# Stage - 2

**Nessus Overview:-**

* **Description:**
* Nessus is widely used vulnerability scanning tool and security software developed by tenable, Inc. It is primarily used to identify and access vulnerabilities in computer systems, networks, and applications.
* **Applications of Nessus:**
* 1. Vulnerability Scanning:

Nessus is primarily known for its vulnerability scanning capabilities. It can target systems for known security issues, misconfigurations, and weaknesses. This helps organizations identify potential entry points for attackers and prioritize their remediation efforts.

* 2. Plugin-Based Architecture:

Nessus uses plugin-in-based architecture, where plugins are small programs or scripts that check for specific vulnerabilities or issues. This architecture allows nessus to support a wide range of vulnerabilities and technologies.

* 3. Comprehensive Coverage:

Nessus is capable of scanning a broad spectrum of system and devices, including servers, workstations, networking equipment, and web applications. It covers various operating systems and software packages.

* 4. Scanning Types: It supports different types of scans, such as credentialed scans, and uncredentialed scans, and compliance scans.
* 5. Risk Management:

Nessus provides a risk management by assigning severity levels to identified vulnerabilities, allowing organizations to focus on the most critical issues first.

* 6.Customization:

Users can customize scans to meet their specific needs. This includes scheduling scans, defining scan policies, and tailoring the scan scope.

* 7.Reporting:

Nessus generates detailed reports that provide a clear overview of the vulnerabilities discovered during the scan. These reports can be useful for compliance purposes and to communicate security status to stakeholders.

* 8. Integration:

It can be integrated with other security tools and systems, such as SIEM (SecurityInformationandEventManagement)solutions,toenhanceanorganization's overall security posture.

## Target ip address:-

* 115.240.194.13
* 52.66.12.101
* 127.0.0.1
* 172.67.222.140

# List of vulnerability :-

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Vulnerability name** | **Severity** | **Plug-in** |
| **Information** |
| 1 | PHP Multiple Vulnerabilities. | Critical. | Published :2022/11/03 Modified : 2023/10/05 |
|
| 2 | PHP Unsupported Version Detection. | Critical. | Published :2012/05/04 Modified : 2022/12/07 |
|
| 3 | SSL Certificate Cannot be trusted. | Medium. | Published :2010/12/15 Modified : 2020/04/27 |
|
| 4 | TLS Version 1.0 Protocol Detection. | Medium. | Published :2017/11/22 Modified : 2023/04/19 |
|
|
| 5 | TLS Version 1.0 Protocol Deprecated. | Medium. | Published :2022/04/04 Modified : 2023/04/19 |
|
|
| 6 | Apache HTTP Server Version. | ----- | Published :2010/07/30 Modified : 2023/08/17 |
| 7 | Backported Security Path Detection. | ----- | Published :2009/06/25Modified : 2015/07/07 |
| 8 | Common Platform Enumeration. | ----- | Published :2010/04/21 Modified : 2023/10/16 |
| 9 | Device Type. | ----- | Published :2011/05/23 Modified : 2022/09/09 |
| 10 | HSTS Missing From HTTPS Server. | ----- | Published :2017/11/22 Modified : 2023/04/19 |
| 11 | HTTP Server Type and Version. | ----- | Published :2000/01/04 Modified : 2020/10/30 |
| 12 | HTTP Information. | ----- | Published :2007/01/30 Modified : 2019/11/22 |
| 13 | Nessus SYN Scanner. | ----- | Published :2009/02/04 Modified : 2023/09/25 |
| 14 | HSTS Missing From HTTPS Server.(RFC 6797) | ----- | Published :2020/11/17 Modified : 2023/06/08 |
| 15 | Web Server allows Password Auto-Completion. | Medium | Published :2009/10/07 Modified : 2023/07/17 |
| 16 | Web Server Transmits clear text credentials. | Low. | Published :2007/09/28 Modified : 2016/11/29 |
| 17 | CGI Generic Tests Load Estimation. | Low. | Published :2009/10/26 Modified : 2022/04/11 |
| 18 | CGI Generic Tests Timeout. | ----- | Published :2009/06/19 Modified : 2021/01/19 |
| 19 | External URL’s. | ----- | Published :2010/10/04 Modified : 2011/08/19 |
| 20 | HTTP Cookie secure property transport mismatch. | ----- | Published :2013/09/10 Modified : 2021/12/20 |
| 21 | HTTP Methods allowed. | ----- | Published :2009/12/10 Modified : 2022/04/11 |
| 22 | Missing content security policy frame ancestors HTTP Response Header. | ----- | Published :2010/10/26 Modified : 2021/01/19 |
| 23 | Nessus Scan information. | ----- | Published :2005/08/26Modified : 2023/07/31 |
| 24 | Web application cookies not marked http only. | ----- | Published :2015/08/24 Modified : 2015/08/24 |
| 25 | Web application cookies not marked secure. | ----- | Published :2015/08/24 Modified : 2015/08/24 |
| 26 | SMB Signing not required. | ----- | Published :2012/01/19 Modified : 2022/10/05 |
| 27 | OS name and installed package Enumeration. | Medium. | Published :2004/07/06 Modified : 2022/09/26 |
| 28 | DCE Services Enumeration. | ----- | Published :2001/08/26 Modified : 2021/10/04 |
| 29 | Host FDQN Resolution. | ----- | Published :2004/02/11 Modified : 2017/04/14 |
| 30 | NTLMSSP Authentication request Remote Network name disclosure. | ----- | Published :2009/11/06 Modified : 2019/11/22 |

**REPORT:-**

## 1.)

**- Vulnerability name:-**PHP Multiple Vulnerabilities.

* **Severity:-**Critical.
* **Plug-in:-** Published :2022/11/03 ,Modified : 2023/10/05
* **Port:-**80(TCP).
* **Description:-**PHP vulnerabilities encompass a range of security issues, including SQL injection, cross-site scripting (XSS), and remote code execution, which can lead to data breaches, service disruptions, and financial losses in web applications.
* **Solution:-**Upgrade to PHP version 7.4.33 or later.
* **Business Impact:-**Multiple PHP vulnerabilities can lead to financial losses, data breaches, reputational damage, and legal consequences, undermining a business's operations and customer trust.

## 2.)

**- Vulnerability name:-** PHP Unsupported Version Detection.

* **Severity:-** Critical.
* **Plug-in:-**Published :2012/05/04 ,Modified : 2022/12/07
* **Port:-** 80(TCP).
* **Description:-**PHP Unsupported Version Detection is a process of identifying outdated and unsupported PHP versions in web applications, which poses security risks and may require an upgrade to maintain system integrity and protect against vulnerabilities.
* **Solution:-** The remote host contains the unsupported version of a web application scripting language.
* **Business Impact:-**Detecting unsupported PHP versions is essential for business security as it helps prevent potential vulnerabilities and data breaches. Failure to address unsupported versions can result in security risks, regulatory compliance issues, and reputational damage.

## 3.)

**- Vulnerability name:-** SSL Certificate Cannot be trusted.

* **Severity:-** Medium.
* **Plug-in:-**Published :2010/12/15 ,Modified : 2020/04/27
* **Port:-** 443(TCP).
* **Description:-** SSL certificate cannot be trusted" indicates that a website's certificate isn't recognized or validated by trusted authorities, potentially exposing users to security risks.
* **Solution:-** Purchase or generate a proper SSL certificate for this service.
* **Business Impact:-**When an SSL certificate is not trusted, it erodes user trust, leads to data breaches, and can result in lost revenue and reputational damage, as customers may avoid the site due to security concerns. Addressing this issue promptly is crucial for maintaining business integrity and security.

## 4.)

**- Vulnerability name:-** TLS Version 1.0 Protocol Detection.

* **Severity:-** Medium.
* **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
* **Port:-** 443(TCP).
* **Description:-** TLS Version 1.0 Protocol Detection is the process of identifying and determining the usage of the TLS 1.0 encryption protocol in a network, which is considered outdated and potentially insecure.
* **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.0
* **Business Impact:-**The detection of TLS 1.0 usage in a business environment can signal security vulnerabilities, increase the risk of data breaches, and lead to regulatory non-compliance, potentially resulting in financial losses, reputational damage, and legal consequences.

## 5.)

**- Vulnerability name:-** TLS Version 1.0 Protocol Deprecated.

* **Severity:-** Medium.
* **Plug-in:-**Published :2022/04/04 ,Modified : 2023/04/19
* **Port:-** 443(TCP).
* **Description:-** "TLS Version 1.0 Protocol Deprecated" means that TLS 1.0, an outdated and insecure encryption protocol, is no longer recommended for use due to known security vulnerabilities.
* **Solution:-** Enable support for TLS 1.2 and 1.3, and disable support for 1.1
* **Business Impact:-**The deprecation of TLS 1.0 mandates its replacement to maintain security standards; non-compliance can lead to data breaches, legal issues, and reputational damage, impacting customer trust and business continuity.

## 6.)

**- Vulnerability name:-** Apache HTTP Server Version.

* **Severity:-** -----
* **Plug-in:-**Published :2010/07/30 ,Modified : 2023/08/17
* **Port:-** 80(TCP).
* **Description:-**  
  The Apache HTTP Server Version is a software component that provides web server capabilities, allowing it to serve web pages to clients over the internet.
* **Solution:- n/a**
* **Business Impact:-**Publicly revealing the Apache HTTP Server version can expose potential vulnerabilities, making the server a target for cyberattacks, which may lead to service disruptions, data breaches, and reputational damage, impacting business operations and customer trust. To mitigate these risks, businesses often hide or obscure server version information and maintain vigilant security practices.

## 7.)

**- Vulnerability name:-** Backported Security Path Detection.

**Severity:-** -----

* **Plug-in:-**Published :2009/06/25 ,Modified : 2015/07/07
* **Port:-** 22(SSH).
* **Description:-** "Backported Security Patch Detection" is the process of identifying and verifying the application of security patches that have been applied to older software versions to address vulnerabilities and improve security.
* **Solution:- n/a**

**Business Impact:-**

Efficient backported security patch detection helps mitigate security risks, reduces the potential for data breaches and service disruptions, and demonstrates a commitment to robust cybersecurity, safeguarding business reputation and customer trust.

Top of Form

Top of Form

## 8.)

**- Vulnerability name:-** Common Platform Enumeration.

* **Severity:-** -----
* **Plug-in:-**Published :2010/04/21 ,Modified : 2023/10/16.
* **Port:- 0(TCP).**
* **Description:-** Common Platform Enumeration (CPE) is a standardized naming scheme to identify and describe software applications and operating systems based on their attributes and version information.
* **Solution:- n/a**
* **Business Impact:-**  
  Common Platform Enumeration (CPE) aids businesses in managing and securing software assets by providing standardized identification, reducing the risk of vulnerabilities, and facilitating compliance, ultimately enhancing cybersecurity posture and minimizing operational risks.

## 9.)

**- Vulnerability name:-** Device Type.

* **Severity:-** -----
* **Plug-in:-**Published :2011/05/23 Modified : 2022/09/09
* **Port:-** 0(TCP).
* **Description:-** Device type refers to the category or classification of a hardware device based on its purpose, design, and functionality, such as a smartphone, laptop, or printer.
* **Solution:- n/a**
* **Business Impact:-**  
  Understanding the device type is critical for businesses to tailor their services, optimize user experience, and ensure compatibility, which can lead to increased customer satisfaction and operational efficiency while minimizing support and compatibility issues.

## 10.)

**- Vulnerability name:-** HSTS Missing From HTTPS Server.

* **Severity:-** -----
* **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
* **Port:-** 443(TCP).
* **Description:-** "HSTS Missing from HTTPS Server" indicates that the server is not implementing HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks.
* **Solution:-** Configure the remote web server to use HSTS.
* **Business Impact:-**  
  The absence of HSTS leaves the website vulnerable to man-in-the-middle attacks and security breaches, potentially eroding customer trust and harming the business's reputation. Implementing HSTS is crucial to enhance security and protect sensitive user data, fostering trust and compliance with security standards.

## 11.)

**- Vulnerability name:-** HTTP Server Type and Version.

* **Severity:-** -----
* **Plug-in:-**Published :2017/11/22 ,Modified : 2023/04/19
* **Port:-** 80(TCP).
* **Description:-** HTTP Server Type and Version refers to the software and version information of the web server handling HTTP requests, which can be used to identify potential vulnerabilities or misconfigurations.
* **Solution:- n/a**
* **Business Impact:-**Revealing HTTP server type and version can expose security weaknesses, making the server a target for cyberattacks and potentially leading to service disruptions, data breaches, and reputational damage, which can negatively impact business operations and customer trust. To mitigate these risks, businesses often hide or obscure server information and maintain vigilant security practices.

## 12.)

**- Vulnerability name:-** HTTP Information.

* **Severity:-** -----
* **Plug-in:-**Published :2007/01/30 , Modified : 2019/11/22
* **Port:-** 80(TCP).
* **Description:-** HTTP Information encompasses data exchanged between a client and server during a Hypertext Transfer Protocol (HTTP) request and response, including headers, status codes, and content.
* **Solution:-** n/a.
* **Business Impact:-** The proper management of HTTP information is essential for ensuring efficient and secure web communication, enhancing user experience, and protecting sensitive data, all of which impact business operations and customer trust.

## 13.)

**- Vulnerability name:-** Nessus SYN Scanner.

* **Severity:-** -----
* **Plug-in:-**Published :2009/02/04, Modified : 2023/09/25
* **Port:-** 22(TCP).
* **Description:-** The Nessus SYN scanner is a network vulnerability scanner that uses SYN packets to identify open ports and potential security vulnerabilities on target systems.
* **Solution:-** Protect your target with an IP filter.
* **Business Impact:-**The Nessus SYN scanner is a crucial tool for businesses to proactively identify and address network vulnerabilities, enhancing overall cybersecurity posture and reducing the risk of data breaches and service disruptions.

## 14.)

**- Vulnerability name:-** HSTS Missing From HTTPS Server.(RFC 6797)

* **Severity:-**Medium.
* **Plug-in:-**Published :2020/11/17 , Modified : 2023/06/08
* **Port:-** 443(TCP).
* **Description:-** "HSTS Missing From HTTPS Server (RFC 6797)" indicates the absence of HTTP Strict Transport Security, a security policy mechanism, which may expose the site to security risks and downgrade attacks, as defined by RFC 6797.
* **Solution:-** Configure the remote web server to HSTS.
* **Business Impact:-**The absence of HSTS as per RFC 6797 increases the risk of security breaches and lowers trust in a website, potentially leading to financial losses and reputational damage.

## 15.)

**- Vulnerability name:-** Web Server allows Password Auto-Completion.

* **Severity:-** Low.
* **Plug-in:-**Published :2009/10/07 Modified : 2023/07/17
* **Port:-** 80(TCP).
* **Description:-** A web server that allows password auto-completion permits browsers to store and autofill login credentials, potentially risking security if used on shared or public computers.
* **Solution:-** Add the attribute ‘autocomplete=off’ to these fields to prevent browsers from caching credentials.
* **Business Impact:-**Allowing password auto-completion can compromise user security, lead to unauthorized access, and damage a business's reputation if sensitive data is exposed due to improper credential handling.

## 16.)

**- Vulnerability name:-** Web Server Transmits cleartext credentials.

* **Severity:-** Low.
* **Plug-in:-**Published :2007/09/28 ,Modified : 2016/11/29
* **Port:-** 80(TCP).
* **Description:-** A web server transmitting cleartext credentials sends login information without encryption, making it susceptible to interception and exposing user data to security risks.
* **Solution:-** Make sure that every sensitive form transmits content over HTTPS.
* **Business Impact:-**  
  The business impact of transmitting cleartext credentials includes the risk of data breaches, potential legal consequences, and damage to customer trust, which can lead to reputational harm and financial losses.

## 17.)

**- Vulnerability name:-** CGI Generic Tests Load Estimation.

* **Severity:-** -----
* **Plug-in:-**Published :2009/10/26, Modified : 2022/04/11
* **Port:-** 80(TCP).
* **Description:-** CGI Generic Tests Load Estimation is a method to assess a web server's capacity to handle Common Gateway Interface (CGI) scripts, helping to determine performance and resource requirements under different loads.
* **Solution:-** n/a
* **Business Impact:-**CGI Generic Tests Load Estimation aids businesses in optimizing web server performance, ensuring reliability under high loads, and preventing service disruptions, ultimately enhancing user experience and reducing operational risks.

## 18.)

**- Vulnerability name:-** CGI Generic Tests Timeout.

* **Severity:-** -----
* **Plug-in:-**Published :2009/06/19, Modified : 2021/01/19
* **Port:- 80(TCP).**
* **Description:-** CGI Generic Tests Timeout is a measure of the maximum time a web server should allow for the execution of Common Gateway Interface (CGI) scripts, preventing excessive delays in serving web requests.
* **Solution:-** Consider increasing the maximum run time preferences from the web application settings in order to prevent the CGI scanning for timming out.
* **Business Impact:-** Properly configuring CGI Generic Tests Timeout is critical to ensure timely server responses, prevent performance bottlenecks, and maintain user satisfaction, thus avoiding potential business disruptions.

## 19.)

**- Vulnerability name:-** External URL’s.

* **Severity:-** -----
* **Plug-in:-**Published :2010/10/04 ,Modified : 2011/08/19
* **Port:-** 80(TCP).
* **Description:-** External URLs are hyperlinks that point to web pages or resources outside the current website's domain or server.
* **Solution:-** n/a.
* **Business Impact:-**  
  The inclusion of external URLs in web content can impact business operations and reputation, as it may introduce security risks and potential loss of control over linked content.

## 20.)

**-Vulnerability name:-** HTTP Cookie secure property transport mismatch.

* **Severity:-** -----
* **Plug-in:-**Published :2013/09/10 ,Modified : 2021/12/20
* **Port:-** 443(TCP).
* **Description:-** An "HTTP Cookie secure property transport mismatch" occurs when a cookie marked as secure is transmitted over an insecure (non-HTTPS) connection, potentially exposing sensitive information to security risks.
* **Solution:-** n/a
* **Business Impact:-**The business impact of an HTTP Cookie secure property transport mismatch includes the risk of data exposure, reduced trust, and potential security breaches, which can lead to financial losses and reputational damage.

## 21.)

**- Vulnerability name:-** HTTP Methods allowed.

* **Severity:-** -----
* **Plug-in:-**Published :2009/12/10 ,Modified : 2022/04/11
* **Port:-** 80(TCP).
* **Description:-**It refers to the types of HTTP request methods (e.g., GET, POST, PUT, DELETE) that a web server permits for communication with the server's resources.
* **Solution:-** n/a
* **Business Impact:-**Properly defining and limiting allowed HTTP methods is crucial to mitigate security risks, prevent unauthorized access, and safeguard sensitive data, protecting business operations and customer trust.

## 22.)

**- Vulnerability name:-** Missing content security policy frame ancestors HTTP Response Header.

* **Severity:-** -----
* **Plug-in:-**Published :2010/10/26 ,Modified : 2021/01/19
* **Port:-** 80(TCP).
* **Description:-** It indicates that a security header specifying who can embed the web page in a frame or if frame is not set, potentially exposing the site to click jacking attacks.
* **Solution:-** Set a non-permissive Consent-Security-policy frame-ancestors header for all requested resources.
* **Business Impact:-**  
  The absence of the Content Security Policy frame-ancestors header can expose a business to click jacking attacks, data theft, and reputation damage, impacting customer trust and security.

## 23.)

**- Vulnerability name:-** Nessus Scan information.

* **Severity:-** -----
* **Plug-in:-**Published :2005/08/26 ,Modified : 2023/07/31
* **Port:-** 0(TCP).
* **Description:-** A Nessus scan provides detailed information about network vulnerabilities, misconfigurations, and security issues, helping organizations assess and improve their cybersecurity posture by identifying potential threats and weaknesses in their infrastructure and applications.
* **Solution:-** n/a
* **Business Impact:-** Nessus scan information has a significant business impact by enabling organizations to proactively address vulnerabilities, reduce the risk of data breaches, maintain compliance, and enhance overall cybersecurity, ultimately safeguarding reputation and customer trust while preventing financial losses.

## 24.)

**- Vulnerability name:-** Web application cookies not marked http only.

* **Severity:-** -----
* **Plug-in:-**Published :2015/08/24, Modified : 2015/08/24
* **Port:-** 80(TCP).
* **Description:-** Web application cookies not marked as "Http Only" lack a security attribute that prevents client-side JavaScript from accessing them, potentially making them vulnerable to cross-site scripting (XSS) attacks or other malicious client-side scripts.
* **Solution:-** Each Cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
* **Business Impact:-**  
  The absence of the "Http Only" attribute in web application cookies can result in security risks, allowing attackers to steal user session data, potentially leading to unauthorized access, data breaches, and reputational damage, which can negatively impact business operations and customer trust.

## 25.)

**- Vulnerability name:-** Web application cookies not marked secure.

* **Severity:- -----**
* **Plug-in:-**Published :2015/08/24 Modified : 2015/08/24
* **Port:-** 80(TCP).
* **Description:-** When web application cookies are not marked as "secure," they can be transmitted over unencrypted HTTP connections, potentially exposing sensitive data to interception and security risks.
* **Solution:-** Each cookie should be carefully reviewed to determine if it contains sensitive data for a security decision.
* **Business Impact:-** Iffailing to mark cookies as secure in a web application can compromise the security of user data and authentication. It's a best practice to use secure cookies, along with proper HTTPS configuration, to protect sensitive information and maintain the privacy and integrity of user sessions.

## 26.)

**- Vulnerability name:-** SMB Signing not required.

* **Severity:-** Medium.
* **Plug-in:-**Published :2012/01/19 Modified : 2022/10/05
* **Port:-** 445(TCP).
* **Description:-** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
* **Solution:-** Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
* **Business Impact:-**The absence of SMB signing can result in significant security vulnerabilities, potentially leading to data breaches, unauthorized access, and compliance issues, which can damage an organization's reputation and incur operational and financial costs.

## 27.)

**- Vulnerability name:-** OS name and installed package Enumeration.

* **Severity:- -----**
* **Plug-in:-**Published :2004/07/06,Modified : 2022/09/26
* **Port:-** 0(TCP).
* **Description:-**  
  OS name and installed package enumeration is the process of identifying the operating system and listing the software packages on a computer or server, crucial for system management and security assessment.
* **Solution:-** n/a
* **Business Impact:-**Accurate OS and package enumeration is essential for effective system management and security monitoring, helping organizations maintain up-to-date software, mitigate vulnerabilities, and ensure regulatory compliance, while failures in this process can lead to security gaps and potential exploitation by attackers.

## 28.)

**- Vulnerability name:-** DCE Services Enumeration.

* **Severity:-** -----
* **Plug-in:-**Published :2001/08/26 ,Modified : 2021/10/04
* **Port:-** 135(TCP).
* **Description:-**  
  DCE (Distributed Computing Environment) services enumeration is the process of identifying and listing the available remote services and their attributes in a DCE-based network.
* **Solution:-** n/a.
* **Business Impact:-**DCE services enumeration can have a significant business impact as it helps in identifying potential vulnerabilities, misconfigurations, or unauthorized services in a network, which, if exploited, could lead to security breaches, data loss, or service disruptions, ultimately affecting the organization's reputation and financial stability.

## 29.)

**- Vulnerability name:-** Host FDQN Resolution.

* **Severity:-** -----
* **Plug-in:-**Published :2004/02/11, Modified : 2017/04/14
* **Port:-** 0(TCP).
* **Description:-**It is the process of converting a human-readable domain name into its corresponding IP address, allowing computers to locate and communicate with remote hosts on the internet or a network.
* **Solution:-** n/a.
* **Business Impact:-**  
  Efficient and accurate FQDN resolution is crucial for businesses as it ensures seamless access to web services, applications, and data, enhancing user experience and productivity. However, issues with FQDN resolution can lead to downtime, connectivity problems, and disrupted operations, potentially resulting in lost revenue and damage to the company's reputation.

## 30.)

**- Vulnerability name:-** NTLMSSP Authentication request Remote Network name disclosure.

* **Severity:-** -----
* **Plug-in:-**Published :2009/11/06, Modified : 2019/11/22
* **Port:-** 445(TCP).
* **Description:-**The NTLMSSP authentication request vulnerability can lead to the disclosure of a remote network name when an attacker exploits weaknesses in the NTLMSSP authentication protocol, potentially revealing sensitive information about a target network.
* **Solution:-**n/a.
* **Business Impact:-**The business impact of NTLMSSP authentication request remote network name disclosure is significant, as it can expose sensitive network information to malicious actors, enabling them to launch targeted attacks, compromise systems, and potentially lead to data breaches, financial losses, and reputational damage for the affected organization.