**NAME:ABIRAMI R**

**REG NO:21BCB0236**

**TASK-1:TOP MOST 10 HACKERS**

**DATE:23/08/2023**

**1.Kevin Mitnick:**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.

**3.Adrian Lamo:**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 Gonzalez:**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—software-based 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:**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'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'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 Level. 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, “I 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.”

**10.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'.

**DATE:25/08/2023**

**TASK2:PORTS ANS VULNERABILITIES**

**A table with different types of ports

Description automatically generated**

**1.Port 20:**

Vulnerabilities:

1.Weak Authentication:FTP can be vulnerable to brute force attacks and password guessding due to weak passwords.

2.Data interception:Data transmitted over FTP is often unencrypted making it susceptible to eavesdropping.

**2.Port 21:**

Vulnerabilities:

1.Brute force attack-Attackers can attempt to gusses username ans passwords to gain unauthorized access to the FTP server.

2.FTP Bounce attack-Attackers use the FTP server to bounce attacks of it,making it appear that the attacks are originationg from the FTP server.

**3.Port 22:**

Vulnerabilities:

1.Bruce force attack-weak or default SSH passwords can be targeted by attackers using automated tools.

2.Protocol Vulnerabilities-Vulnerabilities in the SSH protocol or server software can be exploited by attackers.

**4.Port 23:**

Vulnerabilities:

1.Sniffing:Telnet transmits data in plaintext,allowing attackers to capture sensitive information.

2.Password Exposure:Passwords sent over telnet can be intercepted,leading to unauthorized access.

**5.Port 25:**

Vulnerabilities:

1.Open relay:Misconfigured SMTP services can be exploited by spammers to send bulk unsolicited emails.

2.Email Spoofig:Lack of proper authentication can lead to email spoofing and phishing attacks

**6.Port 53 :**

Vulnerabilities:

1.DNS cache poisoning:Attackers can manipulate DNS responses,redirecting users to malicious websites.

2.DDoS amplification:Misconfigured DNS servers can be abused to launch Distrubuted Denial of service attacks.

**7.Port 69 :**

Vulnerabilities:

1.No authentication:TFTP lacks authentication,allowing unauthorized access of files.

2.Dta Exposure:Files transferred using TFTP are often unencrypted, exposing sensitive data.

**8.Port 80:**

Vulnerabilities:

1.Cross-site-scripting :Web applications on these ports can be vulnerable to code injection attacks.

2.SQL injection:Poorly secured web application can be susceptible to SQL injection attacks.

**9.Port 110:**

Vulnerabilities:

1.Password Exposure:POP3 transmits passwords in plaintext,making them vulnerable to interception.

2.Email spoofing:Lack of proper authentication can lead to email spoofing and phishing attacks.

**10.Port 123:**

Vulnerabilities:

1.Reflection Attacks:Misconfigured NTP services can be abused for Distributed Reflextive Denial Of service attacks.

2.Time sppofig:Manipulating NTP responses can lead to incorrect time synchronization.

**11.Port 142:**

Vulnerabilities:

1.Email Hijacking:Attackers with access to IMAP can manipulate or delete users email messages.

2.Credential Thef:Weak authentication can lead to unauthorized access to mailboxes.

**TASK 3:**

**We are to study the OWASP top 10 which is a regularly updated list of the most critical security risks facing web applications and make a comprehensive report on them including their descriptions and their business impact, and also illustrate an example by picking a cwe IDeD vulnerability and demonstrating it on a real web application.**

**OWASP:**

OWASP stands for the Open Web Application Security Project. It is a well-known nonprofit organization that focuses on improving the security of software and web applications. OWASP provides valuable resources, tools, guidelines, and documentation to help developers, security professionals, and organizations build and maintain secure web applications and software.

**Report on OWASP Top 10 Security Risks**

**Introduction**

The OWASP Top 10 is a list of the most critical security risks facing web applications. It is regularly updated to reflect the evolving threat landscape. This report aims to provide a comprehensive overview of the OWASP Top 10 security risks, their descriptions, and their business impact.

