Ethical Hacking

Information Security: Attacks and Vulnerabilities Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Malware, Worms, viruses, Trojans, Spyware, Rootkits, Types of vulnerabilities: Top 10 OWASP.

Types of attacks and their common prevention mechanisms: Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs

Case-studies: Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit, Media Markt, Kaseya, JBS, Colonial Pipeline, The University of California at San Francisco.

UNIT 1

1. What is malware? Explain Worms and Trojan.

ANS:

Malware:

- Malware is generally defined as software designed to harm or secretly access a computer system without the owner’s informed consent.
- And, often, people in our profession think of it as hostile, intrusive, or annoying, and something to be avoided.
- From the perspective of a hacker, though, some of this may be useable—provided it’s done within the confines of an agreed-upon contract in a pen test.
- *Malware* is a term that covers viruses, worms, Trojans, and logic bombs as well as adware and spyware.
- These types of malware have caused several problems over the years, ranging from simple annoyances to dangerous and malicious exploits.
- Software that fits in the category of malware has evolved dramatically to now include the ability to steal passwords, personal information, and identities as well as damage hardware in some cases (as Stuxnet did).
- The term *malware* is short for *malicious software*, which accurately explains what this class of software is designed to do: perform malicious and disruptive actions.
- Another aspect of malware that has emerged is its use to steal information.
- Malware programs have been known to install what is known as a ***keylogger*** on a system.

- The intention is to capture keystrokes as they're entered, with the intention of gathering information such as credit card numbers, bank account numbers, and similar information.
- For example, malware has been used to steal information from those engaging in online gaming, to obtain players' game account information.
- **Categories of Malware**
    - ***Viruses*** are by far the best-known form of malicious software.
      This type of malware is designed to replicate and attach itself to other files resident on the system.
      Typically, viruses require some sort of user action to initiate their infectious activities.
    - ***Worms*** are a successor to viruses.
      The worm has been around in some shape or form since the late 1980s.
      The first worms were primitive by today's standards, but they had a characteristic that is still seen today: the ability to replicate on their own very quickly.
      Worms that have emerged over the past decade or so have been responsible for some of the most devastating denial-of service attacks known.
    - ***Trojan*** *horses* are a special type of malware that relies in large part on social engineering techniques to start infecting a system and causing harm while appearing to look like a legitimate program.
      Similar to a virus in many respects, this malware relies on the user being somehow enticed into launching the infected program or wrapper, which in turn starts the Trojan.
    - *Rootkits* are a modern form of malware that can hide within the core components of a system and stay undetected by modern scanners.
      What makes rootkits most devastating is that they can be extremely difficult to detect and even more difficult to remove.
    - ***Spyware*** is malware designed to gather information about a system or a user's activities in a stealthy manner.
      Spyware comes in many forms; among the most common are keyloggers.

- ○ ***Adware*** is malware that may replace home pages in browsers, place pop-up ads on a user's desktop, or install items on a victim's system that are designed to advertise products or services.

Worms:

- A *worm* is a **self-replicating malware** computer program that uses a computer network to send copies of itself to other systems without human intervention.
- A worm is a type of virus, but it's self-replicating. A worm spreads from system to system automatically, but a virus needs another program to spread.
- Viruses and worms both execute without the knowledge or desire of the end user.
- Usually it doesn't alter files, but it resides in active memory and duplicates itself, eating up resources and wreaking havoc along the way.
- The most common use for a worm in the hacking world is the creation of bot-nets.
  This army of robot systems can then be used to accomplish all sorts of bad things.
- The most common example of a worm is the **Conficker** worm. This worm disables services, denies access to administrator shared drives, locks users out of directories, and restricts access to security related sites.
- Symptoms include an "Open folder to view files—Publisher not specified" message in the AutoPlay dialog box, as shown in next Figure. (The original, and legitimate, Windows option reads "Open Folder to view files using Windows Explorer.") Conficker spreads as soon as it is opened (by clicking the first option) to open shares, unpatched systems on the network, and systems with weak passwords.
  Systems with up-to-date patches and even decent passwords are usually safe.

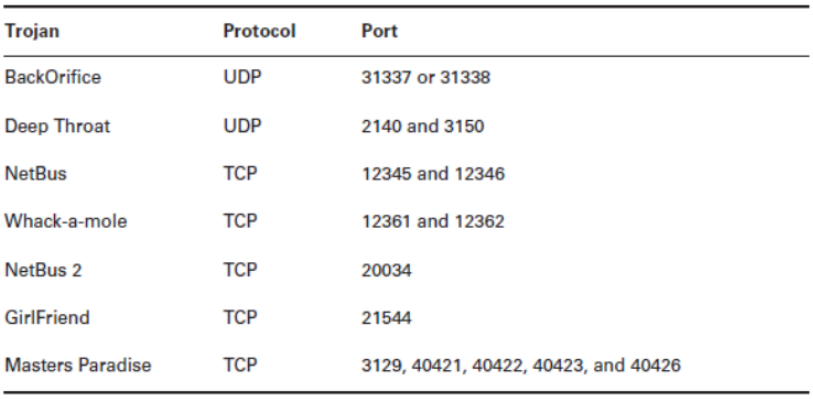
Trojans:

- A *Trojan* is software that appears to perform a desirable function for the user prior to running or installing it, but instead performs a function, usually without the user's knowledge, that steals information or otherwise harms the system (or data).

- To ethical hackers, though, the word ***Trojan* really means a method to gain, and maintain, access on a machine we've been paid to target**.
- The idea of a Trojan is simple.
  First, send an innocent-looking file to your target, inviting them to open it.
  They open it and, unaware, install software that makes your job easier.
  This software might be designed to steal specific types of information to send back, act as a keylogger, or perform 1,000 other equally naughty tasks.
  Some of them can even provide remote control–type access to a hacker any time he feels like it.
- For the ethical hacker, the goal is to provide something we can go back to later— a means to maintain our access.
  Although a **backdoor isn't a Trojan, and a Trojan isn't a backdoor**, they're tied together: **The Trojan is the means to deliver it, and the backdoor provides the open access**.
- Most *malware* Trojans are downloaded from the Internet (usually via some weird Java drive-by vulnerability, peer-to-peer application, or web application "feature"), grabbed via an IRC channel, or clicked on as an attachment in an e-mail.
- The absolute easiest way you can get a target to provide you access to their machine, short of asking them for it (see social engineering), is to send a Trojan.
  Often, they'll open it and happily install whatever you want.
- The question becomes, then, how do you make it look like a legitimate application?
  The answer is to use a **wrapper**.
  Wrappers are programs that allow you to bind an executable of your choice (Trojan) to an innocent file your target won't mind opening.
  For example, you might use a program such as EliteWrap to embed a backdoor application with a game file (.EXE).
  Your target opens the latest version of Elf Bowling and starts rolling strikes. Meanwhile your backdoor is installing and sits there waiting for your use later.
- Once a Trojan is installed on a system, they can cause data theft and loss, and system crashes or slowdowns; they can also be

used as launching points for other attacks such as Distributed Denial of Service (DDOS).

- Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts.
- Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel.
- Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge.
- A Trojan can be sent to a victim system in many ways: as an Instant Messenger (IM) attachment, IRC, an e-mail attachment, or NetBIOS file sharing.
- Many fake programs purporting to be legitimate software such as freeware, spyware-removal tools, system optimizers, screen savers, music, pictures, games, and videos can install a Trojan on a system just by being downloaded.
- Advertisements for free programs, music files, or video files lure a victim into installing the Trojan program; the program then has system level access on the target system, where it can be destructive and insidious.



