TASKS

Name: Shaz Alam Reg.no 21BCY10221

1. **Understanding CIS Policy version 7and write about them**

As of my last knowledge update in September 2021, the Center for Internet Security (CIS) had released version 7 of their Critical Security Controls (CSC), which is a set of best practices and guidelines for improving cybersecurity posture in organizations. Please note that there might have been updates or changes since then, so it's essential to consult the latest documentation for the most accurate information. However, I can provide you with an overview of the key principles and objectives of CIS Policy version 7 based on the information available at that time:

Inventory and Control of Enterprise Assets: This control emphasizes the importance of having a comprehensive inventory of all assets within an organization's network, including hardware, software, and data. The goal is to understand what you have, where it's located, and its importance to security.

Continuous Vulnerability Management: This control focuses on continuously identifying, assessing, and mitigating vulnerabilities in your systems and applications. It includes practices such as regular vulnerability scanning and patch management.

Secure Configuration for Enterprise Assets: Organizations are encouraged to establish and maintain secure configurations for their assets, which involves hardening operating systems, applications, and network devices to reduce security risks.

Controlled Use of Administrative Privileges: This control promotes the principle of least privilege (PoLP), which means granting users and processes only the minimum level of access required to perform their tasks. It helps reduce the risk of unauthorized access and privilege escalation.

Secure Software Development Lifecycle (SDLC): This control guides organizations in integrating security into their software development processes from the initial design phases through coding, testing, and deployment to mitigate software-related vulnerabilities.

Maintenance, Monitoring, and Analysis of Audit Logs: Effective logging and log analysis are crucial for detecting and responding to security incidents. This control encourages organizations to maintain detailed logs and regularly review them for suspicious activities.

Email and Web Browser Protections: To defend against phishing and malware attacks, this control suggests implementing email and web browser protections, such as email filtering and browser security settings, to reduce the attack surface.

Malware Defenses: Organizations are advised to implement comprehensive malware protection measures, including antivirus software, malware scanning, and user education, to detect and mitigate malware threats.

Limitation and Control of Network Ports, Protocols, and Services: Reducing the number of open network ports and services minimizes the attack surface. This control helps organizations identify and restrict unnecessary network services.

Data Recovery Capabilities: This control addresses the need for effective data backup and recovery procedures to ensure business continuity in the event of data loss or system failures.

Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches: Properly configuring network devices and monitoring their settings is essential for network security. This control provides guidelines for securing network infrastructure.

Boundary Defense: Establishing a strong perimeter defense is crucial to protect against external threats. This control covers measures such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Data Protection: Organizations should implement data protection measures, including encryption and access controls, to safeguard sensitive information from unauthorized access or disclosure.

Controlled Access Based on the Need to Know: Following the principle of least privilege, this control emphasizes restricting access to sensitive information only to individuals who require it to perform their job functions.

Wireless Access Control: This control focuses on securing wireless networks and devices to prevent unauthorized access and eavesdropping.

Account Monitoring and Control: Monitoring user accounts for suspicious activity and promptly disabling or revoking access when necessary helps prevent unauthorized access.

Security Skills Assessment and Appropriate Training to Fill Gaps: Organizations should assess their staff's security skills and provide training to bridge any knowledge gaps, ensuring they can effectively protect against cyber threats.

Incident Response and Management: Establishing an incident response plan and team is essential for effectively responding to security incidents and minimizing their impact.

Secure Network Engineering: This control guides organizations in designing and implementing secure network architecture to protect against network-based attacks.

Penetration Testing and Red Team Exercises: Regularly testing your organization's security controls through penetration testing and red team exercises helps identify vulnerabilities and weaknesses before malicious actors can exploit them.

These 20 CIS Critical Security Controls provide a framework for organizations to enhance their cybersecurity posture and defend against a wide range of threats. It's important to adapt these controls to the specific needs and risk profile of your organization and to stay updated with the latest developments and versions of CIS policies for the most effective security measures.

2. Explain any 10 Web Server Attacks determine them using images if

available

Certainly, I can explain ten common web server attacks, but please note that I cannot provide images as my current text-based interface does not support image display. However, I can describe these attacks in detail:

SQL Injection (SQLi):

SQL Injection is an attack where an attacker injects malicious SQL queries into input fields or parameters on a website. If the website does not properly validate or sanitize user inputs, the attacker can manipulate the database, potentially gaining unauthorized access to sensitive data.

Cross-Site Scripting (XSS):

Cross-Site Scripting is an attack in which an attacker injects malicious scripts (usually JavaScript) into web pages viewed by other users. These scripts can steal session cookies, redirect users to malicious websites, or deface web pages.

Cross-Site Request Forgery (CSRF):

CSRF attacks trick a user into performing unwanted actions without their knowledge or consent. The attacker sends a request from the user's browser to perform actions on a different site where the user is authenticated.