**OWASP Top 10 Security Risks**

1. Injection

Description: Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query. This can lead to data leakage, data manipulation, and even remote code execution.

Business Impact: Injection attacks can lead to data breaches, unauthorized access, and significant financial and reputational damage.

Example Vulnerability: SQL Injection (CWE-89)

2. Broken Authentication

Description: Broken authentication vulnerabilities result from weaknesses in user authentication and session management. Attackers can exploit these flaws to gain unauthorized access to accounts and sensitive data.

Business Impact: Breached accounts can lead to identity theft, fraud, and a loss of trust among users.

Example Vulnerability: Session Fixation (CWE-384)

3. Sensitive Data Exposure

Description: Sensitive data exposure occurs when an application fails to adequately protect sensitive information, such as passwords or credit card numbers. Attackers can exploit this weakness to steal confidential data.

Business Impact: Exposing sensitive data can lead to regulatory fines, loss of customer trust, and legal consequences.

Example Vulnerability: Insecure Storage of Sensitive Information (CWE-313)

4. XML External Entities (XXE)

Description: XXE vulnerabilities happen when an application parses XML input insecurely, allowing an attacker to include external entities, leading to information disclosure and denial of service.

Business Impact: XXE attacks can lead to data exposure and service disruption.

Example Vulnerability: XXE Injection (CWE-611)

5. Broken Access Control

Description: Broken access control issues occur when an application does not properly restrict user access to certain functionalities or resources. This can lead to unauthorized actions by users.

Business Impact: Unauthorized access can result in data breaches, fraud, and compromised system integrity.

Example Vulnerability: Inadequate Authorization (CWE-285)

6. Security Misconfiguration

Description: Security misconfigurations occur when an application or its components are not securely configured. This can result in vulnerabilities that attackers can exploit.

Business Impact: Misconfigurations can lead to unauthorized access, data exposure, and service interruptions.

Example Vulnerability: Insecure Server Configuration (CWE-16)

7. Cross-Site Scripting (XSS)

Description: XSS vulnerabilities enable attackers to inject malicious scripts into web pages viewed by other users. This can lead to session hijacking and data theft.

Business Impact: XSS attacks can steal sensitive data, compromise user accounts, and damage an organization's reputation.

Example Vulnerability: Stored XSS (CWE-79)

8. Insecure Deserialization

Description: Insecure deserialization vulnerabilities occur when an application deserializes untrusted data without proper validation. This can lead to remote code execution and other attacks.

Business Impact: Insecure deserialization can result in data breaches and system compromise.

Example Vulnerability: Insecure Deserialization (CWE-502)

9. Using Components with Known Vulnerabilities

Description: Using outdated or vulnerable components in an application can expose it to known security issues. Attackers target these vulnerabilities to compromise the application.

Business Impact: Using vulnerable components can lead to data breaches, downtime, and a damaged reputation.

Example Vulnerability: Outdated Library (CWE-506)

10. Insufficient Logging & Monitoring

Description: Insufficient logging and monitoring can make it difficult to detect and respond to security incidents promptly. Attackers can operate undetected.

Business Impact: Without proper monitoring, breaches can go unnoticed, leading to further damage.

Example Vulnerability: Insufficient Logging (CWE-778)

Vulnerability Demonstration

Example Vulnerability: SQL Injection (CWE-89)

**Description:** SQL Injection occurs when an attacker injects malicious SQL code into input fields, potentially allowing them to manipulate the database.

**Business Impact:** SQL Injection can lead to unauthorized access, data loss, and application compromise.

**Demonstration:** Consider a web application that allows users to search for products using a search bar. An attacker enters a SQL injection payload like '; DROP TABLE Products; --, and if the application does not properly sanitize input, this malicious SQL code could be executed, deleting the "Products" table from the database.

**Conclusion:**The OWASP Top 10 provides a valuable guide for identifying and mitigating the most critical security risks in web applications. Understanding these risks, their descriptions, and their potential business impact is essential for building secure applications and protecting sensitive data.