerts**
    - TP: Attack->Alert
    - FP: No Attack -> Alert
    - FN: Attack -> No Alert
    - TN: No Attack -> No Alert

IPS

- Also considered as an **active IDS** since it is capable of not only detecting..but also preventing..
- Unlike an IDS, which is passive, an IPS is placed **inline in the network**, between the src and dst to **actively analyze the network traffic** and to automatically take decisions
- Types of IDS: Network-based IPS, Host-based IPS
- **Adv over IDS**
    - IPS can block as well as drop illegal packets
    - Be used to monitor activities occurting in a single org
    - Can prevent the occurrence of direct attacks in the network by controlling the amount of network traffic

Firewall

- Hardware or software designed to prevent **unauthorized access** to or from a private network.
- Placed at the junction or **gateway** between two networks, which is usually between a private network and a public network such as the Internet
- **Architecture**
    - **Bastion Host:** A computer system designed and configured to protect network resources from attacks.
    - **Screened Subnet:** The screened subnet or DMZ contains hosts that offer public services.
    - **Multi-homed Firewall:** A firewall with two or more interfaces is present that allows further subdivision of the network based on the specific security objectives of the org
- Technologies operating at each OSI layer

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

- **Technologies**
    - **Packet Filtering**
        - Work at the **network layer** of OSI (or Internet layer of TCP/IP), usually form part of a router
        - Each packet is compared to a set of criteria before it is forwarded
    - **Circuit Level Gateways**
        - **Session** layer of OSI (**Transport** layer of TCP/IP)

        - Info passed to a remote computer through a circuit-level gateway
        - Monitor requests to create sessions and determine if those sessions will be allowed
        - Allow or prevent data stream, not individual packets
    - **Application Level Firewall**
        - Application-level gateways (Proxies) can filter packets at the **application** layer of OSI (**Application** Layer of TCP/IP)
        - Traffic is **restricted to services** supported by the proxy
        - Configured as a web proxy prohibit FTP, gopher, telnet, or other traffic
        - Examine traffic and filter on **application-specific commands** such as http:post and get
    - **Stateful Multilayer Inspection**
        - **Combine the aspects of the other three types** of firewalls
        - Filter packets at the network layer of OSI or the Internet layer of TCP/IP, and evaluate the contents of packets at the application layer
    - **Application Proxies**
        - Work as a proxy server and filter connection for specific services
        - Filter connections based on the services and protocols appropriate to that application
    - **NAT**
        - Work with a router, similar to packet filtering. Modify the packet the router sends simultaneously
        - Have the ability to change the address of the packet and make it appear to have arrived from a valid address
        - It can act as a firewall filtering techniques
    - **VPN**
        - **A private network** constructed using public networks
        - Used for **secure tranmission**, using **encapsulation and encryption**
        - Establish a virtual p2p connection through the **used of dedicated connections**
- Limitations
    - Does not protect the network from new **viruses, backdoors, insider attacks**
    - Do nothing if the network design or configuration is faulty
    - Not an alternative to AV or antimalware protection
    - Do not prevent password misuse
    - Do not block attacks from a **higher level of the protocol stack**
    - Do not protect against attacks from **dial-in connections** or attacks originating from **common ports** and applications
    - Unable to understand **tunneled traffic**

Honeypot

- An info system resource that is expressly set up to **attract and trap** attackers
- Log port access attempts or monitor an **attacker's keystrokes**
- **Types of Honeyports**
    - Low-interaction Honeypots
    - Medium-interaction Honeypots
    - High-interaction Honeypots
    - Pure Honeypots
- **Classfication of honeypots based on strategy**
    - Production Honeypots
    - Research Honeypots
- **Classfication of honeypots based on deception technology**
    - Malware Honeypots
    - Database Honeypots
    - Spam Honeypots
    - Email Honeypots
    - Spider Honeypots
    - Honeynets

Intrusion Detection Tools

- **Snort**
    - Can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and OS fingerprinting attempts
    - Use a flexible rules language to describe traffic
    - Uses of Snort
        - Straight packet sniffer like tcpdump
        - Packet logger
        - Network IPS
    - **Rules:** rule action+rule protocol+rule format direction+rule ip+rule port+alert message

    - Rule Actions
        - Alert

        - Log
        - Pass: Drop (Ignore) the packet
    - IP Protocols
        - TCP
        - UDP
        - ICMP
- **Suricata**
- **AlienBault OSSIM**

IPS Tools

- **AlienVault Unified Security Management (USM)**
- **Firewalls: ZoneAlarm Free Firewall 2019**
- **ManageEngine Firewall Analyzer**

Honeypot Tools

- **KFSensor:** A host-based IDS that acts as a honeypot
- **SPECTER**

IDS Evasion Techniques

- **Insertion Attack**
    - The process by which the **attacker confuses the IDS** by forcing it to read invalid packets
    - An IDS blindly believes and accepts a packet that an end system rejects, and an attacker exploit this condition and **inserts data into the IDS**
    - Occurs when the NIDS is less strict in processing packets than the internal network
    - Obscure extra traffic and the IDS concludes the traffic is safe. The **IDS gets more packets** than the destination.
- **Evasion**
    - An end system **accepts a packet** that an IDS rejects.
    - An attacker **exploits the host computer** without the IDS realizing it,
    - The attacker sends **portions of the request i**n packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the IDS
- **DoS Attack**
    - Many IDSs use a centralized server for logging alerts
    - Attackers can perform DoS on the centralized server
    - The attackers' intrusion attempts will not be loggeg
- **Obfuscating**

    - Attacker who **encode the attack packet payload** that only the des host can decode it.
    - Attackers manipulate the **path referenced in the signature** to fool the HIDS
    - **Encode attack patterns in unicode** to bypass IDS filters, but be understood by an IIS web server
    - **Polymorphic code** is another means to circumvent **signatured-based** IDSs by creating different attack patterns
    - Attacks on **encrypted protocol** are obfuscated
- **FP generation**
    - Craft malicious packets just to generate alerts
    - Use these FP alerts to hide the real attack traffic
- **Session Splicing**
    - **Split the attack traffic** into many packets such no single packet triggers the IDS
    - IDSs stop reassembly if they **do not receive packets within a certain time**
    - The IDS will stop working if the target host keeps the session active for a time longer than the **IDS reassembly time**
- **Unicode Evasion**
    - All the code points are treated differently but it is possible that there could be multiple representations of a single char in the Unicode code space
    - IDS handle unicode improperly as Unicode allows multiple interpretations of the same char
- **Fragmentation Attack**
    - Fragmentation timeouts vary between the IDS and the host
- **Overlapping Fragments**
    - **Generate a series of tiny fragments** with overlapping TCP seq numbers
- **TTL Attacks**
    - The attacker has to have a prior knowledge of the topology of the victim's network
    - The info can be obtained using tools such as craceroute
- **Invalid RST Packets**
    - TCP uses a 16-bits checksum field for error-checking of the header and data
    - The attack makes the IDS think the communication has ended
- **Urgency Flag**
    - Many IDSs **do not consider the urgent pointer** and process all the packets in the traffic, wheras the taraget processes the urgent data only
    - Result in the IDS and the target system having **dfferent sets of packets**, which can be exploited by attackers
- **Polymorphic Shellcode**
    - Include **multiple signatures**

    - **Encode the payload**
    - The **shellcode is completely rewritten** each time it is sent
    - **Evade the ommonly used shellcode strings**
- **ASCII Shellcode**
    - Bypass the IDS signature as the **pattern matching** does not work effectively with the ASCII values
- **Application-layer Attacks**
    - IDS cannot verify the **signature of the compressed file format**
- **Desynchronization**
    - **Pre-Connection SYN:** Send an initial SYN before the real connection is established, but with an invalid TCP checksum
    - **Post-Connection SYN:** Send a post connection SYN packet which will have divergent seq numbers.
- **Encryption**
- **Flooding:** Produce noise

Evading Firewalls

- **Firewalking:** Use TTL value to determine gatyeway ACL filters and it maps networks
- **Banner Grabbing:** Fingerprinting method to detect the vendor of a firewall and its firmware version.
- **IP Address Spoofing**
- **Source Routing:** Allow the sender of a packet to partially or completely specify the route
- **Tiny Fragments:** Create tiny fragments of outgoing packets forcing some of the TCP packet's header info into the next fragment
- **Using an IP Address in Place of a URL**
- **Using a Proxy Server**
- **ICMP Tunneling:** Allow tunneling a backdoor shell in the data portion of ICMP Echo packets. By using **Loki ICMP tunneling** to execute cmds of choice by tunneling them inside the payload of the ICMP echo packets
- **ACK Tunneling:** Allow tunneling a backdoor application with **TCP packets with the ACK bit set**. Tool such as **AckCmd** can be used to…
- **HTTP Tunneling:** Allow attackers to perform various Internet tasks desipte the restrictions imposed by firewall. Encapsulates data inside HTTP traffic. Can use tools such as **HTTPort and HTTHost**, **Super Network Tunnel**
- **SSH**: Tools such as **OpenSSH, Bitvise,** and **Secure Pipes**
- **DNS Tunneling:** Small size constraint on external queries allow the DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Tools such as **NSTX, Heyoka**, and **Lodine** use this technique of tunneling traffic aross DNS port 53.

- **Through External Systems:** Attackers sniff the user traffic and steal the SID and cookie. Redirect users' web browser to the attacker's web server. Download and execute…
- **Through MITM Attack:** Make use of DNS server and routing techniques. DNS poisoning, redirect, download and execute.
- **Through Content:** Send content containing malicious code and trick a user to open it.
- **Through XSS**

Evasion Tools

- **Traffic IQ Professional:** Generate custom attack traffic
- **Packet Fragment Generator Tools:** Colasoft Packet Builider

Detect Honeypots

- Layer7 : Observe the latency of the response.
- Layer4: Analyze the TCP window size
- Tools: **Send-Safe Honeypot Hunter**, checking lists of HTTPS and SOCKS proxies for honey pots.

IDS Evasion Countermeasures

- Shut down switch ports associated with known attack hosts.
- Perform an in-depth analysis of ambiguous network traffic for all possible threats.
- Use TCP FIN or Reset (RST) packet to terminate malicious TCP sessions.
- Look for the nop opcode other than 0x90 to defend against the polymorphic shellcode problem.
- Train users to identify attack patterns and regularly update/patch all the systems and network devices.
- Deploy IDS after a thorough analysis of the network topology, nature of network traffic, and number of hosts to monitor.
- Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS.
- Ensure that IDS normalize fragmented packets and allow those packets to be reassembled in the proper order.
- Define DNS server for client resolver in routers or similar network devices.
- Harden the security of all communication devices such as modems, routers, etc.
- If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a considerable value, ensuring that the end host always receives the packets.
- Regularly update the antivirus signature database.

- Use a traffic normalization solution at the IDS to protect the system from evasions.
- Store the attack information (attacker IP, victim IP, timestamp) for future analysis.

Defend against Firewall Evasoin

- The firewall should be configured such that the IP address of an intruder should be filtered out.
- Set the firewall rule set to deny all traffic and enable only the services required.
- If possible, create a unique user ID to run the firewall services instead of running the services using the administrator or root ID.
- Configure a remote syslog server and adopt strict measures to protect it from malicious users.
- Monitor firewall logs at regular intervals and investigate all suspicious log entries found.
- By default, disable all FTP connections to or from the network.
- Catalog and review all inbound and outbound traffic allowed through the firewall.
- Run regular risk queries to identify vulnerable firewall rules.
- Monitor user access to firewalls and control who can modify the firewall configuration.
- Specify the source and destination IP addresses as well as the ports.
- Notify the security policy administrator about firewall changes and document them.
- Control physical access to the firewall.
- Take regular backups of the firewall rule set and configuration files.
- Schedule regular firewall security audits.

Module 13: Hacking Web Servers

Web Server Operations

- **Components:**
  - **Document Root:** Store critial HTML files related to the web pages of a domain name that will be served in response to the requests.
  - **Server Root:** Store server's configuration, error, executable, and logs
  - **Virtual Document Tree:** Provide storage on a different machine or disk after the original disk if filled up
  - **Virtual Hosting:** Technique of hosting multiple domains or websites on the same server
  - **Web Proxy:** Sit between the web client and web server to prevent IP blocking and maintain anoymity
- **Issues**
  - Attack targets **software vulnerabilities** and configuratrion errors
  - **Network** and **OS level** attacks can be well defended using proper network security measures such as firewalls, IDS, etc. Web server can be accessed from anywhere via the Internet, which renders them highly vulnerable to attacks
- **Why are Web Servers Compromised?**
  - Improper file and dir permissions
  - Installation with default settings
  - Enabling of unnecessary services
  - Security conflicts with businese ease-of-use case
  - Lack of proper security policies, procedures, and maintenance
  - Improper authentication with external systems
  - Default accoutns having default passwords, or no passwords
  - Unnecessary default, backup, or sample files
  - Misconfiguration in web server, OS, and networks
  - Bugs in server software, OS, and web applications
  - Misconfigured SSL certificates and encryption settings
  - Administrative or debugging functions that are enbaled or accessible on web servers
  - Use of self-signed certificates and default certificates

Web Server Attacks

Web Server Attacks

- **DoS/DDoS Attacks**
- **DNS Server Hijacking**
- **DNS Amplification Attack:** Take the adv of the **DNS recursive method** of DNS redirection to perform DNS amplification attacks. Attacks use compromised PCs with **spoofed IP address** to…
- **Directory Traversal Attacks:** Attackers use the **../** seq to access restricted dir outside the web server root dir.
- **MITM/Sniffing Attack**
- **Phishing Attacks**
- **Website Defacement**
- **Web Server Misconfiguration**
- **HTTP Response-Splitting Attack:** Involve adding header response data into the input field so that the server splits the ressponse into two responses. The attacker can control the first response to redirect the user to a malicious website wheras the other responses are discarded by the web browser
- **Web Cache Poisoning Attack:** Attackers **swap cached content** for a random URL with infected content
- **SSH Brute Force Attack:** SSH tunnels can be used to transmit malwars and other exploits to victims without being detected
- **Web Server Password Cracking:** Mainly target SMTP server, Web Shares, SSH Tunnels, Web form authentication cracking, FTP servers.
- **SSRF (Server-side Request Forgbery) Attack:** Attackers **send crafted requests** to the internal or back end servers by exploiting SSRF vulnerabilities in a public web server.