Trojan	Protocol	Port
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423, and 40426

Table Common Trojan Program

- **List the Different Types of Trojans**
    - Trojans can be created and used to perform different attacks.
    - Some of the most common types of Trojans are:
        - → **Remote Access Trojans (RATs)**—
          used to gain remote access to a system
        - → **Data-Sending Trojans**—

used to find data on a system and deliver data to a hacker

→ **Destructive Trojans**—
used to delete or corrupt files on a system

→ **Denial of Service Trojans**—
used to launch a denial or service attack

→ **Proxy Trojans**—
used to tunnel traffic or launch hacking attacks via other system

→ **FTP Trojans**—
used to create an FTP server to copy files onto a system

→ **Security software disabler Trojans**—
used to stop antivirus software

2. What is malware? Explain Viruses.

ANS: **Malware:**

- Malware is generally defined as software designed to harm or secretly access a computer system without the owner's informed consent.
- And, often, people in our profession think of it as hostile, intrusive, or annoying, and something to be avoided.
- From the perspective of a hacker, though, some of this may be useable—provided it's done within the confines of an agreed-upon contract in a pen test.
- *Malware* is a term that covers viruses, worms, Trojans, and logic bombs as well as adware and spyware.
- These types of malware have caused several prob000000000000000000000000000000000000lems over the years, ranging from simple annoyances to dangerous and malicious exploits.
- Software that fits in the category of malware has evolved dramatically to now include the ability to steal passwords, personal information, and identities as well as damage hardware in some cases (as Stuxnet did).
- The term *malware* is short for *malicious software*, which accurately explains what this class of software is designed to do: perform malicious and disruptive actions.
- Another aspect of malware that has emerged is its use to steal information.

- Malware programs have been known to install what is known as a ***keylogger*** on a system.
- The intention is to capture keystrokes as they're entered, with the intention of gathering information such as credit card numbers, bank account numbers, and similar information.
- For example, malware has been used to steal information from those engaging in online gaming, to obtain players' game account information.
- **Categories of Malware**
    - ***Viruses*** are by far the best-known form of malicious software.
      This type of malware is designed to replicate and attach itself to other files resident on the system.
      Typically, viruses require some sort of user action to initiate their infectious activities.
    - ***Worms*** are a successor to viruses.
      The worm has been around in some shape or form since the late 1980s.
      The first worms were primitive by today's standards, but they had a characteristic that is still seen today: the ability to replicate on their own very quickly.
      Worms that have emerged over the past decade or so have been responsible for some of the most devastating denial-of service attacks known.
    - ***Trojan*** *horses* are a special type of malware that relies in large part on social engineering techniques to start infecting a system and causing harm while appearing to look like a legitimate program.
    - Like a virus in many respects, this malware relies on the user being somehow enticed into launching the infected program or wrapper, which in turn starts the Trojan.
    - *Rootkits* are a modern form of malware that can hide within the core components of a system and stay undetected by modern scanners.
      What makes rootkits most devastating is that they can be extremely difficult to detect and even more difficult to remove.
    - ***Spyware*** is malware designed to gather information about a system or a user's activities in a stealthy manner.

Spyware comes in many forms; among the most common are keyloggers.

  - ***Adware*** is malware that may replace home pages in browsers, place pop-up ads on a user's desktop, or install items on a victim's system that are designed to advertise products or services.

Viruses:

- A virus is defined as a self-replicating program that reproduces its code by attaching copies into other executable codes.
- In other words, viruses create copies of themselves in other programs.
- A virus infects another executable and uses this carrier program to spread itself.
- The virus code is injected into the previously benign program and is spread when the program is run.
- Examples of virus carrier programs are macros, games, e-mail attachments, Visual Basic scripts, games, and animations.
- Viruses are classified according to two factors: **what they infect and how they infect**.
- A virus can infect the following components of a system: System sectors, Files, Macros (such as Microsoft Word macros), Companion files (supporting system files like DLL and INI files), Disk clusters, Batch files (BAT files), Source code.
- A virus infects through interaction with an outside system.
- Viruses are categorized according to their infection technique, as follows:
  - **Polymorphic viruses:**
    - These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.
    - This virus mutates its code using a built-in polymorphic engine.
    - These viruses are very difficult to find and remove because their signatures constantly change.
  - **Stealth viruses:**
    - These hide the normal virus characteristics, such as modifying the original time and date stamp of the file to prevent the virus from being noticed as a new file on the system.
  - **Fast and slow infectors:**

    - These can evade detection by infecting very quickly or very slowly.
- **Sparse infectors:**
    - These viruses infect only a few systems or applications.
    - **Armored viruses:** These are encrypted to prevent detection.
    - **Multipartite viruses:** These advanced viruses create multiple infections. Attempts to infect both files and the boot sector at the same time.
    - **Cavity (space-filler) viruses:** These viruses attach to empty areas of files.
    - **Tunnelling viruses:** These are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.
    - **Camouflage viruses:** These viruses appear to be another program.
    - **NTFS and Active Directory viruses:** These specifically attack the NT file system or Active Directory on Windows systems.
    - There are a few of the other virus types and the definitions that go with them:
        - **Boot sector virus:**
          Also known as a system virus, this virus type moves the boot sector to another location on the hard drive, forcing the virus code to be executed first.
          They're almost impossible to get rid of once you get infected.
          You *can* re-create the boot record—old-school fdisk or mbr could do the trick for you—but it's not necessarily a walk in the park.
        - **Shell virus:**
          Working just like the boot sector virus, this virus type wraps itself around an application's code, inserting its own code before the application's.
          Every time the application is run, the virus code is run first.

	✦ **Macro virus:** Usually written with VBA (Visual Basic for Applications), this virus type infects template files created by Microsoft Office—normally Word and Excel. The Melissa virus was a prime example of this. **Metamorphic virus:** This virus type rewrites itself every time it infects a new file.
3.	What is an attack? Explain rootkit attack w.r.t to security.
ANS:	**Rootkits:** • A rootkit is a type of program often used to hide utilities on a compromised system. Rootkits include so called *back doors* to help an attacker subsequently access the system more easily. • A *rootkit* is a collection of software put in place by an attacker that is designed to obscure system compromise. In other words, if a system has a properly introduced rootkit installed, the user and security monitors won't even know anything is wrong. • For example, the rootkit may hide an application that spawns a shell when the attacker connects to a network port on the system. A back door may also allow processes started by a non-privileged user to execute functions normally reserved for the Administrator. • A rootkit is frequently used to allow the programmer of the rootkit to see and access usernames and login information for sites that require them. • Rootkits are designed to provide backdoors for the attacker to use later and include measures to remove and hide evidence of any activity. As per the CEH objectives, there are three types of rootkits: 1. **Application level:** - Application-level rootkits may replace regular application binaries with Trojanized fakes, or they may modify the behaviour of existing applications using hooks, patches, injected code, or other means. - These kits work inside an application and can use an assortment of means to change the application's behaviour, user rights level, and actions.

2. **Kernel level:**
    - These rootkits attack the boot sectors and kernel level of the operating systems themselves, replacing kernel code with backdoor code.
    - This is often accomplished by adding new code to the kernel via a device driver or loadable module, such as loadable kernel modules in Linux or device drivers in Microsoft Windows.
    - Kernel-level rootkits are especially dangerous because they can be difficult to detect without appropriate software.
3. **Library level:**
    - These rootkits basically make use of system-level calls to hide their existence.
    - Library-level rootkits commonly patch, hook, or replace system calls with versions that hide information that might allow the hacker to be identified.
    - Originally, rootkits started in the Linux realm and had two big flavours. In one setup, the rootkit replaced all sorts of actual binaries to hide processes. These were easily detectable, though, due to size—tools such as Tripwire could easily point out the existence of the rootkit. Later, they evolved to being loaded as a drive or kernel extension—via something called a Loadable Kernel Module (LKM).

Early rootkits in the Linux world included Adorm, Flea, and T0rm. Tools for helping discover rootkits already installed on a machine include chkrootkit and Rootkit Hunter.

