TASKS

Devarakonda Sravani
21BEC7224
ECE

TASK-I

Al FOR CYBER SECURITY

23-08-2023

- Top 10 most notorious hackers of all time in this internet world

l.kevin mitnik

- A seminal figure in American hacking, Kevin Mitnick got his career start as a teen. In 1981, he was charged with stealing computer manuals from Pacific Bell.
- In 1982, he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film War Games.
- In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map.

- He was later arrested, convicted and sent to prison.
- During his conditional release, he hacked Pacific Bell's voicemail systems.Throughout his hacking career, Mitnick never exploited the access and data he obtained.
- It's widely believed that he once obtained full control of Pacific Bell's network simply to prove it could be done.
- A warrant was issued for his arrest for the Pacific Bell incident, but Mitnick fled and lived in hiding for more than two years. When caught, he served time in prison for multiple counts of wire fraud and computer fraud.

Although Mitnick ultimately went white hat, he may be part of the both-hats grey area. According to Wired, in 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange," which sells unpatched, critical software exploits to the highest bidder.

2.Anonymous

- Anonymous got its start in 2003 on 4chan message boards in an unnamed forum.
- The group exhibits little organization and is loosely focused on the concept of social justice.
- For example, in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting their search rankings in Google and overwhelming its fax machines with all-black images.
- In March 2008, a group of "Anons" marched passed Scientology centers around the world wearing the now-famous Guy Fawkes mask.
- As noted by The New Yorker, while the FBI and other law enforcement agencies have tracked down some of the group's more prolific members, the lack of any real hierarchy makes it almost impossible to identify or eliminate Anonymous as a whole

- Anonymous" is not an individual hacker but a loosely organized and decentralized collective of hacktivists. They are known for their hacktivist activities, which include various forms of online protests, hacking, and digital activism.
- Anonymous doesn't have a specific ranking of "2 hacker" or any such formal structure. Instead, they operate as a collective with various individuals participating in their actions, often under the "Anonymous" banner.

Here's some information about Anonymous:

1. Anonymous Origins: The origins of Anonymous can be traced back to online imageboards like 4chan, where users would post anonymously and often engage in online pranks and activism.
2. Decentralized Structure: Anonymous does not have a centralized leadership or membership list. Instead, anyone can claim to be part of Anonymous by participating in their activities or adopting their iconic Guy Fawkes mask symbol.
3. Hacktivist Activities: Anonymous is known for conducting various forms of hacktivist activities. These actions have included Distributed Denial of Service (DDoS) attacks, website defacements, data breaches, and leaking sensitive information. They often target organizations or individuals they perceive as engaging in unethical or oppressive behavior.

It's important to note that due to its decentralized nature, Anonymous is not led by a single "2 hacker" but rather a collective of individuals with diverse skills and motivations. While they have been involved in various high-profile actions over the years, their activities have also led to legal consequences for some of their participants.

3.Adrian-Iamo

- In 2001, 20-year-old Adrian Lamo used an unprotected content management tool at Yahoo to modify a Reuters article and add

a fake quote attributed to former Attorney General John Ashcroft.

- Lamo often hacked systems and then notified both the press and his victims. In some cases, he'd help clean up the mess to improve their security.
- As Wired points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures.
- Lamo earned the moniker "The Homeless Hacker" because he preferred to wander the streets with little more than a backpack and often had no fixed address.

4.Albert Gonzales

- According to the New York Daily News, Gonzalez, dubbed "soupnazi," got his start as the "troubled pack leader of computer nerds" at his Miami high school.
- He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators.
- At 22, Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts.
- To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.
- During his time as a paid informant, Gonzalez continued his in criminal activities.
- Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market.
- The New York Times Magazine notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information.

- Using a basic SQL injection, this famous hacker and his team created back doors in several corporate networks, stealing an estimated $256 million from TJX alone.
- During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled."

5.Matthew Bevan and Richard Pryce

- Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI).
- Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems.
- Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC his case bears resemblance to that of Gary McKinnon.
- Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

6.Jeanson James Ancheta

- Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice.
- Instead, Ancheta was curious about the use of bots—softwarebased robots that can infect and ultimately control computer systems.
- Using a series of large-scale "botnets " he was able to compromise more than 400,000 computers in 2005.

- According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems.
- Ancheta was sentenced to 57 months in prison.
- This was the first time a hacker was sent to jail for the use of botnet technology.

7. Michael Calce

- In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers.
- He used their combined resources to disrupt the number-one search engine at the time: Yahoo.
- Within one week, he [1]d also brought down Dell, eBay, CNN and Amazon using a distributed-denial-of-service (DDoS) attack that overwhelmed corporate servers and caused their websites to crash.
- Calce's wake-up call was perhaps the most jarring for cyber crime investors and internet proponents.
- If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce [1]s hack.

8. Kevin Poulsen

- In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon's computer network.
- Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time.
- Instead, he was let off with a warning.
- Poulsen didn't heed this warning and continued hacking.

- In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos.
- When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets.
- According to his own website in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.
- Poulsen was soon arrested and barred from using a computer for three years.
- He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for Wired, The Daily Beast and his own blog Threat

- Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information.
- Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop.
- Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

9.Jonathan James

- Using the alias cOmrade, Jonathan James hacked several companies. According to the New York Times what really earned James attention was his hack into the computers of the United States Department of Defense.
- Even more impressive was the fact that James was only 15 at the time. In an interview with PC Mag, James admitted that he was partly inspired by the book The Cuckoo's Egg, which details the hunt for a computer hacker in the 1980s.

- His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail.

- Jonathan James became the youngest person to be convicted of violating cyber crime laws.
- In 2007, TJX, a department store, was hacked and many customer's private information were compromised.
- Despite a lack of evidence, authorities suspect that James may have been involved.
- In 2008, James committed suicide by gunshot.
- According to the Daily Mail, his suicide note stated, "l have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control."

IO.ASTRA

- This hacker differs from the others on this list in that he has never been publicly identified.
- However, according to the Daily Mail, some information has been released about ASTRA.
- Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician.
- Reportedly, he had been hacking into the Dassault Group, for almost half a decade.

- During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world.
- His hacking cost the Dassault Group $360 million in damages.
- No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.

TASK-2

AI FOR CYBER SECURITY

24-08-2023

Ports and vulnerabilities

1.Port number : 20

- If port number 20 is open on a computer or network, it typically indicates that the File Transfer Protocol (FTP) data port is open. Port 20 is traditionally used for FTP data transfer.
- While having this port open is not inherently a vulnerability, it can pose security risks if not properly configured and secured.
- Here are some potential vulnerabilities or risks associated with an open port 20:

1. **Unauthorized Access:** An open FTP port can be targeted by malicious actors who attempt to gain unauthorized access to the FTP server. If weak or default credentials are in use, this can lead to unauthorized file uploads, downloads, or even complete control of the server.
2. **Data Exfiltration:** If an FTP server is misconfigured or not properly secured, attackers can use an open port 20 to exfiltrate sensitive data from the server, potentially leading to data breaches.

3. **Malware Distribution:** Attackers may use open FTP ports to distribute malware or malicious files. They can upload malicious files to the server, and unsuspecting users or systems may download these files.
4. **Denial of Service (DOS) Attacks:** An open FTP port can be a target for DOS attacks. Attackers may flood the server with connection requests or traffic, causing it to become overwhelmed and unavailable to legitimate users.

2.Port number : 21

- If port number 21 is open on a computer or network, it typically indicates that the File Transfer Protocol (FTP) service is running and listening on that port.
- FTP is a standard network protocol used for transferring files from one host to another over a TCP-based network, like the internet.
- While having port 21 open itself is not necessarily a vulnerability, it can introduce security risks if not properly configured and secured.
- Here are some vulnerabilities and risks associated with an open port 21:

l. **Unauthorized Access:** If FTP is misconfigured, it can allow unauthorized users to gain access to the files and directories on the FTP server. This could lead to data breaches or unauthorized data manipulation.

2. **Brute Force Attacks:** Attackers can attempt to guess usernames and passwords to gain access to the FTP server. If weak or default credentials are used, they can easily compromise the system.

3. Data Interception: FTP is generally unencrypted, which means that data transferred over an FTP connection can be intercepted by attackers. This can expose sensitive information.
4. Malware Distribution: If an attacker gains access to an FTP server, they may use it as a distribution point for malware, infecting files that are being transferred.
5. Denial of Service (DOS) Attacks: Attackers may flood the FTP server with connection requests, causing it to become overwhelmed and unavailable to legitimate users.

3.Port number : 22

- Port 22 is typically associated with the Secure Shell (SSH) service, which is used for secure remote access and administration of a computer system.
- When port 22 is open, it means that the SSH service is running and accepting connections.
- While SSH itself is designed to be secure, there are still potential vulnerabilities and attacks that can be performed if it is misconfigured or not properly secured.
- Some of the common vulnerabilities and attacks associated with an open SSH port (port 22) include:

l. **Brute Force Attacks:** Attackers may attempt to guess usernames and passwords to gain unauthorized access to the system. They use automated tools that try a large number of combinations until they find valid credentials.
2. **Dictionary Attacks**: Similar to brute force attacks, dictionary attacks use a list of common passwords or words to try to guess credentials. This is often more efficient than pure brute force.
3. **SSH Banner Grabbing:** Attackers can use banner grabbing tools to gather information about the SSH server, including its version and configuration. This information can be used to identify known vulnerabilities or weaknesses.

4. **Password Guessing:** Attackers may use social engineering techniques or information gathered from other sources to guess passwords or use default credentials.
5. **SSH Protocol Vulnerabilities:** Over time, vulnerabilities in the SSH protocol itself may be discovered. If the SSH server is not kept up to date with security patches, it could be vulnerable to exploitation.
6. **Key Pair Compromise:** If SSH key pairs are used for authentication, the compromise of a private key can allow unauthorized access. Keeping private keys secure is crucial.
7. **Weak Encryption Algorithms:** Older or misconfigured SSH servers may use weak encryption algorithms, making it easier for attackers to intercept and decrypt traffic.

4.Port number : 23

If port number 23 is open on a system, it typically indicates that the Telnet service is running. Telnet is a protocol that allows for remote command-line access to a computer or device. When port 23 is open and Telnet is enabled, several vulnerabilities and security risks can be exploited:

l**. Clear Text Communication:** Telnet sends data, including login credentials, in clear text. This means that anyone with network access to the traffic can intercept and read sensitive information, such as usernames and passwords. This lack of encryption poses a significant security risk.

2. **Authentication Bypass:** Telnet may have weak or default credentials, which can be exploited by attackers to gain unauthorized access to the system. Some systems have default usernames and passwords, making it easy for attackers to guess or brute-force their way in.
3. **Session Hijacking:** Attackers can use various techniques to hijack an active Telnet session. This allows them to take control

of the user's session and potentially execute malicious commands or access sensitive data.

4. **Denial of Service (DOS) Attacks:** Telnet servers can be vulnerable to DOS attacks, where attackers flood the service with connection attempts or other malicious traffic, causing it to become unresponsive and unavailable for legitimate users.
5. **Remote Code Execution**: If the Telnet service has known vulnerabilities or exploits, attackers can use them to execute arbitrary code on the target system. This can lead to full compromise of the system and unauthorized access.
6. **Port Scanning and Reconnaissance:** An open Telnet port can be an indicator to attackers that a system may have weak security practices. Attackers may perform further reconnaissance and probing to identify additional vulnerabilities or weaknesses.