Web Application Attacks

- Parameter/Form Tampering
- Session Hijacking
- DoS Attack
- CSRF
- Cookie Tampering
- SQL injection
- XSS
- Command Injection Attacks
- Unvalidated Input and File injection Attacks
- Directory Traversal

- Buffer Overflow Attacks
- Source Code Disclosure

Web Server Attack Methodology

- **Info gathering:**
    - Search the **Internet, newsgroups, bulletin boards**…
    - Use tools such as **Whois.net** and **Whois Lookup**.
    - Gather info from **Robots.txt** file, it lists **web server dirs and files** that the web site owner wants to hide from web crawlers.
- **Web Server Footprinting/Banner Grabbing:**
    - Gather **valuable system-level data** such as account detailsm OS, software versions, server names, and database schema details
    - **Telnet** a web server to footprint a web server and gather info such as server name, server type, OS, and applications running
    - Use tools such as **Netcraft, httprecon, and ID Serve** to perform footprinting
    - **Netcat:** Read and write data across network connections, using TCP/IP protocol
    - **Telnet:** Probe HTTP servers to determine the Server field in the HTTP response header
    - **NMAP: Enumerate web server info** by using commands and **NSE scripts**.
- **Website Mirroring**
    - Create a complete profile of the site's **dir structure, file structure, external links**, etc
    - Use tools such as **NCollector Studio**, **HTTrack Web Site Copier**, **WebCopier Pro**, etc.
    - Finding Default Credentials of Web Server **(Independent)**
    - Finding Default Content of Web Server **(Independent)**
    - Finding Directory Listings of Web Server **(Independent)**
- **Vulnerability Scanning**
    - Tools such as **Acunetix Web Vulnerabilitiy Scanner**, **Fortify WebInspect**
- **Session Hijacking**
    - Techniques such as **session fixation, session sidejacking, XSS**, etc.
    - Tools such as **Burp Suite, JHijack, Ettercap**
- **Web Server Passwords Hacking**
    - Tools such as **Hashcat, THC Hydra, Ncrack**

- **Using Application Server as a Proxy (Independent)**
    - Attackers use **GET** and **CONNECT** requests to use vulnerable web servers as proxies to connect…

Web Server Attack Tools

- **Metasploit**
    - **Exploit Module**: Basic module in Metasploit used to e**ncapsulate an exploit**
    - **Payload Module:** Establish **a communication channel** between the MSF and the target. Combine the arbitary code that is executed because of the success of an exploit.
    - **Auxiliary Module:** Can be used to perform arbitrary, one-off actions such as port scanning, DoS, and even fuzzing.
    - **NOPS Module:** Generate a no-operation instruction used for blocking out buffers. Use **generate** command to generate a NOP sled of arbitrary size and display it in a specific format.
- **Immunity's CANVAS**

Countermeasures

- Place web servers in separate secure server security segment on Network
- Patches and updates
- Protocols and Accounts
- Files and Dirs

Detect Web Server Hacking Attempts

- A website change detection system
- Ports, Server Certificates, Machine.config, Code Access Security

Defend against HTTP RespONSE-Splitting and Web Cache Poisoning

- **Server Admin**
- **Application Developers:** Comply with **RFC 2616** specifications for **HTTP/1.1**

- **Proxy Server:** Avoid sharing **incoming TCP connections** among different clients. Use different TCP connections with the proxy for different **virtuals hosts**. Implement "maintain request host header" corrently.

Defend Against DNS Hijacking

- Choose a registrar accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) and encourage them to set REGISTRAR-LOCK on the domain name.
- Safeguard the registrant's account information.
- Include DNS hijacking in incident response and business continuity planning.
- Use DNS monitoring tools/services to monitor the IP address of the DNS server and set up alerts.
- Avoid downloading audio and video codecs and other downloaders from untrusted websites.
- Install an antivirus program and update it regularly.
- Change the default router password.
- Restrict zone transfers and use script blockers in the browser.
- **Domain Name System Security Extensions (DNSSEC):** It adds an extra layer to DNS that prevents it from being hacked.
- **Strong Password Policies and User Management:** The use of strong passwords further enhances security.
- **Better Service Level Agreements (SLAs) from DNS Service Providers:** When signing up for DNS servers with DNS service providers, learn who to contact when an issue occurs, how to receive good-quality reception and support, and whether the DNS server's infrastructure is hardened against attacks.
- **Configuring a Master-Slave DNS within your Network:** Use a master-slave DNS and configure the master without Internet access. Maintain two slave servers so that even if an attacker hacks a slave, it will update only when it receives an update from the master.
- **Constant Monitoring of DNS Servers:** The constant monitoring of DNS servers ensures that a domain name returns the correct IP address.
- **Ensure Router Safety:** Change the default username and password of the router. Keep the firmware up to date for ensuring safety from new vulnerabilities.
- **Use VPN Service:** Establish virtual private network (VPN)-encrypted tunnels for secure private communication over the Internet. This feature protects messages from eavesdropping and unauthorized access.

Patches and Hotfixes

- **Hotfix:** An update fo fix a specific customer issue
- **Patch:** Small piece of software designed to fix problems
- **Patch Management:** A process used to fix known vulnerabilities by ensuring the appropriate patches are installed.
- **Patch Management Process**
    - **Detect**
    - **Assess**
    - **Acquire**
    - **Test**
    - **Deploy**
    - **Maintain**
- Patch Management Tools: **GFI LanGuard**

Web Application Security Scanners

- Syhunt Hybrid
- N-Stalker X
- ScanMyScanner

Web Server Malware Infection Monitoring Tools

- QualysGuard Malware Detectoin

Web Server Security Tools

- Fortify WebInspect

Web Server Pentesting Tools

- CORE Impact
- Immunity CANVAS

Module 14: Hacking Web Applications

Web Applications

- Interface between end users and web servers
- Services: An application or software that is deployed over the internet and uses standard messaging protocols such as **SOAP, UDDI, WSDL**, and **REST** to enable communication
- Types of web services
    - **SOAP:** Based on the **XML format** and is used to transfer data between a service provider and requestor
    - **RESTful:** Based on **a set of constraints** using underlying HTTP concepts to improve performance
- Components of web service architecture
    - **UDDI: Universal Description, Discovery, and Integration** 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 sercices security** plans 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.

Web Applications Threat

- OWASP Top10
    - **Injection**
    - **Broken Authentication**
    - **Sensitive Data Exposure**
    - **XML External Entity**
    - **Broken Access Control**
    - **Security Misconfiguration**
    - **Cross-Site Scripting**
    - **Insecure Deserialization**
    - **Using Components with Known Vulnerabilities**
    - **Insufficient Logging and Monitoring**
- Injection
    - Allow untrusted data to be interpreted and executed as part of a cmd or query

    - **SQL injection:** bypass normal security measures and obtain access, executed from the address bar, applications fields…
    - **Cmd injection:** shell injection, html embedding (deface website virtually), file injection
    - **File injection**
    - **LDAP injection**
    - **Server-Side JS injection**
    - **Server-Side Includes Injectoin**
    - **Server-Side template injection**
    - **Log injection**
    - **HTML injection**
    - **CRLF (Carriage return line feed) injection:** inject carriage return (\n) and linefeed (\n) char into user input to trick a web server, web application, or user to terminate the input of a current object and initial a new object
- Broken Authentication
    - Session ID is URLs
    - Password Exploitation
    - Timeout Exploitation
- Sensitive Data Exposure
    - Poorly written encryption code
- XXE
    - A SSRF attack that occur when a misconfigured XML parser allows applications to parse XML input
- Broken Access Control
    - Security Misconfiguration
    - Unvalidated Inputs
    - Parameter/Form tampering
    - Improper error handling
    - Insufficient transport layer protection
- XSS
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring
- Other Web application threats
    - **Directory Traversal:** Manipulate variables that reference files with “dot-dot-slash (../)” sequences and its variations.
    - **Unvalidated Redirects and Forwards**
    - **Watering hole attack**

    - **CSRF**
    - **Cookie/Session poisoning**
    - **Web service attacks**
    - **Cookie Snooping**
    - **Hidden Field Manipulation**
    - **Authentication Hijacking**
    - **Obfuscation appliiciation**
    - **Broken session management**
    - **Broken account management**
    - **DoS**
    - **Buffer Oveflow**
    - **CAPTCHA Attacks**
    - **Platform exploits**
    - **Network access attacks**
    - **DMS protocol attacks**
    - **Web-based timing attacks**
    - **MarioNet attack**
    - **RC4 NOMORE attack:** Against RC4 stream cipher
    - **Clickjacking atack**
    - **JS hijacking**
    - **DNS Rebinding attack:** Bypass the same-origin policy's security constraints and communicate with or make arbitrary requests to local domains through a milicous web page

Web Application Hacking Methodology

- Footprint web infrastructure
    - **Server Discovery:** whois, dns interrogation, port scanning
    - **Service Discovery:** nmap, netscantools pro…
    - **Server Identification:** banner grabbing, telnet
    - **Detect web app firewalls and proxies:** trace method, WAFW00F
    - **Hidden Content Discovery:** OWASP ZAP, burpsuite
    - **Load Balancer Detection:** host, dig, lbd, Halberd
- Analyze Web Applications
    - **Identify entry points for user input:** User-agent, referer, accept, accept-language, host headers
    - **identify server-side technologies:** Error message, HTTP headers, HTML code

    - **identify server-side functionality:** GNU Wget, Teleport Pro, BlackWidow
    - **identify files and dirs:** Gobuster, Nmap nse script http-enum
    - **identify web application vulnerabilities:** Vega
    - **map the attack surface**
- Bypass Client-Side controls
    - **Attack Hidden Form Fields**
    - **Attack Browser Extensions**
    - **Perform Source Code Review**
    - **Evade XSS Filters:** Encoding char, Embedding whitespaces, Manipulate tags
- Attack Authentication Mechanism
    - **Username Enumeration**
    - **Password Attacks**
    - **Cookie Exploitation**
    - **Session Attacks**
    - **Bypass authentication:** SAML (Security Assertion Markup Language) messages are encrypted using base64 encoding
- Attack Authorization Schemes
    - URI
    - POST data
    - Query String and Cookie
    - Parameter Tampering
    - HTTP Headers
    - Hidden Tags
- Attack Access Controls
    - Exploiting insecure access controls
- Attack Session Management Mechanism
- Perform Injection Attacks/Input validation attacks
    - Web Scripts injection
    - OS cmd injection
    - SMTP injection
    - SQL injection
    - LDAP injection
    - XPath injection
    - Buffer Overflow
    - File injection
- LFI (Local File Inclusion): Enable attackers to add their own files on a server
- Attack Application Logic Flaws

- Attack Shared Environments
- Attack Database Connectivity
    - **Connection String injection:** Inject para in a connection string by appending them with **semicolon (;)** char
    - **CSPP (Connection String Parameter Pollution) Attacks:** Overwrite para values in the connection string to steal user IDs to hijack web credentials
    - **Connection Pool DoS:** Construct a large malicious SQL query
- Attack Web App Client
    - XSS
    - HTTP header injection
    - Request Forgery Attack
    - Privacy Attack
    - Redirection attacks
    - Frame injection
    - Session fixation
    - ActiveX attacks
- Atack Web Services
    - Probing Attacks
    - SOAP Injection, similar to sql injection
    - **SOAPAction Spoofing**: SOAPActoin is an additional HTTP header used when SOAP messages are transmitted using HTTP. **WS-Attacker** can be used to manipulate the operations included in the SOAPAction headers.
    - **WS-Address Spoofing**: WS-address provides additional routing info in the SOAP meader to support **asynchronous conmmunication**. Attackers send a SOAP message containing fake WS-address info to the server
    - **XML Injection**
    - **Parsing Attacks:** DoS attack or logical errors in web service request processing
    - **Tools:** SoapUI Pro, XMLSpy

WEB Service APIs

- **SOAP API:** Enable interactions between applications running on different platforms.
- **REST (Representation State Transfer) API :** An architectural style for web services that serves as a communication medium between various systems on the web

- **RESTful API:** Known as RESTful services, are designed using REST principles and HTTP communication protocols. A collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE
- **XML-RPC**
- **JSON-RPC**

Webhooks

- **User-defined HTTP callback** or push APIs that are raised based on events triggered
- Allow applications to **update other appliucations** with the latest info
- Are enrolled along with the **domain registration** via user interface or API to inform clients

OWASP Top10 API Security Risks

- Broken Object Level Authorization
- Broken User Authentication
- Excessive Data Exposure
- Lack of Resources and Rate Limiting
- Broken Function Level Authorization
- Mass Assignment
- Security Misconfiguration
- Injection
- Improper Assets Management
- Insufficient Logging and Monitoring

API Vulnerabilities

- Enumerated resources
- Sharing resources via Unsigned URLs
- Vulnerabilities in Third-Party Libs
- Improper Use of CORS
- Code Injections
- RBAC (Role-based access control) Privilege Escalation
- No ABAC (Attribute-based access control) Validation
- Business Logic Flaws

