**Vulnerability Scan Report:**

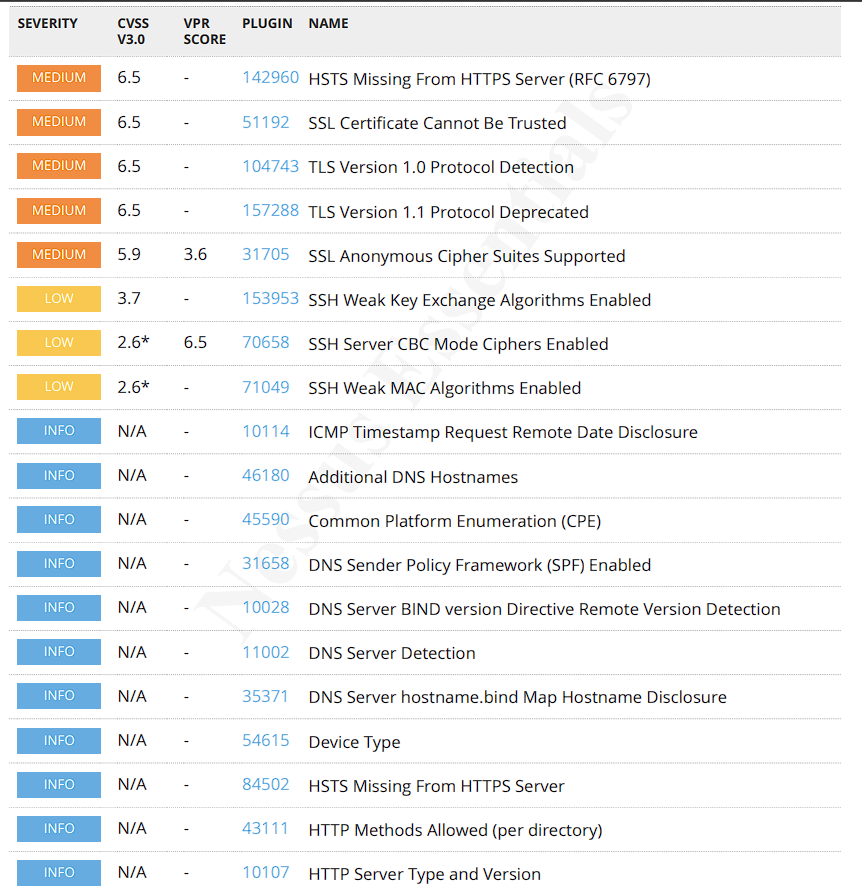
**Team Number:** Team 4.2

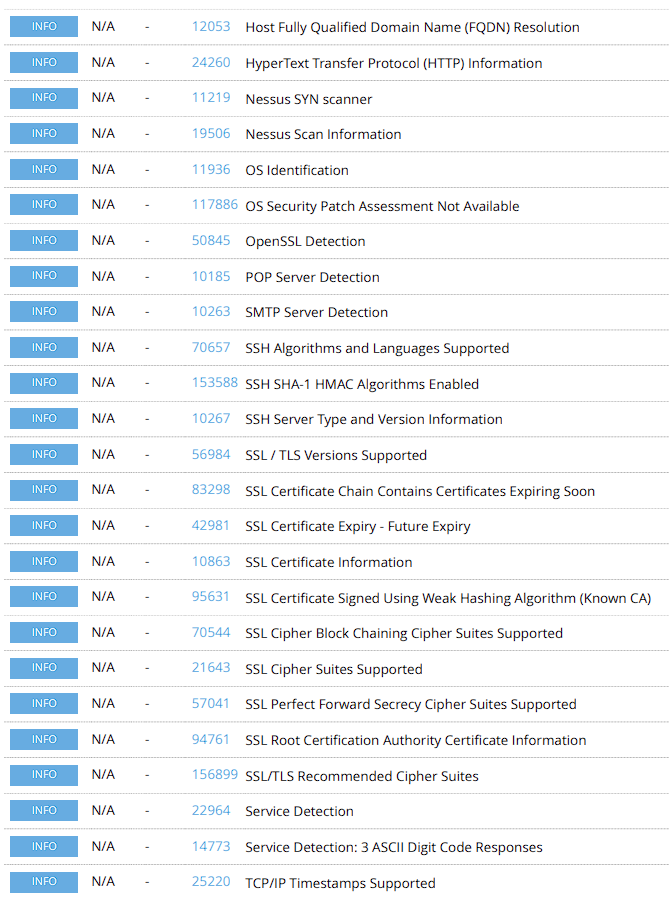
**Team Members:** Vishnu Veerapu  
 Mungali Chetan Sai Raju  
 Promodh Krishna  
 Charith Anil Kumar Nagar

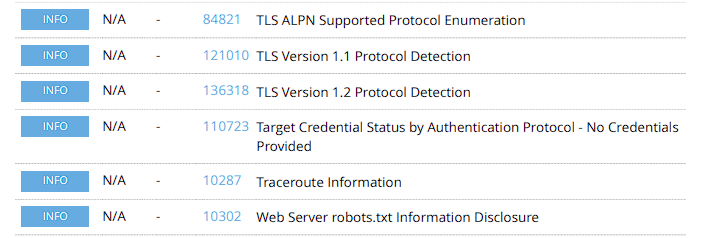
**Project Name:** Network Anomaly detection