4. Explain in brief about Attacks and Attack Surface.

ANS: Attacks

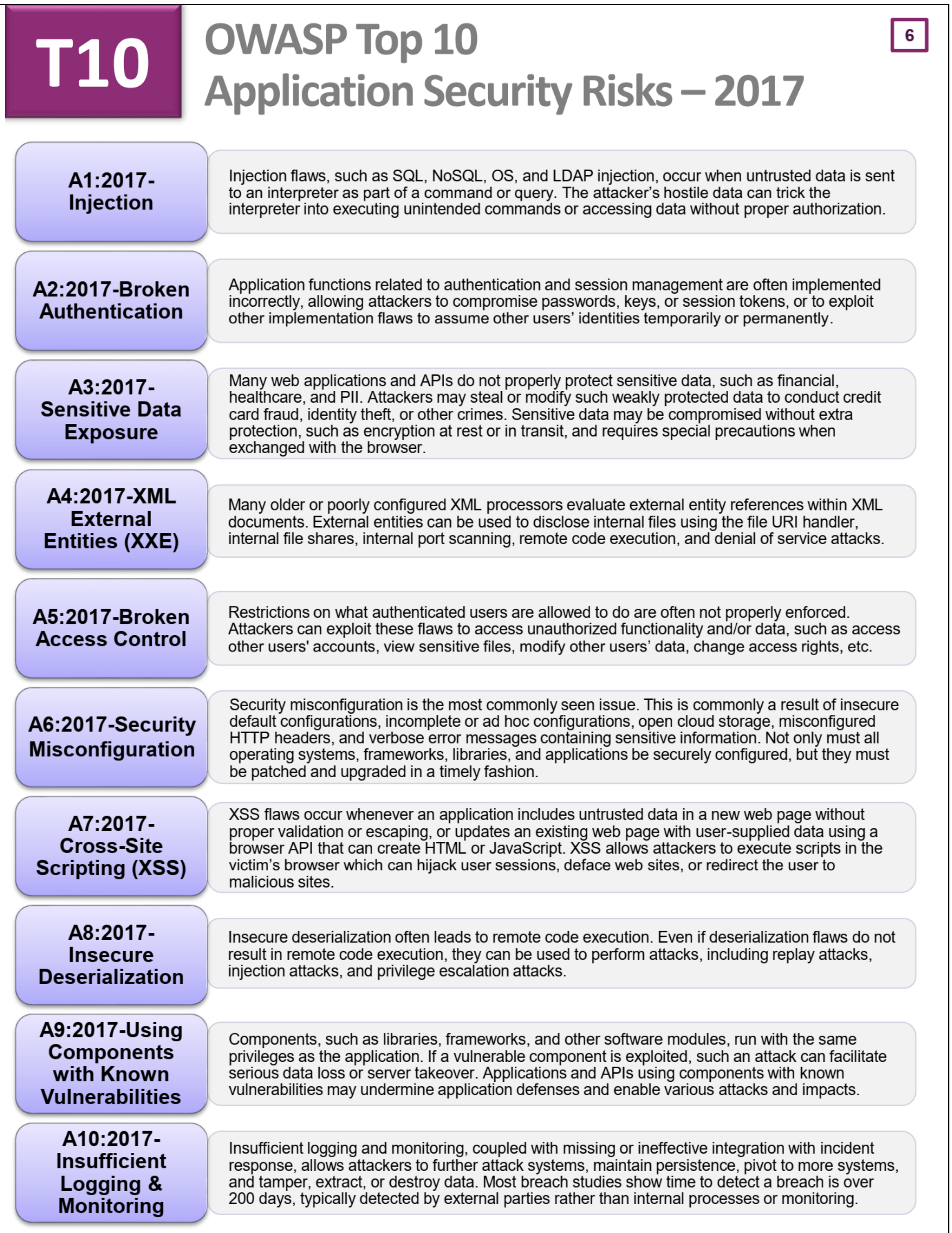
- Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by threat agent which damages or steals organization’s information
- Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information
- Backdoor: gaining access to system or network using known or previously unknown/newly discovered access mechanism

- Password crack: attempting to reverse calculate a password
- Brute force: trying every possible combination of options of a password
- Dictionary: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses
- Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
- Target system cannot handle successfully along with other, legitimate service requests
- May result in system crash or inability to perform ordinary functions § Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously
- Spoofing: technique used to gain unauthorized access; intruder assumes a trusted IP address
- Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network
- Spam: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks
- Mail bombing: also, a DoS; attacker routes large quantities of e-mail to target
- Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
- Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker
- Buffer overflow: application error occurring when more data is sent to a buffer than can be handled
- Timing attack: explores contents of a Web browser's cache to create malicious cookie
- Side-channel attacks: secretly observes computer screen contents/electromagnetic radiation, keystroke sounds, etc.

http://web.cse.ohio-state.edu/~champion.17/4471/4471_lecture_2.pdf

ATTACK SURFACE

	• An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a hacker. • Anyone trying to break into a system generally starts by scanning the target's attack surface for possible attack vectors, whether for an active attack or passive attack, ethical hacking or a hacking competition. • Attack surfaces can be divided in to a few categories: – The network attack surface. – The software attack surface. – The physical attack surface. https://whatis.techtarget.com/definition/attack-surface
5.	What is OWASP Top 10? List the Ten Most Critical Web Application Security Risks.
ANS:	• The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. • At OWASP, you'll find free and open: – Application security tools and standards. – Complete books on application security testing, secure code development, and secure code review. – Presentations and videos. – Cheat sheets on many common topics. – Standard security controls and libraries. – Local chapters worldwide. – Cutting edge research. – Extensive conferences worldwide. – Mailing lists. • A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. • The Top 10 provides basic techniques to protect against these high risk problem areas, and provides guidance on where to go from here.



T10

OWASP Top 10
Application Security Risks – 2017

6

A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

6. What is OWASP Top 10? Explain in brief any one of the Ten Most Critical Web Application Security Risks.

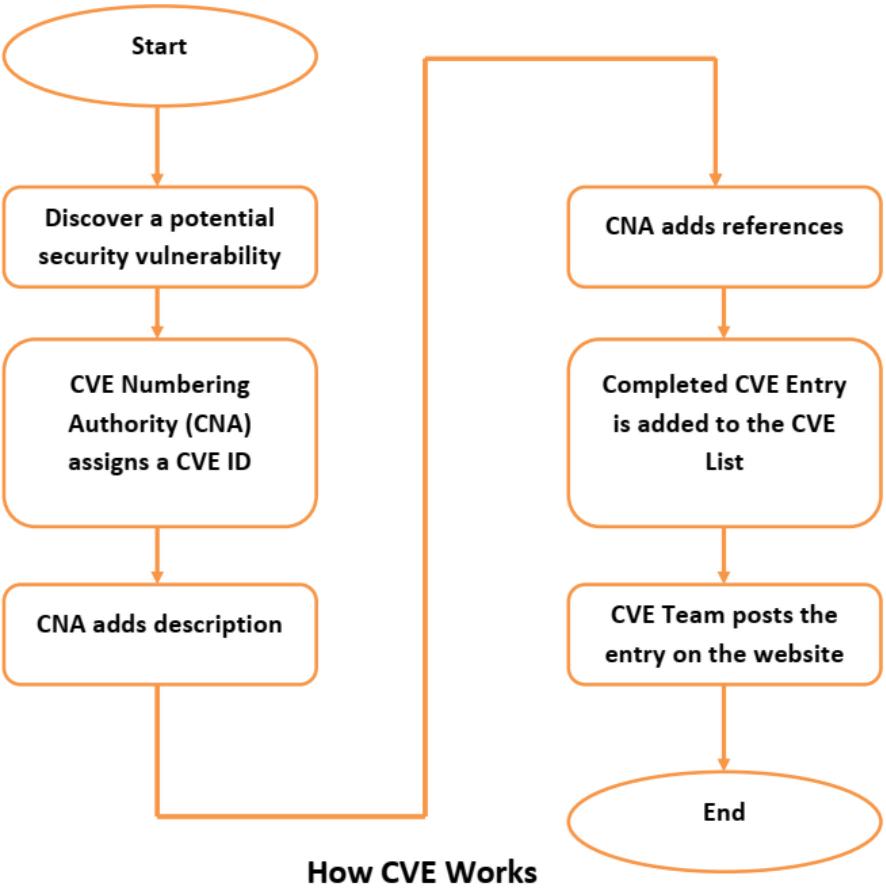
ANS: OWASP TOP 10 pdf

7. Write a short note on CVE Database.

ANS:

- Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cybersecurity vulnerabilities.

- Use of CVE Entries, which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.
- CVE is:
    - One identifier for one vulnerability or exposure
    - One standardized description for each vulnerability or exposure
    - A dictionary rather than a database
    - How disparate databases and tools can "speak" the same language
    - The way to interoperability and better security coverage
    - A basis for evaluation among services, tools, and databases
    - Free for public download and use
    - Industry-endorsed via the CVE Numbering Authorities, CVE Board, and numerous products and services that include CVE
- **How CVE Works:**
    - The process of creating a CVE Entry begins with the discovery of a potential security vulnerability.
    - The information is then assigned a CVE ID by a CVE Numbering Authority (CNA), the CNA writes the Description and adds References, and then the completed CVE Entry is added to the CVE List and posted on the CVE website by the CVE Team.


Start
Discover a potential security vulnerability
CVE Numbering Authority (CNA) assigns a CVE ID
CNA adds description
CNA adds references
Completed CVE Entry is added to the CVE List
CVE Team posts the entry on the website
End

How CVE Works

- **CVE Entry Format:**
  - Each CVE Entry includes:
    - CVE ID number (i.e., "CVE-1999-0067", "CVE-2014-10001", "CVE-2014-100001")
    - Brief Description of the security vulnerability or exposure
    - Any pertinent References (i.e., vulnerability reports and advisories)
    - *CVE ID:* CVE IDs have the format CVE-YYYY-NNNN, which is CVE prefix + year + sequence number digits. Sequence number digits can have 4 or more digits. The YYYY portion is the year that the CVE ID was assigned OR the year the vulnerability was made public.
    - *Description:* The "Description" portion of CVE Entries are typically written by CVE Numbering Authorities (CNAs), the CVE Team, or individuals. Descriptions include

	details such as the name of the affected product and vendor, a summary of affected versions, the vulnerability type, the impact, the access that an attacker requires to exploit the vulnerability, and the important code components or inputs that are involved. + *References:* Each CVE Entry includes appropriate References. Each reference used in CVE: (1) identifies the source (2) includes a well-defined identifier to facilitate searching on a source's website (3) notes the associated CVE ID • **States of CVE Entries:** – A CVE Entry can be marked as Reserved, Disputed or Reject. – *Reserved:* A CVE Entry is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher, but the details of it are not yet populated. – *Disputed:* When one party disagrees with another party's assertion that an issue in software is a vulnerability, a CVE Entry assigned to that issue may be designated as being "DISPUTED". – *Reject:* A CVE Entry listed as "REJECT" is a CVE Entry that is not accepted as a CVE Entry. The reason a CVE Entry is marked REJECT is stated in the description of the CVE Entry. Possible examples include it being a duplicate CVE Entry, it being withdrawn by the original requester, it being assigned incorrectly, or some other administrative reason.
8.	W.r.t to attacks in security explain the following with an example: a. Keystroke Logging b. Denial of Service (DoS /DDoS) c. brute force d. phishing and fake WAP e. Eavesdropping f. Man-in-the-middle g. Session Hijacking h. Cookie Theft i. Buffer Overflow j. ARP poisoning

k. Identity Theft
l. Waterhole attack
m. Clickjacking.
n. URL Obfuscation
o. IoT Attacks

ANS:

a. Keystroke Logging

- Keylogger is spy software to be installed on a computer or a spying device to be plugged into a computer.

- Basic keylogger saves all text typed using a computer keyboard.

- Advanced models have more functions like taking screenshots, sending reports to e-mail, storing history of browsing and opened apps.

- Installation of **software keylogger, which sends logs on a pre-defined e-mail address**, usually takes less than a minute.

- Thanks to a **keylogger that sends stored data straight to your e-mail**, you just need to open your inbox to learn what pages a person spied on visited, what messages they wrote and to whom and more.

- **Keylogger sends report to a predefined e-mail address**.

- It is **super simple – just type in the address** in an appropriate place.

- Hardware keylogger also **stores files with computer logs**.

- If you have access to the monitored computer, all you need to do is press the **appropriate key combination** to see the whole log.

- In this way, you can also check if the keylogger works correctly after plugging it into a computer.

- A keylogger (short for keystroke logger) is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored.

- This is usually done with malicious intent to collect your account information, credit card numbers, user names, passwords, and other private data.

- Legitimate uses do exist for keyloggers.

- Parents can monitor their children's online activity or law enforcement may use it to analyse and track incidents linked to the use of personal computers, and employers can make sure their employees are working instead of surfing the web all day.

- Nevertheless, keyloggers can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard.

- As a result, cybercriminals can get PIN codes and account numbers for your financial accounts, passwords to your email and social networking accounts and then use this information to take your money, steal your identity and possibly extort information and money from your friends and family.

- **How would I get a keylogger?**

  - Keyloggers spread in much the same way that other malicious programs spread.

  - Excluding cases where keyloggers are purchased and installed by a jealous spouse or partner, and the use of keyloggers by security services, keyloggers are installed on your system when you open a file attachment that you received via email, text message, P2P networks, instant message or social networks.

  - Keyloggers can also be installed just by you visiting a website if that site is infected.

- **How do you detect a keylogger?**

  - Keyloggers are tricky to detect. Some signs that you may have a keylogger on your device include: slower performance when web browsing, your mouse or keystrokes pause or don't show up onscreen as what you are typing or if you receive error screens when loading graphics or web pages.

- **What can you do to protect yourself?**

  - Just as you maintain your own health on a daily basis by eating well-balanced meals, getting plenty of rest and exercising, you must also maintain your computer or mobile device's health.

  - That means avoiding keyloggers by avoiding actions that could negatively affect your computer, smartphone or tablet, like visiting dangerous websites or downloading infected programs, videos or games.

  - Here are some tips:

    - **Use caution when opening attachments** – files received via email, P2P networks, chat, social networks, or even text messages (for mobile devices) can be embedded with malicious software that has a keylogger.

- **Watch your passwords** – Consider using one-time passwords and make sure key sites you log into offer two-step verification. You could also use a password manager like McAfee SafeKey that is available with McAfee LiveSafe™ service, which will automatically remember your user name and passwords, but also prevent keylogging since you are not typing in any information on the site as the password manager will do that for you.

- **Try an alternative keyboard layout** – Most of the keylogger software available is based on the traditional QWERTY layout so if you use a keyboard layout such as DVORAK, the captured keystrokes do not make sense unless converted.

- **Use a comprehensive security solution** – Protect all your devices—PCs, Macs, smartphones and tablets—with a solution like McAfee LiveSafe, that offers antivirus, firewall, as well as identity and data protection.

b. Denial of Service (DoS /DDoS)

- A "denial of service" or DoS attack is used to tie up a website's resources so that users who need to access the site cannot do so.
- Many major companies have been the focus of DoS attacks.
- Because a DoS attack can be easily engineered from nearly any location, finding those responsible can be extremely difficult.
- DoS attacks have evolved into the more complex and sophisticated "distributed denial of service" (DDoS) attacks.
- Attackers include hacktivists (hackers whose activity is aimed at promoting a social or political cause), profit-motivated cybercriminals, and nation states.
- DoS attacks generally take one of two forms. They either flood web services or crash them.
- Flooding attacks
  - Flooding is the more common form DoS attack.
  - It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle.
  - The system eventually stops.
  - An ICMP flood — also known as a ping flood — is a type of DoS attack that sends spoofed packets of information that hit every computer in a targeted network, taking advantage of misconfigured network devices.
  - A SYN flood is a variation that exploits a vulnerability in the TCP connection sequence.
  - This is often referred to as the three-way handshake connection with the host and the server.

