Stage: 2 Report

NESSUS Vulnerability Report

Overview

Performing a vulnerability assessment for a college website is crucial to identify and address potential security weaknesses that could be exploited by attackers. Security is an ongoing process, and continuous monitoring and improvement are essential to maintain a robust defense against potential threats. Additionally, if you lack the expertise to conduct a thorough assessment, it is wise to seek assistance from qualified cybersecurity professionals. Verify that the website is secure and displays correctly on various devices and browsers. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process. Document all identified vulnerabilities, along with their severity and potential impact. Prioritize fixes based on criticality and help the college's IT team or web developers with the remediation process.

Nessus is a popular vulnerability assessment tool that is widely used by cybersecurity professionals and organizations to identify and address security weaknesses in their networks, systems, and applications. Here are some of the key uses of Nessus:

Vulnerability Scanning: Nessus is primarily used for automated vulnerability scanning. It scans networks, servers, endpoints, and applications to detect known vulnerabilities and misconfigurations. This helps organizations identify potential entry points for attackers and prioritize their security efforts.

Patch Management: The scan results generated by Nessus provide information about missing patches and updates for various software and operating systems. This assists in maintaining an up-to-date and secure IT environment by ensuring that critical security patches are applied promptly.

Compliance Auditing: Nessus can be used to assess whether an organization's systems and configurations comply with industry standards and regulatory requirements, such as PCI DSS, HIPAA, NIST, CIS, and more. It helps organizations identify gaps and achieve compliance with security best practices.

Web Application Scanning: Nessus can scan web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), and other issues that may expose web applications to potential attacks.

Network Inventory and Asset Management: Nessus can provide valuable information about the devices and systems connected to the network, assisting in maintaining an up-to-date inventory and understanding the network's attack surface.

Security Awareness and Training: By generating detailed vulnerability reports, Nessus helps security teams and IT personnel gain insights into the security posture of their systems. This information can be used to improve security awareness and training programs.

Risk Assessment: Nessus assigns severity levels to identified vulnerabilities, helping organizations prioritize their efforts by focusing on high-risk vulnerabilities first.

Penetration Testing Support: Nessus can complement manual penetration testing efforts by providing an initial overview of potential vulnerabilities before more extensive manual testing is conducted.

Cloud Infrastructure Security: Many organizations are now using cloud infrastructure. Nessus can assess cloud environments and identify misconfigurations or vulnerabilities that might affect the security of cloud-based resources.

Continuous Monitoring: Nessus can be used to implement continuous monitoring strategies, enabling organizations to regularly assess their security posture and detect changes that may introduce new vulnerabilities.

Threat Intelligence Integration: Nessus can be integrated with threat intelligence feeds to cross-reference scan results with known exploits and threats, providing a more comprehensive view of potential risks. Nessus is an excellent tool for identifying known vulnerabilities and misconfigurations, it should be part of a comprehensive security strategy that includes regular manual assessments, threat hunting, and ongoing security awareness efforts to address emerging and zero-day threats.

Target Website: Vignan's Foundation for

Science Technology & Research website :

www.vignan.ac.in Target IP :

180.179.213.196

Here are some of the Initial screenshot of Nessus doing the vulnerability scanning of IP address 180.179.213.196

