TASKS

Task 1

Top 10 hackers in the world?

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.

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 allblack 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.

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.

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."

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.

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.

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 numberone 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.

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 sociopolitical 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 opensource 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.

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."

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-yearold 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'.

Task2

Determine the vulnerabilities in the open ports Port nos(20,21,22,23,25,53,69,80,110,123,143,443)

Port 20 and 21 (FTP):
Vulnerabilities: Weak FTP passwords, anonymous access, FTP bounce attacks.
Mitigation: Use strong passwords, limit anonymous access, consider using SFTP or FTPS for encrypted transfers.

Port 22 (SSH):
Vulnerabilities: Weak SSH passwords, brute force attacks, outdated SSH versions. Mitigation: Use strong SSH keys or passwords, disable root login, keep SSH software up to date.

Port 23 (Telnet):
Vulnerabilities: Unencrypted communication, plaintext credentials.
Mitigation: Avoid using Telnet, use SSH instead for secure remote access.

Port 25 (SMTP):
Vulnerabilities: Open relay, email spoofing, email flooding.
Mitigation: Configure SMTP servers to prevent open relay, use SPF, DKIM, and DMARC for email authentication.

Port 53 (DNS):
Vulnerabilities: DNS cache poisoning, DNS amplification attacks.
Mitigation: Keep DNS software updated, implement DNSSEC for authentication, restrict access to DNS servers.

Port 69 (TFTP):
Vulnerabilities: No authentication, lack of security features.
Mitigation: Avoid using TFTP if possible, implement access controls and encryption.

Port 80 (HTTP):
Vulnerabilities: Web application vulnerabilities, SQL injection, cross-site scripting (XSS), outdated software.
Mitigation: Regularly update web applications and server software, implement security best practices, use a Web Application Firewall (WAF).

Port 110 (POP3):
Vulnerabilities: Weak POP3 passwords, plaintext communication.
Mitigation: Use strong passwords, consider using POP3S with SSL/TLS for encrypted communication.

Port 123 (NTP):
Vulnerabilities: NTP amplification attacks, vulnerable NTP server software.
Mitigation: Keep NTP software updated, configure access controls to prevent misuse

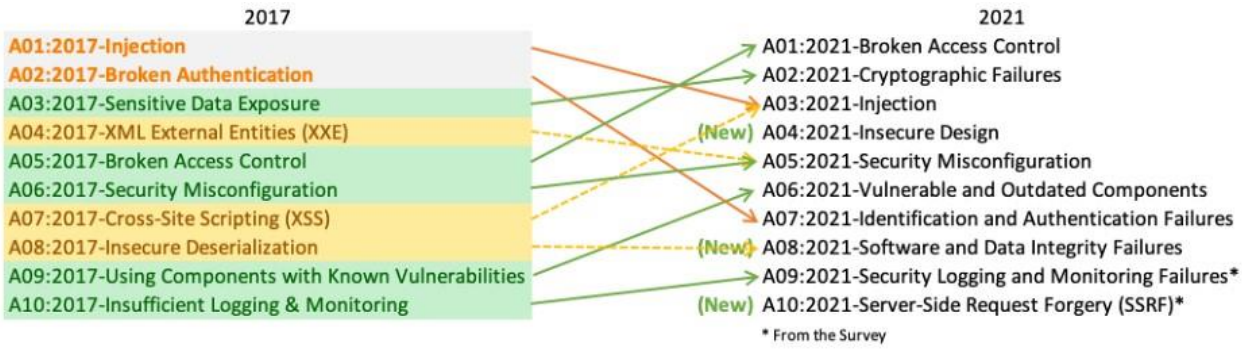
Port 143 (IMAP):
Vulnerabilities: Weak IMAP passwords, plaintext communication.
Mitigation: Use strong passwords, consider using IMAPS with SSL/TLS for encrypted communication.