    - Here’s how it works:
        - The targeted server receives a request to begin the handshake.
        - But, in a SYN flood, the handshake is never completed.
        - That leaves the connected port as occupied and unavailable to process further requests.
        - Meanwhile, the cybercriminal continues to send more and more requests, overwhelming all open ports and shutting down the server.
- Crash attacks
    - Crash attacks occur less often, when cybercriminals transmit bugs that exploit flaws in the targeted system.
    - The result? The system crashes.
    - Crash attacks — and flooding attacks — prevent legitimate users from accessing online services such as websites, gaming sites, email, and bank accounts.
- How a DoS attack works
    - Unlike a virus or malware, a DoS attack doesn’t depend on a special program to run.
    - Instead, it takes advantage of an inherent vulnerability in the way computer networks communicate.
    - Here’s an example.
    - Suppose you wish to visit an e-commerce site to shop for a gift.
    - Your computer sends a small packet of information to the website.
    - The packet works as a “hello” – basically, your computer says, “Hi, I’d like to visit you, please let me in.”
    - When the server receives your computer’s message, it sends a short one back, saying in a sense, “OK, are you real?” Your computer responds — “Yes!” — and communication is established.
    - The website’s homepage then pops up on your screen, and you can explore the site.
    - Your computer and the server continue communicating as you click links, place orders, and carry out other business.
    - In a DoS attack, a computer is rigged to send not just one “introduction” to a server, but hundreds or thousands.
    - The server — which cannot tell that the introductions are fake — sends back its usual response, waiting up to a minute in each case to hear a reply.
    - When it gets no reply, the server shuts down the connection, and the computer executing the attack repeats, sending a new batch of fake requests.
    - DoS attacks mostly affect organizations and how they run in a connected world.
    - For consumers, the attacks hinder their ability to access services and information.
- Other types of attacks: DDoS

    - Distributed denial of service (DDoS) attacks represent the next step in the evolution of DoS attacks as a way of disrupting the Internet.
    - Here's why DDoS attacks have become the weapon of choice for disrupting networks, servers, and websites.
    - The attacks use large numbers of compromised computers, as well as other electronic devices — such as webcams and smart televisions that make up the ever-increasing Internet of Things — to force the shutdown of the targeted website, server or network.
    - Security vulnerabilities in Internet-of-Things devices can make them accessible to cybercriminals seeking to anonymously and easily launch DDoS attacks.
    - In contrast, a DoS attack generally uses a single computer and a single IP address to attack its target, making it easier to defend against.
- How to help prevent DoS attacks
    - If you rely on a website to do business, you probably want to know about DoS attack prevention.
    - A general rule: The earlier you can identify an attack-in-progress, the quicker you can contain the damage.
    - Here are some things you can do.
        - *Method 1: Get help recognizing attacks*
            - Companies often use technology or anti-DDoS services to help defend themselves.
            - These can help you recognize between legitimate spikes in network traffic and a DDoS attack.
        - *Method 2: Contact your Internet Service provider*
            - If you find your company is under attack, you should notify your Internet Service Provider as soon as possible to determine if your traffic can be rerouted.
            - Having a backup ISP is a good idea, too.
            - Also, consider services that can disperse the massive DDoS traffic among a network of servers.
            - That can help render an attack ineffective.
        - *Method 3: Investigate black hole routing*
            - Internet service providers can use "black hole routing."
            - It directs excessive traffic into a null route, sometimes referred to as a black hole.
            - T0his can help prevent the targeted website or network from crashing.
            - The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.
        - *Method 4: Configure firewalls and routers*
            - Firewalls and routers should be configured to reject bogus traffic.

        - Remember to keep your routers and firewalls updated with the latest security patches.
    - *Method 5: Consider front-end hardware*
        - Application front-end hardware that’s integrated into the network before traffic reaches a server can help analyse and screen data packets.
        - The hardware classifies the data as priority, regular, or dangerous as they enter a system.
        - It can also help block threatening data.

c. brute force

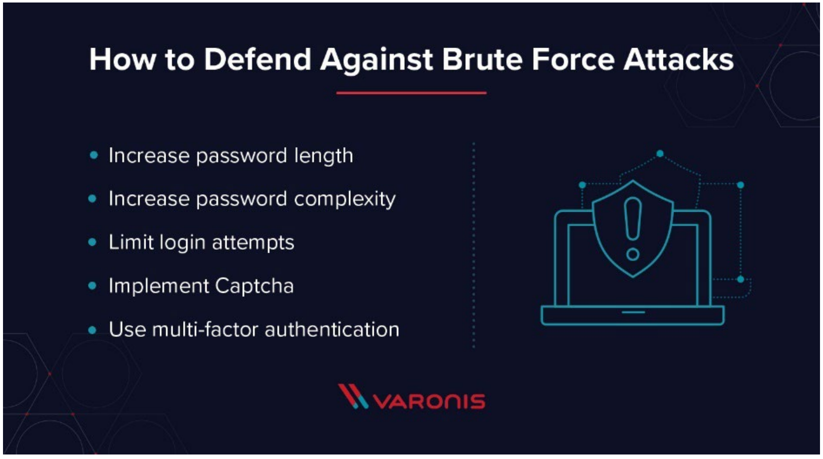
- An attacker could launch a brute force attack by trying to guess the user ID and password for a valid user account on the web application.
- If the brute force attempt is successful, the attacker might be able to access:
- Confidential information, such as profile data for users or confidential documents stored on the web application
- Administration tools used by the System Administrator for the web application to manage (modify, delete, add) web application content, manage user provisioning, or to assign different privileges to users
- Sections of the web application that might expose vulnerabilities or advanced functions not available to non-Administrator users
- Types of brute force attacks
- An attacker might try the following attack methods to find out valid authentication credentials for a web application:

Attack type	**Attack description**
Dictionary attacks	Automated tools that try to guess user names and passwords from a dictionary file. A dictionary file might contain words gathered by the attacker to understand the user of the account about to be attacked, or to build a list of all the unique words available on the web site.
Search attacks	Covers all possible combinations of a character set and ranges of password length. This attack might take some time because of the large amount of possible combinations.
Rule-based search attacks	Uses rules to generate possible password variations from part of a user name or from modifying pre-configured mask words in the input.

Table 1. Brute force attacks

- Brute force attacks are simple and reliable.
- Attackers let a computer do the work – trying different combinations of usernames and passwords, for example – until they find one that works.
- Catching and neutralizing a brute force attack in progress is the best counter: once attackers have access to the network, they're much harder to catch.
- Types of Brute Force Attacks

  - The most basic brute force attack is a dictionary attack, where the attacker works through a dictionary of possible passwords and tries them all.
  - Dictionary attacks start with some assumptions about common passwords to try to guess from the list in the dictionary.
  - These attacks tend to be somewhat outdated, given newer and more effective techniques.
  - Computers are so fast that they can brute force decrypt a weak encryption hash in mere months.
  - These kinds of brute force attacks are known as an exhaustive key search, where the computer tries every possible combination of every possible character to find the right combination.
  - Credential recycling is another type of brute force attack that reuses usernames and passwords from other data breaches to try to break into other systems.
  - The reverse brute-force attack uses a common password like "password," and subsequently tries to brute force a username to go with that password.
- How to Defend Against Brute Force Attacks



How to Defend Against Brute Force Attacks

- Increase password length
- Increase password complexity
- Limit login attempts
- Implement Captcha
- Use multi-factor authentication

- Brute force attacks need time to run.
- Some attacks can take weeks or even months to provide anything usable.
- Most of the defences against brute force attacks involve increasing the time required for success beyond what is technically possible, but that is not the only defence.