WEB API hacking methodology

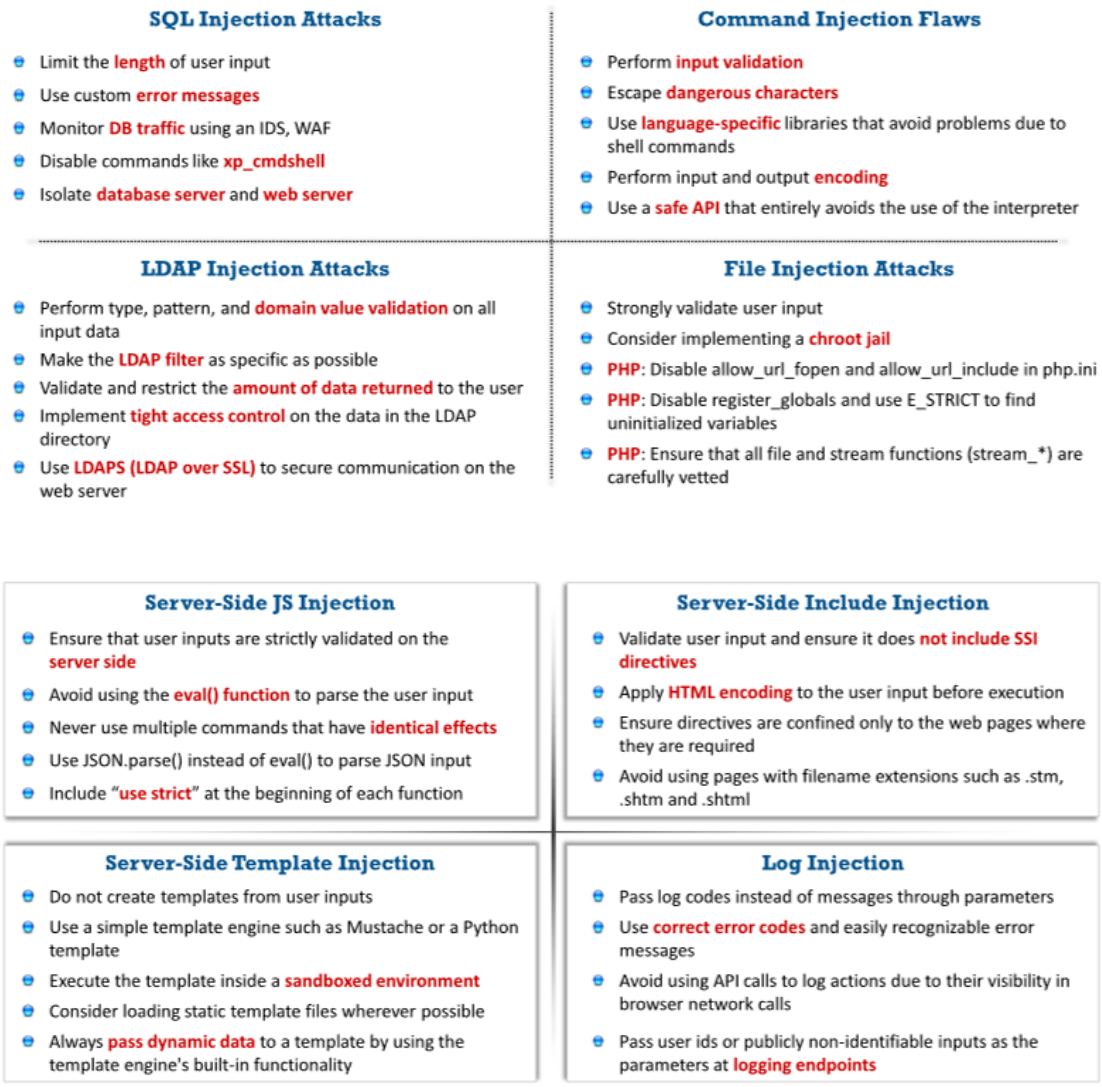
- Identify the target
    - SOAP and REST mostly use HTTP protocols
    - JSON for REST API, XML for SOAP API
- Detect security standards
    - SOAP and REST implement different authentication/authorization standards such as **OpenID Connect, SAML**, OAuth 1.x and 2.x, and WS-Security
    - SSL **only encrypt sensitive user data**
- Identify the attack surface
    - API metadata reveals a lot of technical info such as paths, parameters, and message formats
    - Attacker monitors and records the communication between the API and a client to identify an initial attack surface
- Launch attacks
    - Fuzzing
    - Invalid input attacks
    - Malicious input attacks
    - Injection attacks
    - Insecure SSL configuration
    - IDOR (Insecure direct object references)
    - Insecure session/Authentication handling
    - Login/ Credential Stuffing Attacks
    - API DDOS attacks
    - Authorization attacks on API:
        - OAuth is an authorization protocol that allows a user to **grant limited access** to their resources on a site to a different site without having to expose their credentials
    - reverse engineering
    - user spoofing
    - MITM attack
    - Session replay attacks
- REST API Vulnerabilitiy Scanning: **Astra, OWASP ZAP**
- Bypass IDOR via parameter pollution

Web Shells

- A malicious piece of code or script that is developed using **server-side languages** such as PHP, ASP, PERL, RUBY, and Python and are then installed on a target server
- Attackers **inject malicious script** by exploiting most common vulnerabilities such as remote file inclusion (RFI), local file inclusion (LFI), exposition of administration interfaces, and SQL injection.
- Tools: WSO php webshell
- Gain backdoor access:
    - Attackers exploit **non-validated file uploads** to inject malicious script in a target webserver to gain backdoor access
    - Use tool such as **Weevely** to gain backdoor access to a website without being traced
    - Weevely also helps attackers in performing administrative tasks, maintaining persistence, and spreading backdoors across the target network
- Web Shell Detection Tools: **Web shell detector**

Web Application Securtity Testing

- **Manual web app security testing**
- **Automated web app security testing**
- **SAST (Static application security testing):** white-box
- **DAST (Dynamic application security testing):** black-box
- **Fuzz testing:** a black-box testing method. Huge amounts of **random data** will be generated and used against…
- **Source code review**
- **Encoding schemes:** URL encoding, HTML encoding, unicode encoding, base64 encoding, hex encoding
- **Defend against injection**



- RASP for protecting web servers: **Runtime application self protection** can detect runtime attacks.
- Testing tools: Acunetix **WVS, N-Stalker Web App Security Scanner**
- **Firewalls:** dotDefender

Module 15: SQL Injection

Concept

- It is a flaw in web apps and not a database or web server issue
- Technique to take advantage of un-sanitized input vulnerabilitie to pass SQL cmds through a web app for execution by a backend database
- Gain unauthorized access, retrieve info

Technologies

- Server-side technology
- Exploit
- Susceptible databases
- Attack

Types of SQL injection

- **In-band sql injection:** The same communication channel to perform the attack and retrieve the results.
- **Blind/inferential sql injection:** Have no error messages from the system to work on.
- **Wait for delay, BENCHMARK()**
    - **Boolean Exploitation:** compare the response page to infer whether the injection is successful
    - **Hevay Query:** Use multiple joins on system table, retrieve a significant amount of data and taks a long time to execute. **Example:** SELECT * FROM products WHERE id=1 AND 1 < SELECT count(*) FROM all_users A, all_users B, all_users C
- **Out-of-band sql injection:** Different communication channels to perform the attack and obtain the results
    - For example, in a Microsoft SQL Server, an attacker exploits the x**p_dirtree command t**o send DNS requests to a server controlled by the attacker Copyright

SQL injection methodology

- Information gathering and vulnerability detection
    - identify data entry paths: analyze web GET and POST requests
    - extract info through error messages

- Launch attack
    - perform union sql injection, exreact database name, tables, column names, 1st field data
    - perform error based sql injection
    - bypass website logins using sql injection
    - perform double blind sql injection, based on time delays.
    - perform blind sql injection using out-of-band exploitation technique
    - exploit second-order sql injection
    - bypass firewall:
        - normalization method
        - HPP (HTTP parameter pollution) technique
        - HPF(HTTP parameter fragmentation) technique
        - blind sql injection
        - signature bypass
        - buffer overflow method
        - crlf technique
        - integration method
- advanced sql injection
    - database, table, column enumeration
    - create datavase accounts
    - password grabbing
    - grabbing sql server hashes
    - transfer database to attacker's machine: An sql server can be linked back to an attacker's DB via **OPENROWSET**. This can be accomplished by connecting to a remote machine on port **80**.
    - interact with os
    - interact with the file system, **LOAD_FILE(), INFTO OUTFILE()**
    - network reconnaissance
    - PL/SQL exploitation
    - Create server backdoors
    - http header-based sql injection: X-Forwarded-For, User-Agent, Referer
    - DNS exfiltration

Tools

- sqlmap
- Mole
- blisqy

Evasion Techniques

- **In-line Comment:** Obscures input strings by inserting in-line comments between SQL keywords.

- **Char Encoding:** Uses a built-in CHAR function to represent a character.
- **String Concatenation:** Concatenates text to create an SQL keyword using DB-specific instructions.
- **Obfuscated Code:** Obfuscated code is an SQL statement that has been made difficult to understand.
- **Manipulating White Spaces:** Obscures input strings by inserting a white space between SQL keywords.
- **Hex Encoding:** Uses hexadecimal encoding to represent an SQL query string.
- **Sophisticated Matches:** Uses alternative expression of "OR 1=1".
- **URL Encoding:** Obscures an input string by adding the percent sign (%) before each code point.
- **Null Byte:** Uses the null byte (%00) character prior to a string to bypass the detection mechanism.
- **Case Variation:** Obfuscates SQL statement by mixing it with upper and lower case letters.
- **Declare Variables:** Uses variables to pass a series of specially crafted SQL statements and bypass the detection mechanism.
- **IP Fragmentation:** Uses packet fragments to obscure the attack payload, which goes undetected by the signature mechanism.
- **Variations:** Uses a WHERE statement that is always evaluated as "true", so that any mathematical or string comparison can be used.

Countermeasure

- disabled shell access to the database
- IDS, IPS
- reject entries contain binary data, escape sequences, and common char
- Use type-safe sql parameters
- defenses in the application: input validation
- detect sql injection attacks, detect regular expressions used in sql injection
- Tools: OWASP ZAP, DSSS, Snort

Module 16: Hacking Wireless Networks

Concept

- GSM
- Bandwidth
- AP
- **BSSID:** Mac address of an AP
- ISM band
- Hotspot
- Association
- **SSID:** Name of a WLAN
- OFDM
- MIMO-OFDM
- DSSS (Direct-sequence Spread Spectrum)
- FHSS

Wireless Network

- Types
    - Extension to a wired network
        - SAPs (Software APs)
        - HAPs (Hardware APs)
    - Multiple Access Points
    - LAN-to-LAN wireless network
- Wireless Standards

Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

- SSID: Maximum length of 32 bytes, a human-readable text string

    - WIFI authentication modes
        - Open system authentication process
        - Client->AP: Probe request
        - AP->Client: Proble response
        - Client->AP: Open system authentication request
        - AP->Client: Open system authentication response
        - Client->AP: Association request
        - AP->Client: Association response
    - Shared key authentication process
        - Client->AP: Authentication request
        - AP->Client: Challenge text
        - Client->AP: Encrypted challenge text
        - AP->Client: Decrypt challenge text, if corrent, authenticate
        - Client->AP: Connect
- WIFI authentication process using a centralized authentication server
    - A centralized authentication server known as the **RADIUS (Remote authentication dial in user service)** sends authentication keys to both the **AP** and the client.
- Types of wireless antennas
    - Directional antenna
    - omnidirectional antenna: **360 degree** jprozpmta; radoatopm pattern
    - parabolic grid antenna
    - yagi antenna
    - dipole antenna
    - reflector antenna

Wireless Encryption

- 802.11i
- WEP
    - Use **24bit IV** to form stream cipher RC4 and CRC-32 checksum
- EAP
- LEAP: Proprietary version of EAP developed by cisco
- WPA: use **TKIP** and **MIC** to provide strong…
    - Use **TKIP (Temporal Key Intergrity Protocol)** that utilizes the RC4 with **128bit** keys and 64bits MIC
    - TKIP elimimateds the weakness of WEP by including **per-packet mixing functions, MIC, extended IV, re-keying mechanisms**
- TKIP: Used in **WPA** to replace WEP
- WPA2: Use **AES** and **CCMP**
    - **WPA2-Person:** Use **PSK (pre-shared key)**
    - **WPA2-Enterprise:** Include **EAP** or **RADIUS**
- AES: Used in **WPA2** to replace TKIP

- CCMP (chaining message authentication code protocol): Used in **WPA2**
- WPA2 Enterprise: Integrate **EAP**
- RADIUS: a centralized authentication and authorization management system
- PEAP
- WPA3: use **AES-GCMP-256** and **HMAC-SHA-384**
    - **WPA3-person:** Mainly used to deliver password-based authentication usging the **SAE** protocol, also known as **Dragonfly Key Exchange.** Resistant to offline dictionary attacks and key recovery attacks
    - **WPA3-enterprise:** Using **GCMP-256** for encryption, **HMAC-SHA-384** for generating keys, **ECDSA-384** for exchanging keys

Comparison of WEP, WPA, WPA2, and WPA3

-

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Issues in WEP, WPA, WPA2

- **WEP**
    - **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet:** By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
    - **IVs are of 24 bits:** The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
    - **WEP is vulnerable to known plaintext attacks:** When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
    - **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
    - **WEP is vulnerable to DoS attacks:** This is because associate and disassociate messages are not authenticated.

    - **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
    - **A lack of centralized key management makes it difficult to change WEP keys regularly. All Rights Reserved. Reproduction is Strictly Prohibited.**
    - **IV is a value used to randomize the keystream value, and each packet has an IV value:** The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message.
    - **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
    - **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages**
- **WPA**
    - **Weak passwords:** If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
    - **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
    - **Vulnerability to packet spoofing and decryption:** Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
    - **Predictability of the group temporal key (GTK):** An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
    - **Guessing of IP addresses:** TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

- **WPA2**
    - **Weak passwords:** If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.
    - **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
    - **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks:** The Hole96 vulnerability in WPA2 allows attackers to

exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
    - **Predictability of GTK:** An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
    - **KRACK vulnerabilities:** WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
    - **Vulnerability to wireless DoS attacks:** Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
    - **Insecure WPS PIN recovery:** In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

Wireless Threats

- **Access control attacks**
    - **WarDriving:** WLANs are detected by sending probe requests over a connection or by listening to web beacons
    - **Rogue AP:** An AP is installed on a trusted network without authorization
    - MAC spoofing
    - AP Misconfiguration
    - **Ad hoc association:** Using any USB adapter or wireless card, connect the host to an unsecured client to attack a specific client or to avoid AP security
    - Promiscuous client
    - Client mis-association
    - Unauthorized association
- **Integrity attacks**
    - Data frame injection
    - WEP injection
    - Bit-flipping attacks
    - Extensible AP replay
    - Data replay
    - IV replay attacks
    - RADIUS replay
    - Wireless network virus
- **Confidentiality attacks**

    - Eavesdropping
    - Traffic analysis
    - Cracking wep key
    - Evil twin ap
    - Honeypot ap
    - Session hijacking
    - **Masquerading:** Pretend to be an authorized user to gain…
    - MITM attack
    - **Wormhole attack:** Exploit dynamic routing protocols. Attackers locate himself strategically in the target network to sniff and record the ….
- **Availablility Attacks**
    - AP theft
    - Disassociation attacks
    - EAP-failure
    - Beacon flood
    - DoS
    - De-authenticate flood
    - Routing attacks
    - Authenticate flood
    - ARP cache poisoning attack
    - Power saving attacks
    - TKIP MIC exploiot
    - Jamming signal attack
- **Authentication attacks**
    - PSK cracking
    - LEAP cracking
    - VPN login cracking
    - Domain login cracking
    - Key reinstallation attacks
    - ID theft
    - Shared key guessing
    - Password speculation
    - Application login theft
    - **aLTEr attack:** Usually perrformed on LTE devices. Install a virtual comunication tower between authentic endpoints intending too mislead the victim
    - **Sinkhole attack:** Use a malicious node and advertise this node as the shortest possible route to reatch the base station.