Figure 1: DNS Records for the Website

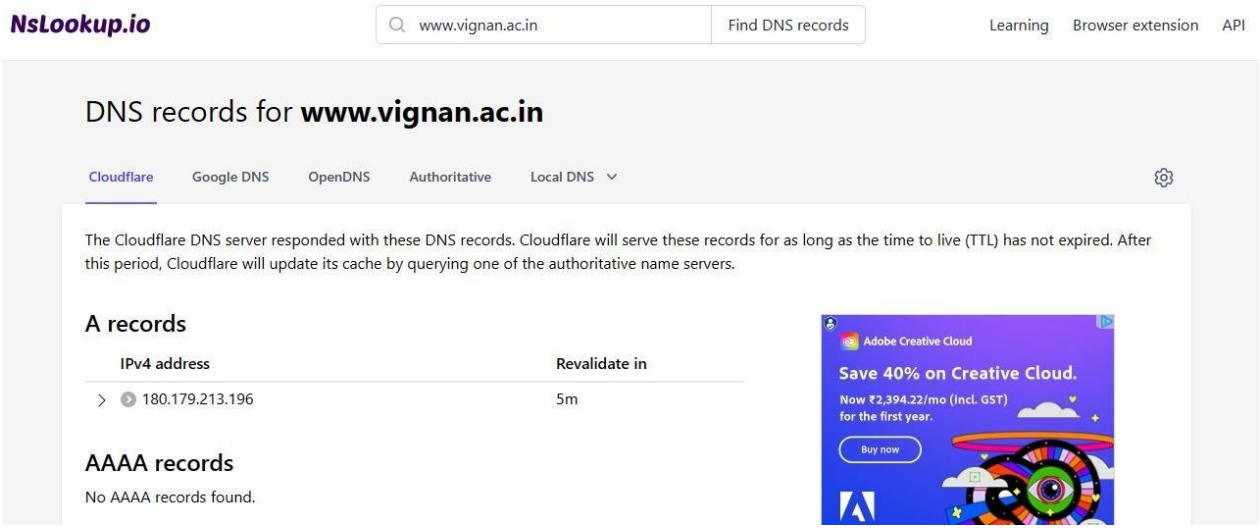
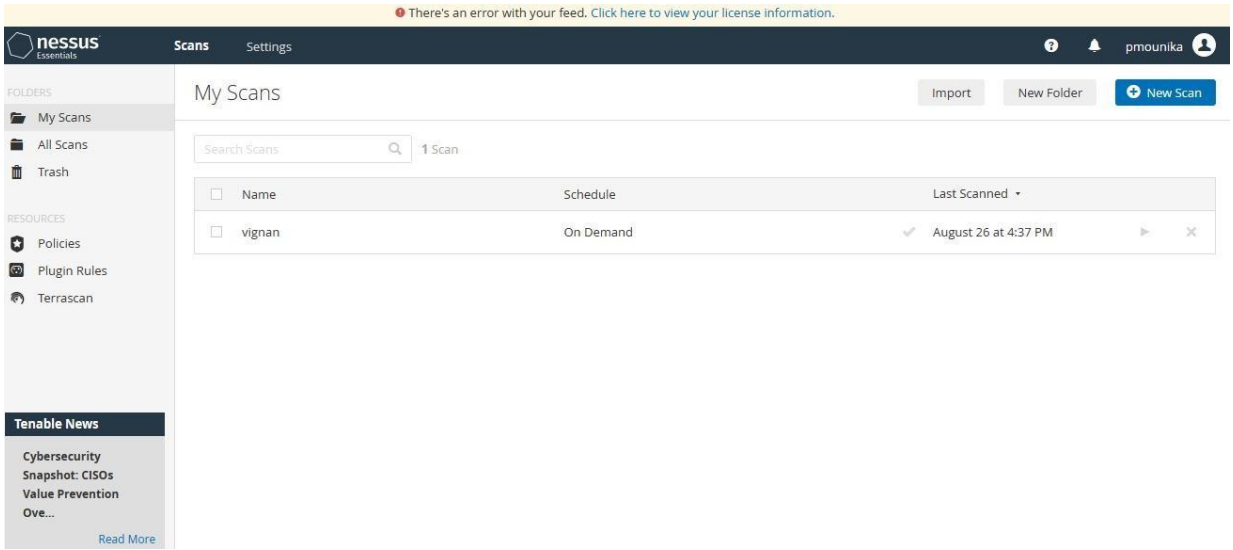


Figure 2: Home page of the Nessus vulnerability scanning.