- ✦ **Increase password length**: More characters equal more time to brute force crack
- ✦ **Increase password complexity**: More options for each character also increase the time to brute force crack
- ✦ **Limit login attempts**: Brute force attacks increment a counter of failed login attempts on most directory services – a good defence against brute force attacks is to lock out users after a few failed attempts, thus nullifying a brute force attack in progress
- ✦ **Implement Captcha**: Captcha is a common system to verify a human is a human on websites and can stop brute force attacks in progress
- ✦ **Use multi-factor authentication**: Multi-factor authentication adds a second layer of security to each login attempt that requires human intervention which can stop a brute force attack from success

– The proactive way to stop brute force attacks starts with monitoring.

– It's better to detect an attack in progress and actively stop the attack than it is to hope your passwords are un-crackable.

– Once you detect and stop the attack, you can even blacklist IP addresses and prevent further attacks from the same computer.

d. phishing and fake WAP

PHISHING

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Common Features of Phishing Emails

→ **Too Good To Be True -** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true, it probably is!

→ **Sense of Urgency -** A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

- **Hyperlinks -** A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.
- **Attachments -** If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
- **Unusual Sender -** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

➢ *What is phishing*

- Phishing is a devious approach that cybercrooks use to trick you into revealing personal information, such as passwords or credit card, social security, and bank account numbers.
- They do this by sending you fake emails or directing you to a fake website.

➢ *Where phishing attacks come from*

- Phishing messages seem to be from legitimate organizations like PayPal, UPS, a government agency or your bank; however, these are in fact clever cons.
- The emails politely request updates, validation or confirmation of account information, often suggesting that there is a problem.
- You're then redirected to a fake site and tricked into entering account information, which can result in identity theft.

➢ *How to recognize a phishing scam*

- You get messages asking you to reveal personal information, usually via email or via a website.
- Anti-phishing tools help detect **phishing emails and websites**. Avast Internet Security offers you the best anti-phishing software.

➢ *How to remove phishing*

- While phishing lures can't be "removed," they can be detected.
- Monitor your website and be aware of what should and shouldn't be there.
- If possible, change the core files of your website on a regular basis.

➢ *How to prevent phishing*

- Have good habits and don't respond to links in unsolicited emails or on Facebook.
- Don't open attachments from unsolicited emails.
- Protect your passwords and don't reveal them to anyone.
- Don't give sensitive information to anyone—on the phone, in person or through email.

- Look at a website's URL (web address). In many phishing cases, the web address may look legitimate, but the URL may be misspelled or the domain may be different (.com when it should be .gov).
- Keep your browser up to date and apply security patches.
- Use anti-phishing software to detect phishing emails and websites.

FAKE WAP

- Everyone always hears about hackers and hacking and thinks that it is something that only happens to big companies.
- Or they think it only happens to important people.
- This is not the case, especially when we start looking at public WiFi.
- More than anything, hackers love a vulnerable audience.
- They want an audience that is going to take something without thinking.
- Who doesn't want to take free WiFi at every opportunity? Hackers know this, and that's why they have come up with a common hack known as a fake WAP.

➢ **The fake WAP: Stealing your information made easy**

- A fake WAP hack takes place in public spaces where there is free WiFi.
- This includes your local coffee shop, the airport, and shopping centers.
- Most fake WAP hacks start when a hacker downloads a program.
- You don't need any special hacking skills. You just download a program.
- In some instances, you don't even have to download a program as most phones already have this built into them. It is called a 'hot spot' in common parlance.
- Once a device is setup to broadcast its own WiFi signal is when the true hacking will start.
- Hackers will then use another tool, one which is usually built into Aircrack-NG Suite, for jamming and deauthentication.
- Once the local Wi-Fi signal has been jammed or deauthenticated they can then force you to connect to the wireless access point that they have set up.
- This is where problems start.

➢ **What is the point of a fake WAP?**

– There are three main things that hackers are trying to do with a fake WAP:
  - **Steal your password and login:** Since so many people use the same password and login for all of their accounts, hackers will require you to enter one to connect to their fake WiFi. They will then take that information and try to use it to sign into other websites. Think about your Amazon account, eBay, banking, etc. This will be done using basic brute force tools.
  - **Man in the middle attack:** Hackers will use something like Ettercap for a man-in-the-middle attack. This hack will sniff any data that you send over their wireless access point, giving them free access to your data. Again, they're looking for login details and passwords. If you do any banking over this public WiFi you can say goodbye to your money.

- **Device control:** Hackers can take control of your device using a tool like the Metasploit Project. You won't have to worry about your passwords or logins anymore, you will no longer have control of your computer.

➢ **Defend against the fake WAP**

- Here are the steps you need to take to protect yourself from a fake WAP in a public setting:

- **Get the correct WiFi:** When you are in a public setting you will no doubt find a number of open WiFi networks. Be sure to find the person responsible for administering it before you connect. Talk to a security guard in the mall. Talk to the librarian. Make sure that you are connecting to an official WiFi account using the correct name.
- **Unique passwords:** The most basic fake WAP hack can be easily thwarted by simply creating new passwords for each account. If you can't do that, do yourself a favor and do not connect to the wireless access point if it asks for signin details. 1Password can help you with this as well.
- **Using encryption:** Encryption does not have to be scary. It is just another tool that is used in today's modern world. The easiest way to get encryption on public WiFi is by using a VPN service. These tools will automatically encrypt all of the data that you send over any WiFi network. This isn't just beneficial to protect yourself against a fake WAP, but a number of other possible hacks and online tracking activities.

- **VPN blockage:** You will know for certain that you do not want to be on a WiFi network when it blocks you from using a VPN. Even if it is a legitimate WiFi access point, the owner still doesn't want you to protect yourself. Would you get into a car on the condition that you not put on a seatbelt? I hope not…
- **Spoofing:** Another common problem is that once you connect to a WiFi network it sends you to spoof websites. Again, this can be where they ask for login details.
- **Becoming free:** This is when you go to a place where you know the WiFi is regularly paid, or guarded. A hacker can see this and try to play into your gullibility by suddenly changing it to being free available… Using their own WAP with the same name.
- **Auto connect:** You have to turn off the auto connect on your computer. It will want to connect to the most powerful signal in your area. A hacker can make their WAP the most powerful quite easily with a single command line.

e. Eavesdropping

➢ *What is an Eavesdropping Attack*

- An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network.
- An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

➢ *BREAKING DOWN Eavesdropping Attack*

- Eavesdropping attacks involve a weakened connection between client and server that allows the attacker to send network traffic to itself.
- Attackers can install network monitoring software (a sniffer) on a computer or a server to carry out an eavesdropping attack and intercept data during transmission.
- Any device in the network between the transmitting device and the receiving device is a point of weakness, as are the initial and terminal devices themselves.
- Knowing what devices are connected to a network and what software is installed on those devices is one way to protect against eavesdropping attacks.
- Using personal firewalls, updated antivirus software, and virtual private networks (VPN) – and avoiding public networks, especially for sensitive transactions – can help prevent eavesdropping attacks as well.
- Public Wi-Fi networks are an easy target for eavesdropping attacks.
- Anyone with the easily available password can join the network and use free software to monitor network activity and steal login credentials and valuable data that users transmit over the network.
- This is one-way people get their Facebook and email accounts hacked.
- Users can sometimes limit their exposure to such attacks by making sure their phones are running the most recent operating system version.
- However, sometimes users do not have access to the latest software version because the phone vendor does not make it available immediately.