5.Port number : 25

If port number 25 is open on a computer or network, it typically means that the Simple Mail Transfer Protocol (SMTP) service is running. Port 25 is used for email communication, specifically for sending email messages. While it's not a vulnerability in itself to have port 25 open, there are several potential security risks and vulnerabilities associated with SMTP and email services that can be exploited if not properly secured. Here are some of the common vulnerabilities and risks:

l. **Email Relay:** Open SMTP servers can be used as relay points for sending spam or phishing emails. Attackers can abuse open relays to hide the source of their malicious emails, making it difficult to trace them.
2. **Email Spoofing:** Attackers can forge the sender's email address, making it appear as if an email is coming from a

legitimate source. This can be used for phishing attacks and spreading malware.

3. **Brute Force Attacks:** Attackers may attempt to guess SMTP server passwords through brute force attacks to gain unauthorized access to the server.
4. **Denial of Service (DOS) Attacks:** SMTP servers can be overwhelmed with a high volume of email traffic, leading to a denial of service for legitimate users.
5. **Vulnerabilities in Email Software:** Like any other software, email server software may have vulnerabilities that can be exploited by attackers. It's crucial to keep the email server software up to date with security patches.
6. **Data Exfiltration:** If an attacker gains access to the SMTP server, they may be able to intercept and exfiltrate sensitive email content.

6.Port number : 53

If port number 53 is open on a system, it typically indicates that the system is running a DNS (Domain Name System) service. Port 53 is commonly associated with DNS, and it is used for DNS queries and responses. While having port 53 open is necessary for the proper functioning of DNS, it can also be a potential security risk if not properly configured or if the DNS server software is vulnerable. Here are some potential vulnerabilities and attacks that can be performed if port 53 is open and the DNS server is not properly secured:

l. **DNS Spoofing or Cache Poisoning:** An attacker could attempt to inject malicious data into the DNS cache, redirecting users to malicious websites or intercepting their traffic.

2. **DNS Amplification Attacks:** Attackers can misuse open DNS servers to amplify and launch distributed denial-of-service (DDoS) attacks on other targets, causing them to become overwhelmed with traffic.

3. **Zone Transfer Attacks:** If the DNS server allows zone transfers to unauthorized parties, attackers can gather information about your network structure, potentially aiding in further attacks.
4. **DNS Tunneling**: Attackers may use DNS tunnels to bypass security measures and exfiltrate data from your network.
5. **DNS Query Floods:** Attackers can flood your DNS server with a high volume of DNS queries, causing it to become unresponsive, leading to a denial-of-service (DOS) condition.
6. **Resource Exhaustion:** By constantly querying the DNS server for non-existent or invalid domain names, an attacker may deplete the server's resources, making it less effective for legitimate queries.
7. **Exploiting DNS Software Vulnerabilities:** If the DNS software running on the server has known vulnerabilities, attackers could exploit them to gain unauthorized access or disrupt the service.

7.Port number : 69

Port 69 is typically associated with the Trivial File Transfer Protocol (TFTP). When this port is open, it means that a system is listening for TFTP requests. TFTP is a simple and lightweight file transfer protocol often used for network booting, firmware updates, and other purposes where minimal file transfer capabilities are required.

However, having an open port 69 can pose security risks if not properly configured and secured. Here are some common vulnerabilities and potential risks associated with an open TFTP port:

l. **Unauthorized Access:** If the TFTP server is not configured correctly, it may allow unauthorized users to read or write files on the server. This can lead to data leakage or unauthorized changes to system files.

2. **Malware Distribution:** Attackers can use open TFTP servers to distribute malware or malicious files to other systems on the network, as TFTP is a common vector for malware propagation.
3. **Denial of Service (DOS) Attacks:** Attackers can flood an open TFTP server with requests, overwhelming it and causing a denial of service for legitimate users.
4. **Information Disclosure:** If the TFTP server is misconfigured, it may inadvertently disclose sensitive information or files to unauthorized users.

8.Port number : 80

An open port 80 typically indicates that an HTTP service is running on a server. Port 80 is the default port for HTTP traffic, and it is used for web communication. If port 80 is open and accessible from the internet, it can potentially lead to several security vulnerabilities and attacks :

1. **HTTP Enumeration:** Attackers can use tools to scan for open HTTP ports and gather information about the web server, such as the server software version and the technologies in use. This information can be used to identify known vulnerabilities in the web server software.
2. **Brute Force Attacks:** Attackers may attempt to brute force usernames and passwords for web applications running on port 80, such as web-based admin panels or login pages. Weak or default credentials can be exploited in this manner.
3. **Directory Traversal:** Attackers can try to access files and directories on the web server that are not meant to be publicly accessible. This can lead to the exposure of sensitive information or even the execution of arbitrary code if a vulnerability exists.
4. **SQL Injection:** If the web application running on port 80 is not properly secured, attackers can attempt SQL injection attacks to manipulate the database and gain unauthorized access to data.

5. **Cross-Site Scripting (XSS):** Port 80 is commonly used for web applications, and XSS attacks can be launched to inject malicious scripts into web pages viewed by other users, potentially leading to session hijacking, data theft, or other malicious actions.
6. **Denial of Service (DOS) and Distributed Denial of Service (DDoS):** Attackers may flood the web server on port 80 with a high volume of requests, causing it to become overwhelmed and unavailable to legitimate users.
7. **Remote Code Execution:** If the web server or its applications have vulnerabilities that allow remote code execution, an attacker can potentially take control of the server or execute malicious code.
8. **Zero-Day Exploits:** If the web server software or any of its components have undisclosed vulnerabilities (zero-day exploits), attackers can target those vulnerabilities to gain unauthorized access or compromise the server.

9.Port number : 110

If port number 110 is open, it typically indicates that the server is running the POP3 (Post Office Protocol version 3) service. This protocol is used for receiving email from a mail server. An open port 110 does not necessarily represent a vulnerability on its own, but it can potentially be exploited if the server running the POP3 service is misconfigured or has security weaknesses. Here are some common vulnerabilities and risks associated with an open POP3 port:

l. **Brute Force Attacks**: Attackers may attempt to guess usernames and passwords to gain unauthorized access to email accounts on the server. Weak or easily guessable passwords are particularly vulnerable.
2. **Password Sniffing:** If the server is not configured to use secure authentication methods, attackers can capture usernames and

passwords as they are transmitted in plaintext, making it relatively easy to intercept login credentials.

3. **Security Misconfigurations**: Improperly configured mail servers can expose sensitive email data, allow unauthorized access, or provide attackers with information about the email system's internal structure.
4. **Denial of Service (DOS) Attacks:** Attackers can flood the POP3 service with a large number of requests, causing it to become overwhelmed and unavailable to legitimate users.
5. **Mail Spoofing:** Attackers may send emails from spoofed addresses using the compromised POP3 server, potentially leading to phishing or spam campaigns.

10.Port number : 123

If port number 123 is open on a network or system, it typically indicates that the Network Time Protocol (NTP) service is running on that port. NTP is used to synchronize the time on devices within a network. While having NTP open is essential for many network operations, leaving it open without proper security measures can lead to vulnerabilities and potential attacks. Here are some common vulnerabilities and attacks associated with an open NTP port (port 123):

l. NTP Amplification Attack: This is a Distributed Denial of Service (DDoS) attack where an attacker sends a small NTP request to a vulnerable NTP server with a spoofed source IP address, making it appear as if the request is coming from the victim's IP address. The NTP server then sends a large response to the victim's IP, overwhelming its resources and causing a denial of service.

2. **Reflection Attacks:** Similar to amplification attacks, reflection attacks involve an attacker sending forged requests to NTP servers with the victim's IP as the source address. The NTP servers respond to the victim, creating a DDoS situation.

3. **Exploiting Vulnerabilities:** Like any software or service, NTP implementations may have vulnerabilities that can be exploited if not properly maintained and patched. Attackers could exploit execute arbitrary code, or disrupt NTP services.

11.Port number : 143

Port 143 is typically associated with the Internet Message Access Protocol (IMAP), which is used for retrieving email from a mail server. When port 143 is open, it means that the server is listening for incoming IMAP connections. This doesn't necessarily represent a vulnerability by itself, but it does indicate a potential attack surface. Whether or not there are vulnerabilities depends on the configuration and security measures in place on the server.

Here are some potential vulnerabilities or security risks that could be exploited if the IMAP server on port 143 is not properly secured:

l. Brute Force Attacks: Attackers might attempt to guess usernames and passwords through brute force attacks. If weak or default credentials are used, this could lead to unauthorized access to email accounts.

2. **Authentication Bypass**: Vulnerabilities in the IMAP server's authentication mechanism could allow an attacker to bypass authentication and gain access to email accounts without a valid username and password.
3. **Denial of Service (DOS) Attacks:** Attackers could flood the IMAP server with excessive requests, causing it to become unresponsive or crash, leading to a denial of service for legitimate users.
4. **Exploitation of Known Vulnerabilities:** If the IMAP server software has known vulnerabilities, attackers could exploit these vulnerabilities to gain unauthorized access or compromise the server.

5. **Data Exfiltration:** If an attacker gains access to an email account through a vulnerability, they could exfiltrate sensitive data, such as emails and attachments.

12.Port number : 443

If port number 443 is open on a computer or network, it typically means that the system is running an HTTPS (Hypertext Transfer Protocol Secure) service. Port 443 is the default port for HTTPS, which is used to secure web communication through encryption. While having port 443 open and running HTTPS is generally considered a secure practice, there are still potential vulnerabilities and attacks that can be attempted:

l. **SSL/TLS Vulnerabilities:** SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols used to secure communication over the internet. Vulnerabilities in these protocols can be exploited to compromise the security of the HTTPS connection. Examples include the Heartbleed vulnerability and POODLE attack.

2. **Cipher Suite Weaknesses:** The choice of cipher suites used in the SSL/TLS handshake can impact the security of the connection. Weak or outdated cipher suites can be targeted by attackers to perform attacks like BEAST (Browser Exploit Against SSL/TLS) or FREAK (Factoring Attack on RSAEXPORT Keys).

3. **Certificate Issues:** SSL/TLS relies on digital certificates to establish trust between the server and client. If the certificate is invalid, expired, or improperly configured, it can lead to security vulnerabilities. Attackers can perform Man-in-the-Middle (MitM) attacks by impersonating the server or intercepting traffic.

4. **Brute Force Attacks:** Attackers may attempt to perform brute force attacks to guess the server's private key used for encryption.

While this is computationally challenging, it's not impossible, especially if weak keys are used.

5. **DDoS Attacks**: Port 443 being open makes the server susceptible to Distributed Denial of Service (DDoS) attacks, where attackers flood the server with traffic to overwhelm its resources and make it unavailable.
6. **Vulnerabilities in Web Applications:** If port 443 is used to host a web application, vulnerabilities within the application itself, such as SQL injection, cross-site scripting (XSS), or remote code execution, can be exploited by attackers.
7. **Server Misconfigurations:** Incorrect server configurations can lead to security vulnerabilities. For example, leaving directory indexing enabled or not properly securing sensitive files can expose data or provide entry points for attackers.
8. **Logjam Attack:** This attack targets the Diffie-Hellman key exchange used in SSL/TLS to establish a secure connection. Attackers can downgrade the connection to use weaker encryption and potentially decrypt the traffic.