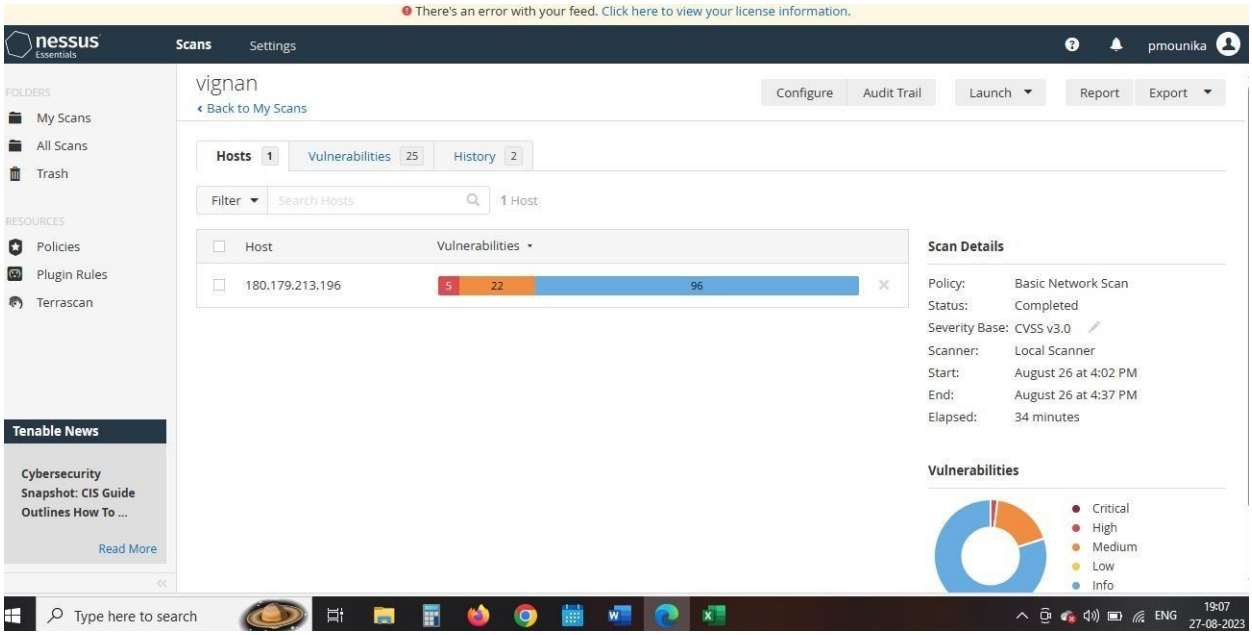


Figure 3: It show Nessus vulnerability scanning details like policy, status, etc.

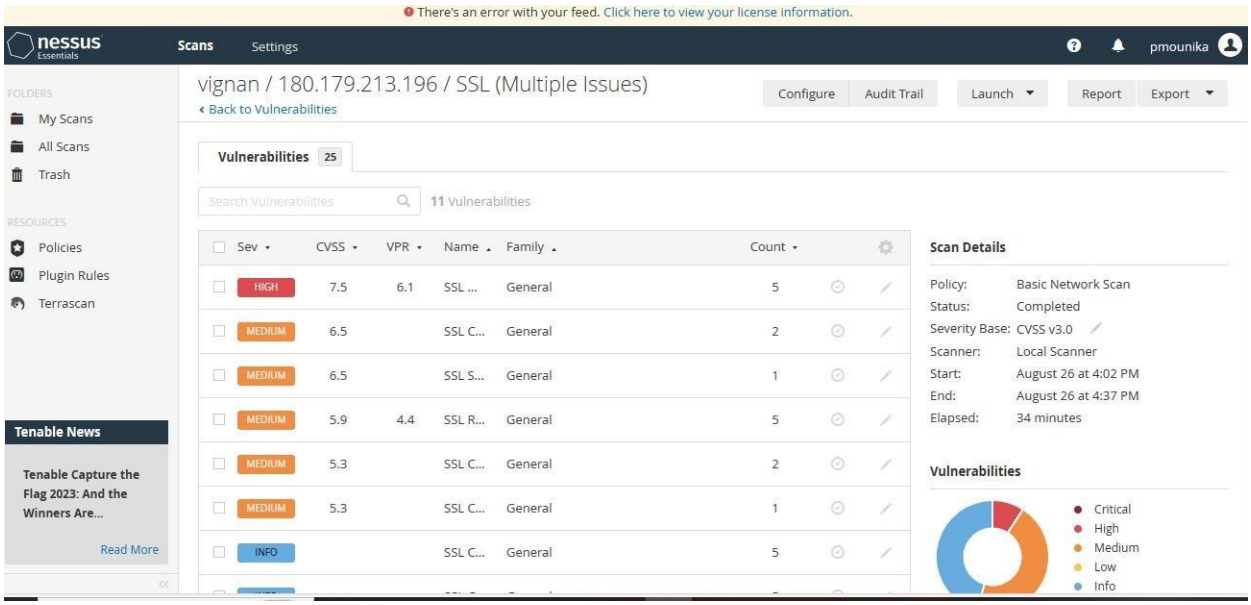


Figure 4: It show number of vulnerability and types.

S.No	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port

1	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	42873	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	The presence of SSL medium strength cipher suites such as SWEET32 in a business's security infrastructure can have significant repercussions. Positively, addressing these vulnerabilities enhances data protection and compliance with security standards, bolstering customer trust. However, the negative impact lies in the potential security breaches and data compromises that these weak cipher suites can invite, potentially leading to data breaches, regulatory non-compliance, financial losses, and reputational damage. Thus, mitigating SSL medium strength cipher suites is imperative for sustaining a secure operational environment and safeguarding the business's interests.	143, 993,8443,990, 995
2	SSL Certificate Cannot Be Trusted	Medium	51192	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when	Purchase or generate a proper SSL certificate for this service.	The occurrence of an "SSL certificate cannot be trusted" message when users attempt to access a business's website can have critical implications. On the positive side, addressing this issue promptly can bolster cybersecurity, ensuring encrypted and authenticated connections, thereby enhancing customer trust and data confidentiality. However, the negative impact involves potential loss of credibility as users may refrain from sharing sensitive information due to security concerns, resulting in reduced website traffic, lower conversion rates, and damage to the brand's reputation. Therefore, rectifying the SSL certificate trust problem is crucial for maintaining a secure online presence and fostering user confidence in the business's digital offerings.	990, 8443

				intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. *- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.* *- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's*			

				issuer using a signing algorithm that Nessus either does not support or does not recognize. *If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.*			
3	*SSL Self-Signed Certificate*	*Medium*	*57582*	*The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.* *Note that this plugin does not check for certificate chains that end in a certificate that is not self-*	*Purchase or generate a proper SSL certificate for this service.*	*SSL Self-Signed Certificate*	*990*

				signed, but is signed by an unrecognized certificate authority.			
4	*SSL RC4 Cipher Suites Supported (Bar Mitzvah)*	*Medium*	*65821*	*The remote host supports the use of RC4 in one or more cipher suites.* *The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.* *If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.*	*Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.*	*The presence of SSL RC4 cipher suites, particularly those vulnerable to attacks like Bar Mitzvah, can have significant consequences for businesses. On one hand, promptly addressing these vulnerabilities can enhance the security posture, ensuring safe and encrypted communication, and preserving customer trust. On the other hand, failing to mitigate these vulnerabilities can expose sensitive data to potential breaches, leading to compromised customer information, regulatory non-compliance, financial losses, and reputational harm. Therefore, taking decisive action to eliminate SSL RC4 cipher suite vulnerabilities is essential for maintaining robust cybersecurity, safeguarding customer interests, and preserving the business's reputation.*	*143, 993, 8443, 990, 995*

5	SSL Certificate Expiry	Medium	15901	This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.	Purchase or generate a new SSL certificate to replace the existing one.	The expiry of an SSL certificate can have substantial implications for businesses. On a positive note, renewing certificates in a timely manner ensures the continuation of secure encrypted connections, maintaining customer trust and data protection. Conversely, the negative impact includes potential disruptions to website functionality, customer transactions, and communication due to browsers displaying security warnings. This can result in decreased website traffic, abandoned transactions, damaged reputation, and potential financial losses. Thus, actively managing SSL certificate expiration is vital for sustaining smooth online operations, preserving user confidence, and upholding the business's digital integrity.	990, 8443
6	SSL Certificate with Wrong Hostname	Medium	45411	The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.	Purchase or generate a proper SSL certificate for this service.	The presence of an SSL certificate with a wrong hostname can have significant ramifications for businesses. Correcting this issue promptly is essential for maintaining security and ensuring encrypted, authenticated connections, thereby fostering customer trust and data confidentiality. However, the negative impact includes potential security vulnerabilities, as users may become targets of phishing attacks or fraudulent websites due to the mismatched hostname. This can lead to compromised customer data, financial losses, tarnished reputation, and potential legal liabilities. Hence, addressing	990