Wireless Hacking Methodology

- Wifi discovery
    - Passive footprinting: Sniff the packets from the airwave

    - Active footprinting: Send out a probe
    - Wifi chalking techniques
        - **Warwalking:** Walk around with WIFI enabled laptops to detect open wireless network
        - **Warchalking:** Draw symbols in public places to advertise open WIFI networks
        - **Warflying:** Use drones to detect open wireless network
        - **WarDriving:** Drive arount with WIFI enabled laptops to detect…
    - Find wps-enabled aps: **sudo wash -I wlan0**
    - Tools: **inSSIDer Plus, NetSurveyor**
- GPS mapping: Track the location of…
    - Tools: Maptitude Mapping Software, Skyhook
- Wireless traffic analysis
    - Sniff
    - Spectrum analysis: measure the power of the specture
- Launch of wireless attacks
    - Tool: Aircrack-ng Suite
        - **Airbase-ng:** It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
        - **Aircrack-ng**: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.
        - **Airdecap-ng:** It decrypts WEP/WPA/ WPA2 and can be used to strip wireless headers from Wi-Fi packets.
        - **Airdecloak-ng**: It removes WEP cloaking from a pcap file.
        - **Airdrop-ng:** This program is used for the targeted, rule-based de-authentication of users.
        - **Aireplay-ng:** It is used for traffic generation, fake authentication, packet replay, and ARP request injection.
        - **Airgraph-ng:** This program creates a client–AP relationship and common probe graph from an airodump file.
        - **Airmon-ng:** It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
        - **Airodump-ng**: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
        - **Airolib-ng:** This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
        - **Airserv-ng:** It allows multiple programs to independently use a Wi-Fi card via a client–server TCP connection.
        - **Airtun-ng:** It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
        - **Easside-ng:** This program allows the user to communicate via a WEP-encrypted AP without knowing the WEP key.
        - **Packetforge-ng:** Attackers can use this program to create encrypted packets that can subsequently be used for injection.

        - **Tkiptun-ng:** It injects frames into a WPA TKIP network with QoS and can recover MIC keys and keystreams from Wi-Fi traffic.
        - **Wesside-ng:** This program incorporates various techniques to seamlessly obtain a WEP key in minutes.
        - **WZCook:** It is used to recover WEP keys from the Wireless Zero Configuration utility of Windows XP.
    - Detection of hidden ssids
        - run **airmon-ng** in monitor mode
        - start **airodump-ng** to discover SSIDs
        - use **aireplay-ng** to **de-authenticate** the client to reveal hidden SSID
        - switch to airodump to view the revealed SSID
    - Fragmentation attack
        - When successful, can obtain **1500 bytes of PRGA (pseudo random generation algorithm)**
        - **Do not recover the WEP key** itself
        - PRGA can be used to generate packets with **packetforge-ng**, used for injection attacks
        - At least one packet to be received from the AP
    - MAC Spoofing attack
        - Tools: Technitium MAC Address Changer
    - DoS: Disassociation and De-authentication attacks
    - MITM
        - run **airmon-ng** in monitor mode
        - start **airdump** to discover ssid
        - de-authenticate the client using **aireplay-ng**
        - associate your wireless card with the AP you are accessing with airplay-ng
    - Wireless ARP poisoning
        - Tools: **Ettercap**
    - Rouge AP
        - Tools: MANA Toolkit
    - Evil Twin
    - aLTEr attack
    - Wi-jacking attack
- Wifi encryption cracking
    - WEP encryption cracking
        - airmon-ng
        - airodump
        - associate your wireless card with the target AP
        - inject packets using **aireplay-ng**
        - wait for more than **50000** IVs, crack WEP key using **aircrack-ng**
    - WPA PSK
        - airmon-ng

        - airodump-ng
        - deauthenticate the client: **aireplay-ng**
        - run the capture file through **aircrack-ng**
- Cracking WPA/WPA2 using Wifiphisher
- Cracking WPS using reaver
    - **airmon-ng**
    - Use **wash utility** to detect wps-enabled devices
    - Or **airodump-ng**
    - use reaver
- WPA3
    - dragonblood is a set of vulnerabilities in the WPA3 security standard
    - Tools: **dragonslayer, dragonforce, dragondrain, dragontime**
- WEP cracking and WPA brute forcing
    - WEP cracking tool: **wesside-ng**
    - WPA/WPA2 brute forcing tool: **Fern wifi cracker**
- Compromise the wifi network

Wireless Hacking Tools

- WEP/WPA/WPA2 Cracking Tools: **Elcomsoft wireless security auditor**
- Packet snifffer: **SteelCentral Packet Analyzer**, **Omnipeek Network Protocol Analyzer, Kismet, CommView for WIFI**
- Traffic analyzer tools: **AirMagnet Wifi Analyzer PRO**

Bluetooth Stack

- A short range wireless communication technology
- Share data over short distances
- Bluetooth hacking
    - **Bluesmacking:** DoS attack, **overflowing bluetooth-enabled devices** with random packets
    - **Bluejacking: send unsolicited messages** via **OBEX** protocol
    - **Bluesnarfing:** the **theft of info** from a wireless device through a bluetooth connection
    - **BlueSniff:** proof of concept code for a bluetooth **wardriving** utility
    - **Bluebugging:** remotely accessing a device and using its features
    - **BluePrinting:** collect info about devices, such as manufacturer, model…
    - **Btlejacking:** bypass security mechanism and listen to info being shared
    - **KNOB attack:** exploit a vulnerability in bluetooth to **eavesdrop all the data** being shared, such as keystrokes, chats, and documents.
    - **MAC Spoofing attack**
    - **MITM / Impersonation attack**
- Bluetooth reconnaissance using **BlueZ**

- Btlejacking using **BtleJack**
- Tools: **Bluetooth View, BlueScan**

Countermeasure

- Use WPA2 with AES/CCMP
- Use VPN
- Implement a NAC (Network Access control) or NAP

Wireless Security Tools

- Wireless IPS
- Wifi security auditing tools: **Cisco adaptive wireless IPS**
- **WatchGuard WIPS**
- Wifi predictive planning tools: **AirMagnet Planner**
- Wifi vulnerability scanning tools: Zenmap

Module 17: Hacking Mobile Platform

Attack Vector

- OWASP Top10 mobile risks-2016
    - Improper platform usage
    - Insecure data storage
    - Insecure Communication
    - Insecure authentication
    - Insufficient crypto
    - Insecure authorization
    - Client code quality
    - Code tempering
    - Reverse engineering
    - Extraneous functionality
- Mobile attack vector
    - malware
    - data exfiltration
    - data tampering
    - data loss
- **SMS phishing (Smishing)**
- **Agent smith attack**
    - persuade the victim to install attacker's app
    - replace legitimate app
    - produce a hugh volume of ads
- **SS7 vulnerabilitiy**
    - SS7 is a **communication protocol** that allows mobile users to exchange communication through another celular network
    - Operated depending on mutual trust between operators without any authentication
    - Exploit this vulnerability to perform a MITM
- **Simjacker:** SIM Card attack, a vulnerability associated with a SIM card's S@T browser, a pre-installed software on SIM.

Hacking Android OS

- Include an OS, middleware, and key applications
- Android is a linux-based OS
- Android device administration API: provide **device administration features** at the system level. Allow developers to create **security-aware** apps that useful in enterprise setting.

- Android Rooting
    - Allow users to **attain privileged control**
    - Involve exploiting security vulnerabilities in the **device firmware** and copying the SU binary to a location in the current process's PATH and granting it exetuable permission with the **chmod command**
    - Tools: **KingoRoot, One Click Root, TunesGo Root Android Tool**
- Blocking WIFI access using **NetCut**
- Identify attack surfaces using **drozer**
- Hacking with **zANTI** and **Network Spoofer**
- Launch DoS using **LOIC**
- Session hijacking using DroidSheep
- Hacking with **Orbot Proxy**: A proxy app that empowers other apps to privately use the Internet
- Exploiting android device through **ADB (Android Debug Bridge)** using **PhoneSploit**
    - ADB: Allow attackers to communicate with the target device
- Sniffer: FaceNiff
- Launch **MITD (Man in the disk)** attack: Lead to the installation of potential malicious app
- Launch spearphone attack: Allow apps to **record loudspeaker data** without privileges.
- Android trojans: **Gustuff, xHelper**
- Hacking tools: **cSploit, Fing-Network Tools**
- Security tools: **Kaspersky mobile av**
- Device tracking tools: **google find my device**
- Vulnerability scanners: **X-ray**
- Online Android analyzers: **Online APK analyzer**

Hacking IOS

- Jailbreaking IOS
    - The process of **installing a modified set of kernel patches** that allow users to run third-party apps not signed by the OS vendor
    - Provide root access
    - Remove **sandbox restrictions**
    - Types of jailbreaking
        - Userland exploit: Allow **user level access**
        - iBoot Exploit: Allow both user level access and iboot level access
        - Bootrom Exploit: Allow both user level access and iboot level access
    - Jailbreaking techniques

        - **Untethered jailbreaking:** In an 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; in other words, **the device will be jailbroken after each reboot.**
        - **Semi-tethered jailbreaking:** In a semi-tethered jailbreak, 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.

        - **Tethered jailbreaking:** With a tethered jailbreak, if the device starts up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; to start it completely and with a patched kernel, it essentially must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on.
        - **Semi-untethered Jailbreaking:** A semi-untethered jailbreak is similar to a **semi-tethered jailbreak**. In this type of jailbreak, when the device reboots, the kernel is not patched. However, the kernel can be patched without using a computer; it is patched using an app installed on the device.
    - Jailbreaking IOS 13.2 using **Cydia**
    - Jailbreaking IOS 13.2 using **Hexxa Plus**
- Tools: **Apricot**, a web-based mirror operating system for all the latest iphones
- Hacking using **Spyzie**
- Hacking network using **Network Analyzer Pro**
- **IOS trustjacking:** A vulnerability that can be exploited to read messages and emails and capture sensitive info from a remote location without the victim's knowledge. Exploit the "ITunes WIFI Sync" feature, where the victim connects their phone to any trusted computer that is already infected by an attacker
- Malware: **Clicker Trojan malware, Trident**
- Hacking tools: **Elcomsoft Phone breaker**
- Security Tools: **Avira mobile security**
- Tracking tools: **Find my iphone**

Mobile Device Management (MDM)

- Solutions: **IBM MaaS360, Citrix Endpoint Management**
- **BYOD**: Bring your own device is a policy that…
- BYOD Policy implementation:
    - Define requirements
    - Select the device and build a technology portfolio

    - Develop policies
    - Security
    - Support

Mobile Security Guidelines and Tools

- OWASP Top10 Mobile Controls
    - Identify and protect sensitive data on the mobile device
    - Handle password credentials securely on the device
    - Ensure sensitive data are protected in transit
    - Implement user authentication, authorization, and session management correctly
    - Keep the backend APIs (services) and platform (server) secure
    - Secure data integration with third-party services and applications
    - Pay specific attention to the collection and storage of consent for the collection and use of the user's data
    - Implement controls to prevent unauthorized access to paid-for resources
    - Ensure secure distribution /provisioning of mobile apps
    - Carefully check any runtime interpretation of code for errors
- Reverse Engineering Mobile app
- Source code analysis tools: **z3A Advanced App Analysis**
- Reverse Engineering Tools: **Apktool**
- App repackaging detector
    - repackaging is the process of **extracting details of an app** from legitimate app stores
    - **Promon Shield**
- Protection tools: **Lookout Personal, Zimperium's zIPS, BullGuard Mobile Security**
- Anti-spyware: **Malwarebytes for Android**
- Pentesting toolkit: **ImmuniWeb MobileSuite**

Module 18: IoT and OT Hacking

Concepts

- How the IoT works
    - Sensing technology
    - IoT gateway: Bridge the gap between an IoT device and the end-user
    - Cloud server/data storage
    - Remote control using mobile app
- IoT architecture
    - Application Layer
    - Middleware Layer
    - Internet Layer
    - Access Gateway Layer
    - Edge Technology Layer

IoT technologies and Protocols

- Short-range wireless communication
    - BLE (bluetooth low energt)
    - LIFI (Light-Fidelity)
    - NFC (Near Field Communication)
    - QR CODE AND Barcodes
    - RFID (Radio frequency identification)
    - Thread
    - WIFI
    - Wifi Direct
    - Z-wave
    - ZigBee
    - ANT
- Medium-range wireless communication
    - Ha-Low
    - LTE-advanced
    - 6LoWPAN
    - QUIC
- Wired communication
    - Ethernet

    - MoCA (Multimedia over Coax Alliance)
    - PLC (Power-line Communication)
- Long-range communication
    - LPWAN (Low-power wide-area networking)
    - VSAT (Very small aperture terminal)
    - Cellular
    - MQTT **(Message Queuing Telemetry Transport)**
    - NB-IoT
- OS
    - Win10 IoT
    - Amzon FreeRTPS
    - Contiki
    - Fuchsia
    - RIOT
    - Ubuntu Core
    - ARM mbed OS
    - Zephyr
    - Nucleus RTOS
    - NuttX RTOS
    - Integrity RTOS
- Application Protocols
    - CoAP
    - Edge
    - LWM2M
    - Physical Web
    - XMPP
    - Mihini/M3DA