**Practise website:** https://www.shodan.io/

**Scanned Vulnerabilities are:**

****

****

****

**Some of the Vulnerabilities Description and Business Impacts are:**

1. HSTS Missing from HTTPS Server (RFC 6797)  
   **Vulnerability:** Cookie Hijacking, Cryptographic failure  
   **CWE: CWE-319 (Cleartext Transmission of Sensitive Information)**

**Description:**

HSTS (HTTP Strict Transport Security) is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks. When HSTS is missing from an HTTPS server, it means that the server is not enforcing a secure connection, making it vulnerable to attacks where an attacker can intercept and modify the communication between the server and the client.

**Business Impact:**

This vulnerability can lead to unauthorized access, data interception, and modification of sensitive information, potentially damaging the reputation of the organization and causing financial losses.

**Solution:**

Configure the remote web server to use HSTS.

1. SSL Certification cannot be trusted:  
   **Vulnerability:** Man in the middle attack, Broken Access Control  
   **CWE: CWE-297 (Improper Validation of Certificate with Host Mismatch)**

**Description:**

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 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 'not Before' dates, or after one of the certificate's 'not After' 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.  
**Business Impact:**

Users' trust can be compromised, leading to potential phishing attacks, data theft, and loss of sensitive information. It can also lead to legal consequences and damage to the organization's reputation.

**Solution:**

Purchase or generate a proper SSL certificate for this service.

1. TLS version 1.0 Protocol Detection:

**Vulnerability:** Cryptographic design flaw, Brute Force Attack **CWE: CWE-326 (Inadequate Encryption Strength)**

**Description**: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 they connect) that can be verified as not being susceptible to any known exploits.**Business Impact**:

Weak encryption can be exploited by attackers to intercept and decrypt sensitive data, leading to unauthorized access, data breaches, and legal liabilities.  
**Solution:**

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

1. TLS Version 1.1 Protocol Detection:

**CWE: CWE-326 (Inadequate Encryption Strength)**

**Description:**

Similar to TLS version 1.0, TLS version 1.1 is deprecated and no longer considered secure due to known vulnerabilities. Detection of TLS version 1.1 indicates the usage of outdated encryption algorithms that can be exploited by attackers.

**Business Impact:** Deprecated encryption protocols can be exploited by attackers, potentially leading to unauthorized access, data breaches, and legal consequences. It also undermines users' trust in the security of the communication.  
**Solution**

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

1. SSL Anonymous Cipher suits supported  
   CWE: CWE-326 (Inadequate Encryption Strength)  
   **Description**

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.  
  
Note: This is considerably easier to exploit if the attacker is on the same physical network.

**Business Impacts:**

Support for anonymous cipher suites weakens the security of the communication channel, making it vulnerable to eavesdropping, data tampering, and unauthorized access. This can lead to compromise of sensitive information and harm the organization's reputation.

**Solution**

Reconfigure the affected application if possible to avoid use of weak ciphers.

1. Sensitive File Disclosure (HTTP)

CWE ID: CWE-538

**Description:** Sensitive file disclosure occurs when an attacker gains access to files on a web server that should not be publicly accessible. This vulnerability can expose sensitive information such as configuration files, source code, or database credentials.

**Business Impact:** Potential unauthorized access to sensitive information, leading to data breaches, reputation damage, and legal consequences.

1. POP3 Unencrypted Cleartext Login

CWE ID: CWE-319

**Description:** POP3 Unencrypted Cleartext Login refers to the use of plain text communication in the authentication process of POP3 email servers. Attackers can intercept and read login credentials, potentially leading to unauthorized access to email accounts.

**Business Impact:** Unauthorized access to email accounts, potential data theft, privacy breaches, and misuse of sensitive information.

1. SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

CWE ID: CWE-478

**Description:** This vulnerability occurs when the Diffie-Hellman key exchange algorithm is configured with weak parameters, making it susceptible to cryptographic attacks. Attackers can exploit this weakness to decrypt encrypted communication.

Business Impact:\* Potential interception of sensitive data, man-in-the-middle attacks, loss of confidentiality, and compromised communication integrity.

1. Weak Encryption Algorithm(s) Supported (SSH)

CWE ID: CWE-327

**Description:** This vulnerability occurs when SSH servers support weak encryption algorithms that can be easily exploited by attackers to decrypt communication. Weak algorithms compromise the confidentiality and integrity of SSH connections.

**Business Impact:** Potential interception of sensitive data, unauthorized access to systems, loss of confidentiality, and compromised communication integrity.

1. ISC BIND Security Bypass Vulnerability - Active Check

CWE ID: CWE-284

**Description:** This vulnerability allows attackers to bypass security mechanisms in ISC BIND DNS servers. By exploiting this flaw, attackers can gain unauthorized access, disrupt DNS services, or launch further attacks within the compromised network.

**Business Impact:** Disruption of DNS services, potential data manipulation, unauthorized access to sensitive DNS information, and compromise of network integrity.