TASK-3

AI FOR CYBER SECURITY

25-08-2023

OWASP TOP TEN LIST

1.CWE-284-Improper Authorization

OWASP CATEGORY: AOI 2021Broken Access Control

Description: Broken Access Control is a security weakness where an application fails to properly enforce restrictions on what users are allowed to access or do. This can lead to unauthorized users gaining access to sensitive data or functionality they shouldn't have.

Business Impact: The business impact of Broken Access Control includes data breaches, unauthorized actions, data integrity loss, legal and compliance issues, reputation damage, and financial losses. It can result in regulatory fines, customer trust erosion, and increased security costs to remediate issues and prevent future incidents.

2.CWE-916:use of password hash with insufficient computational effort

OWASP CATEGORY: A02:2021 — Cryptographic Failures

Description: Cryptographic Failures encompass a range of vulnerabilities related to the improper use or implementation of cryptographic functions in software. These vulnerabilities can result from weaknesses in encryption algorithms, key management, or other cryptographic processes. Cryptographic Failures can include weak encryption, insufficient key length, insecure random number generation, and misuse of cryptographic libraries.

Business Impact: The business impact of Cryptographic Failures can be significant. It may lead to data breaches, exposing sensitive information to unauthorized parties. This can result in legal consequences, loss of customer trust, regulatory fines, and damage to the organization's reputation. Additionally, compromised cryptographic security can lead to financial losses and the need for costly remediation efforts to strengthen the cryptographic protections.

3. CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP CATEGORY: A03:2021 — Injection

Description: Code Injection (CWE-94) occurs when an application takes untrusted data from a user or an untrusted source and uses it as

part of a command or query to an interpreter. Attackers can inject malicious code, such as SQL or shell commands, leading to the execution of unintended and potentially harmful actions by the application.

Business Impact:

l. **Data Loss or Theft:** Code Injection can lead to data breaches, exposing sensitive information to unauthorized parties. This can result in legal liabilities, financial losses, and damage to the organization's reputation.

2. **Malicious Actions:** Attackers can use code injection to carry out malicious actions within the application, such as unauthorized data modifications, deletion, or manipulation. This can disrupt business operations and affect data integrity.

3. **Service Disruption:** Code injection attacks can lead to service disruptions or downtime, impacting business continuity and customer satisfaction. This downtime can result in revenue loss and increased operational costs.

4. **Legal and Compliance Consequences:** Organizations may face legal and regulatory consequences if code injection vulnerabilities lead to data breaches or non-compliance with industry standards. Fines and legal actions can have significant financial implications.

5. **Reputation Damage:** Security incidents involving code injection can erode trust in the organization, causing customers and partners to lose confidence. This can lead to a loss of business opportunities and a damaged brand image.

6. **Operational Costs:** Remediating code injection vulnerabilities can be expensive and time-consuming. Resources must be allocated to fix the vulnerabilities and implement security measures to prevent future attacks.

4. CWE-657: Violation of Secure Design Principles

OWASP CATEGORY: A04:2021 - Insecure design

Description: CWE-657 refers to the violation of secure design principles when developing software or systems. Secure design principles are best practices and guidelines for building software with security in mind. Violations of these principles can result in weaknesses and vulnerabilities that attackers can exploit.

Business Impact: The business impact of violating secure design principles includes increased security risks and potential vulnerabilities in the software. This can lead to data breaches, system compromises, financial losses, damage to the organization's reputation, and legal and regulatory consequences. Inefficient or costly efforts may also be required to retrofit security measures into an insecurely designed system.

5.CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

OWASP CATEGORY: A05:2021-Security Misconfiguration

Description: CWE-614 refers to a vulnerability where sensitive cookies are transmitted over HTTPS (a secure protocol) but lack the 'Secure' attribute in their configuration. The 'Secure' attribute should be set for cookies that contain sensitive information to ensure they are only transmitted over secure (HTTPS) connections. Without this attribute, the cookies may be exposed to potential interception if an attacker can downgrade the connection to HTTP.

Business Impact: The business impact of CWE-614 includes:

1. Data Exposure: Sensitive data contained in cookies, such as session tokens or authentication credentials, can be intercepted by attackers if they manage to downgrade the connection from HTTPS to HTTP. This could lead to unauthorized access to user accounts and data.
2. **Session Hijacking:** Attackers may exploit this vulnerability to hijack user sessions, impersonate users, and perform actions on their behalf. This can result in unauthorized transactions, data manipulation, or data theft.
3. **Loss of Trust:** Customers and users may lose trust in the application or website if it fails to protect their sensitive information adequately. This can damage the organization's reputation and lead to a loss of customers.
4. **Regulatory Non-Compliance:** Depending on the type of sensitive data involved, this vulnerability may result in noncompliance with data protection regulations, potentially leading to legal consequences and fines.
5. **Security Costs:** Remediation of this vulnerability may require code changes and configuration adjustments to ensure that cookies with sensitive data have the 'Secure' attribute set. This can incur development and testing costs.

6.CWE-1395: Dependency on vulnerable third-party components

OWASP CATEGORY: A06:2021-Vu1nerab1e and outdated components

Description: This weakness involves an application or system relying on third-party software or components that have known vulnerabilities. These vulnerabilities can be exploited by attackers to compromise the security of the application or system.

Business Impact: The business impact of CWE-1395 includes:

1. **Security Risks:** Dependency on vulnerable third-party components exposes the organization to security risks. Attackers can exploit these vulnerabilities to gain unauthorized access, steal data, or disrupt operations.
2. **Data Breaches:** Exploiting vulnerabilities in third-party components can lead to data breaches, potentially exposing sensitive customer information and causing reputational damage.
3. **Compliance Violations:** Depending on the industry and regulatory requirements, the use of vulnerable components may lead to compliance violations, resulting in fines and legal consequences.
4. **Costs of Remediation:** Organizations may incur significant costs in identifying and mitigating vulnerabilities in third-party components. This includes patching, testing, and potentially replacing components.
5. **Downtime and Disruption:** Exploiting vulnerabilities in thirdparty components can lead to system downtime and disruption of services, impacting revenue and customer satisfaction.
6. **Reputation Damage:** Customers and partners may lose trust in the organization if it is discovered that their systems rely on insecure third-party components, damaging the organization's reputation.

7.CWE-521: Weak password requirements

OWASP CATEGORY: A07:2021-identification and authentication failures

Description: Weak Password Requirements is a security weakness where an application or system has lax password policies. This allows users to create weak, easily guessable, or common passwords, making it easier for attackers to gain unauthorized access to accounts and systems.

Business Impact: Weak password requirements can lead to various negative consequences, including:

l. **Account Compromises:** Attackers can easily guess or crack weak passwords, leading to unauthorized access to user accounts, systems, and sensitive data.

2. **Data Breaches:** Weak passwords increase the risk of data breaches, as malicious actors can exploit weak authentication to access confidential information.

3. **Identity Theft:** Weak passwords make it easier for attackers to impersonate legitimate users, potentially leading to identity theft and fraud.

4. **Reduced Security Posture:** Weakened security due to poor password policies can damage an organization's overall security posture and reputation.

5. **Regulatory Non-Compliance**: In some cases, weak password requirements can lead to non-compliance with data protection regulations, resulting in legal consequences and fines.

6. **Increased Support Costs:** Organizations may incur higher support costs to deal with account lockouts, password resets, and security incidents related to weak passwords.

8.CWE-521: Reliance on cookies without validation and integrity checking

OWASP CATEGORY: A08:2021-Software and data integrity failures

Description: CWE-521 represents a security weakness where an application relies on cookies for critical functionality or data without properly validating and ensuring the integrity of these cookies. Inadequate validation and integrity checking can make the application vulnerable to various attacks, such as cookie tampering or session hijacking, where attackers manipulate cookies to gain unauthorized access or modify user data.

Business Impact: The business impact ofCWE-521 can be significant:

1. **Unauthorized Access:** Attackers can manipulate cookies to gain unauthorized access to user accounts, potentially compromising sensitive information or performing actions on behalf of the victim.
2. **Data Tampering:** If cookies are not adequately validated and protected, attackers can modify cookie values to tamper with data, which may lead to data corruption, unauthorized transactions, or other malicious activities.
3. **Session Hijacking:** Insufficient cookie security can allow attackers to hijack user sessions, impersonate legitimate users, and carry out actions with their privileges.
4. **Loss of Trust:** Security vulnerabilities related to cookie handling can erode user trust in the application, potentially causing users to abandon the service due to concerns about data security and privacy.
5. **Legal and Regulatory Consequences:** Failing to protect user data and privacy can lead to legal and regulatory issues,

including fines and penalties for non-compliance with data protection laws.

6. **Financial Impact:** Addressing security breaches, conducting investigations, and mitigating the fallout can result in financial losses for the organization.

9.CWE-532: Insertion of sensitive information into log files

OWASP CATEGORY: A09:2021-security logging and monitoring failures

Description: This weakness occurs when an application logs sensitive information, such as passwords, credit card numbers, or personally identifiable information, into log files. Logging sensitive data poses a significant security risk because log files are often not adequately protected, and unauthorized access to them can expose sensitive information.

Business Impact: The business impact of inserting sensitive information into log files can be severe, including:

l. **Data Exposure:** Sensitive information in logs can be accessed by unauthorized individuals or attackers, leading to data breaches.

2. **Privacy Violations:** Storing sensitive data in logs can result in violations of privacy regulations, leading to legal and financial consequences.

3. **Reputation Damage:** Customers may lose trust in the organization if they learn that their sensitive data is being mishandled, damaging the company's reputation.

4. **Compliance Issues:** Violations of data protection and privacy regulations can result in fines and legal actions against the organization.
5. **Operational Disruption:** Unauthorized access to log files or exposure of sensitive information can disrupt operations and require costly incident response efforts.
6. **Increased Attack Surface:** Attackers may target log files as a source of sensitive data, using it for further attacks, such as identity theft or fraud.

10.CWE-918:server side request forgery

OWASP CATEGORY: AIO:2021- server side request forgery

Description: SSRF is a vulnerability where an attacker can manipulate a server into making requests to other internal or external systems, often with malicious intent. The attacker tricks the server into initiating requests on their behalf, potentially leading to unauthorized access, data leakage, or service disruption.

Business Impact: The business impact includes unauthorized access to internal resources, data exposure, service disruption, and potential legal consequences. SSRF can lead to data breaches, compromised systems, and reputational damage, affecting customer trust and operational costs.

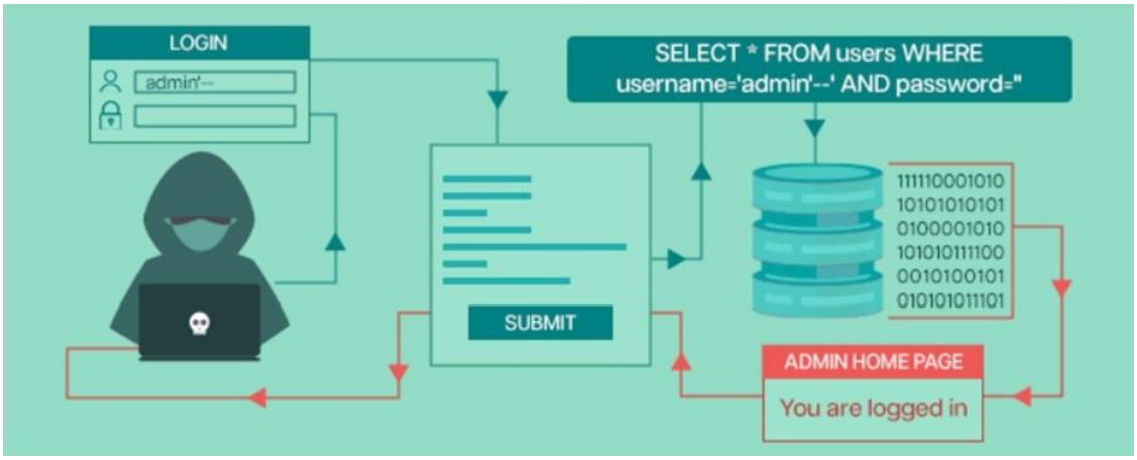
TASK-4

AI FOR CYBER SECURITY

28-08-2023

Understanding top 10 web Application attacks

I.SQL Injection



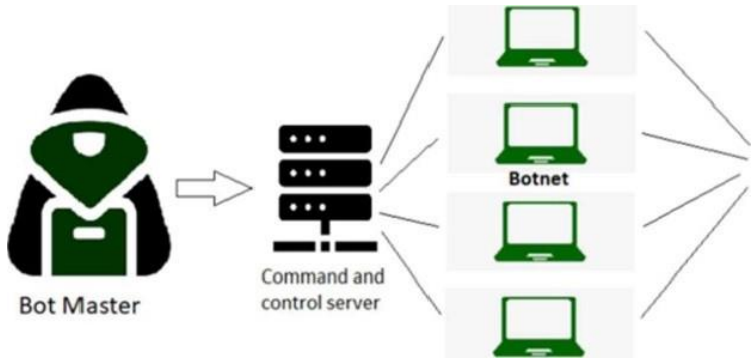
- In SQL injection attacks, malicious SQL queries are injected into input fields or URLs, taking advantage of poorly sanitized user inputs.
- If successful, attackers can manipulate the database, steal data, or even gain unauthorized access to the server.

- .Developed in the 1970s, Structured Query Language (SQL) is a language for accessing and manipulating data from the database. An application can communicate with the database using SQL statements.
- With the use of SQL statements, the application can perform some standard SQL commands such as "SELECT," "UPDATE," "INSERT," "DELETE," "CREATE," and "DROP."

Attackers use the input fields in web applications to run arbitrary queries (injection) on the server. Hence, the attack process is called SQL Injection or SQLi attack.

They gain access to information that is not intended to be displayed. These injection attacks are categorized as 'high impact severity' by OWASP Top 10.

2. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIALOFSERVICE

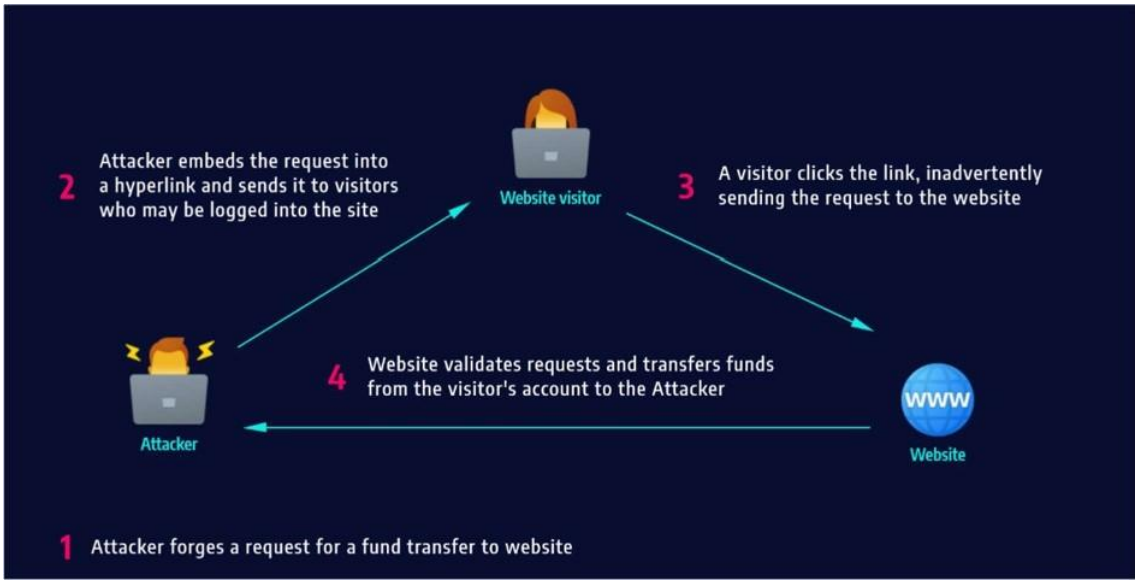


- Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DOS attack.

- ADDoS attack uses multiple servers and Internet connections to flood the targeted resource.
- ADDoS attack is one of the most powerful weapons on the cyber platform.
- When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic.
- Thus, crashing the website or computer due to overloading.

3,Cross Site Request Forgery (CSRF)

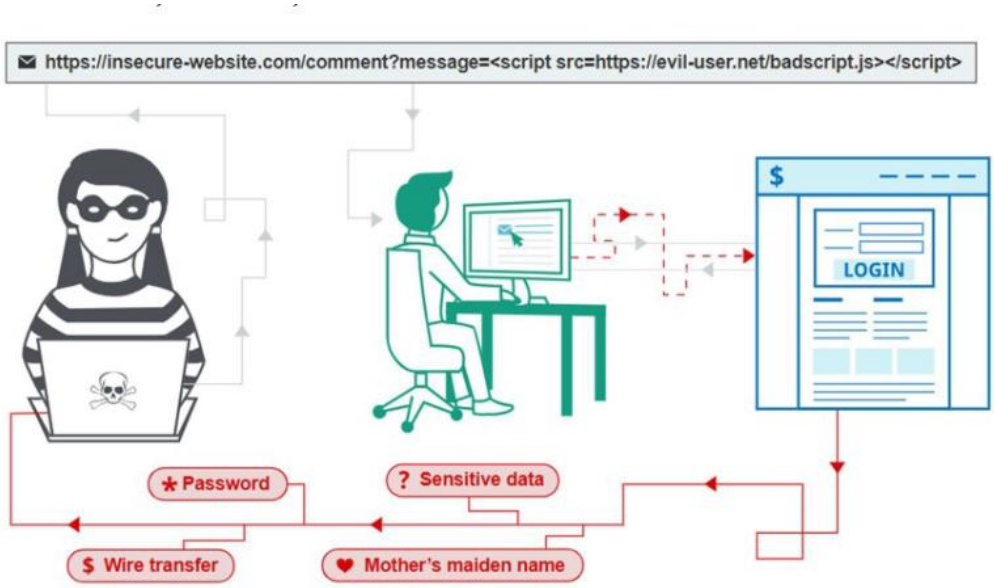
- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
- With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth.
  - If the victim is an administrative account, CSRF can compromise the entire web application



- This blog post introduces our newest addition to our pentestion arsenal, the ssh-putty-brute.psl.
- This tool can turn the well-known PuTTY SSH client (putty.exe or plink.exe) into a reliable SSH login brute force tool which in addition also evades any Antivirus or endpoint protection solution.

4 CROSS SITE SCRIPTING (XSS):

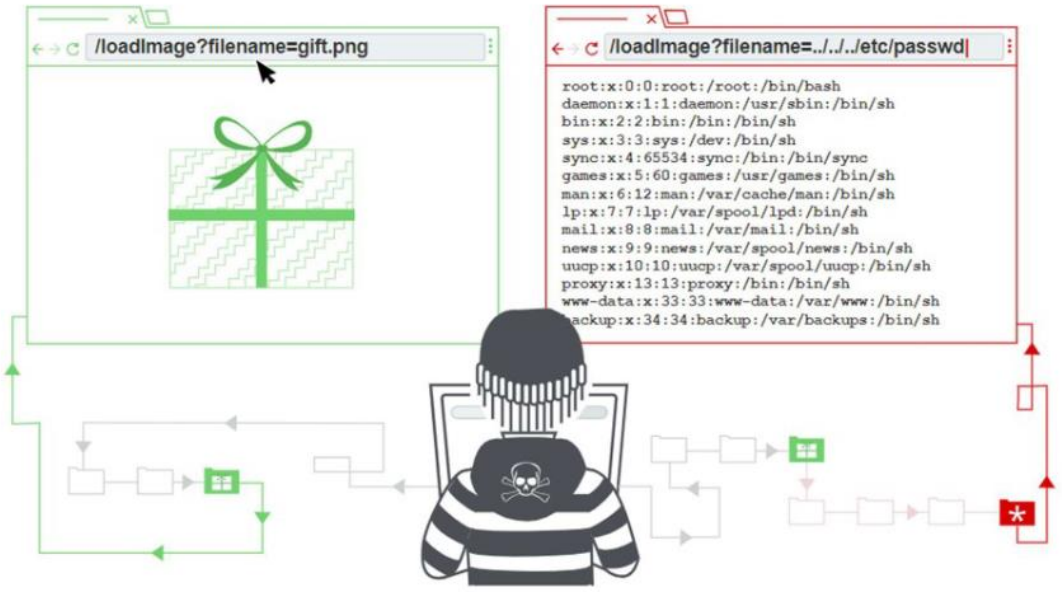
- This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting.
- The script will give the hacker access to web app data such as sessions, cookies, and so on.



- Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users.
- When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

5 DIRECTORY TRAVERSAL:

- Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration.
- The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.