						SSL certificates with incorrect hostnames is crucial for upholding cybersecurity, safeguarding user interests, and preserving the business's reputation and bottom line.	
7	*TLS Version 1.0 Protocol Detection*	*Medium*	*1E+05*	*The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.* *As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.* *PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which*	*Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.*	*Detecting the use of TLS version 1.0 protocol in a business's network can have several implications. Positively, identifying and addressing this outdated and insecure protocol can enhance the organization's overall security posture, protecting sensitive data and ensuring compliance with modern security standards. However, the negative impact involves potential vulnerabilities, as TLS 1.0 is susceptible to various attacks. Continued usage can lead to data breaches, unauthorized access, compromised customer information, regulatory non-compliance, reputational damage, and even legal consequences. Thus, swiftly discontinuing the use of TLS 1.0 is crucial for maintaining robust cybersecurity, preserving customer trust, and safeguarding the business's interests.*	*143, 993, 8443, 990, 995*

				they connect) that can be verified as not being susceptible to any known exploits.			
8	*TLS Version 1.1 Protocol Deprecated*	*Medium*	*2E+05*	*The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS*	*Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.*	*The deprecation of the TLS 1.1 protocol can yield enhanced security and regulatory compliance for businesses by moving to more secure protocols; however, it might also lead to compatibility issues, operational disruptions, and development efforts as outdated systems and devices struggle to adapt to the change, potentially impacting user experience and necessitating careful migration planning.*	*143, 993, 8443, 990, 995*

				1.1 *As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.*			
9	*TLS Version 1.1 Protocol Detection*	*Info*	*1E+05*	*The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1* *As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.*	*Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.*	*Detecting the continued use of the deprecated TLS 1.1 protocol within a business's network can trigger both positive and negative effects. On the positive side, such detection can facilitate proactive security measures by highlighting vulnerabilities that need immediate attention, enabling the organization to fortify its cybersecurity posture. Additionally, it aligns with regulatory requirements and industry standards, reducing the risk of compliance violations and associated penalties. However, this detection might also uncover compatibility challenges, as systems and applications reliant on TLS 1.1 could face disruptions. Mitigating these impacts necessitates careful planning for migration to more secure protocol versions, potentially incurring development costs and temporarily affecting user experience during the transition.*	*143, 993, 8443, 990, 995*

10	HSTS Missing From HTTPS Server (RFC 6797)	Medium	1E+05	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.	Configure the remote web server to use HSTS.	The absence of HTTP Strict Transport Security (HSTS) headers in an organization's HTTPS server can have notable business consequences. On the negative side, it exposes the business to increased security risks, as HSTS plays a crucial role in preventing protocol downgrade attacks and enhancing overall website security. Without HSTS, users could potentially be vulnerable to attacks like man-in-the-middle and cookie hijacking, damaging the business's reputation and eroding customer trust. Furthermore, the lack of HSTS implementation might lead to lower search engine rankings, impacting online visibility and potentially reducing website traffic. On the positive side, rectifying this issue by implementing HSTS headers can significantly enhance cybersecurity measures, boost user confidence in data protection, and improve the overall browsing experience, potentially translating into higher customer retention rates and a stronger online presence.	8443

11	HSTS Missing From HTTPS Server	Info	84502	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.	Configure the remote web server to use HSTS.	The absence of HTTP Strict Transport Security (HSTS) from an organization's HTTPS server could have several business impacts. It might result in heightened security risks, leaving the website and its users vulnerable to attacks like man-in-the-middle and protocol downgrade attacks. Such vulnerabilities could compromise sensitive user data, damage the company's reputation, and erode customer trust, potentially leading to financial losses and legal liabilities. Additionally, search engines might prioritize websites with HSTS enabled, affecting the website's visibility and potentially reducing organic web traffic. By implementing HSTS, the business can enhance its security posture, protect user data, maintain regulatory compliance, and bolster customer confidence, potentially leading to improved customer loyalty and online performance.	8443