IoT Communication Models

- Device-to-Device model
- Device-to-Cloud model
- Device-to-Gateway model
- Back-end Data-Sharing model

Challenges of IoT

- Lack of security and privacy
- Vulnerable web interfaces
- Legel, regulatory, and right issues
- Default, weak, and hardcoded credentials
- Clear text protocols and unnecessary open ports
- Coding errors (buffer overflow)
- Storage issues
- Difficult to update firmware and OS
- Interoperability standard issues
- Physical theft and tampering
- Lack of vendor support for fixing vulnerabilities
- Emerging economy and development issues

IoT attacks

- **Application:** validation of the inputted str, AuthN, AuthZ, no automatic security updates, default password
- **Network:** Firewall, improper communication encryption, services, lack of automatic updates
- **Mobile:** Insecure API, lack of communication channel encryption, authentication, lack of storage security
- **Cloud:** improper authentication, no encryption for storage and communication, insecure web interface
- **IoT:** Application+Network+Mobile+Cloud

OWASP Top10 IoT threats

- Weak, Guessable, or Hardcoded passwords
- Insecure network services
- Insecure ecosystem interfaces
- Lack of secure update mechanisms
- Use of insecure or outdated components
- Insufficient privacy protection
- Insecure data transfer and storage
- Lack of device management
- Insecure default settings
- Lack of physical harding

OWASP IoT attack surface area

- Ecosystem
- Device memory
- Device physical interfaces
- Device web interface
- Device fireware
- Device network services
- Administrative interface
- Local data storage
- Cloud web interface
- Third-party backend apis
- Update mechanism
- Mobile application
- Vendor backend APIs
- Ecosystem communication
- Network traffic
- Authenticatio/Authorization
- Privacy
- Hardware

IoT Threats

- **DDoS attack**
- **Attack on HVAC systems**: Heating, Ventilation, and Air conditioning systems have many security vulnerabilites that can be exploited to steal…
- **Rolling Code attack:** Jam and sniff the signal to obtain the code transferred to a vehicle's receiver
- **BlueBorne attack:** exploit the vulnerabilities of the bluetooth protocol to compromise the device
- **Jamming attack:**
- **Remote access using backdoor**
- **Remote access using telnet**
- **Sybil attack:** Use multiple forged identities to create a strong illusion of traffic congestoin
- **Exploit kit**
- **MITM attack**
- **Replay attack**

- **Forged malicious device**
- **Side channel attack**
- **Ransomware**
- **Client impersonation**
- **SQL injection attack**
- **SDR-based attack:** Software Defined radio is used to examine the communication signals in the IoT network and sends spam content…
- **Fault injection attack:** Perturbation attacks, occur when a perpetrator injects any fault or malicious program into the system to compromise the system security
- **Network privoting**
- **DNS rebinding attack**

Dyn Attack

- Mirai is a **piece of malware** that finds the IoT devices and infect them
- Once infected, Mirai adds the infected device to a botnet

IoT Hacking Methodology

- Info gathering: **Shodan, MultiPing, FCC ID Search, IoTSeeker**
- Vulnerability scanning
    - Scanning
        - Nmap
        - RIoT Vulnerability Scanner
    - Sniffing:
        - Foren6: Capture **6LoWPAN** traffic
        - Wireshark
    - Analyzing spectrum and IoT Traffic
        - Gqrx (spectrum)
        - IoT inspector (traffic)
- Launch attacks
    - Rolling code attack using **RFCrack**
    - Hacking Zigbee Devices with **Attify Zigbee Framework**
    - BlueBorne attack using **HackRF One**
    - Replay attack using **HackRF One**
    - SDR-Based attacks using **RTL-SDR** and **GNU Radio**
    - Side channel attack using **ChipWhisperer**
- Gain remote access

    - Gain remote access using **Telnet**
- Maintain access
    - Maintain access by **exploiting fireware**

Fireware analysis and reverse engineering

- Obtain fireware
- Analyze fireware
- Extract the filesystem
- Mount the filesystem
- Analyze the filesystem
- Emulate fireware

IoT Hacking tools

- Info-gathering
    - Censys
    - Thingful
- Sniffing
    - Suphacap
- Vulnerability-scanning
    - beSTORM
- Perform SDR-Based attack
    - **Universal Radio Hacker:** investigate unknown wireless protocols
- **Firmalyzer Enterprise:** perform an automated security assessment

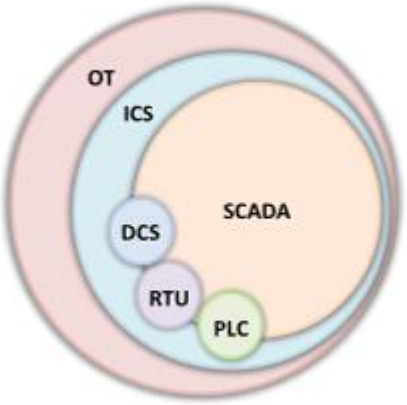
Countermeasure

- Defend against IoT Hacking
    - Disable guest and demo user account
    - implement IDS, IPS
    - Using encryption and sue PKI
    - Use VPN
    - Disable telnet
    - Disable UPnP port on routers
    - Monitor traffic on port 48101
    - ...

- General guidelines for IoT device manufacturing companies
    - SSL/TLS used for communication
    - Mutual check on SSL certificates, the certificate revocation list
    - Strong password
    - Secure with a chain of trust
    - Implement account lockout mechanism
    - Lock and devices
    - Checking the device for unused tools, using whitelisting to allow…
    - Use secure boot chain
- IoT device management
- security tool: **SeaCat.io, DigiCert IoT Security Solution**

OT Concepts

- **Operational technology** is the software and hardware designed to **detect or cause changes in industrial operations** through direct monitoring and controlling of industrial physical devices
- OT consists of **Industrial Control Systems (ICS)** that include **Supervisory Control and Data Acquisition (SCADA)**, **Remote Terminal Units (RTU)**, **Programmable Logic Controllers (PLC)**, **Distributed Control System (DCS)**, etc., to monitor and control the industrial operations



- Essential terminology
    - asset
    - **zones and conduits**: **A network segregation** technique used to isolate the networks and assets to impose and maintain strong access control mechanisms
    - industrial network
    - business network

    - industrial protocols
    - network perimeter
    - electronic security perimeter
    - critical infrastructure
- **IIOT (IT/OT Convergence, Industrial IoT):** the integration of IT computing system and OT operation monitoring system to bridge the gap between…
- **The purdue model:** Derived from the PERA (Purdue enterprise reference architecture) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks

<table>
<tr><td rowspan="2">IT Systems (Enterprise Zone)</td><td>Level 5</td><td>Enterprise Network</td></tr>
<tr><td>Level 4</td><td>Business Logistics Systems</td></tr>
<tr><td colspan="3">Industrial Demilitarized Zone (IDMZ)</td></tr>
<tr><td rowspan="4">OT Systems (Manufacturing Zone)</td><td>Level 3</td><td>Operation Systems/Site Operations</td></tr>
<tr><td>Level 2</td><td>Control Systems/Area Supervisory Controls</td></tr>
<tr><td>Level 1</td><td>Basic Controls/Intelligent Devices</td></tr>
<tr><td>Level 0</td><td>Physical Process</td></tr>
</table>

- **ICS:** a collection of different types of control systems and their associated equipment..
    - An ICS consists of several types of control systems like **SCADA, DCS, BPCS, SIS, HMI,PLCs, RTU, IED, etc**
    - Three mode:
        - **open loop:** The output of the system depends on the preconfigured settings
        - **closed loop:** The output always has an effect on the input to acquire the desired objective.
        - **manual mode:** The system is totally under the control of humans
    - **SCADA:** supervisory control and data acquisition
    - **DCS:** distributed control system
    - **BPCS:** basic process control systems
    - **SIS:** safety instrumentation system
    - **HMI:** human machine interface
    - **PLC:** programmable logic controller
    - **RTU:** remote terminal unit
    - **IED:** intelligent electronic device
- OT Technologies and Protocols

Level 4, 5	DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi
Level 3	CC-Link, DDE, GE-SRTP, HSCP, ICCP (IEC 60870-6), IEC 61850, ISA/IEC 62443, MODBUS, NTP, Profinet, SuiteLink, Tase-2, TCP/IP
Level 2	6LoWPAN, CC-Link, DNP3, DNS/DNSSEC, FTE, HART-IP, IEC 60870-5-101/104, IPv4/IPv6, ISA/IEC 62443, OPC, NTP, SOAP, TCP/IP
Level 0, 1	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

OT Attacks

- HMI-based attack
    - HMI is the core hub that **controls the critical infrastructure**
    - Gain access to the HMI system to cause **physical damage to the SCADA devices** or collect…
    - SCADA vulnerabilities exploited by attackers to perform HMI-based attacks
        - Memory corruption
        - Credential management
        - Lack of authorization/Authentication and Insecure defaults
        - Code injection
- Side channel attacks
    - Timing analysis
    - Power analysis
- Hacking PLC
    - Tamper with the integrity and availability of PLC system by exploiting **pin control operations**
- Hacking industrial system through RF remote controllers:
    - Replay attack
    - Command injection
    - Re-pairing with Malicious RF controller
    - Malicious Reprogramming Attack
- OT Malware: MegaCortex, LockerGoga Ransomware

OT Hacking Methodology

- Information gathering
    - Identify **ICS/SCADA** Systems using **Shodan (port 502)**
    - Gather default passwords using **CRITIFENCE**
    - Scan using **Nmap**
    - Enumerate slave controllers using **SCADA Shutdown Tool,** it is an ICS testing and automation tool
- Vulnerability Scanning
    - Scan using **Nessus**
    - **Skybox Vulnerability Control**
    - Analyze modbus/TCP traffic using **wireshark**
    - Discover ICS/SCADA network topology using **GRASSMARLIN**
- Launch Attacks
    - Hacking ICS hardware
    - Hacking Modbus slaves using Metaslpoit
    - Hacking PLC using modbus-cli
- Gain remote access
    - Using DNP3
- Maintain access

OT Hacking Tools

- Info gathering tools
    - SearchDiggity
- Sniffing and vulnerability-scanning tools
    - SmartRF Packet Sniffer
    - CyberX (scanning)
- OT Hacking Tools:
    - ICS Exploitation Framework (ISF)

Countermeasures

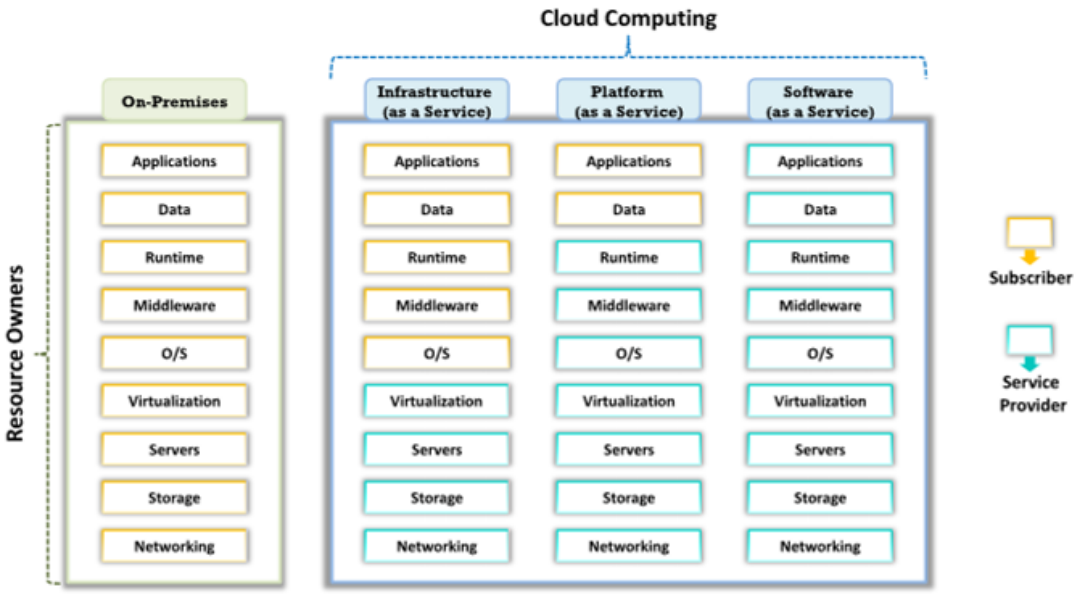
- International OT security Org
    - OTCSA (Operational Technology Cyber Security Alliance)
- Security Tools: **Flowmon**

Module 19: Cloud Computing

Concept

- An on-demand delivery of IT capabilities
- Characteristics of Cloud Computing
    - On-demand self-service
    - Distributed storage
    - Rapid elasticity
    - Automated management
    - Broad network access
    - Resource pooling
    - Measure service
    - Virtualization technology
- Types
    - IaaS (Infrastructure)
        - Provides **virtual machines** and other abstracted hardware and operating systems which may be controlled **through a service API**
        - E.g., Amazon EC2, GoGrid, Microsoft OneDrive, or Rackspace
    - PaaS (Platform)
        - Offers **development tools, configuration management, and deployment platforms** on-demand that can be used by subscribers to **develop custom applications**
        - E.g., Google App Engine, Salesforce, or Microsoft Azure
    - SaaS (Software)
        - Offers **software to subscribers** on-demand **over the Internet**
        - E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, or Freshbooks
          Function
    - IDaaS (Identity)
        - Offers **IAM services** including SSO, MFA, IGA, and intelligence collection
        - E.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, or Okta
    - SECaaS (Security)