Brute Force Attack:

In a brute force attack, an attacker tries multiple combinations of usernames and passwords until they find the correct credentials to gain unauthorized access to a web server.

Directory Traversal Attack:

Directory Traversal attacks exploit vulnerabilities in the web server's file handling. Attackers use "../" or other techniques to navigate outside the intended directory, potentially accessing sensitive files or directories.

DDoS (Distributed Denial of Service):

DDoS attacks flood a web server with a high volume of traffic or requests, overwhelming its capacity and making it unavailable to legitimate users. These attacks can be carried out by a network of compromised computers (botnets).

Server-Side Request Forgery (SSRF):

SSRF attacks manipulate a web server into making requests to internal or external resources, potentially revealing sensitive information or facilitating further attacks.

File Inclusion Vulnerabilities:

File inclusion vulnerabilities occur when a web application allows users to include files from the server's file system. Attackers can exploit this to execute malicious code or access sensitive files.

XML External Entity (XXE) Attack:

XXE attacks exploit vulnerabilities in XML parsers to disclose internal files or carry out denial-of-service attacks on a web server by injecting malicious XML content.

Remote File Execution (RCE):

RCE attacks target vulnerabilities that allow an attacker to execute arbitrary code on the web server. This can lead to complete compromise of the server, potentially granting unauthorized access and control.

To protect against these web server attacks, it's crucial to implement strong security measures, including input validation, parameterized queries, proper access controls, regular security patching, and the use of web application firewalls (WAFs). Security professionals should also stay informed about the latest threats and vulnerabilities to proactively defend against emerging attack techniques.

3. Top 10 Notorious Hackers in the World Summary and which

The category of hackers comes under

The term "hacker" can encompass a wide range of individuals with varying motivations and ethical stances. Some hackers use their skills for malicious purposes, while others work to improve cybersecurity and protect systems. Here's a summary of ten individuals who gained notoriety in the hacking world, along with the categories of hackers they fall under:

Kevin Mitnick (Black Hat):

Kevin Mitnick is one of the most famous black hat hackers turned cybersecurity consultant. He was convicted of multiple computer-related crimes, including hacking into major corporations. After serving prison time, he became an advocate for ethical hacking and cybersecurity.

Adrian Lamo (Gray Hat):

Adrian Lamo was known for ethical hacking as well as controversial actions. He reported Chelsea Manning to authorities for leaking classified documents, leading to Manning's arrest. Lamo's actions straddle the line between ethical and controversial hacking.

Gary McKinnon (Gray Hat):

Gary McKinnon, a British hacker, infiltrated U.S. government computers in search of evidence of UFOs and free energy technology. His actions were illegal but driven by personal curiosity rather than malicious intent.

Julian Assange (Gray Hat):

Julian Assange founded WikiLeaks, an organization that publishes classified and confidential information. While some see him as a whistleblower advocate, others view his actions as hacking and publishing sensitive information illegally.

Albert Gonzalez (Black Hat):

Albert Gonzalez was a prolific black hat hacker responsible for large-scale credit card data thefts. He orchestrated major data breaches against multiple companies and was sentenced to prison for his cybercrimes.

Anonymous (Gray Hat):

Anonymous is a loosely organized collective of hackers and activists known for their hacktivist activities. They have targeted various organizations and governments, often advocating for causes related to free speech and government transparency.

LulzSec (Black Hat):

LulzSec, short for "Lulz Security," was a hacking group known for high-profile cyberattacks on organizations such as Sony, PBS, and Nintendo. Their actions were often driven by a desire for notoriety and amusement.

Kevin Poulsen (Gray Hat):

Kevin Poulsen, also known as "Dark Dante," was a hacker who gained notoriety for hacking into phone systems and winning a Porsche in a radio contest by manipulating phone lines. He later became a journalist and cybersecurity advocate.

Robert Tappan Morris (Gray Hat):

Robert Tappan Morris is best known for creating the Morris Worm, one of the first computer worms to spread widely across the internet. His actions were unauthorized and led to the development of early cybersecurity practices.

Jeanson James Ancheta (Black Hat):

Jeanson James Ancheta was responsible for creating a botnet that infected a large number of computers, which he then used for various cybercrimes, including distributed denial of service (DDoS) attacks.

It's important to note that hacking can fall into various categories, including black hat (malicious), white hat (ethical), and gray hat (ambiguous or with mixed motives). Some hackers may transition between these categories over time or based on their activities. Ethical hackers, also known as white hat hackers, wrk to improve cybersecurity and protect systems from vulnerabilities and threats.

4.:Top 5 OWASP CWE description with Business Impact

The Open Web Application Security Project (OWASP) and Common Weakness Enumeration (CWE) are two different but related frameworks for identifying and mitigating software security vulnerabilities. Below are descriptions of five common OWASP vulnerabilities along with their business impact:

Injection (OWASP Top 10 #1):

Description: Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query. This allows attackers to manipulate the interpreter and execute malicious commands or access unauthorized data.