12	SSL/TLS Recommended Cipher Suites	Info	2E+05	The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites: TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8	Only enable support for recommened cipher suites.	The selection of appropriate SSL/TLS cipher suites can significantly impact a business's security, performance, and user experience. Implementing recommended cipher suites can enhance data protection and privacy, reducing the risk of data breaches and cyberattacks. Strong cipher suites contribute to compliance with industry regulations and standards, avoiding potential legal consequences and financial penalties. Moreover, the right cipher suites can optimize website and application performance by ensuring efficient encryption and decryption processes. On the flip side, inadequate or outdated cipher suites can expose the business to vulnerabilities, potentially leading to data breaches, reputational damage, and financial losses. It might also result in compatibility issues with modern browsers and devices, hampering user experience and potentially causing customers to abandon the platform. Prioritizing recommended cipher suites aligns the business with security best practices, fosters trust among users, and safeguards the overall integrity of its digital operations.	993, 8443, 143, 995, 990

				ECDHE-RSA-CHACHA20-POLY1305 *- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256* *- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384* *This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.*			

13	SSL Root Certification Authority Certificate Information	Info	94761	The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.	Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.	The accuracy and proper management of SSL Root Certification Authority (CA) certificate information can have substantial business implications. Maintaining up-to-date and valid SSL root certificates is crucial for establishing trust with customers, partners, and users who rely on secure online communication. Failure to manage these certificates effectively can lead to security warnings, loss of user confidence, and potential disruptions in online transactions, which may result in decreased sales or engagement. Additionally, non-compliance with industry standards and browser requirements might lead to website inaccessibility or reduced search engine visibility, impacting online presence and revenue. Conversely, managing SSL root certificates properly ensures secure connections, mitigates security risks, and helps maintain regulatory compliance. By proactively staying informed about certificate expiration, renewals, and updates, businesses can prevent security breaches, uphold customer trust, and ensure the continuity of their digital services.	143, 993, 995, 8443

14	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Info	95631	The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.	Contact the Certificate Authority to have the certificate reissued.	Using SSL certificates signed with weak hashing algorithms from known Certificate Authorities (CAs) can have serious business repercussions. Such certificates are vulnerable to cryptographic attacks, potentially allowing malicious actors to intercept and manipulate sensitive data transmitted between users and the business's servers. This can lead to data breaches, compromised user information, and severe reputational damage, eroding customer trust and loyalty. Furthermore, browsers and security software might flag websites with weakly signed certificates as insecure, deterring users from accessing the platform and leading to reduced website traffic and conversion rates. Non-compliance with industry standards and security best practices can also result in legal liabilities and penalties. To mitigate these risks, businesses should prioritize obtaining SSL certificates signed with strong, secure hashing algorithms, ensuring robust data protection, maintaining user confidence, and upholding the integrity of their online operations.	8443

				Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates. *Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.*			

15	Nessus SYN scanner	Info	11219	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.	Protect your target with an IP filter.	Implementing the Nessus SYN scanner can yield positive outcomes for businesses by proactively identifying vulnerabilities in their network infrastructure, bolstering cybersecurity measures, and aiding compliance efforts. However, its usage requires careful planning to avoid potential negative impacts such as network disruptions, false positives, and resource overloads. When deployed effectively, the Nessus SYN scanner can enhance data protection, reduce the risk of breaches, and contribute to regulatory adherence, while cautious execution is necessary to mitigate operational disturbances.	21, 25, 80, 110, 143,443, 990, 993, 995, 2000, 5060, 8443

16	POP Server Detection	Info	10185	The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.	Disable this service if you do not use it.	Detecting the presence of a POP (Post Office Protocol) server within a business's network can have significant business implications. On the positive side, identifying a POP server can enable efficient email communication, benefiting internal communication, customer interactions, and business operations. It can also streamline email management, making it easier to organize and retrieve messages. However, the use of POP servers might pose security risks, as they often lack robust encryption and can expose sensitive information during transmission. Additionally, the lack of synchronization across devices can lead to data inconsistencies. Therefore, businesses should carefully consider the security implications and explore alternative email protocols like IMAP (Internet Message Access Protocol) that offer improved security and synchronization features to mitigate potential risks associated with POP server usage.	110, 995

