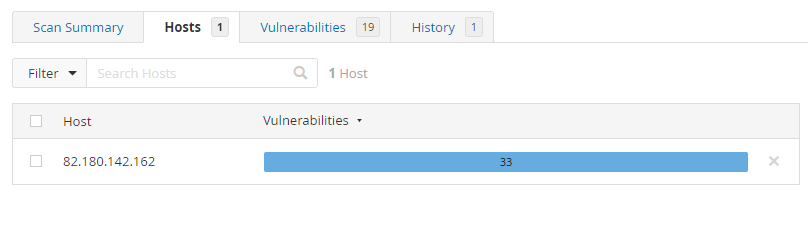
**Stage 2 (Nessus)**

**Overview :**

Nessus stands as a powerful vulnerability scanner renowned for its adeptness in detecting security issues across networks, systems, and applications. Leveraging a comprehensive database of known vulnerabilities, it conducts meticulous scans, identifying weaknesses, misconfigurations, and potential entry points for cyber attacks. Its multifaceted approach encompasses various scan types, including credentialed and non-credentialed scans, ensuring a thorough assessment of security postures. Nessus furnishes detailed reports, categorizing vulnerabilities by severity levels and offering actionable insights for remediation. This tool facilitates continuous monitoring by enabling scheduled scans and integrating with other security frameworks. Its user-friendly interface and robust feature set make it adaptable to diverse environments, supporting various platforms and configurations. Nessus aids in compliance adherence by assessing systems against regulatory standards and industry best practices. Incorporating Nessus into cybersecurity strategies enhances proactive threat identification and fortifies defenses against evolving security threats. Its versatility and accuracy empower organizations to proactively manage vulnerabilities, bolstering their overall security posture.

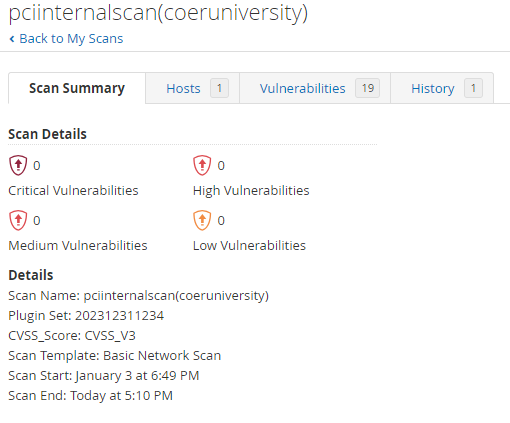
**Target website : https://coeruniversity.in/**