Business Impact: Injection vulnerabilities can lead to data breaches, unauthorized access, data manipulation, and service disruption. These can result in loss of customer trust, regulatory penalties, and legal repercussions.

Broken Authentication (OWASP Top 10 #2):

Description: Broken authentication vulnerabilities occur when an application's authentication and session management mechanisms are not secure. Attackers can exploit these weaknesses to impersonate users or gain unauthorized access to sensitive data or functionality.

Business Impact: Broken authentication can lead to unauthorized access, data breaches, and identity theft. It can result in compromised user accounts, reputation damage, and regulatory fines.

Sensitive Data Exposure (OWASP Top 10 #3):

Description: Sensitive Data Exposure vulnerabilities occur when an application fails to adequately protect sensitive information such as passwords, credit card numbers, or personal data. Attackers can exploit these vulnerabilities to steal sensitive data.

Business Impact: Sensitive data exposure can result in financial losses due to data breaches, legal consequences, loss of customer trust, and reputational damage.

Security Misconfiguration (OWASP Top 10 #5):

Description: Security misconfigurations happen when an application or its components are not securely configured. This can include open ports, default credentials, or excessive permissions, making it easier for attackers to exploit vulnerabilities.

Business Impact: Security misconfigurations can lead to unauthorized access, data leaks, service disruptions, and breaches. It can also result in compliance violations, financial losses, and damage to an organization's reputation.

Cross-Site Scripting (XSS) (OWASP Top 10 #7):

Description: Cross-Site Scripting vulnerabilities occur when an application includes untrusted data in a web page, allowing attackers to execute malicious scripts in the context of a user's browser. This can lead to session hijacking, defacement, and data theft.

Business Impact: XSS attacks can result in compromised user accounts, theft of sensitive data (e.g., cookies, session tokens), and defacement of websites. This can harm user trust, damage brand reputation, and lead to legal liabilities.

Addressing these OWASP vulnerabilities is crucial for businesses to protect their applications and data. Implementing robust security practices, regularly testing for vulnerabilities, and promptly addressing issues can help mitigate these risks and minimize their business impact.

5. Understanding any Top 10 web applications Vulnerabilities (other than Top 10 OWASP) write a paragraph about that and add an image to the respective vulnerability

XML External Entity (XXE) Injection:

XXE vulnerabilities occur when an application processes XML input insecurely. Attackers can exploit this to read internal files, perform denial-of-service attacks, or execute arbitrary code. Proper input validation and disabling external entity references can help mitigate this risk.

Server-Side Template Injection (SSTI):

SSTI vulnerabilities arise when user-controlled data is directly embedded into server-side templates. Attackers can manipulate templates to execute arbitrary code. Developers should validate and sanitize user input and use templates carefully.

Insecure Deserialization:

Insecure deserialization vulnerabilities occur when an application fails to validate or sanitize serialized data. Attackers can exploit this to execute code or perform denial-of-service attacks. Safe deserialization practices and input validation are essential to mitigate this risk.

Server-Side Request Forgery (SSRF):

SSRF vulnerabilities enable attackers to make requests from the web server to internal or external resources. This can lead to data exposure, internal network scanning, or remote code execution. Proper input validation and network filtering are essential for defense.

XML Injection (XQuery Injection):

XML injection vulnerabilities involve attackers manipulating XML queries to access or modify data. This can lead to data exposure or unauthorized data changes. Strong input validation and encoding are necessary to prevent this type of attack.

Content Security Policy (CSP) Bypass:

CSP bypass vulnerabilities allow attackers to execute malicious scripts by evading CSP rules. A well-configured CSP can mitigate these risks, but misconfigurations can lead to bypasses and script execution.

HTTP Header Injection:

HTTP header injection vulnerabilities occur when attackers manipulate HTTP headers to inject malicious content. This can lead to response splitting, cross-site scripting (XSS), or other attacks. Proper encoding and validation of user input in headers are crucial.

CORS (Cross-Origin Resource Sharing) Misconfiguration:

CORS misconfigurations allow unauthorized websites to access restricted resources. Attackers can exploit this to steal sensitive data. Proper CORS configuration is essential to prevent data leaks.

Path Traversal (Directory Traversal):

Path traversal vulnerabilities occur when attackers manipulate file paths to access unauthorized directories or files. This can lead to data exposure or remote code execution. Input validation and secure file access mechanisms are critical.

API Security Flaws:

API security flaws encompass various vulnerabilities, such as insecure authentication, excessive data exposure, or lack of proper authorization. Securing APIs through strong authentication, access controls, and encryption is vital to prevent data breaches.

For visual representations or examples of these vulnerabilities, I recommend consulting trusted resources and security documentation that include relevant diagrams and illustrations.