        - Provides **penetration testing, authentication, intrusion detection,** anti-malware, security incident, and event management services
        - E.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, or McAfee Managed Security Services
    - Caas (Container)
        - Offers v**irtualization of container engines**, and management of containers, applications, and clusters, through a web portal or API
        - E.g., Amazon AWS EC2, or Google Kubernetes Engine (GKE) END
    - Faas (Function)
        - Provides a platform for developing, running, and managing **application functionalities for microservices**
        - E.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, or Oracle Cloud Fn
          Copyright
- Separation of responsibilities in cloud

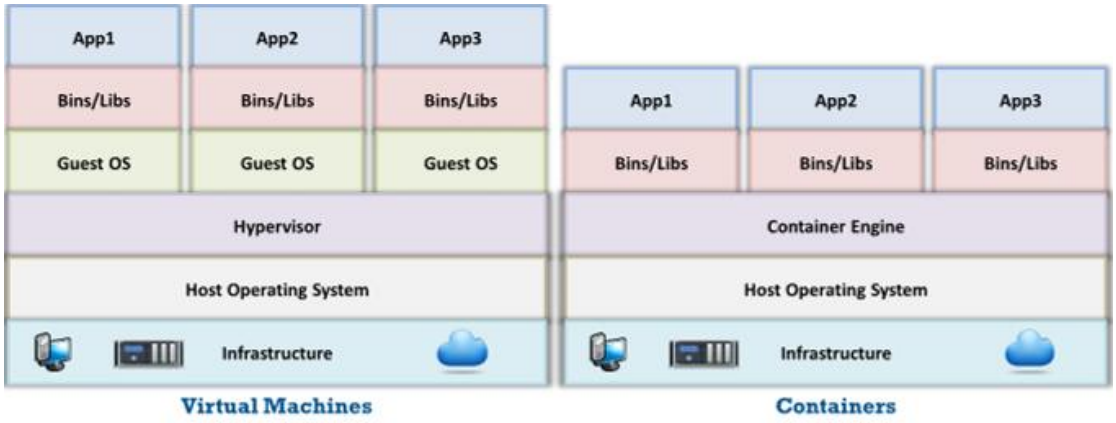


- Cloud Deployment models
    - **Public cloud:** Services are rendered over a network that is **open for public use**
    - **Private cloud**: Cloud infrastructure is operated for a **single organization only**
    - **Community cloud:** Shared infrastructure **between several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)

    - **Hybrid cloud: Combination of two or more clouds** (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models
    - **Multi cloud:** Dynamic heterogeneous environment that **combines workloads across multiple cloud vendors**, managed via one proprietary interface to achieve long term business goals
- NIST Cloud deployment reference architecture
    - Cloud Consumer
    - Cloud Provider
    - Cloud carrier
    - Cloud Auditor
    - Cloud Broker
- Cloud storage architecture
    - Front-end
    - middleware
    - Back-end
- AI in cloud computing
- VR and Augmented Reality on Cloud
- Cloud service provider
    - AWS
    - Azure
    - GCP (Google cloud platform)
    - IBM Cloud

Container Technology

- A package of an **app/software** including all its dependencies such as lib files, configuration files,etc. that run independently of other process in the cloud environment
- Container vs VM
    - VM: **Run multiple OS on a single physical system** and share underlying resources
    - Container: Placed on the top of one physical server and host OS, and **share the OS's kernel binaries and libs**



Virtual Machines	Containers
Heavyweight	Lightweight and portable
Run on independent operating systems	Share a single host operating system
Hardware-based virtualization	OS-based virtualization
Slower provisioning	Scalable and real-time provisioning
Limited performance	Native performance
Completely isolated making it more secure	Process-level isolation, partially secured
Created and launched in minutes	Created and launched in seconds

- **Docker:** An open source technology used for developing, packaging, and runing apps and all its dependencies in the **form of containsers**. It provide a PaaS through **OS-Level virtualization** and delivers containerized software packages
- Docket networking
- **Container Orchestration:** an automated process of managing the lifecycles of software containers and their dynamic environments
- **Kubernetes:** Known as K8s, an open-source, portable, extensible, orchestration platform for managing containerized apps and microservices
- **Container management platforms:** Docxker
- **Kubernetes Platform:** Kubernetes

Serverless Computing

- Known as serverless architecture or **FaaS**, is a cloud-based application architecture
- Simply the **process of app deployment** and eliminate the need for managing the server and hardware by the dev
- Serverless computing frameworks: **Azure functions, AWS Lambda**

Threat

- OWASP Top10 Cloud Security Risks
    - Accountability and Data ownership
    - User identity federation
    - Regulatory compliance
    - Business continunity and resillency
    - User privacy and secondary usage of data
    - Service and data integration
    - Multi tenacy and physical security
    - Incidence analysis and forensic support
    - Infrastructure security
    - Non-production environment exposure
- OWASP Top10 Serverless Security Risks (**Same with Web Top10**)
- Cloud computing threats
- Cloud attacks: Service hijacking using social engineering, Sniffing
- Cloud attacks: Side channel attacks or Cross-guest VM breaches
- **Wrapping attack:** Attacker duplicates the body of the messages and sends it to the server as a legitimate user
- **MITC attack:** advanced version of MITM attack
- **Cloud hopper attack:** Trigered at the **managed service providers (MSPs)** and their users.
- **Cloud Cryptojacking:** Unauthorized use of the victim's computer to stealthily mine digital currency.
- **Cloudborne attack:** A vulnerability residing in a bare-metal cloud server that enables the attackers to implant a malicious backdoor in its fireware.

Cloud Hacking

- Vulnerability scanning using **Trivy**
- Kubernetes Vulnerability Scanning using **Sysdig**
- Enumerating S3 Buckets
    - S3 is a scalable **cloud storage service** used by **Amazon AWS**
    - Attackers try to find the bucket's location and name
    - Inspecting HTML
    - Brute-force URL
    - Finding subdomains
    - Reverse IP Search
    - Advanced google hacking
    - Identify open s3 buckets using **S3Scanner**

- Enumerate Kubernetes etcd
    - etcd is a distributed and consistent **key-value storage**
    - Attackers **examine etcd processes**, configuration files, open ports, etc. to identify endpoints connected to the Kubernetes environment
    - **ps -ef | grep apiserve**r is used to identify the location of the etcd server and PKI info
- Enumerate AWS account IDs
- Enumerate IAM roles
- Enumerate bucket permissions using **S3Inspector**
- Exploiting Amazon Cloud Infrastructure using **Nimbostratus**
- Exploiting Misconfigured AWS S3 Buckets
    - Identify s3 buckets
    - Setup aws cmd interface
    - Extract access keys
    - Configure aws-cli
    - Identify vulnerable s3 buckets
    - Exploit s3 buckets
- Compromising AWS IAM Credentials
- Hijacking Misconfigured IAM Roles using **Pacu**
- Cracking AWS Access Keys using **DumpsterDiver**
- Exploiting Docker Containers on AWS using **Cloud Container Attack Tool (CCAT)**
- Gaining Access by Exploiting **SSRF Vulnerability**
- Escalating Privileges of Google Storage Buckets using **GCPBucketBrute**
- Backdooring Docker Images using **dockerscan**
- AWS Hacking Tool: **AWS pwn**

Cloud Security

- Cloud security control layer
    - Application
    - Information
    - Management
    - Network
    - Trusted Computing
    - Computation and Storage
    - Physical
- NIST Recommendation for Cloud security

    - **Assess the risk** posed to the client's data, software and infrastructure
    - Select an appropriate **deployment model** according to the needs
    - Ensure **audit procedures** are in place for data protection and software isolation
    - **Renew SLAs** in case of **security gaps** found between the organization's security requirements and the cloud provider's standards
    - Establish appropriate **incident detection** and **reporting mechanisms**
    - Analyze what are the **security objectives** of the organization
    - Enquire about **who is responsibl**e for data privacy and security issues in the cloud
- Zero trust networks:
    - A security implementation that assumes that every user trying to access the network is not a trusted entity by default and verifies every incoming connection before allowing access to the network
    - **Trust no one and validate before providing a cloud service**
- International Cloud Security Organizations: **Cloud Security Alliance (CSA)**
- Cloud Security Tools: **Qualys Cloud Platform**
- Container Security Tools: **Aqua**
- Kubernetes Security Tools: **Kube-bench**
- Serverless Application Security Solutions: **Protego**

Module 20: Cryptography

Concept

- **Types:** Symmetric encryption, Asymmetric encryption
- **GAK (Government access to key)**: software companies will give **copies of all keys** (or at least a sufficient proportion of each key that the remainder could be cracked) to the government

Algorithms

- Classic ciphers
    - substitution cipher
    - transposition cipher
- Modern ciphers:
    - Based on type of key
        - Symmetric-key algorithms
        - Asymmetric-key algorithms
    - Based on the type of input data
        - Block cipher
        - Stream cipher
- DES (Data encryption standard): blocks of **64bits data**, **56bit keys**
- AES (Advanced encryption standard)
- RC4
- RC5: 128bits
- RC6
- Twofish: 128bits, 256bits
- Threefish: 256bits, 512bits, 1024bits
- Serpent: **128 bit block**
- TEA: **Feistel cipher**, **128bits key** with **64bits blocks**
- CAST-128: 64bit block size
- DSA (Digital signature algorithm)
- RSA
- Diffie-Hellman: A cryptographic protocol that allows two parties to establish **a shared** key over an **insecure channel**, does not provide any authentication for the key exchange.
- YAK: A public-key based authenticated key exchange protocol

Message Digest Functions

- **MD5:** output **128 bits** fingerprint
- **MD6:** uses a Merkle tree-like structure to allow for immense parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attacks
- **Secure Hashing Algorithm (SHA-1): 160 bits** digest
- **SHA2**: SHA256 uses **32bits** words, SHA512 uses **64bits** words
- **SHA3:** Use the **sponge construction**, in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted
- **RIPEMD-160**: **RACE Integrity Primitives Evaluation Message Digest (RIPEMD)** is a **160-bit** hash algorithm
- **HMAC:** A type of **message authentication code (MAC)** that combines a cryptographic key with a cryptographic hash function. Verify the **integrity** of the data and **authentication** of a message
- **ECC (Elliptic Curve Cryptography):** A modern public-key cryptography developed to **avoid larger cryptographic key usage**
- Quantum Cryptography: Based on quantum mechanics, such as **quantum key distribution (QKD)**
- **Homomorphic Encryption:** Allows users to secure and leave their data in an encrypted format even while it is being processed or manipulated

Comparison of Crypographic Algorithms

-

Algorithm	Working Structure	Key/Block Size (bits)	Known Attacks
DES	Feistel	56 (8 bits parity)/ 64	Brute-force attack
AES	Substitution-permutation	Up to 256/128	Side-channel attack
RC4	Random-permutation	Up to 2048/2064	NOMORE attack
RC5	Feistel	Up to 2040/128	Timing attack
RC6	Feistel	Up to 256/128	Brute force attack
Twofish	Feistel	Up to 256/128	Power analysis attack
Threefish	Tweakable block cipher/Non-Feistel	Up to 1024/1024	Boomerang attack
Serpent	Substitution-permutation	Up to 256/128	XSL and Meet-in-the-Middle attack
TEA	Feistel	Up to 128/64	Related-key attack
CAST-128	Feistel	Up to 128/64	Known-plaintext attack
GOST Block Cipher	Feistel	256/64	Chosen-key attack

Algorithm	Working Structure	Key/Block Size (bits)	Known Attacks
RSA	Factorization	Variable	Brute force and timing attack
Diffie-Hellman	Elliptic Curves/Algebraic	Variable	Man-in-the-Middle attack
YAK	Nondeterministic Finite automation (NFA)	Variable	Key share and key replication attack
MD5	Merkle-Damgard Construction	Variable	Collision attack
MD6	Merkle-Damgard Construction	Variable	Brute-force attack/ Birthday attack
SHA	Merkle-Damgard Construction	160/512	Collision attack
RIPEMD - 160	Merkle-Damgard Construction	Up to 320 /512	Collision attack
HMAC	Merkle-Damgard Construction	Variable	Brute-force attack

Tools

- MD5 and MD6 Hash Calculators

- HashMyFiles
- BCTextEncode

PKI

- A set of **hardware, software, people, policies**, and **procedures** required to create, manage, distribute, use, store, and revoke **digital certificates**
- Components:
    - **Certificate Management System:** Generates, distributes, stores, and verifies certificates
    - **Digital Certificates:** Establish people's credentials in online transactions
    - **VA (Validation Authorizaty):** Stores certificates (with their public keys)
    - **CA (Certificate Authority):** Issues and verifies digital certificates
    - **End User**
    - **RA (Registration Authority):** Acts as the verifier for the certificate authority
- CA: Comodo, IdenTrust, GoDaddy
- Signed Certificate Vs Self-Signed Certificate
    - Signed certificate
        - User approaches a trustworthy **certification authority (CA)** and purchases a digital certificate
        - User gets the **public key** from the CA and signs the document using it
        - The signed document is delivered to the receiver
        - The receiver can verify the certificate by enquiring with **validation authority (VA)**
        - VA verifies the certificate to the receiver, but it does not **share the private key**
    - Self-signed certificate
        - User creates public and private keys using a tool, such as **Adobe Acrobat Reader, Java's keytool, or Apple's Keychain**
        - User uses public key to **sign the document**
        - The **self-signed document** is delivered to the receiver
        - The receiver request the **private key** from the user
        - User **shares the private key** with the receiver

Email Encryption

- **Digital Signature:** Use asymmetric cryptography to simulate the security properties of a signature in digital rather than written form
- **SSL:** An application layer protocol developed by Netscape for managing the security of message transmission on the Internet. Use **RSA asymmetric (public key) encryption.**
- **TLS:** A protocol to **establish a secure connection** between a client and a server and ensure the privacy and integrity of information during transmission. Use the **RSA algorithm** with 1024-and 2048-bit strengths
- Cryptography Toolkits: **OpenSSL** is an open-source cryptography toolkit implementing **SSL v2/v3** and **TLS v1** network protocols and the related cryptography standards required by them
- **PGP (Pretty good privacy)**
    - A protocol used to encrypt and decrypt data that provides **authentication** and **cryptographic privacy**
    - Used for **data compression, digital signing, encryption** and **decryption** of **messages, emails, files, directories**, and to enhance the privacy of email communications
    - Combine the best features of both conventional and **public key cryptography** and is therefore known as a **hybrid cryptosystem**
- **GPC (GNU Privacy Guard)**:
    - A **software replacement** of PGP and free implementation of the OpenPGP standard
    - Use both symmetric key cryptography and asymmetric key cryptography
    - Use both symmetric key cryptography and asymmetric key cryptography
- **WOT (Web of Trust)**
    - **A trust model of PGP**, OpenPGP, and GnuPG systems
    - WoT is **a chain of a network** in which individuals intermediately validate each other's certificates using their signatures
    - Every user in the network has a **ring of public keys** to encrypt the data, and they introduce many other users whom they trust
- Email Encryption Tools: **RMail**