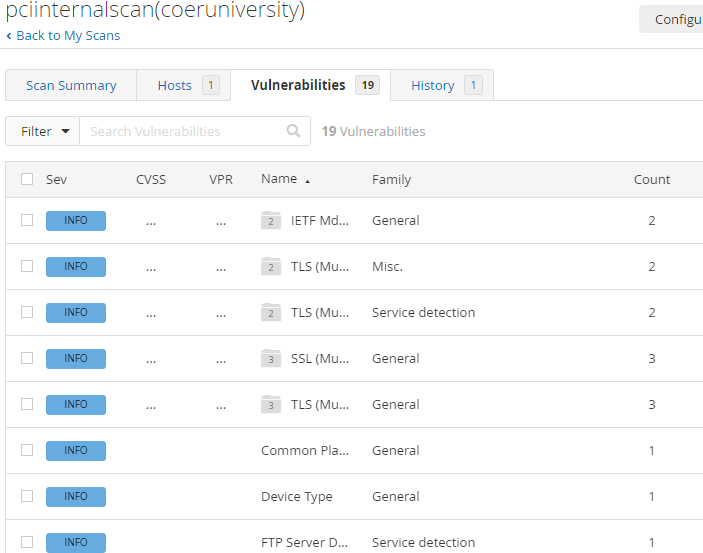
**Target ip address: 82.180.142.162**

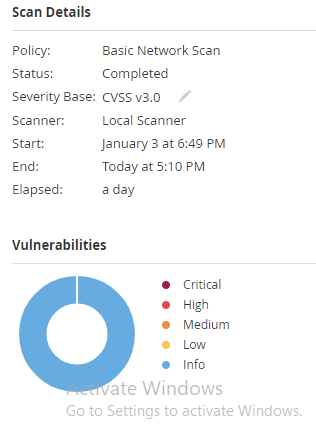


**List of vulnerability**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No** | **Vulnerability Name** | **Family** | **Severity** | **Plugins** |
| 1 | SSL Certificate Information | General | Info | **10863** |
| 2 | SSL Cipher Suites Supported | General | Info | **21643** |
| 3 | SSL Perfect Forward Secrecy Cipher Suites Supported | General | Info | **57041** |
| 4 | SSL / TLS Versions Supported | General | Info | **56984** |
| 5 | SSL/TLS Recommended Cipher Suites | General | Info | **156899** |
| 6 | TLS Next Protocols Supported | General | Info | **62564** |
| 7 | SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) | General | Info | **95631** |
| 8 | SSL Root Certification Authority Certificate Information | General | Info | **94761** |
| 9 | TLS ALPN Supported Protocol Enumeration | Misc. | Info | **84821** |
| 10 | TLS NPN Supported Protocol Enumeration | Misc. | Info | **87242** |
| 11 | TLS Version 1.2 Protocol Detection | Service detection | Info | **136318** |
| 12 | TLS Version 1.3 Protocol Detection | Service detection | Info | **138330** |
| 13 | Nessus SYN scanner | Port scanners | Info | **11219** |
| 14 | Service Detection | Service detection | Info | **22964** |
| 15 | HTTP Server Type and Version | Web Servers | Info | **10107** |
| 16 | Common Platform Enumeration (CPE) | General | Info | **45590** |
| 17 | Device Type | General | Info | **54615** |
| 18 | FTP Server Detection | Service detection | Info | **10092** |
| 19 | FTP Service AUTH TLS Command Support | FTP | Info | **42149** |
| 20 | ICMP Timestamp Request Remote Date Disclosure | General | Info | **10114** |
| 21 | MySQL Server Detection | Databases | Info | **10719** |







#### **Vulnerability Name :** SSL Certificate Information

**Severity : Info**

**Plugin:10863**

**Port :21/tcp/ftp**

**Description:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Business Impact: Exposes potential weaknesses in SSL certificates, risking data integrity and confidentiality.

Solution: Regularly update and renew SSL certificates, ensuring they meet industry standards. Employ strong encryption algorithms.

#### **Vulnerability Name :** SSL Cipher Suites Supported

**Severity : Info**

**Plugin:21643**

**Port : 21/tcp/ftp**

Description : This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Business Impact: Weak cipher suites may lead to unauthorized access or data interception.

Solution: Disable insecure cipher suites, follow best practices for secure configurations, and keep systems updated.

1. **Vulnerability Name : SSL Perfect Forward Secrecy Cipher Suites Supported**

**Severity : Info**

**Plugin:** **57041**

**Port : 21/tcp/ftp**

Description : The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Business Impact: Lack of Perfect Forward Secrecy may expose past communication to decryption.

Solution: Enable and prioritize cipher suites that support Perfect Forward Secrecy to enhance data confidentiality.

1. **Vulnerability Name : SSL / TLS Versions Supported**

**Severity : Info**

**Plugin: 56984**

**Port : 21/tcp/ftp**

Description : This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Business Impact: Outdated versions may have known vulnerabilities, risking security.

Solution: Use the latest TLS versions and regularly update systems to protect against known exploits.

1. **Vulnerability Name : SSL/TLS Recommended Cipher Suites**

**Severity : Info**

**Plugin: 156899**

**Port : 21/tcp/ftp**

Description : The remote host has open SSL/TLS ports which advertise discouraged cipher suites.

Business Impact: Choosing insecure cipher suites can compromise data security.

Solution: Follow industry best practices for recommended cipher suites, keeping security configurations up to date.

1. **Vulnerability Name : TLS Next Protocols Supported**

**Severity : Info**

**Plugin: 62564**

**Port : 21/tcp/ftp**

Description :This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections. Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

Business Impact: Unsecure protocols may expose systems to attacks or unauthorized access.

Solution: Disable insecure protocols, maintain a list of secure ones, and update configurations.

1. **Vulnerability Name : SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)**

**Severity : Info**

**Plugin:** **95631**

**Port : 21/tcp/ftp**

**Description** 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.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.

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.

Business Impact: Weakly signed certificates may be vulnerable to unauthorized issuance or forgery.

Solution: Regularly update certificates, use strong hashing algorithms, and monitor certificate authorities.

1. **Vulnerability Name : SSL Root Certification Authority Certificate Information**

**Severity : Info**

**Plugin: 94761**

**Port : 21/tcp/ftp**

Description: The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

Business Impact: Compromised root certificates may lead to trust issues in secure communications.

Solution: Securely manage and update root certificates, regularly audit and verify certificate authorities.

1. **Vulnerability Name :TLS ALPN Supported Protocol Enumeration**

**Severity : Info**

**Plugin: 84821**

**Port : 21/tcp/ftp**

Description:The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

Business Impact: Enumeration can reveal potentially exploitable information about supported protocols.