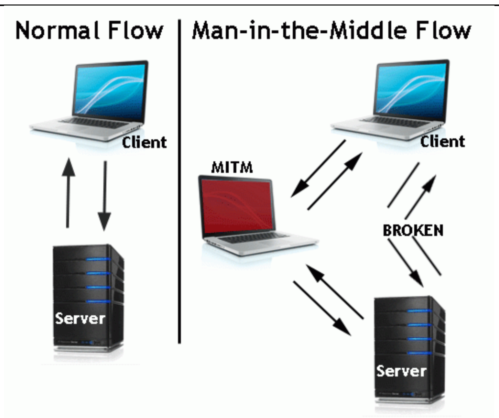
➢ *Examples of Eavesdropping Attacks*

- In May 2011, most Android smartphones were vulnerable to an eavesdropping attack involving authentication tokens sent over unencrypted Wi-Fi networks.
- Eavesdroppers using a sniffing program called Wireshark could view, steal, modify, and delete private calendar data, contact data, and Picasa Web Album data this way.
- The attacker could change a victim’s contact data to trick the victim's contacts into sending sensitive data to the attacker.
- HTTP should not be used to transmit sensitive information such as passwords or credit card numbers because it is not encrypted and is therefore vulnerable to attack; HTTPS or SSH (secure shell) encryption should be used instead to offer a measure of protection against eavesdropping attacks.

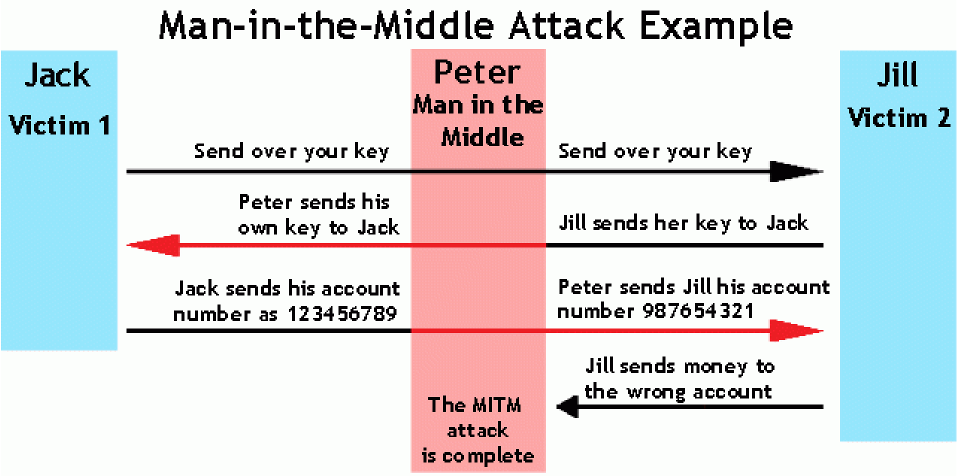
- However, attackers may still be able to decrypt encrypted communications to gain access to confidential information.
- In April 2015, at least 25,000 iOS apps were vulnerable to eavesdropping attacks because of a bug in an open-source code library called AFNetworking that could take down HTTPS encryption.
- The attacker only needed a valid certificate to eavesdrop on or modify an encrypted SSL (secure socket layer) session involving one of the affected apps.

f. Man-in-the-middle

- *What Is a Man-in-the-Middle Attack?*
  - A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
  - A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.
  - Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.
- *Key Concepts of a Man-in-the-Middle Attack*
  - Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
  - A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
  - Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.
- *Man-in-the-Middle Attack Examples*



- In the image above, you will notice that the attacker inserted him/herself in-between the flow of traffic between client and server.
- Now that the attacker has intruded into the communication between the two endpoints, he/she can inject false information and intercept the data transferred between them.
- Below is another example of what might happen once the man in the middle has inserted him/herself.


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

- The hacker is impersonating both sides of the conversation to gain access to funds.
- This example holds true for a conversation with a client and server as well as person-to-person conversations.
- In the example above, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.

➢ *Interactions Susceptible to MITM Attacks*

- Financial sites – between login and authentication
- Connections meant to be secured by public or private keys
- Other sites that require logins – where there is something to be gained by having access

g. **Session Hijacking**

- ***What is Session Hijacking?***

- The session hijacking is a type of web attack.
- It works based on the principle of computer sessions. The attack takes advantage of the active sessions.
- ***How Does Session Hijacking Works?***
- As we know, the http communication uses many TCP connections and so that the server needs a method to recognize every user's connections.
- The most used method is the authentication process and then the server sends a token to the client browser.
- This token is composed of a set of variable width and it could be used in different ways, like in the URL, in the header of http requisition as a cookie, in other part of the header of the http request or in the body of the http requisition.
- The attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the web server.
- This compromising of session token can occur in different ways.

- ***Session Sniffing***
- The first step by the attacker is getting this session id.
- The attacker uses a sniffer to get the session id. When the session id is captured, the attacker uses this session id to gain unauthorized access to the web server.
- ***The Cross-Site Script Attack***
- The cross-site script attack is a way to get the session id with the helping of running malicious code or script from the client side.
- In this attack, the attacker executes malicious scripts, also known as malicious payloads into a legitimate website or web application.
- By using this attack, the attacker does not target a victim directly, but the attacker could exploit a vulnerability in a website that the victim would visit and use the website to deliver malicious script to the victim's browser.
- ***How to prevent the Session Hijacking?***
- The method often used to steal session id is by installing a malicious code on the client website and then the cookie is stealing.
- The best way to prevent session hijacking is enabling the protection from the client side.
- It is recommended that taking preventive measures for the session hijacking on the client side.
- The users should have efficient antivirus, anti-malware software, and should keep the software up to date.
- There is a technique that uses engines which fingerprints all requests of a session.

- In addition to tracking the IP address and SSL session id, the engines also track the http headers.
- Each change in the header adds penalty points to the session and the session gets terminated as soon as the points exceeds a certain limit.
- This limit can be configured.
- This is effective because when intrusion occurs, it will have a different http header order.
- These are the recommended preventive measures to be taken from both the client and server sides to prevent the session hijacking attack.

h. Cookie Theft

Cookie Theft

- One risk associated with the use of cookies is that a user's cookies can be stolen by an attacker.
- If the session identifier is kept in a cookie, cookie disclosure is a serious risk, because it can lead to session hijacking.
- Cookie theft occurs when a third party copies unencrypted session data and uses it to impersonate the real user.
- Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network.
- Although the username and password for a given site will be encrypted, the session data traveling back and forth (the cookie) is not.
- By mimicking a person's cookie over the same network, a hacker can access sites and perform malicious actions.
- Depending on the sites accessed while the hacker is monitoring the network, this could be anything from making false posts in that individual's name to transferring money out of a bank account.
- Hacking software has made it easier for hackers to carry out these attacks by monitoring the packets going back and forth.
- Cookie theft can be avoided by only logging in over SSL connections or employing HTTPS protocol to encrypt the connection.
- Otherwise, it is best not to access sites over unsecured networks.

➢ *WhatsApp Security Flaw (2012)*

- In 2012, a well-known security bug on the famous WhatsApp messenger app allowed users on the same local WiFi network to read each other's messages – all messages!
- An app called WhatsApp Sniffer was made available on Google Play and took advantage of this bug.
- The app hijacked the user's session on the same network, read all his messages from WhatsApp servers and shared them with all other WiFi peers.

i. Buffer Overflow

- A buffer overflow, or buffer overrun, is a common software coding mistake that an attacker could exploit to gain access to your system.

➢ ***Key Concepts of Buffer Overflow***

- This error occurs when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage.
- This vulnerability can cause a system crash or, worse, create an entry point for a cyberattack.
- C and C++ are more susceptible to buffer overflow.
- Secure development practices should include regular testing to detect and fix buffer overflows.
- These practices include automatic protection at the language level and bounds-checking at run-time.

➢ *Definition of a Buffer Overflow*

✦ A buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers.

✦ A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle.

✦ The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwriting the data held in that space.

✦ This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code or manipulate the coding errors to prompt malicious actions.

✦ Many programming languages are prone to buffer overflow attacks.

✦ However, the extent of such attacks varies depending on the language used to write the vulnerable program.

✦ For instance, code written in Perl and JavaScript is generally not susceptible to buffer overflows.

✦ However, a buffer overflow in a program written in C, C++, Fortran or Assembly could allow the attacker to fully compromise the targeted system.