Disk Encryption

- **VeraCrypt**: Establishi and maintain an **on-the-fly-encrypted** volume. On-the-fly encryption means that data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded
- **Symantec Drive Encryption:** Provide **full disk encryption** for all data

- **BitLocker Drive Encryption:** Provide offline data and operating system protection for your computer

Cryptanalysis

- **Linear cryptanalysis:** A known plaintect attack
- **Differential cryptanalysis**
- Integral cryptanalysis: Useful against block ciphers based on **substitution-permutation networks**, an extension of differential cryptanalysis
- **Attacks**

Ciphertext-only Attack	Attacker has access to the cipher text; the goal of this attack is to **recover the encryption key** from the ciphertext
Adaptive Chosen-plaintext Attack	Attacker makes a **series of interactive queries**, choosing subsequent plaintexts based on the information from the previous encryptions
Chosen-plaintext Attack	Attacker **defines their own plaintext**, feeds it into the cipher, and analyzes the resulting ciphertext
Related-Key Attack	Attacker can obtain ciphertexts encrypted under **two different keys**; this attack is useful if the attacker can obtain the plaintext and matching cipher text
Dictionary Attack	Attacker constructs a **dictionary of plaintext** along with its corresponding ciphertext that they have learnt over a certain period of time

Known-plaintext Attack	Attacker has **knowledge of some part of the plain text**; using this information, the key used to generate ciphertext is deduced to decipher other messages
Chosen-ciphertext Attack	Attacker obtains plaintexts corresponding to an **arbitrary set** of ciphertexts of their own choosing
Rubber Hose Attack	Extraction of cryptographic secrets (e.g., the password to an encrypted file) from a person by **coercion or torture**
Chosen-key Attack	Attacker usually breaks an **n bit** key cipher into $2^{n/2}$ operations
Timing Attack	It is based on repeatedly measuring the **exact execution times** of modular exponentiation operations
Man-in-the-middle Attack	Attacker performs this attack on the **public key cryptosystems** where key exchange is required before communication takes place

- **Birthday attack:** A class of brute-force attacks against cryptographic hashes that makes the brute forcing easier
- **Meet-in-the-Middle attack on Digital Signature Schemes: Encrypt from one end** and **decrypt from the other end**, thus meeting in the middle

- **Side channel attack**

- **Hash collision attack**
- **DUHK attack:** DUHK (Don't Use Hard-Coded Keys) is a cryptographic vulnerability that allows an attacker to obtain encryption keys used to secure VPNs and web sessions
- **Rainbow table attack**
- **Related-key attack: Exploite the mathematical relationship between keys** in a cipher to gain access over encryption and decryption functions
- **Padding oracle attack:** Exploit the padding validation of an encrypted message to decipher the ciphertext. Mainly performed on algorithms that operate in CBC mode
- **DROWN Attack:** a **cross-protocol weakness** that can communicate and initiate an attack on servers that support recent SSLv3/TLS protocol suites. Make the attacker **decrypt the latest TLS connection** between the victim client and server by launching malicious SSLv2 probes using the same private key.
- **Tools:** CrypTool

Countermeasures

- **Key strectching:** Process of strengthening a key that might be slightly too weak, usually by making it longer.
- **PBKDF2 (Password-Based Key Derivation Function 2):** A part of **PKCS #5 v. 2.01**. It applies some function (such as hash or HMAC) to the password or passphrase along with Salt to produce a derived key
- **Bcrypt:** Essentially uses a derivation of the **Blowfish algorithm**, converted to a hashing algorithm to hash a password and add Salt to it

Module : Appendix

Operating System

- **Windows OS family Tree**

Windows OS Family Tree		
MS-Dos-based and 9x Windows OS Versions	NT Kernel-Based Windows OS Version	
	For PC	For Server
MS-DOS 1.0	Windows NT 3.1	Windows Server 2003
MS-DOS 2.0	Windows NT 3.51	Windows Server 2003 R2
MS-DOS 2.1X	Windows NT 3.5	Windows Server 2008, Windows Home Server
MS-DOS 3.0	Windows NT 4.0	Windows Server 2008 R2
MS-DOS 3.1X	Windows 2000	Windows Server 2012
Windows 95	Windows XP	Windows Server 2012 R2
Windows 98	Windows XP Professional X64 Edition	Windows Server 2016
Windows 98 SE	Vista	Windows Server 2019
Windows ME	Window7	
	Windows 8	
	Windows 8.1	
	Windows 10	

- The processors of the Windows system works in two different modes: **User mode**, **Kernel Mode:**
- **Windows Command**
    - **ipconfig**
    - **netstat:** Display all active network connections and ports
    - **nslookup:** Display info that we can use to diagnose DNS infrastructure
    - **ping**
    - **chdir:** Show the current dir name or change the current folder
    - **dir**
    - **echo**
    - **format:** Format the disk
    - **help**
    - **label**
    - **mkdir**
    - **nbtstat:** Display protocol statistics and current TCP/IP connections
    - **systeminfo:** Display comprehensive configuration info about a computer and its OS
- **UNIX OS**
    - **Three main components**
        - **Kernel:** Allocate time and memory to programs. Handle file store and communicates with system calls
        - **Shell**
        - **Programs**
    - **Command**

            - ls
            - cd
            - mkdir
            - rmdir
            - cp
            - rm
            - mv
            - passwd
            - grep
            - diff
            - head
            - ispell
            - pr
            - pwd
            - id
- **MAC OS X OS**
    - Layers of MAC OS X
        - Cocoa Application layer
        - Media layer
        - Core Services layer
        - Core OS layer
        - Kernel and Device Driver layer

File System

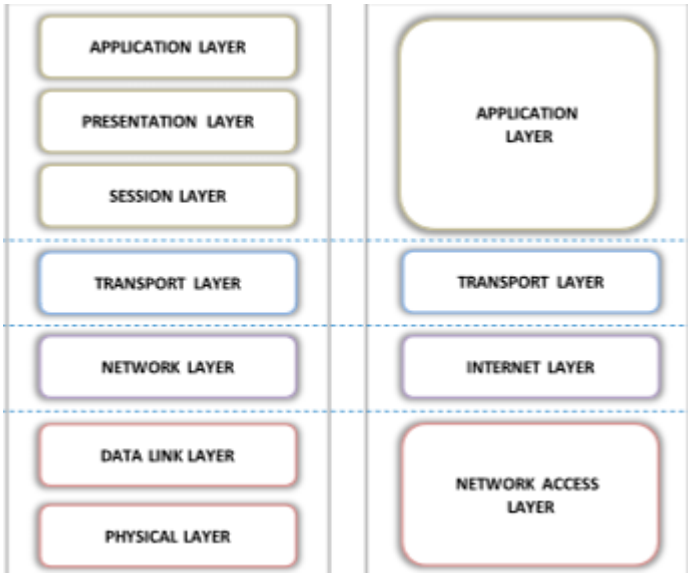
- Major file systems include **FAT, NTFS, HFS, HFS+, APFS, Ext2, Ext3, Ext4**, among others
- Windows File System
    - EFS: Encrypting File System
    - Sparse Files
- Linux File System
    - FHS: Filesystem Hierarchy Standard
    - EXT: Extended File System
- Mac OS X File System
    - HFS: Hierarchical File System
    - HFS Plus
    - UFS: UNIX File System

Computer Network

- **OSI Model**

OSI MODEL			
	Data Unit	**Layer**	**Function**
Host Layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption, and decryption; convert data to machine understandable format
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability, and flow control
Media Layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal, and binary transmission

- **Comparing OSI and TCP/IP**



- Types of Networks: **LAN, WAN, MAN, PAN, CAN, GAN**
- Wireless technologies
    - WIMAX
    - Microwave Transmission
    - Optical Wireless communication
    - 2G
    - 3G
    - 4G
    - Tetra
    - Bluetooth:
        - Cover distances of **up to 10m**
        - Transfer data at **less than 1Mbps**
        - Come under **IEEE 802.15**
        - Use a radio technology called **Frequency-hopping spread spectrum**

- **Network Topologies**
  - **Bus topology**
  - **Star topogoly**
  - **Ring topology**
  - **Mesh topology**
  - **Tree topology**
  - **Hybird topology:** Star-bus or Star-ring are widely used
- **TCP/IP Protocol Suite**

Application Layer Protocol	Transport Layer Protocol	Internet Layer Protocol	Link Layer Protocol
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token ring
DNSSEC	SSL	IPsec	WEP
HTTP	TLS	ICMP	WPA
S-HTTP		ARP	WPA2
HTTPS		IGRP	TKIP
FTP		EIGRP	EAP
SFTP		OSPF	LEAP
TFTP		HSRP	PEAP
SMTP		VRRP	CDP
S/MIME		BGP	VTP
PGP			STP
Telnet			PPP
SSH			
SOAP			
SNMP			
NTP			
RPC			
SMB			
SIP			
RADIUS			
TACACS+			
RIP			

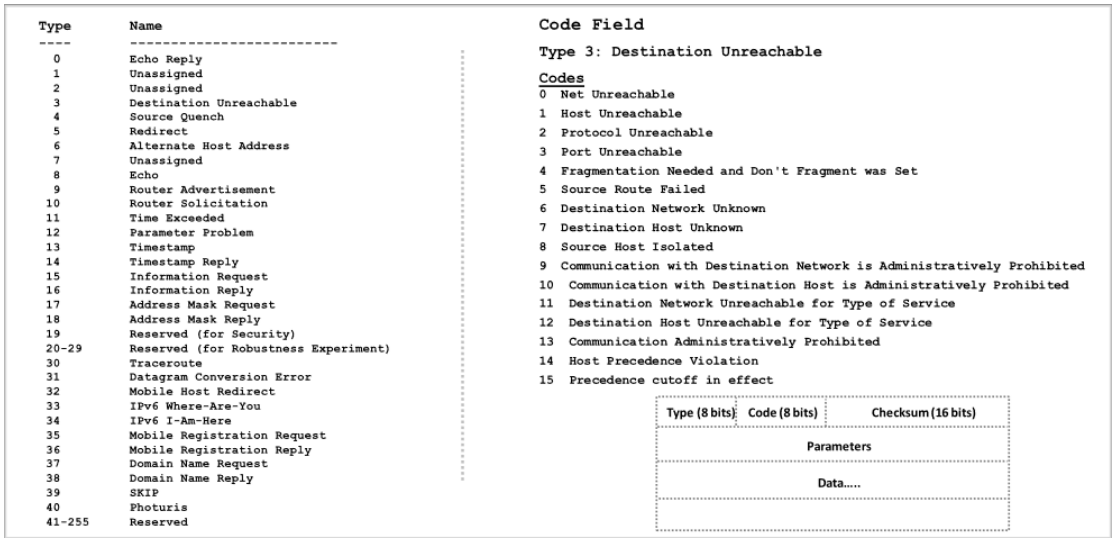
- DNS Hierarchy: **Root->Top-level domains->Second level domains->sub-domains**
- **DNSSEC: (Application layer)**
  - A suite of the IETF (Internet Engineering Task Force)
  - Shield Internet users from **artifical DNS data**
  - Secure certain types of info provided by **DNS**
  - Work by digitally signing records for **DNS lookup** using public-key crypto
  - Guarantee: **Authenticity, Integrity, The non-existence of a domain name or type**
  - Do not guarantee: **Confidentiality, Protect against DoS**
- **HTTP**
- **S-HTTP:** The alternate for the HTTPS (SSL) protocol
- **HTTPS:**
  - Against **MITM**
  - Be vulnerable to **DROWN** (Decrypting RSA with Obsolete and Weakened eNcryption)
- **FTP**
  - Active mode
  - Passive mode
- **SFTP**
  - A secure version of FTP and an extension of SSH2 protocol
- **TFTP**
  - **A lockstep communication protocol**

    - Both direction
    - Generally used only with **LAN**
    - Vulnerable to DoS
    - Vulnerable to Dir traversal vulnerability
- **SMTP**
- **S/MIME**
    - Use RSA for its digital signature and DES for message encryption
- **PGP**
    - An application layer protocol provides **crypto privacy** and authentication for…
    - Encrypt and decrypt email communication and authenticates message with **digital signatures** and encrypts stored files
- **Telnet**
    - Vulnerable to DoS, Packet sniffing
    - Used on a LAN
- **SSH**
- **SOAP (Simple Object Access Protocol)**
    - Equivalent to **RPC**
    - Disad: Stateless, reliance on HTTP, Slower than CORBA
- **SNMP**
    - Vulnerable to DDoS, Remote Code Execution
- **NTP**
- **RPC**
    - Allow inter-process communication between two programs
- **SMB (Server Message Block)**
    - **Application layer** network protocol
    - Provide an authenticated inter-process communication mechanism
    - The transport layer protocol that **Microsoft SMB Protocol,** is most often used with is **NetBIOS over TCP/IP (NBT)**
- **SIP (Session Initiation Protocol)**
- **RADIUS**
- **TACACS+**
    - **Client server** model
    - No integrity checking
    - Vulnerable to **replay a**ttacks
    - Accounting info is sent in plain text
    - Weak encryption
- **RIP**
    - **Distance Vector routing protocol**, used for **smaller** networks
- **TCP (Transport layer)**
- **UDP**
- **SSL**
    - Use **RSA encryption**
    - Provide a secure authentication mechanism between two…