Solution: Limit information disclosure, disable unnecessary protocols, and keep systems patched.

1. **Vulnerability Name :TLS NPN Supported Protocol Enumeration**

**Severity : Info**

**Plugin:** **87242**

**Port : 21/tcp/ftp**

Description The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

Business Impact: Revealing supported protocols may aid attackers in crafting targeted exploits.

Solution: Minimize protocol information exposure, disable unnecessary protocols, and apply security patches promptly.

1. **Vulnerability Name :TLS Version 1.2 Protocol Detection**

**Severity : Info**

**Plugin: 136318**

**Port : 21/tcp/ftp**

**Description** :The remote service accepts connections encrypted using TLS 1.2.

Business Impact: Detection of older TLS versions may indicate vulnerability to known exploits.

Solution: Upgrade to the latest TLS versions, disable obsolete protocols, and apply security updates.

1. **Vulnerability Name :TLS Version 1.3 Protocol Detection**

**Severity : Info**

**Plugin: 138330**

**Port : 21/tcp/ftp**

Description :The remote service accepts connections encrypted using TLS 1.3.

Business Impact: Detection of outdated TLS versions may expose systems to potential vulnerabilities.

Solution: Ensure systems are updated to the latest TLS version and disable older protocols.

1. **Vulnerability Name :Nessus SYN scanner**

**Severity : Info**

**Plugin: 11219**

**Port : 21/tcp/ftp , 80/tcp/www , 443/tcp/www , 3306/tcp/mysql**

Description :This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.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.

Business Impact: SYN scanning may be an attempt to identify vulnerabilities in network services.

Solution: Implement proper network security measures, such as firewalls and intrusion detection systems, to mitigate SYN scan risks.

1. **Vulnerability Name :Service Detection**

**Severity : Info**

**Plugin:22964**

**Port : 21 / tcp / ftp, 80 / tcp / www , 443 / tcp / www**

Description Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Business Impact: Unauthorized service detection may reveal information about the network, aiding potential attackers.

Solution: Employ network segmentation, firewall rules, and disable unnecessary services to limit exposure.

1. **Vulnerability Name :HTTP Server Type and Version**

**Severity : Info**

**Plugin: 10107**

**Port : 443 / tcp / www , 80 / tcp / www**

Description :This plugin attempts to determine the type and the version of the remote web server.

Business Impact: Disclosing server details may expose vulnerabilities specific to the server type and version.

Solution: Limit server information disclosure, use generic server banners, and keep software up to date.

1. **Vulnerability Name :Common Platform Enumeration (CPE)**

**Severity : Info**

**Plugin: 45590**

**Port : NA**

Description :By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Business Impact: Enumeration may reveal details about system platforms, aiding targeted attacks.

Solution: Minimize information disclosure, regularly update systems, and employ intrusion detection systems.

1. **Vulnerability Name :Device Type**

**Severity : Info**

**Plugin: 54615**

**Port :NA**

Description:Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Business Impact: Identifying device types may assist attackers in crafting targeted exploits.

Solution: Use generic naming conventions, restrict access to device details, and regularly update device firmware.

1. **Vulnerability Name :FTP Server Detection**

**Severity : Info**

**Plugin: 10092**

**Port : 21/tcp/ftp**

Description:It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Business Impact: Revealing FTP server details may expose vulnerabilities or aid in unauthorized access attempts.

Solution: Disable unnecessary FTP services, implement secure configurations, and keep software updated.

1. **Vulnerability Name :FTP Service AUTH TLS Command Support**

**Severity : Info**

**Plugin: 42149**

**Port : 21/tcp/ftp**

Description: The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

Business Impact: Lack of secure FTP authentication support may expose credentials during transmission.

Solution: Enable FTP over TLS (FTPS), use secure authentication methods, and encrypt FTP traffic.

1. **Vulnerability Name :ICMP Timestamp Request Remote Date Disclosure**

**Severity : Info**

**Plugin: 10114**

**Port : 0 / icmp**

Description: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

##### Solution : Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Business Impact: Disclosure of system time may assist attackers in synchronization and planning attacks.

Solution: Disable ICMP timestamp responses, employ network security measures, and keep systems synchronized.

1. **Vulnerability Name :MySQL Server Detection**

**Severity : Info**

**Plugin: 10719**

**Port : 3306 / tcp / mysql**

Description: The remote host is running MySQL, an open source database server.

Business Impact: Revealing MySQL server details may expose vulnerabilities or aid in unauthorized access attempts.

Solution: Limit MySQL information disclosure, apply security best practices, and regularly update MySQL server software.