➢ *Executing a Buffer Overflow Attack*

✦ Cybercriminals exploit buffer overflow problems to alter the execution path of the application by overwriting parts of its memory.

✦ The malicious extra data may contain code designed to trigger specific actions — in effect sending new instructions to the attacked application that could result in unauthorized access to the system.

✦ Hacker techniques that exploit a buffer overflow vulnerability vary per architecture and operating system.

- ➢ *Buffer Overflow Causes*
- ✦ Coding errors are typically the cause of buffer overflow.
- ✦ Common application development mistakes that can lead to buffer overflow include failing to allocate large enough buffers and neglecting to check for overflow problems.
- ✦ These mistakes are especially problematic with C/C++, which does not have built-in protection against buffer overflows.
- ✦ Consequently, C/C++ applications are often targets of buffer overflow attacks.
- ➢ *Buffer Overflow Attack Example*
- ✦ In some cases, an attacker injects malicious code into the memory that has been corrupted by the overflow.
- ✦ In other cases, the attacker simply takes advantage of the overflow and its corruption of the adjacent memory.
- ✦ For example, consider a program that requests a user password in order to grant the user access to the system. In the code below, the correct password grants the user root privileges.
- ✦ If the password is incorrect, the program will not grant the user privileges.
- ✦ However, there is a possibility of buffer overflow in this program because the gets() function does not check the array bounds.

j. ARP poisoning

- **ARP is the acronym for Address Resolution Protocol**.
- It is used to convert IP address to physical addresses [MAC address] on a switch.
- The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address].
- The resolved IP/MAC address is then used to communicate.
- **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic**.
- ➢ *ARP Poisoning Countermeasures*
    - → Static ARP entries:
        - ∗ These can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets.
        - ∗ The disadvantage of this method is, it’s difficult to maintain on large networks.
        - ∗ IP/MAC address mapping has to be distributed to all the computers on the network.
    - → ARP poisoning detection software:
        - ∗ These systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated.
        - ∗ Uncertified IP/MAC address resolutions can then be blocked.
    - → Operating System Security:

- This measure is dependent on the operating system been used.
- The following are the basic techniques used by various operating systems.

- **Linux based**: these work by ignoring unsolicited ARP reply packets.
- **Microsoft Windows**: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
  - **AntiARP**– provides protection against both passive and active sniffing
  - **Agnitum Outpost Firewall**–provides protection against passive sniffing
  - **XArp**– provides protection against both passive and active sniffing
- **Mac OS**: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

- 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 system to find out other machines' MAC addresses.
- ARP Poisoning is also known as **ARP Spoofing**.
- Here is how ARP works −
  - 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 MAC address.
  - If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
  - The requesting computer will store the address pair in its ARP table and communication will take place.

➢ *What is ARP Spoofing?*

✦ ARP packets can be forged to send data to the attacker's machine.

✦ ARP spoofing constructs many forged ARP request and reply packets to overload the switch.

✦ The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

- Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

k. Identity Theft

- Identity theft occurs when someone steals your personal information, such as your date of birth, name, and address history.
- Criminals can then use this information to commit identity fraud, typically using your identity to gain financially.
- Unfortunately, identity theft can happen to anyone. If your identity is stolen and used to commit identity fraud, you could face serious consequences.
- Perpetrators may:

– Max out your bank or credit card funds.
– Leave you liable for debts you didn't accrue.
– Use your identity to commit non-financial crimes.
– Severely damage your credit score so you are unable to take out loans or mortgages.

- Though it might be possible for you to clear your name or regain lost funds, the emotional toll and financial worries can linger for a long time.
- Therefore, it's important that you are aware of the common types of identity theft and how criminals steal information, so you can protect yourself.

➢ *Common Types of Identity Theft*

- Identity thieves are always finding new ways to steal and use personal and confidential information. Below are some examples of how a criminal might commit identity fraud.
- Driver's license fraud. Driver's license fraud occurs when a criminal has a driver's license issued to themselves under another person's identity. They might use the license to commit traffic violations that end up on your record and you could lose your license.
- Financial identity theft. Criminals are able to use your stolen personal information to take over your financial accounts or create their own, which can be very serious and stressful. It can take you months or years to rectify the effects of financial identity theft and it could result in large volumes of debt and a poor credit score.
- Child identity theft. Child identity theft is usually committed by a relative who will take out loans and credit cards in the child's name. As children have no reason to check or monitor their credit reports, they will usually remain unaware of the fraudulent activity until they come of age and require loans. This type of fraud can take years to sort out and could stop you from being able to buy a house

or car. It’s also likely to increase the interest rates on any loans you might be offered.

- Change of address fraud. A fraudster could change your mailing address, diverting it to themselves instead. This allows them to look through all your mail and find out bank details, credit card details and other personal information.
- Employment identity theft. Criminals, illegal immigrants and the jobless use stolen identification and personal details to obtain employment. By using stolen identification, they are able to conceal their real personal history from their employers.

➢ *How does Identity Theft Happen?*

- Identity theft can happen to anyone.
- Because of this, it’s important that you understand how criminals steal data so you know how to protect yourself.
- *Theft*
  - Theft of your personal belongings, such as a purse or wallet, or of credit card or bank statements can provide criminals with your sensitive information.
  - Criminals might even go rooting through your rubbish in search of discarded bank statements, so be cautious and shred them or block out sensitive information like your name, address and account numbers.
  - Alternatively, they might attempt to steal new statements or cards directly from your mailbox.
  - You should inform your local post office immediately if you notice your mailbox has been tampered with.
- *Phishing*
  - Phishing is a type of email scam.
  - The sender might pose as a real company, organisation or agency and prompt you to enter your personal information.
  - If an email asks you for a large amount of personal data, such as your name, address, card details or bank account numbers, do not click on any links and register the email as spam.
  - Additionally, if the email contains poor spelling or grammar, claims you won contests you didn’t enter, has offers that are too good to be true or makes unrealistic threats, it’s probably spam.
- *Cold Calling*
  - Cold calling is when a criminal call you, pretending to be a real company, organisation or agency, and coerces you into providing them with your personal information.
  - You should always ignore unsolicited phone calls and assume they have bad intentions.
  - Never give them any of your personal details.
- *Hacking*

	– From banks to retail chains, criminals can hack into computer systems and steal personal credit card and bank information. – Organisations will have systems in place to warn you in the event of a security breach, but before reacting to a message check with the company that your data has been compromised. – Once you know the alert is legitimate, takes steps to close any affected cards if necessary. ∗ *Identity fraud can be costly, both emotionally and financially.* ∗ *However, by understanding the ways criminals go about committing identity fraud and taking measures to stop people getting hold of your personal information, you can reduce the risks of being the victim of identity theft.*
9.	What are BOTs and BOTNETs? Explain. From book
10.	
11.	a.

Q4. Explain dictionary attack

Ans.

- A dictionary attack is a technique or method used to breach the computer security of a password-protected machine or server.
- A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password or trying to determine the decryption key of an encrypted message or document.
- Dictionary attacks are often successful because many users and businesses use ordinary words as passwords.
- These ordinary words are easily found in a dictionary, such as an English dictionary.
- However, this is also the weakest form of authentication, because users frequently use ordinary words as passwords.
- Antagonistic users such as hackers and spammers take advantage of this weakness by using a dictionary attack.
- Hackers and spammers attempt to log in to a computer system by trying all possible passwords until the correct one is found.
- Two countermeasures against dictionary attacks include:
    - Delayed Response: A slightly delayed response from the server prevents a hacker or spammer from checking multiple passwords within a short period of time.

    - Account Locking: Locking an account after several unsuccessful attempts (for example, automatic locking after three or five unsuccessful attempts) prevents a hacker or spammer from checking multiple passwords to log in.
- Dictionary attacks are not effective against systems that make use of multiple-word passwords, and also fail against systems that use random permutations of lowercase and uppercase letters combined with numerals.