- **TLS**
    - Use a **symmetric key** for **bulk encryption**, an **asymmetric key** for **authentication** and **key exchange**, and **MAC** for **message integrity**
    - Use RSA with 1024-and 2048-bit strengths
- **IP (Internet layer)**
- **IPv6**
    - Store a larger address space
    - Have more security features built into its foundation
    - VS

IPv4	IPv6
Length of addresses is 32 bits (4 bytes)	Length of addresses is 128 bits (16 bytes)
Header consists of a checksum	Header does not consist of a checksum
Header consists of options	Extension headers support optional data
IPsec header support is optional	IPsec header support is required
Address can be organized physically or through DHCP	Stateless auto-organized link-local address can be obtained
ARP uses broadcast ARP request to solve IP to MAC/Hardware address	Multicast neighbor solicitation communication solves both IP and MAC addresses
Broadcast addresses are used to send traffic to all nodes on a subnet	IPv6 uses an all-nodes multicast address with a link-local scope

- **IPsec**
- **ICMP**
    - Unreliable method for the delivery of network data
    - Format of an ICMP message



Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20-29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41-255	Reserved

- **ARP**
    - A stateless procotol
- **IGRP (Interior Gateway Routing Protocol)**
    - Distance-Vector protocol
- **EIGRP (Enchanced Interior Gateway Routing protocol)**

    - Hybrid routing protocol
- **OSPF**
    - An interior gateway protocol
    - Link-state routing protocol
- **HSRP (Hot standby router protocol)**
- **VRRP (Virtual router redundancy protocol)**
- **BGP**
- **FDDI (Link layer protocol)**
- **Token Ring**
- **CDP (Cisco discovery protocol)**
- **VTP (VLAN Trunking protocol)**
- **STP (Spanning Tree protocol)**
    - Vulnerable to: MITM, DoS, DNS Spoofing, Session hijacking…
- **PPP (Point to point)**

IP Addressing and Port numbers

- **IANA (Internet assigned number authority)**
    - Responsible for the global coordination of DNS Root, IP addressing, and …
    - Well-known ports are assigned by IANA, **0-1023**
- **IPv6**

Allocation	Format prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256

Network Terminology

- **Routing**
    - Static routing
    - Dynamic routing
- **NAT**
- **PAT**
- **VLAN**
- **Shared media network**
- **Switched Media Network**

Network Troubleshooting

- **Tools**
    - ping
    - Tracert/traceroute
    - ipconfig/ifconfig
    - nslookup
    - netstat: **display both the incoming and outgoing TCP/IP traffic**
    - PuTTY/Tera Term
    - Subnet and IP calculator
    - Speedtest.net
    - Pathping/mtr
    - Route

Virtualization

- **Characteristics of virtualization**
    - partitioning
    - isolcation
    - encapsulation
- **Virtual firewall**
- **Virtual OS**
- **Virtual Database**

NFS (Network File System)

- A distributed file system protocol
- IP-based networks
- Methods of securing access controls in NFS
    - Root squashing
    - nosuid
    - noexec

Web Markup and Programming Languages

- HTML
- XML
- Java
- .Net
- C#
- JSP

- ASP
- PHP
- Perl
- JS
- Bash scripting
- PowerShell: **Object-orirented** command line shell and scripting language
- C
- C++
- CGI (Common Gateway Interface)
    - The standard way for a web server to connect to external applications

Application Development Frameworks and Their Vulnerabilities

- .NET
    - Remote code execution
    - DoS
    - Feature Bypass
    - Modifying the framework Core
- J2EE
    - XSS
    - Execute arbitrary programs
    - DoS
    - Sensitive info disclosure
- Cold Fusion
    - Dir traversal
    - DoS
    - CSRF
    - Unvalidated browser input
- Ruby On Rails
    - Remote code execution
    - Authentication bypass
    - DoS
    - Dir Traversal
    - XSS
- AJAX
    - XSS
    - CSRF
    - SQL injection
    - XPATH injection

Web Subcompoinents

- Thin and Thick clients
- Applet: A java program that is embedded in a webpage
- Servlet
- ActiveX
- Flash Application

Info Security Controls

- **EISA** (Enterprise info security architecture)
    - A set of requirements, processes, principles, and models that determines the structure and behavior of an org's info systems
- **Administrative Security Controls:**
    - Administrative acess controls implemented by …
- **Regulatory Framework Compliance**
    - Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary **improvements** to cybersecurity
- **Info security policies**
    - The foundation of **security infrastructure**
    - Define the basic security requirements and rules to be implemented in order to protect and **secure an organization's information systems**
    - Types
        - **Promiscuous policy:** No restrictions
        - **Permissive policy:** Begin wide open and only known dangerous srvs, attacks, and behaviors are blocked
        - **Prudent policy:** Block all srvs and only safe or necessary srvs are individually enbaled, everything is logged
        - **Paranoid policy:** Forbid everything
- Privacy policies at the workplace
- HR or Legal Implication of Security Policy Enforcement
- Security Awareneess and Training
- Employee Awareness and Training: Physical Security
- Social Engineering
- Data classification
- Separation of Duties (SoD)
- Least Privileges (POLP)
- Physical Security Contorl
    - Lock
    - Fences
    - Badge systems
    - Security guards
    - Mantrap door
    - Biometric systems

    - Lighting
    - Motion detectors
    - Closed-circuit TVs
    - Alarms
- Types of Physical Security Controls
    - Preventive Controls: **Door lock, security guard, etc.**
    - Detective Controls: **Motion detectors, alarm systems, video surveillance**…
    - Deterrent Controls: **Warning signs**
    - Recovery Controls: **Disaster recovery, business continuity plans, backup systems…**
    - Compensating Controls: **Hot sites, backup power systems…**
- Access control
    - DAC (Discretionary access control)
    - MAC (Mandatory access control)
    - Role-based Access
- IAM (Identity and Access management)
- Types of authentication
    - Password
    - 2FA
    - Biometric
        - Fingerprinting
        - Retinal scanning: **Layer of blood vessels at the back of their eyes**
        - Iris scanning: **Colored part of the eye**
        - Vein Structure recognition
        - Face recognition
        - Voice recognition
    - Smart Card
        - **Crypto-based** authentication, stronger than password authentication
        - Insert smart card and type PIN
    - SSO
- Accounting

Network Security Solution

- SIEM (Security Incident and Event Management)
- UBA (User behavior analytics)
- UTM (Unified Threat Management)
- Load Balancer
- NAC (Network access control)
- VPN

    - Components
        - Vpn client
        - Tunnel terminating device
        - NAS (Network access server)
        - VPN protocol
    - **VPN Concentrators**
        - A network device used to create secure VPN connections
        - Act as a VPN router which is generally used to create a remote access or site-to-site VPN
    - Functions
        - Encrypt and decrypt data
        - Authenticate users
        - Manage data transfer across the tunnel
        - Negotiate tunnel parameter
        - Manage security key
        - Establish tunnels
        - Assign user address
        - Manage inbound and outbound data transfer as a tunnel endpoint or router
- Data Leakage
    - **DLP (Data loss prevention)**
- Data backup
    - **RAID (Redundant array of independent disks)**: A method of combining multiple hard drives into a single unit and writing data across several disk drives that offers fault tolerance
    - Method
        - Hot backup (online)
        - Cold backup (offline)
        - Warm backup (nearline): a combination of a hot and cold backup
- Data recovery

Risk Management

- ERM (Enterprise risk management framework)
- NIST risk management framework
- COSO ERM framework
- COBIT framework
- Enterprise network risk management policy
- Risk mitigation
- Control the risks
- Risk calculation formulas
    - **Asset Value (AV):** The value you have determined an asset to be worth

    - **Exposure Factor (EF):** The **estimated percentage** of damage or impact that a realized threat would have on the asset
    - **Single Loss Expectancy (SLE):** The projected loss of a single event on an asset
    - **Annual Rate if Occurrence (ARO):** The estimated number of times over a period the threat is likely to occur
    - **Annualized Loss Expectancy (ALE):** The projected loss to the asset based on an annual estimate
    - Qualitative risk: A subjective assessment
    - Quantitative Risk: A numeric assessment, **ARO*SLE=ALE**

Business Continuity and Disaster Recovery

- BC (Business continuity)
- DC (Disaster Recovery)
- BIA (Business Impact Analysis)
- RTO (Recovery Time Objective)
- RPO (Recovery Point Objective)
- BCP (Business Continuity Plan)
- DCP (Disaster Recovery Plan)

Cyber Threat Intelligence

- CIF (Collective Intelligence Framework)
- Threat intelligence data collection
- Threat intelligence sources
    - OSINT (Open-source intelligence): Publicly available sources
    - HUMINT (Human intelligence): Interpersonal contacts
    - SIGINT (Signals intelligence): Intercepting signals
    - …
- Collect IoCs (Indicator of compromise)

Penetration Testing

- **Security audit:** Check **whether the org is following a set of standard**…
- **Vulnerability assessment: Discover the vulnerabilities** in the info system, but **do not indicate** whether the system can be exploited successfully
- **Penetration testing:** Encompass the security audit and vulnerability assessment and demonstrate if the vulnerabilities in the system can be successfully exploited
- **Blue Team**
- **Red Team**
- Black box

- White box
- Grey box: Limited knowledge of the infrastructure to be tested
- Phases of penetration testing
    - Pre-attack
    - Attack
    - Post-attack
- Security testing methodology
    - OWASP
    - OSSTMM
    - ISSAF
    - EC-Council LPT Methodology
- ROE (Role of engagement)

Software Development Security

- **N-tier Application Architecture**
    - Presentation tier
    - Logic tier
    - Data tier
- **3-Tier Application Architecture**
    - Presentation tier
    - Application tier
    - Database tier

Network

- ICMP Type code:
  - ICMP Type Numbers
  - Code Fields
    - Type 0 — Echo Reply
    - Type 1 — Unassigned
    - Type 2 — Unassigned
    - Type 3 — Destination Unreachable
    - Type 4 — Source Quench (Deprecated)
    - Type 5 — Redirect
    - Type 6 — Alternate Host Address (Deprecated)
    - Type 7 — Unassigned
    - Type 8 — Echo
    - Type 9 — Router Advertisement
    - Type 10 — Router Selection
    - Type 11 — Time Exceeded
    - Type 12 — Parameter Problem
    - Type 13 — Timestamp
    - Type 14 — Timestamp Reply
    - Type 15 — Information Request (Deprecated)
    - Type 16 — Information Reply (Deprecated)
    - Type 17 — Address Mask Request (Deprecated)
    - Type 18 — Address Mask Reply (Deprecated)
    - Type 19 — Reserved (for Security)
    - Types 20-29 — Reserved (for Robustness Experiment)
    - Type 30 — Traceroute (Deprecated)
    - Type 31 — Datagram Conversion Error (Deprecated)
    - Type 32 — Mobile Host Redirect (Deprecated)
    - Type 33 — IPv6 Where-Are-You (Deprecated)
    - Type 34 — IPv6 I-Am-Here (Deprecated)
    - Type 35 — Mobile Registration Request (Deprecated)
    - Type 36 — Mobile Registration Reply (Deprecated)
    - Type 37 — Domain Name Request (Deprecated)
    - Type 38 — Domain Name Reply (Deprecated)
    - Type 39 — SKIP (Deprecated)
    - Type 40 — Photuris
    - Type 41 — ICMP messages utilized by experimental mobility protocols such as Seamoby
    - Type 42 — Extended Echo Request
    - Type 43 — Extended Echo Reply
    - Types 44-252 — Unassigned
    - Type 253 — RFC3692-style Experiment 1
    - Type 254 — RFC3692-style Experiment 2
  - ICMP Extension Object Classes and Class Sub-types
    - Sub-types — Class 1 — MPLS Label Stack Class
    - Sub-types — Class 2 — Interface Information Object
    - Sub-types — Class 2 — Interface Information Object — Interface Roles
    - Sub-types — Class 3 — Interface Identification Object
    - Sub-types — Class 4 — Extended Information
- **The Internet Printing Protocol (IPP)** uses port **631**.
- A **dual-homed host** (or dual-homed gateway) is a system fitted with **two network interfaces (NICs)** that sits between an untrusted network (like the Internet) and trusted network (such as a corporate network) to provide secure access
- **Heartbleed:** It was a security bug in the **OpenSSL cryptography library**, which is a widely used implementation of the Transport Layer Security (TLS) protocol.
- **Shellshock:** Shellshock is a vulnerability that allows systems containing a vulnerable version of **Bash** to be exploited to execute commands with higher privileges. This allows attackers to potentially take over that system
- **POODLE:** The POODLE attack (Padding Oracle on Downgraded Legacy Encryption) exploits a vulnerability in the **SSL 3.0 protocol** (CVE-2014-3566). This vulnerability

lets an attacker **eavesdrop on communication** encrypted using SSLv3

- **US CSIRT (Computer Security Incident Response Team):** Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
- **Tear Drop Attack:** A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine
- **Tcptrace:** It is a tool for analysis of TCP dump files.
- **Common Criteria:** International standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation.
- **SQL Slammer:** SQL Slammer is a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic
- **MS Blaster:** A computer worm. MS Blaster scans the Internet for computers that are vulnerable to its attack. Once found, it tries to enter the system through the port **135** to create a buffer overflow. TCP ports **139** and **445** may also provide attack vectors.
- **802.1x:** An IEEE Standard for port-based Network Access Control
- **Iris Scan**: Color of eyes
- **Retinal Scan:** Measure the layer of blood vessels
- **RFC:** Request for comments, it is the document used to describe a protocol
- **DAR:** Date at rest encrypts a system until correct credentials are provided at pre-boot.
- **RoT:** Roots of Trust are hardware or software components that are inheretly trusted by the OS
- **NIST cyber security framework:** Identify, protect, detect, response, recover
- **ISO 27001 cycle:** Plan, Do, Check, Act
- **Authentication Factor Types**
  - **Type1:** Something you **know**, such as a **password**
  - **Type2:** Something you **have**, such as a **smart card**
  - **Type3:** Something you **are**, such as a **fingerprint** or other **biometric method**
- **N-tier Application Architecture**
  - **Presentation tier**
  - **Logic tier**
  - **Data tier**
- **3-Tier Application Architecture**
  - **Presentation tier**
  - **Application tier**
  - **Database tier**
-