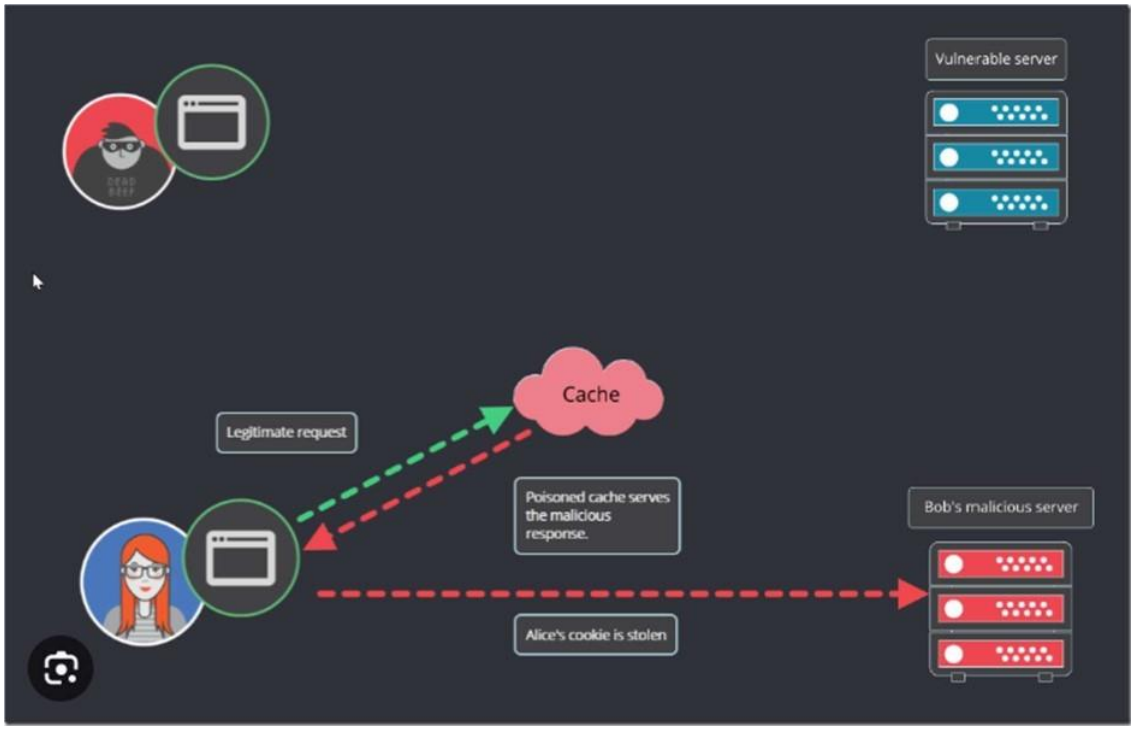
Path traversal is also known as directory traversal. These vulnerabilities enable an attacker to read arbitrary files on the server that is running an application. This might include:

- Application code and data.
- Credentials for back-end systems.
- Sensitive operating system files.

In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

6 HTTP RESPONSE SPLITTING ATTACK:

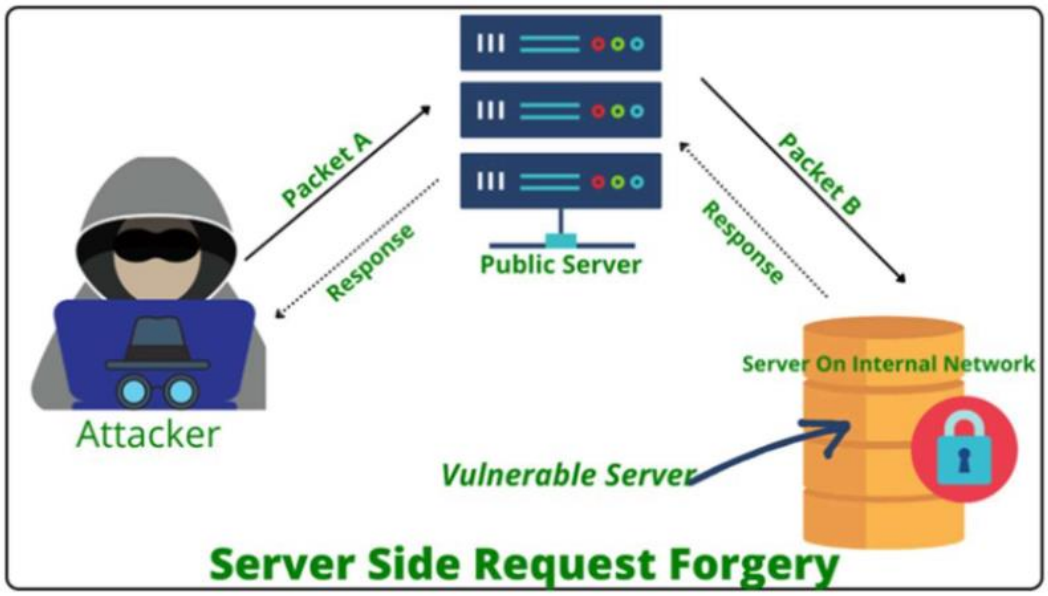
- HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering.
- Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data,
- it works just as well with HTTPS. The attack can be carried out in a variety of ways.



7. Server-Side Request Forgery (SSRF):

- In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources.
- The attacker can supply or modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs,

- the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.

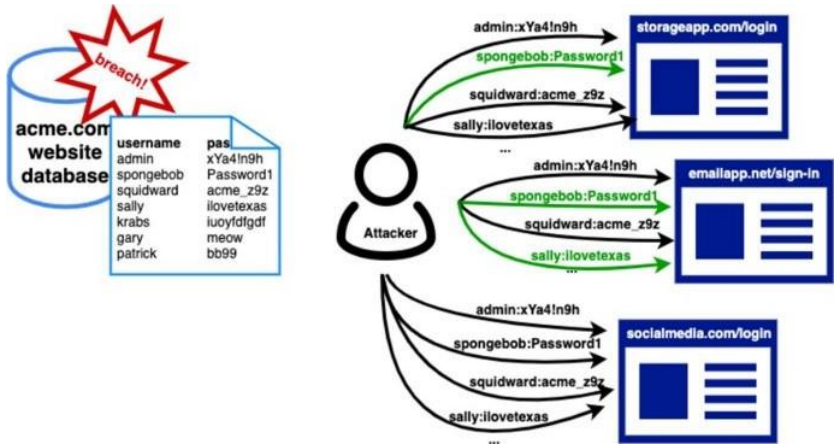


8.Brute Force and Credential Stuffing:

- Credential stuffing is the automated injection of stolen username and password pairs ("credentials") in to website login forms, in order to fraudulently gain access to user accounts.
- Since many users will re-use the same password and username/email, when those credentials are exposed (by a database breach or phishing attack, for example)

- submitting those sets of stolen credentials into dozens or hundreds of other sites can allow an attacker to compromise those accounts too.
- Credential Stuffing is a subset of the brute force attack category. Brute forcing will attempt to try multiple passwords against one or
- multiple accounts; guessing a password, in other words. Credential Stuffing typically refers to specifically using known (breached) username / password pairs against other websites.

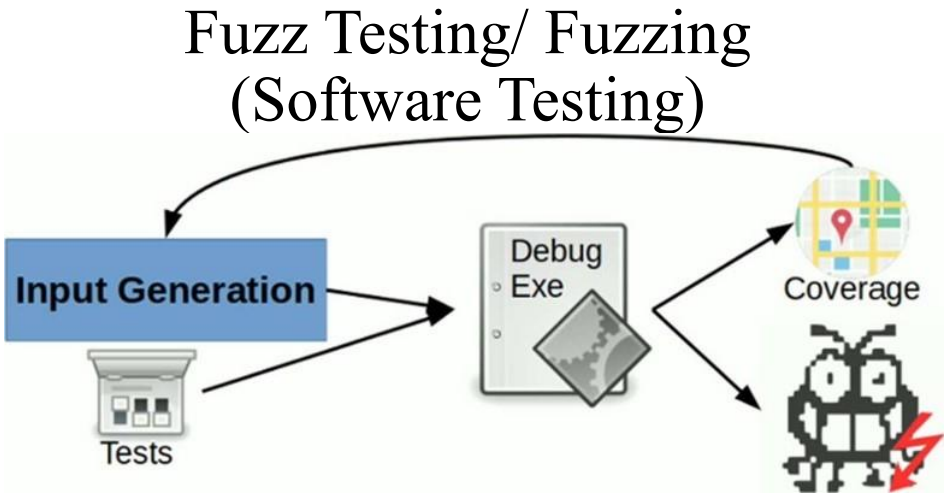
Diagram



9. Fuzz Testing (Fuzzing)

- Fuzz testing, also known as fuzzing, is a technique used to discover vulnerabilities in a web application by sending it random or invalid input data.
- The goal of fuzz testing is to identify how the web application responds to different inputs and to find errors and crashes.
- Fuzz testing can be performed manually or with the help of automated tools.
- Fuzz testing can uncover vulnerabilities that may not be detected by other security testing methods such as penetration testing.

- To perform effective fuzz testing, a tester needs to understand the web application's input and output mechanisms and the types of data that the application processes.



10. Command Injection

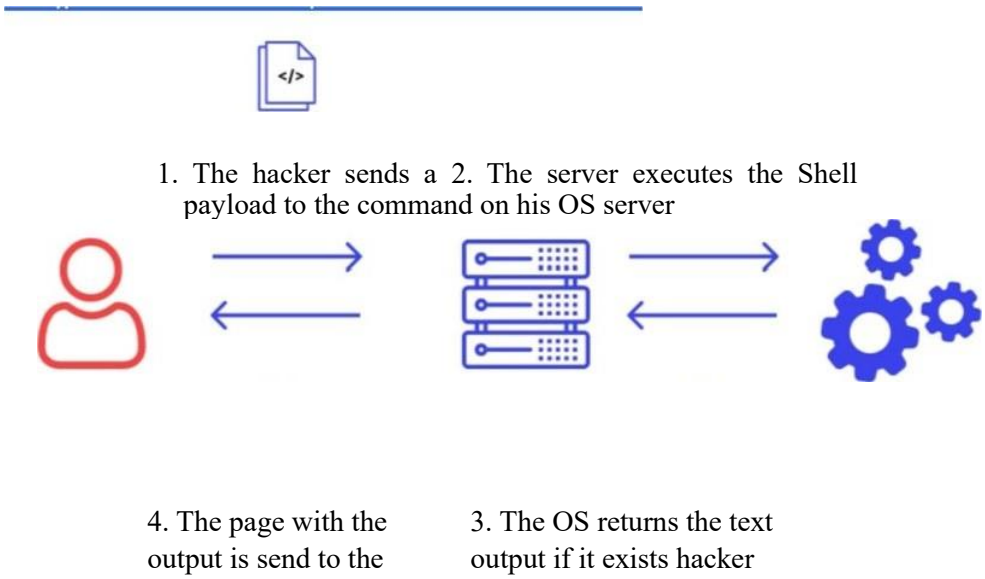
- Command injection attacks occur when attackers inject malicious commands into input fields or parameters that are executed by the server's operating system.
- This can lead to unauthorized access and data manipulation.
  Code Injection Vs. Command Injection
- As both aim to disintegrate the host server and implicate injecting manipulated elements, it is apparent to consider them alike. However, that's not 100% true.
- Code injection interests exploited code introduction using an app and banks upon the ill-handling of non-trustful data inputs by the end-user.

- All the attacks, using this mode of action, happen due to the absence of (one of multiple essential) end-user data validation

  at any stage. The code introduction can be done locally or over the internet.

- Speaking of the harms caused, injecting corrupted code can only hamper the targeted system/application.

- For instance, if a threat actor introduces a corrupted PHP code, then the code will be highly driven by the host machine's PHP functionalities and permissions. Its execution is simple and looks very much similar to Trojan horses.