17	Additional DNS Hostnames	Info	46180	Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.	If you want to test them, re-scan using the special vhost syntax, such as : www.example.com[192.0.32.10]	Incorporating additional DNS hostnames into a business's infrastructure can have diverse business impacts. On the positive side, it can enhance online presence and accessibility, allowing customers to reach the business through different domain variations. This can lead to improved brand recognition and customer engagement. Additionally, utilizing multiple DNS hostnames can distribute web traffic more efficiently, enhancing website performance and user experience. However, there are considerations: improper management of DNS entries can lead to misdirection of traffic or downtime, impacting customer access and potentially resulting in lost revenue. Security should also be a concern, as poorly configured DNS can be exploited by cybercriminals for phishing attacks or unauthorized access. Overall, adding DNS hostnames can offer strategic advantages, but prudent management, security measures, and potential performance enhancements should be carefully weighed.	N/A

18	Reverse NAT/Intercepting Proxy Detection	Info	3142 2	Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address. Based on OS fingerprinting results, it seems that different operating systems are listening on different remote ports. Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.	Make sure that this setup is authorized by your security policy	Detecting the use of reverse NAT (Network Address Translation) or intercepting proxies within a business's network can have various business implications. On the positive side, such detection can help in identifying potential security vulnerabilities or unauthorized activities, allowing the business to take proactive measures to safeguard its network and data. By identifying and addressing these elements, the organization can enhance its cybersecurity posture and protect sensitive information from external threats. However, there can be negative aspects as well. Unauthorized reverse NAT or intercepting proxies might indicate unauthorized network configuration or potential data exfiltration attempts, leading to breaches of confidential data and potential legal consequences. In certain cases, legitimate use of these technologies might be for monitoring and security purposes, but their presence could raise concerns about user privacy and data protection. In summary, detecting reverse NAT or intercepting proxies is crucial for maintaining network security, but careful evaluation of their origins and purposes is necessary to mitigate risks and ensure compliance with privacy and security regulations.	N/A

19	Inconsistent Hostname and IP Address	Info	46215	The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.	Fix the reverse DNS or host file.	Experiencing inconsistent hostname and IP address mappings within a business's network can have significant business impacts. On the negative side, these inconsistencies can lead to operational disruptions, as services and applications might fail to communicate properly, resulting in downtime and reduced productivity. This can also impact customer experience if online services become inaccessible or unreliable. Furthermore, inconsistent mappings can complicate troubleshooting and diagnostics, potentially prolonging issue resolution and increasing IT support costs. From a security perspective, these inconsistencies can be exploited by attackers for various types of cyberattacks, including man-in-the-middle attacks or unauthorized access. On the positive side, addressing these inconsistencies can lead to improved network reliability, better user experiences, streamlined operations, and enhanced security posture. It's crucial to maintain accurate and up-to-date records of hostname and IP address mappings to prevent these negative impacts and ensure the smooth functioning of the business's digital infrastructure.	n/A

20	Web Server robots.txt Information Disclosure	info	10302	The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.	Review the contents of the site's robots.txt file, use Robots META tags. instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive. material.	The inadvertent disclosure of web server robots.txt files can have notable business impacts. On the negative side, it can expose sensitive directory structures, URLs, and potentially confidential information to the public or malicious actors, leading to increased security risks, targeted attacks, and potential data breaches. This could damage the company's reputation, erode customer trust, and result in legal and regulatory implications, especially if sensitive customer or business data is exposed. Moreover, competitors could gain insights into the company's website structure and strategies, impacting the business's competitive edge. On the positive side, identifying and rectifying such disclosure issues promptly can enhance cybersecurity, protect sensitive information, and prevent potential attacks. Maintaining robust web server configurations and ensuring that robots.txt files are correctly configured can mitigate the risks associated with unintentional information disclosure, preserving the company's reputation and customer trust.	8443