Port 443 (HTTPS):
Vulnerabilities: SSL/TLS vulnerabilities, certificate issues.
Mitigation: Keep SSL/TLS libraries up to date, use reputable SSL certificates, implement secure SSL/TLS configurations.

Task3

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Crosssite Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

Task4

A web application attack refers to a malicious attempt to exploit vulnerabilities in a web application's security. These attacks can compromise the confidentiality, integrity, or availability of the application's data or functionality. As an ethical hacker, I can provide you with information about various types of web application attacks:

1. **SQL Injection (SQLi):** In this attack, malicious SQL queries are injected into input fields of a web application to manipulate its database. This can lead to unauthorized access, data leakage, or even the complete compromise of the database.

2. **Cross-Site Scripting (XSS):** XSS involves injecting malicious scripts into web pages viewed by other users. When these scripts execute in other users' browsers, attackers can steal information, perform actions on behalf of the victim, or spread malware.

3. **Cross-Site Request Forgery (CSRF):** In CSRF attacks, a user is tricked into performing an unintended action without their knowledge. This can lead to actions being performed on their behalf, such as changing account settings or making unauthorized transactions.

4. **Cross-Site Script Inclusion (XSSI):** Similar to XSS, XSSI involves injecting malicious scripts into web pages. However, in this case, the attacker aims to manipulate the behavior of other scripts running on the page rather than targeting the users' browsers.

5. **Session Hijacking/Session Fixation:** Attackers steal or manipulate session identifiers to gain unauthorized access to user accounts. This can allow them to impersonate legitimate users and perform actions on their behalf.

6. **Directory Traversal/Path Traversal:** This attack exploits improperly sanitized input to access files and directories that the application shouldn't allow. Attackers can use this to view sensitive files or execute malicious code.

7. **Server-Side Request Forgery (SSRF):** Attackers manipulate a web application to make requests to other internal or external systems, often leading to unauthorized data exposure or even remote code execution.

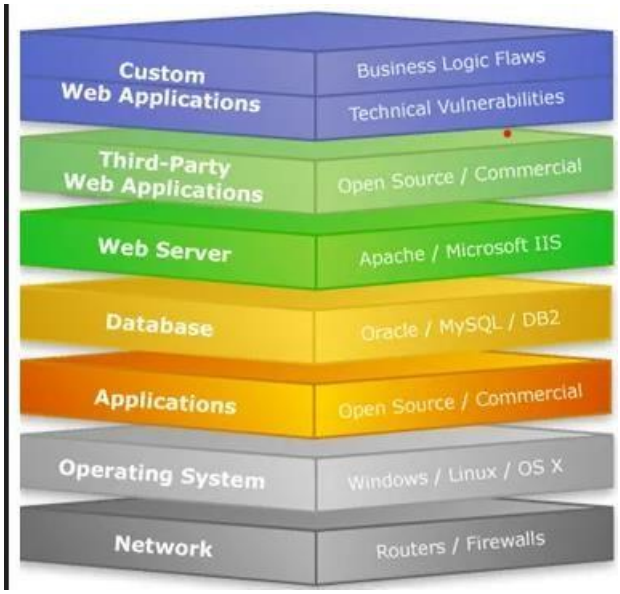
8. **File Upload Vulnerabilities:** Insecure file upload mechanisms can allow attackers to upload malicious files, leading to code execution or unauthorized access.

9. **Remote Code Execution (RCE):** If an attacker can execute code on a web server, they may be able to take control of the server and potentially compromise the entire system.

10. **Brute Force Attacks:** Attackers attempt to guess usernames and passwords through automated trial-and-error methods, exploiting weak credentials.

Task5

Web server attacks:



1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OF-SERVICE (DDOS): Denial of Service is when an internet hacker causes the web to provide a response to a large number of requests. This causes the server to slow down or crash and users authorized to use the server will be denied service or access. Government services, credit card companies under large corporations are common victims of this type of attack

2. WEB DEFACEMENT ATTACK: 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 vulnerabilities

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.