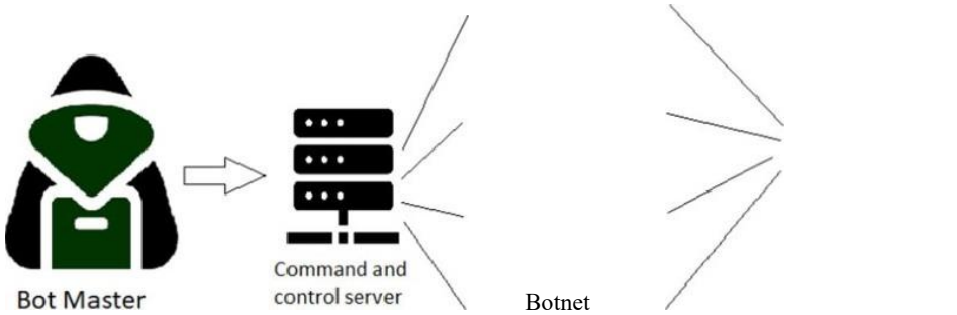
TASK-5

AI FOR CYBER SECURITY

29-08-2023

Ten web server attacks

1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OFSERVICE



Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DOS attack.

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.

2. WEB DEFACEMENT ATTACK:

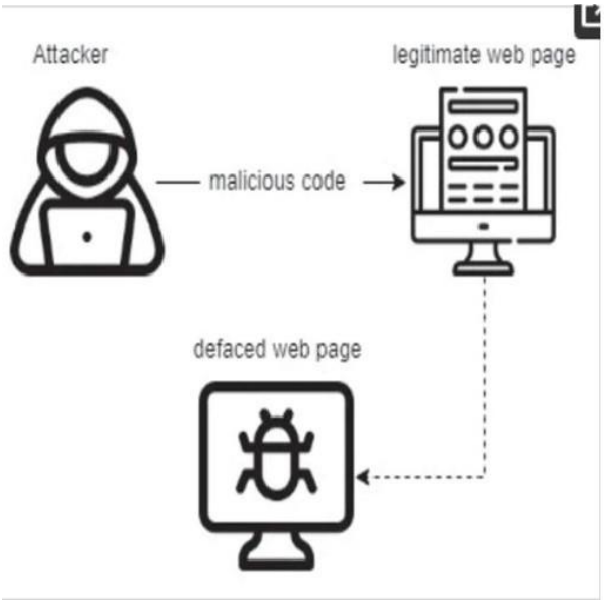


Figure1. Overview of website defacement.

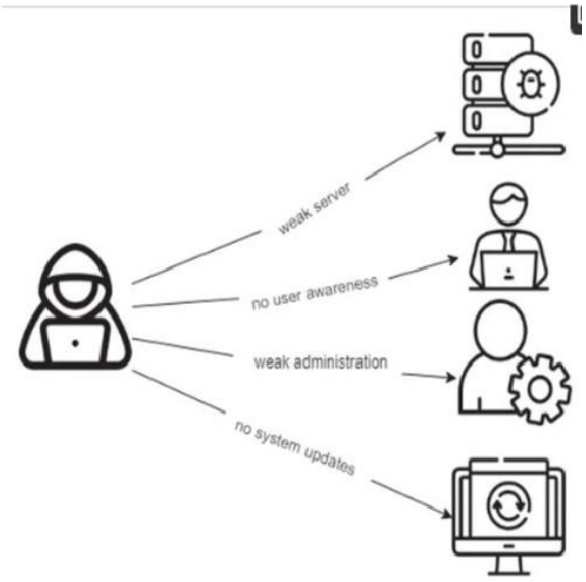


Figure 2. Defacement causes.

In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim. The attackers hack into a web server and replace a website hosted with one of their own.

3.SSH BRUTE FORCE ATTACK:

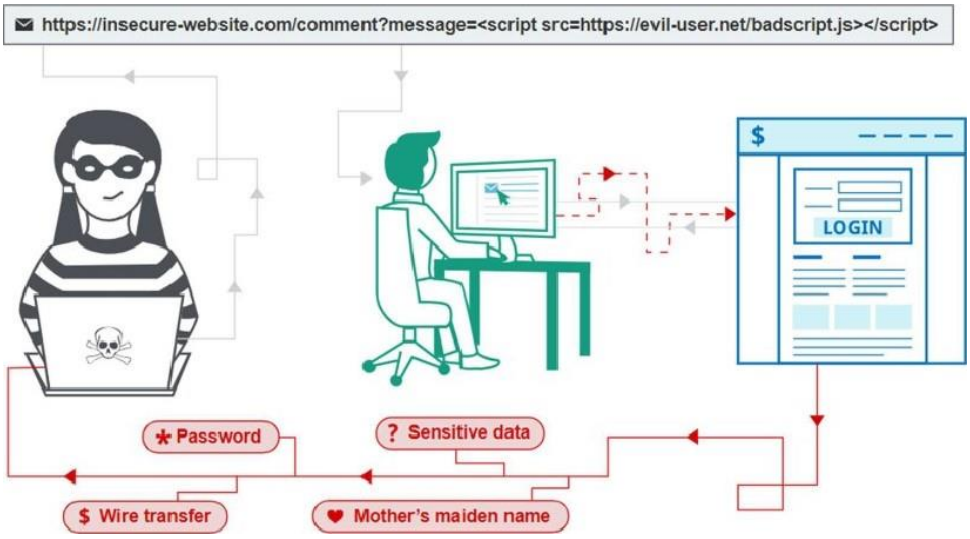
By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access. This exploit can be used to send

malicious files without being noticed. Unlike a lot of other tactics used by hackers, brute force attacks aren't reliant on existing

This blog post introduces our newest addition to our pentestion arsenal, the ssh-putty-brute.psl. This tool can turn the wellknown PuTTY SSH client (putty.exe or plink.exe) into a reliable SSH login brute force tool which in addition also evades any Antivirus or endpoint protection solution.

4 CROSS SITE SCRIPTING (XSS):

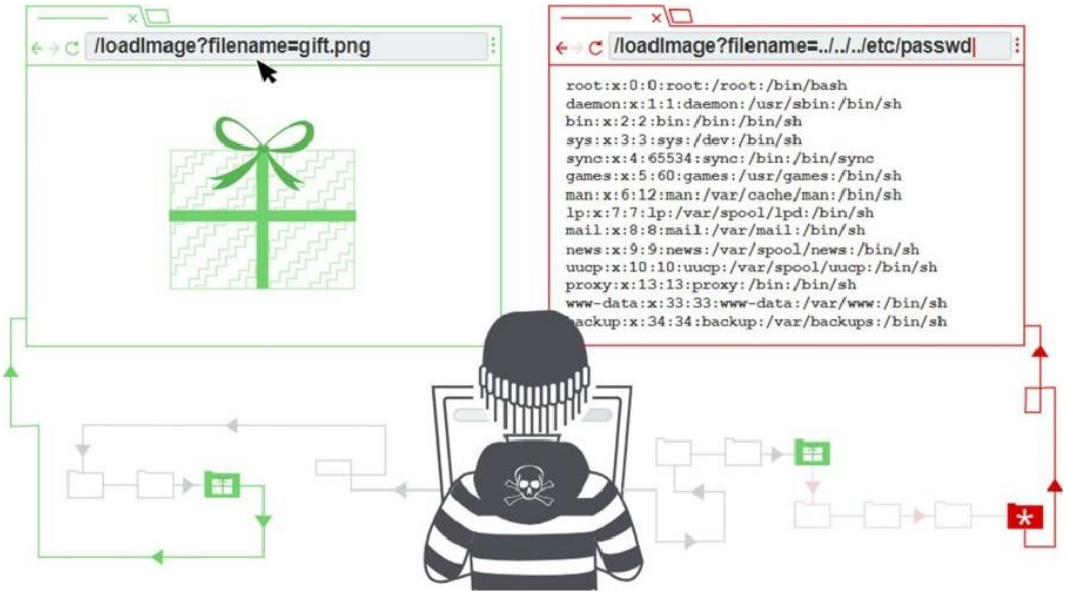
This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.



Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

5 DIRECTORY TRAVERSAL:

Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration. The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.



Path traversal is also known as directory traversal. These vulnerabilities enable an attacker to read arbitrary files on the server that is running an application. This might include:

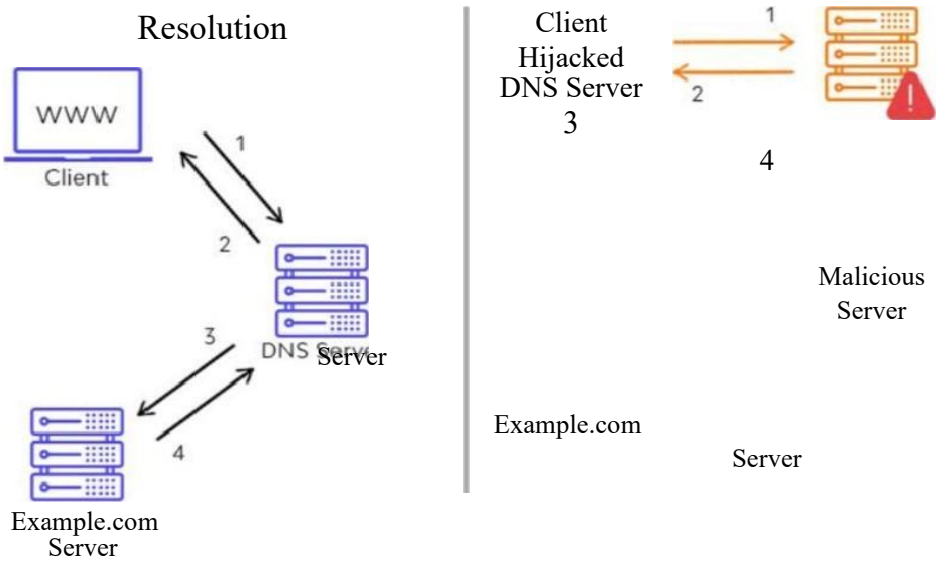
- Application code and data.
- Credentials for back-end systems.
- Sensitive operating system files.

In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

6 **DNS SERVER HIJACKING:**

DNS Hijacking refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up. DNS Redirection is another name for this.

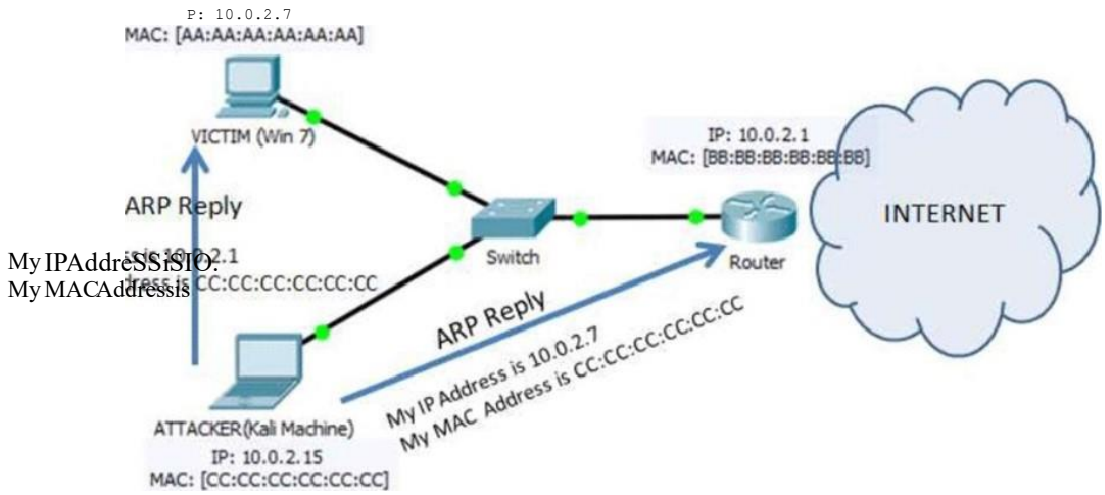
Normal DNS DNSHijacking



DNS hijacking is an attack on a domain name system (DNS). In some cases, it could be an attack on the DNS to make it unavailable for use, while in others, it could be a stealth mode of redirecting the website's users to go to an alternative website. Either way, DNS hijacking attacks use the DNS as a significant part of the attack process. Usually, during a DNS hijacking, attackers incorrectly resolve DNS queries sent by users and redirect them to bogus sites without the users' notice. Afterward, the website user inadvertently proceeds to the linked harmful website or continues using the internet on a server that cyber attackers have compromised.

7 MITMATTACK:

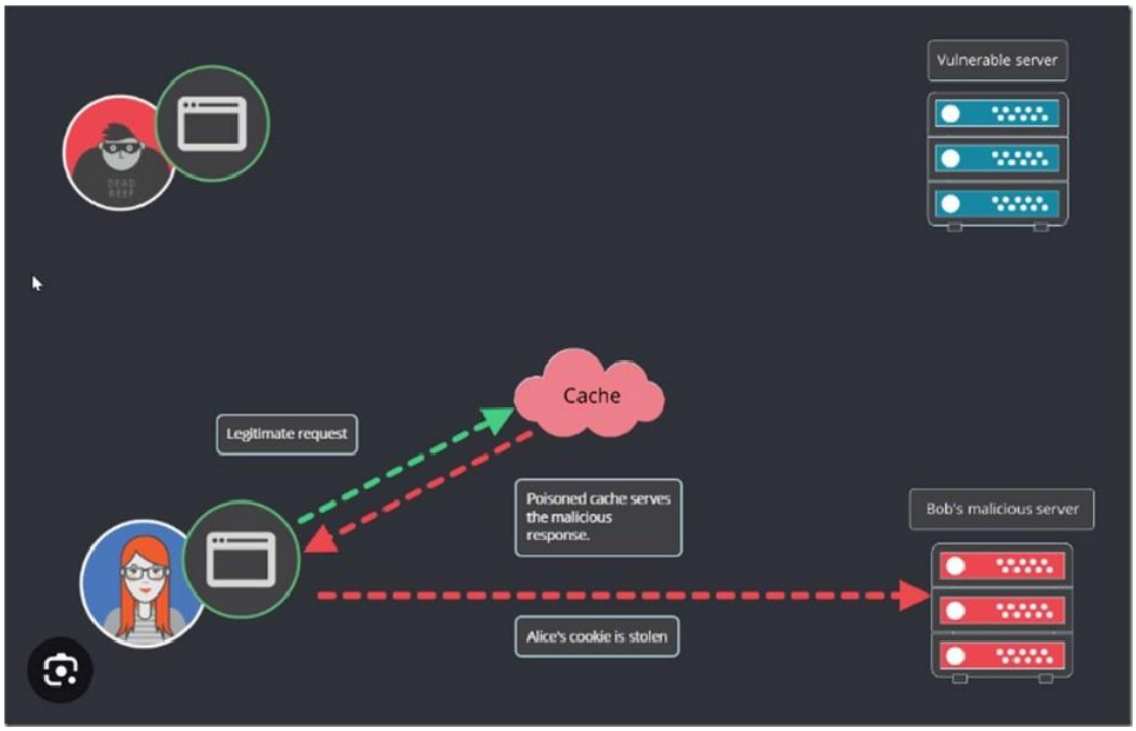
Man-in-the-Middle (MITM) attack allows the attacker to access sensitive information by blocking and modifying the connection between the end-user and web servers. In MITM attacks or smells, the hacker captures or corrects modified messages between the user and the web server by listening or intervening in the connection. This allows the attacker to steal sensitive user information such as online banking details, usernames, passwords, etc., which are transmitted online to the webserver. The attacker entices the victim to attach to an Internet server by pretending to be an agent



Sample MITM Attack by Deceiving Gateway.

8 HTTP RESPONSE SPLITTING ATTACK:

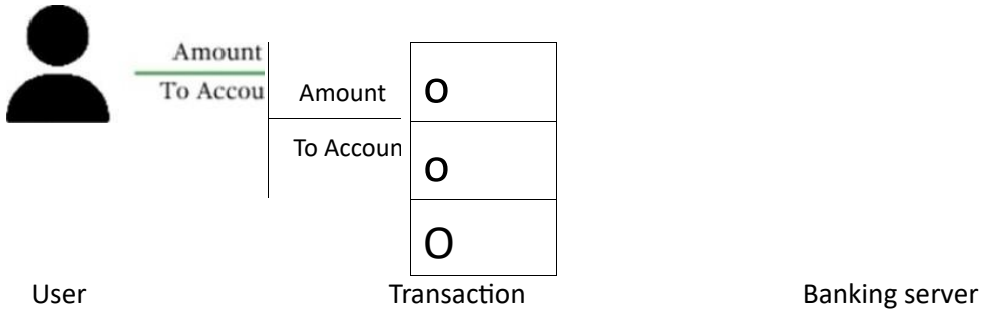
HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering. Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data, it works just as well with HTTPS. The attack can be carried out in a variety of ways.

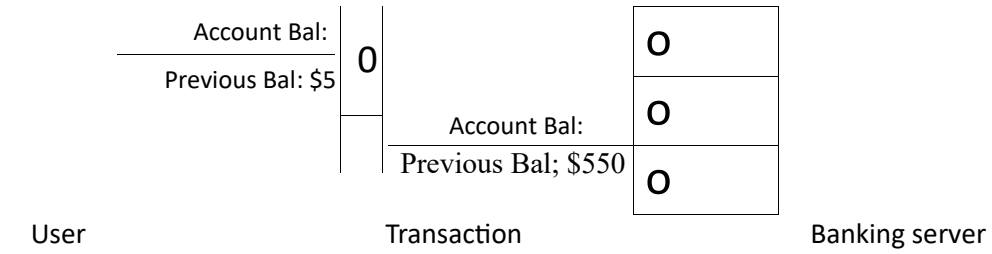


9. Trojans

A Trojan is not a virus, though it is part of the "malware" family. Unlike a computer virus, a Trojan Horse doesn't replicate itself by infecting other files or computers. A trojan is a decoy that may well end up downloading viruses onto your machine, but it is not itself a virus. A Trojan is basically a small piece of malicious software hidden inside a useful program. Once installed, a Trojan can:

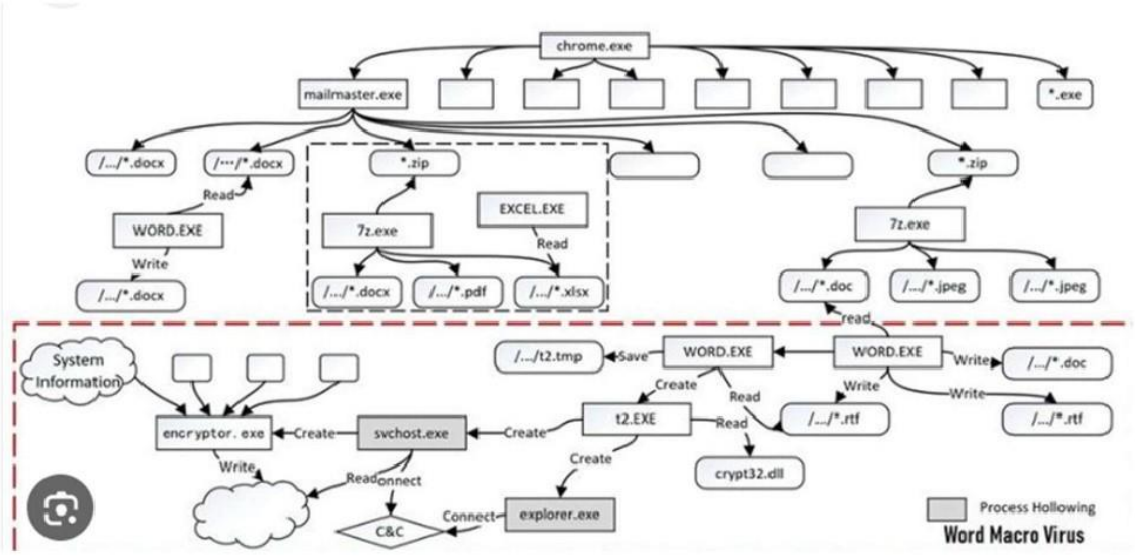
Banking Trojans Archives





10. Macro viruses

Macro viruses infect applications like Microsoft Word or Excel. They're called macro viruses because they're written in the macro language used by the apps they infect. A macro language is a simple programming language that enables users to write and execute automated tasks in sequence. That "shortcut" is called a macro. If macros are enabled in the app, legitimate macros and macro viruses will run during an application's initialization sequence. Thankfully, Microsoft has now disabled them by default, but many users enable them to work more productively. Hence, despite Microsoft's mitigation, macro viruses remain a serious infection vector.


chrome.exe
mailmaster.exe
*.exe
/.../*.docx
/···/*.docx
*.zip
*.zip
Read
WORD.EXE
7z.exe
EXCEL.EXE
7z.exe
Write
Read
/.../*.docx
/.../*.docx
/.../*.pdf
/.../*.xlsx
/.../*.doc
/.../*.jpeg
/.../*.jpeg
read
System Information
/.../t2.tmp
Save
WORD.EXE
WORD.EXE
Write
/.../*.doc
Create
Read
Write
Write
encryptor.exe
Create
svchost.exe
Create
t2.EXE
Read
/.../*.rtf
/.../*.rtf
Write
Create
crypt32.dll
Read
onnect
Connect
C&C
explorer.exe
Process Hollowing
Word Macro Virus

TASK-6

Al FOR CYBER SECURITY

30-08-2023

UNDERSTANDING THE CIS POLICIES

1 : Inventory and Control of Hardware Assets

- Control I helps the CIS to actively manage (inventory, track, and correct) all hardware devices on the network.
- This ensures only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- "Attackers, who can be located anywhere in the world, are continuously scanning the address space oftarget organizations, waitingfor new andpossibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go offofthe enterprise 's network such as laptops or Bring-Your-Own-Device (BYOD) which might be out of synchronization with security updates or might already be compromised.
- Attacks can take advantage ofnew hardware that is installed on the network one evening but not configured andpatched with appropriate security updates until thefollowing day. Even devices that are not visiblefrom the Internet can be used by attackers who

have already gained internal access and are huntingfor internal pivot points or victims.

- Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.,,

2: Inventory and Control of Software Assets

- The focus of this control is to actively manage (inventory, track, and correct) software installed on systems within the organization. A fundamental aspect of risk management is discovering risk by tracking software present on information systems.
- Ensuring only authorized software is used by the organization will increase the effectiveness of risk management efforts. Being able to quickly identify unauthorized and unmanaged software can prevent security breaches and increase the productivity of users. The CIS states this control is critical:
- "Attackers continuously scan target organizations lookingfor vulnerable versions ofsoftware that can be remotely exploited. Some attackers also distribute hostile web pages, documentfiles, media files, and other content via their own web pages or otherwise trustworthy third-party sites.
- When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control ofthe system.
- Some sophisticated attackers may use zero-day exploits, which take advantage ofpreviously unknown vulnerabilities for which no patch has yet been released by the software vendor.
- Without proper knowledge or control ofthe software deployed in an organization, defenders cannot properly secure their assets.

3 .Continuous Vulnerability Management

- The Center for Internet Security (CIS) provides Critical Security Controls to help organizations improve cybersecurity.
- Control 7 addresses continuous vulnerability management (this topic was previously covered under CIS Control 3).
- Continuous vulnerability management is the process of identifying, prioritizing, documenting and remediating weak points in an IT environment.
- Vulnerability management must be continual because sensitive data is growing at an unprecedented rate and attacks are increasing in both frequency and sophistication.
- This control outlines 7 best practices that can help organizations minimize risks to their critical IT resources.

4: Controlled Use of Administrative Privileges

- The focus of this control is to ensure that all users with administrative level access use a dedicated or secondary account for any elevated activity.
- This administrator account should not be used for any other purpose, and should not be used for email, web-browsing, or similar activity.

The CIS states this Control is critical:

- "The misuse ofadministrative privileges is a primary methodfor attackers to spread inside a target enterprise. livo very common attacker techniques take advantage ofuncontrolled administrative privileges.
- In thefirst, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers.

- Thefile or exploit contains executable code that runs on the victim Is machine either automatically or by tricking the user into executing the attacker content.
- If the victim user 's account has administrative privileges, the attacker can take over the victim Is machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data.
- Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

- The focus of this control is to maintain documented security configuration standards for all authorized operating systems and software.
- Organizations must establish a baseline security configuration, implement a configuration management and change control process, and actively be able to report on the security configuration of all endpoint devices such as:

  Mobile devices
  Laptops
  Servers
  Workstations

The CIS states this Control is critical:

"As delivered by manufacturers and resellers, the default configurationsfor operating systems and applications are normally geared towards ease-of-deployment and ease-of-use — not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unneeded software can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability ofindividual users, requiring analysis ofpotentially hundreds or thousands ofoptions in order to make good choices (the Procedures and Tools section below provides resources for secure configurations). Even ifa strong initial configuration is developed and installed, it must be continually managed to avoid security "decay " as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation ofnew software or support new operational requirements. Ifnot, attackers willfind opportunities to exploit both network accessible services and client software.,,

- The journey of implementing the CIS Controls continues with the Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.

Organizations are directed to develop strong, secure baseline configurations for each deployed software system. Organizations are also directed to maintain documented security configuration standards for all authorized operating systems and software.

6: Maintenance, Monitoring and Analysis of Audit Logs

- The focus of this control is to collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The CIS states this Control is critical:

"Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence ofa successful attack. Many organizations keep audit recordsfor compliance purposes, but

attackers rely on thefact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised.

- Because ofpoor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. ',
- The journey of implementing the CIS Controls continues with the Maintenance, Monitoring and Analysis of Audit Logs.
  Organizations are directed to ensure that local logging has been enabled on all systems and networking devices.
- The specific sub-controls that are part of Implementation

7: Email and Web Browser Protections

- The Center for Internet Security (CIS) publishes Critical Security Controls that help organization improve cybersecurity.
  CIS Control 9 covers protections for email and web browsers.
- Attackers target email and web browsers with several types of attacks. Some of the most popular are social engineering attacks, such as phishing.
- Social engineering attempts to manipulate people into exposing sensitive data, providing access to restricted systems or spreading malware.
- Techniques include attaching a file containing ransomware to an email that purports to be from a reputable source, or including a link that appears to be for a legitimate websites but actually points to a malicious site that enables the hacker to collect valuable information, such as the user's account credentials.
- Certain features of email clients can leave them particularly vulnerable, and successful attacks can enable hackers to breach your network and compromise your systems, applications and data.

8: Malware Defenses

- The internet can be a dangerous place, whether you're a big organization or just an everyday user. And, while digital technologies open up to new possibilities, cybercriminals are getting smarter and smarter in taking advantage of them.
- According to the CrowdStrike 2022 Global Threat Report, there were 82% more ransomware-related data leaks last year. At the same time, State-backed Iranian hackers were recently found guilty of spying on users via fake VPN apps. Phishing campaigns, like the recent one targeting shoppers this Black Friday, are often the simpler way to strike.
- What all these attacks have in common is malicious software managing to elude the security infrastructure of one or more devices to inflict harm on their users. That's what, in technical jargon, is known as malware.
- You might be inclined to think that just downloading one of the best antivirus apps is everything you need to secure your information. However, to truly protect your device from being infected, the truth is less straightforward. As malware can be so varied, your protection plan needs to be diversified too.
- The best defense against malware doesn't lie on a mere combination of security software, either. You must know your enemy before defeating it. Knowledge and precautions are the first weapons necessary to fight back!

9: Limitation and Control of Network Ports, Protocols, and Services

- The focus of this control is to manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
- A common denominator is that attackers will always search for, and attempt to exploit, accessible and vulnerable network

services. The most common attacks are generally against hosts such as web servers, mail servers, file and printer servers, etc. The CIS states this Control is critical:

"Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety ofdifferent device types, often without a business needfor the given service. Many software packages automatically install services and turn them on as part ofthe installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit these services, often attempting to exploit default user IDs and passwords or widely available exploitation code. ”

10: data recovery

- Enterprise data recovery is the process of restoring lost, corrupted, accidentally deleted, or otherwise inaccessible data to its server, computer, mobile device, or storage device (or to a new device if the original device no longer works).
- Typically, the data is restored from a backup copy that is stored in another location. The more recent the backup copy, the more completely the data can be recovered in the event of loss or damage.
- For any business, successful data recovery—data recovery that prevents a greater-than-tolerable loss of data or discontinuity of business due to loss of data—requires the business to have a backup and restore plan that meets specific data recovery objectives, usually as part of a larger disaster recovery plan.

1 1 Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

- The focus of this control is to establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The CIS states this Control is critical:

"As deliveredfrom manufacturers and resellers, the default configurationsfor network infrastructure devices are gearedfor ease-of-deployment and ease-of-use — not security. Open services and ports, default accounts (including service accounts) or passwords, supportfor older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state. The management ofthe secure configurations for networking devices is not a one-time event, but a process that involves regularly reevaluating not only the configuration items but also the allowed trafficflows. Attackers take advantage ofnetwork devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk ofthe exception is neither properly analyzed nor measured against the associated business need and can change over time.

12: Boundary Defense

- Boundary defense is control 12 of the CIS Critical Controls and is part of the network family. There are ten subsections to this control that cover your DMZ, firewalls and proxies, IDS/IPS, NetFlow, and remote access.
- Boundary defense is typically an organization's first line of protection against outside threats. Today, many attackers

focus on exploiting systems that they can reach across the internet; they are

- constantly probing perimeters for vulnerabilities and information needed to build their attack plan.

13 Data Protection

- Data protection is the process of protecting sensitive information from damage, loss, or corruption.
- As the amount of data being created and stored has increased at an unprecedented rate, making data protection increasingly important. In addition, business operations Increasingly depend on data, and even a short period of downtime or a small amount of data loss can have major consequences on a business.
- The implications of a data breach or data loss incident can bring organizations to their knees. Failure to protect data can cause financial losses, loss of reputation and customer trust, and legal liability, considering most organizations today are subject to some data privacy standard or regulation.
- Data protection is one of the key challenges of digital transformation in organizations of all sizes.

14 :Controlled Access Based on the Need to Know

- The focus of this control is to ensure users are only allowed access to information they are authorized or needed to perform job duties. There are several layers to this complex problem, beginning with network segmentation, and growing to data classification and Data Loss Prevention (DLP) products.

The CIS states this Control is critical:

"Encrypting data provides a level ofassurance that even ifdata is compromised, it is impractical to access the plaintext without significant resources; however, controls should also be put in place to mitigate the threat ofdata exjiltration in thefirst place. Many attacks occurred across the network, while others involvedphysical theft of

laptops and other equipment holding sensitive information. Yet, in many cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

15 Wireless Access Control

- Experience the seamless convenience and enhanced security offered by wireless access control systems. At Monarch, we specialize in providing cutting-edge solutions for businesses seeking advanced access control.
- With wireless technology, you can say goodbye to traditional wiring limitations and embrace the flexibility and scalability that wireless systems offer. Our team of security experts is here to help you navigate the world of wireless access control, ensuring your premises are protected with the latest innovations.
- Connect with us today to explore how wireless access control can revolutionize your security infrastructure.

16: Account Monitoring and Control

- Everybody wants the latest and greatest next-gen product to get rid of the APTs and h4x0r$ hiding within their networks.
- But what if I told you...

You don't need all those bells and whistles to have a great security program? Specifically, by following CIS Critical

- Control 1 6: Account Monitoring and Control, which focuses on processes to manage the lifecycle (creation, use, dormancy, and deletion) of system and application accounts, you can do much good by practicing one of the most

17 implement security awareness training

- Find the right time to voice out your ideas and concerns about your company's network security to your senior management. Explain why security awareness training is essential in today's world and its benefits.
- Tailor the pitch and sharpen your message by blending in the organisational goals or values. Once the company leaders see how your initiative fits into the big picture, they'll be more willing to devote resources to it. Take reference from our article and learn how to persuade the senior management in order to get a budget.
- Getting support with a top-down approach can help you quickly acquire needed material and resources. It will also empower you to get authority and credibility to increase the likelihood for employees to adopt the training.

1 8: Application Software Security

- Application security is the process of making apps more secure by finding, fixing, and enhancing the security of apps. Much of this happens during the development phase, but it includes tools and methods to protect apps once they are deployed.
- This is becoming more important as hackers increasingly target applications with their attacks.
- Application security is getting a lot of attention. Hundreds of tools are available to secure various elements of your applications portfolio, from locking down coding changes to assessing inadvertent coding threats, evaluating encryption options and auditing permissions and access rights.
- There are specialized tools for mobile apps, for network-based apps, and for firewalls designed especially for web applications.

19 Incident Response Management

- Incident response management is a systematic strategy that allows an organization to address cybersecurity incidents and security breaches. The goal of incident response is to identify real security incidents, get the situation under control, limit the damage caused by an attacker, and reduce the time and costs of recovery.

- Incident response management typically includes formal documentation describing incident response procedures. These procedures should cover the entire incident response process, including preparation, detection, analysis, containment, and post-incident cleanup. By following these procedures, organizations can limit damage, prevent further losses, and comply with applicable compliance regulations.

20 Penetration Tests and Red Team Exercises

- Follow recommendations from Azure Security Center on performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers.

- Use a third-party solution for performing vulnerability assessments on network devices and web applications. When conducting remote scans, do not use a single, perpetual, administrative account. Consider implementing JIT provisioning methodology for the scan account. Credentials for the scan account should be protected, monitored, and used only for vulnerability scanning.