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.

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.

7. MITM ATTACK: 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.

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.

How to Prevent Different Attacks in Web Security?

- Keep your system up to date: Not updating the software regularly makes it weaker and leaves the system more vulnerable to attacks. Hackers take advantage of these flaws, and cybercriminals take advantage of them to get access to your network.
- Prevent connecting to the public WiFi network: An unsecured Wi-Fi connection can be used by hackers to spread malware. If you allow file-sharing across a network, a hacker can simply infect your computer with tainted software. The ability of a hacker to put himself between you and the connection point poses the greatest threat to free Wi-Fi security.
- Install Anti-virus, and update it regularly: Antivirus software is designed to identify, block, and respond to dangerous software, such as viruses, on your computer. Because computers are continuously threatened by new viruses, it is critical to keep antivirus software up to date. Anti-virus updates include the most recent files required to combat new threats and safeguard your machine. These signature files are provided on a daily basis, if not more frequently.
- Use IDS and firewall with updated signatures: NIDS are security threat detection and prevention systems that identify and prevent security threats from infiltrating secure networks. The use of NIDS has a negligible effect on network performance. NIDS are typically passive devices that listen to a network without interfering with the network's normal operation.
- Backup your data: The fundamental purpose of a data backup is to keep a safe archive of your vital information, whether it's classified documents for your business or priceless family photos so that you can quickly and effortlessly recover your device in the event of data loss. Backup copies allow data to be restored from a previous point in time, which can aid in the recovery of a business after an unanticipated occurrence. Protecting against primary data loss or corruption requires storing a copy of the data on a secondary medium.
- Install a Firewall: Firewalls defend your computer or network from outside cyber attackers by filtering out dangerous or superfluous network traffic. Firewalls can also prevent harmful malware from gaining internet access to a machine or network.

Task6:

Understanding CIS Policy version 7and write about them

The CIS Controls version 7 is a set of 18 cybersecurity controls that are designed to help organizations of all sizes mitigate the most common cyber threats. The controls are developed by the Center for Internet Security (CIS), a non-profit organization that is dedicated to promoting cybersecurity best practices.

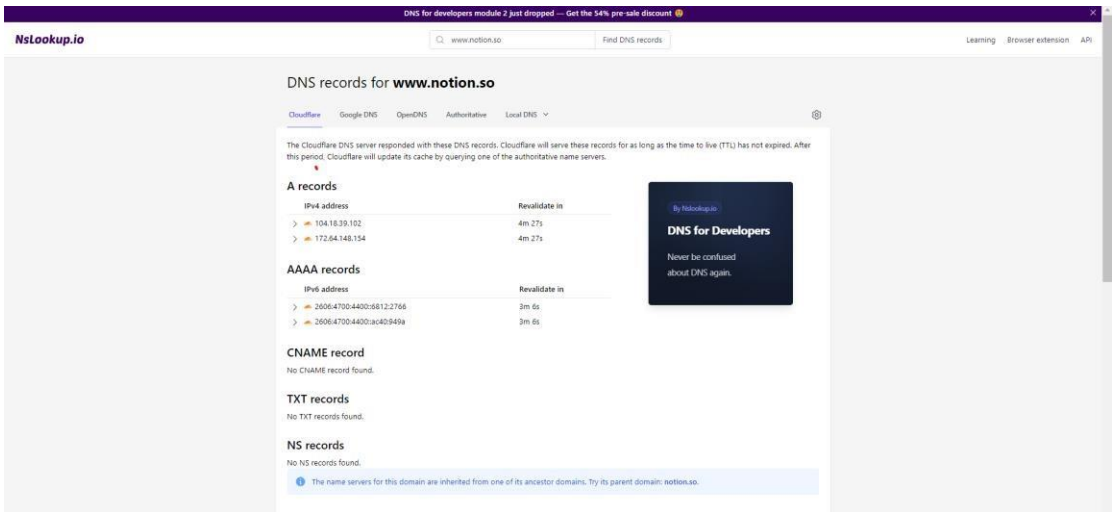
The CIS Controls are divided into three categories:

Basic: These controls are essential for all organizations, regardless of size or industry.
Foundational: These controls build on the basic controls and provide additional protection against more sophisticated cyber threats.
Organizational: These controls are tailored to the specific needs of an organization, such as its size, industry, and risk tolerance.
The CIS Controls are organized into the following 18 categories:

Inventory and Control of Hardware Assets
Inventory and Control of Software Assets
Secure Configuration of Systems
Continuous Vulnerability Management
Controlled Use of Administrative Privileges
Maintenance, Monitoring, and Analysis of Audit Logs
Email and Web Browser Protections
Malware Defenses 9. Limited and Controlled Access to Networks and Data
Data Loss Prevention
Secure Network Architecture
Boundary Defense
Intrusion Detection and Prevention Systems
Wireless Access Control
Mobile Device Management
Incident Response
Application Development Security
Security Awareness and Training
The CIS Controls are based on the principle of defense-in-depth, which means that multiple layers of security controls are implemented to protect against cyber threats. The controls are also designed to be scalable, so that they can be implemented by organizations of all sizes.

The CIS Controls are widely adopted by organizations around the world, and they are considered to be one of the most effective cybersecurity frameworks available.

Task7



Task8

220.158.183.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	15	10	2	28

Vulnerabilities — Total: 57

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	133845	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	111069	Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilites
HIGH	8.6	4.7	161159	Apache Tomcat 9.0.0.M1 < 9.0.21 vulnerability
HIGH	8.1	9.2	103699	Apache Tomcat 9.0.0.M1 < 9.0.1 Multiple Vulnerabilities
HIGH	7.5	3.6	121124	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	4.4	166906	Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability
HIGH	7.5	4.4	176310	Apache Tomcat 9.0.0.M1 < 9.0.10 multiple vulnerabilities
HIGH	7.5	6.7	126312	Apache Tomcat 9.0.0.M1 < 9.0.16 DoS
HIGH	7.5	6.7	126245	Apache Tomcat 9.0.0.M1 < 9.0.20 DoS
HIGH	7.5	6.7	132419	Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability
HIGH	7.5	4.4	138098	Apache Tomcat 9.0.0.M1 < 9.0.36 DoS
HIGH	7.5	5.1	138591	Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities
HIGH	7.5	8.4	147164	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities
HIGH	7.5	4.4	171657	Apache Tomcat 9.0.0.M1 < 9.0.71
HIGH	7.5	3.6	122447	Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability
HIGH	7.5	5.1	144050	Apache Tomcat 9.x < 9.0.40 Information Disclosure
HIGH	7.0	8.4	136806	Apache Tomcat 9.0.0 < 9.0.35 Remote Code Execution

MEDIUM	6.5	4.2	151502	Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability
MEDIUM	6.5	4.4	106978	Apache Tomcat 9.0.0.M1 < 9.0.5 Insecure CGI Servlet Search Algorithm Description Weakness
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.1	3.8	180194	Apache Tomcat 9.0.0.M1 < 9.0.80
MEDIUM	5.3	1.4	152182	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	4.3	1.4	141446	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up
MEDIUM	4.3	2.2	118037	Apache Tomcat 9.0.0.M1 < 9.0.12 Open Redirect Weakness
MEDIUM	4.3	2.2	173251	Apache Tomcat 9.0.0.M1 < 9.0.72
LOW	3.7	2.2	159464	Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations
LOW	3.7	1.4	106713	Apache Tomcat 9.0.0.M22 < 9.0.2 Insecure CGI Servlet Search Algorithm Description Weakness
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	66334	Patch Report
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown