Research Report 3 Vulnerability Scanning with Shields Up and Nessus

By: Farzaneh Noroozi
Professor: Dr. Murray Jennex

What did you do?

Conducting Vulnerability Scans with Shields UP!!:

For the vulnerability scans, I utilized Shields UP!!, a valuable online service offered by Gibson Research Corporation. The process involved accessing the ShieldsUP! website and initiating two port scans: "Common Ports" and "All Service Ports." After running these scans, I carefully examined the results to evaluate the status of commonly targeted ports and all available ports on my computer. The scans provided invaluable insights into potential vulnerabilities, including open, closed, and stealth-mode ports, enabling me to comprehensively assess my system's security status. "All Service Ports" scan covered all 65,535 ports available on my computer.

Conducting Vulnerability Scans with Nessus:

In addition to Shields UP!!, I also employed Nessus, a powerful and widely-used vulnerability scanning tool. To start the process, Despite facing initial rejections from my current company and several other businesses, I successfully obtained permission from the Shiraz Oil Refining Company in Iran to use their network for a Nessus vulnerability scan. Unfortunately, due to restrictions, no results were obtained. Eventually, Cascade Park Community Library allowed me to conduct the scan on their network using the IP address 10.1.4.113. I visited the URL provided to obtain the activation code for Nessus Essentials. During the downloading phase, I encountered an error that prompted me to trust the network, which was resolved by selecting the "trust" option. Subsequently, I selected the "Basic Network Scan" option and entered the target IP addresses, ensuring the scan remained within the limit of 16 IP addresses. Once the scan configuration was saved, I launched the vulnerability scan and waited for it to complete, considering the network complexity and the number of IP addresses scanned.

Understanding Nessus Software Functionality:

Nessus, a powerful vulnerability scanning tool, played a vital role in identifying security weaknesses within networks, systems, and applications. It effectively employed various scanning techniques, such as SYN 'half-open' port scanning, to detect open ports and potential vulnerabilities. The software produced detailed reports encompassing security risks, misconfigurations, and potential threats. This enabled administrators to proactively address weaknesses and enhance the overall security posture of their systems and networks.

How Shields UP!! Works:

Shields UP!! is a free online service provided by Gibson Research Corporation. It empowers users to perform port scanning and security testing on their computer's internet connection. By conducting a series of tests, Shields UP!! checks the visibility of open ports from the internet and assesses the firewall protection level. This helps users identify potential security risks and vulnerabilities that might be exposed to potential threats from the outside world. Through Shields UP!!, users can gain valuable insights into the accessibility of specific ports, enabling them to take appropriate measures to enhance their network security and privacy.

Analyzing Output in Nessus:

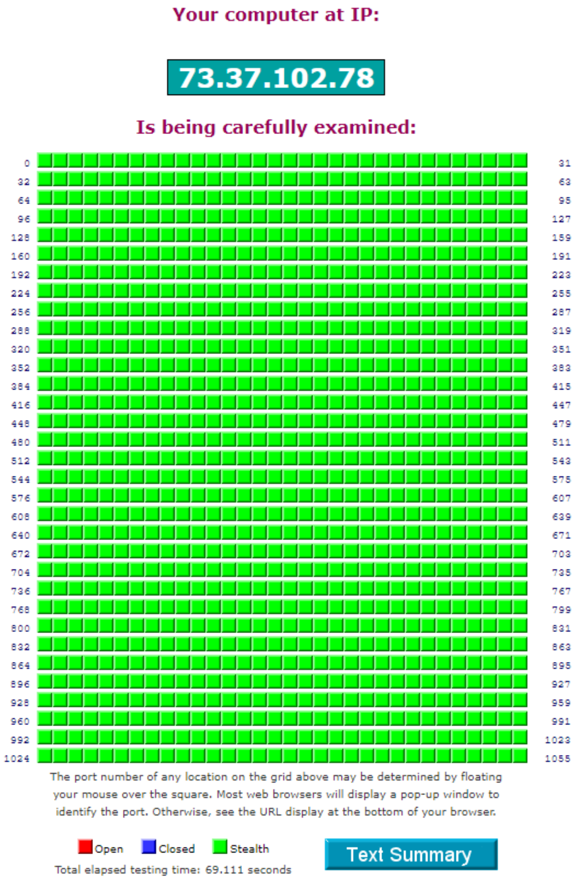
After the Nessus vulnerability scan was completed, I meticulously reviewed the generated results to gain a comprehensive understanding of the system's security status. The scan provided detailed reports on security weaknesses, misconfigurations, and potential threats found within the network, systems, and applications. I paid particular attention to the severity ratings assigned to each identified vulnerability, as this allowed me to prioritize critical issues that required immediate attention. By analyzing the output, I could assess the impact of vulnerabilities on the overall security posture and devise appropriate mitigation strategies. The actionable insights provided by Nessus facilitated the implementation of targeted security measures, enabling me to proactively safeguard the network against potential risks and potential cyber threats.

Analyzing Output in Shields UP!!:

Upon completing the vulnerability scans using Shields UP!!, I closely analyzed the results obtained from both the "Common Ports" and "All Service Ports" scans. The report provided valuable insights into the visibility of open ports from the internet and the effectiveness of firewall protection. By assessing the status of commonly targeted ports and all available ports on my computer, I could identify potential vulnerabilities, including open, closed, and stealth-mode ports. The analysis allowed me to gain a better understanding of the network's exposure to potential threats from external sources. I focused on evaluating any open ports, as these could serve as potential entry points for unauthorized access or cyberattacks. This analysis enabled me to take proactive measures to address the identified vulnerabilities and enhance the network's security by closing unnecessary open ports and implementing appropriate security configurations. Overall, the output analysis in Shields UP!! equipped me with valuable insights to improve the network's resilience against potential security risks.

What are the Results?

Shields UP!!



Your computer at IP:

73.37.102.78

Is being carefully examined:

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

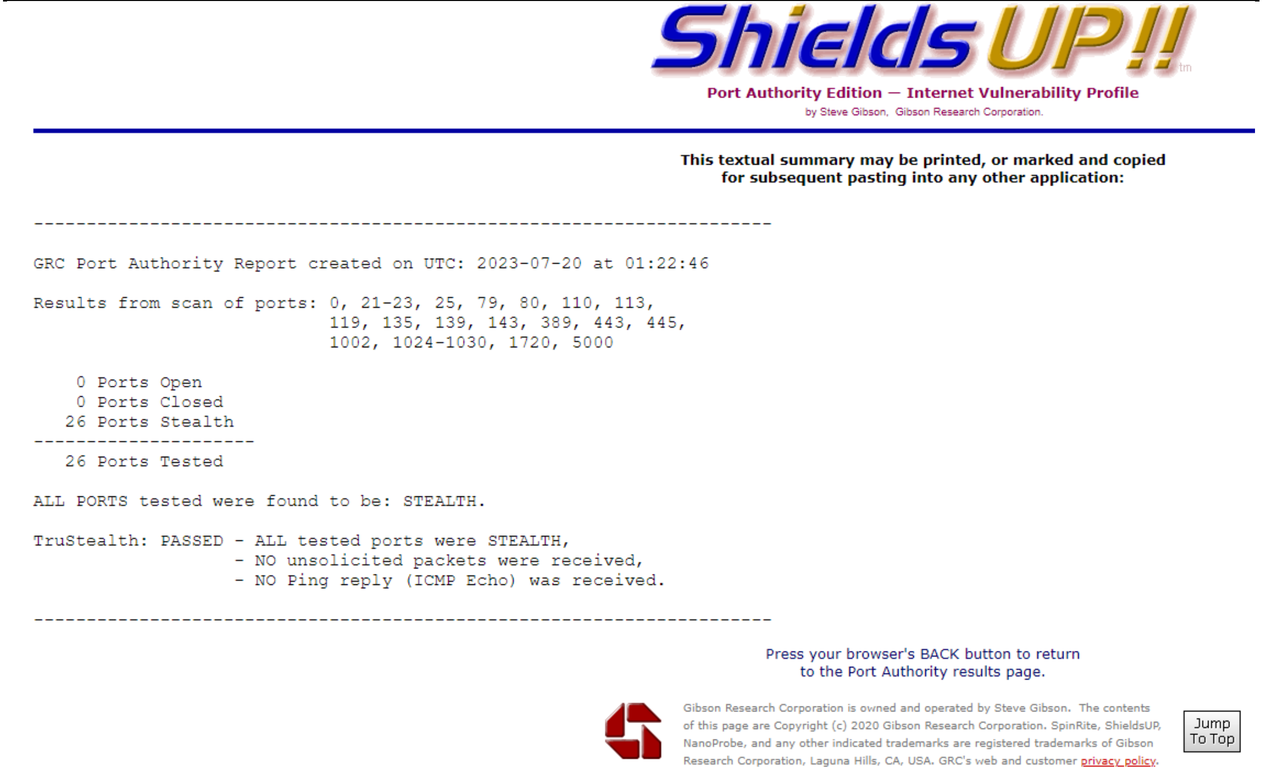
🟥 Open 🟦 Closed 🟩 Stealth

Total elapsed testing time: 69.111 seconds

Research Report 3 Vulnerability Scanning with Shields Up and Nessus

By: Farzaneh Noroozi

Professor: Dr. Murray Jennex


ShieldsUP!!
tm
Port Authority Edition — Internet Vulnerability Profile
by Steve Gibson, Gibson Research Corporation.

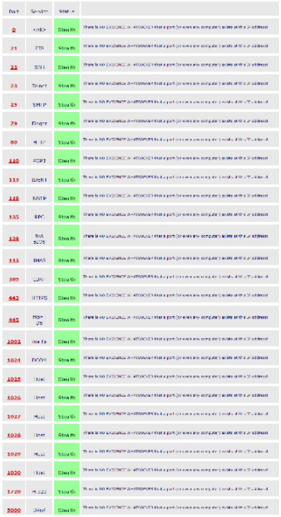
This textual summary may be printed, or marked and copied for subsequent pasting into any other application:

```
----------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2023-07-20 at 01:22:46

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                            119, 135, 139, 143, 389, 443, 445,
                            1002, 1024-1030, 1720, 5000

    0 Ports Open
    0 Ports Closed
   26 Ports Stealth
---------------------
   26 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED - ALL tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - NO Ping reply (ICMP Echo) was received.

----------------------------------------------------------------------
```

Press your browser's BACK button to return to the Port Authority results page.

Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2020 Gibson Research Corporation. SpinRite, ShieldsUP, NanoProbe, and any other indicated trademarks are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer privacy policy.

“Common Ports” Analyzing Results



Port	Service	Status	
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
79	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
80	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
119	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
139	Net BIOS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
143	IMAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
389	LDAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
443	HTTPS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
445	MSFT DS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1002	ms-ils	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1024	DCOM	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1025	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1026	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1027	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1028	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1029	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1030	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
1720	H.323	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address
5000	UPnP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address

- GRC Port Authority Report created on UTC: 2023-07-29 at 20:14:26
- Results from the scan of ports: 0, 21-23, 25, 79, 80, 110, 113, 119, 135, 139, 143, 389, 443, 445, 1002, 1024-1030, 1720, 5000
- 0 Ports Open
- 0 Ports Closed
- 26 Ports Stealth

Summary:

- Total Ports Tested: 26

All tested ports were found to be in "STEALTH" mode, meaning they did not respond to the scan attempts.

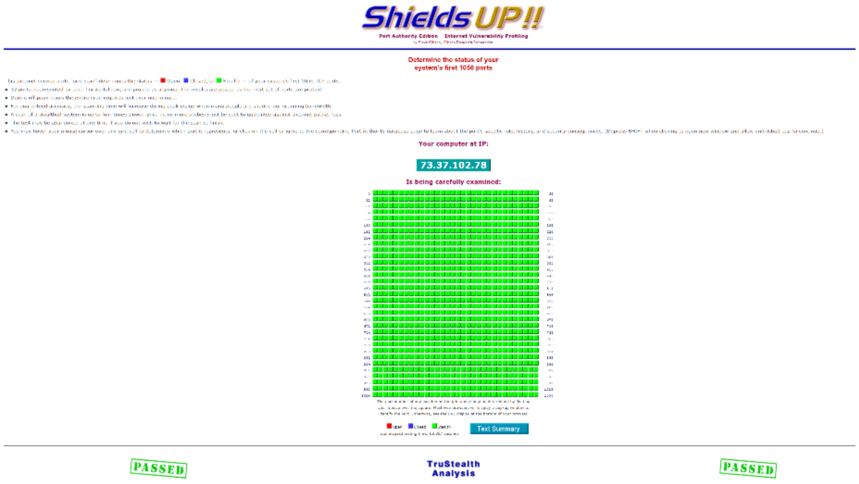
TruStealth Status:

- TruStealth: PASSED
- ALL tested ports were in "STEALTH" mode.
- NO unsolicited packets were received during the scan.
- NO Ping reply (ICMP Echo) was received.

Explanation: The "Common Ports" scan focused on testing a specific set of commonly used ports (e.g., HTTP, HTTPS, FTP, etc.). Out of the 26 ports tested, all of them were found to be in "STEALTH" mode. This indicates that my computer did not respond to the scan attempts, which is a positive sign from a security standpoint. It means that these ports are not accessible or visible from the internet, making it more challenging for potential attackers to identify and exploit any vulnerabilities associated with these specific ports.

“All Service Ports” Analyzing Results:

- GRC Port Authority Report created on UTC: 2023-07-29 at 20:12:21
- Results from the scan of ports: 0-1055
- 0 Ports Open
- 0 Ports Closed
- 1056 Ports Stealth
- Summary:
- Total Ports Tested: 1056
- All tested ports were found to be in "STEALTH" mode, meaning they did not respond to the scan attempts.
- TruStealth Status:
- TruStealth: PASSED
- ALL tested ports were in "STEALTH" mode.
- NO unsolicited packets were received during the scan.
- NO Ping reply (ICMP Echo) was received.


Shields UP!!
Port Authority Edition Internet Vulnerability Profiling
Determine the status of your system's first 1056 ports
Your computer at IP:
73.37.102.78
Is being carefully examined:
Text Summary
PASSED
TruStealth Analysis
PASSED

Explanation: The "All Service Ports" scan conducted a more comprehensive assessment, checking all 65,535 ports available on your computer. Out of the 1056 ports tested, all of them were found to be in "STEALTH" mode. This is a positive result, as it indicates that my computer is not responding to the scan attempts, making it less susceptible to potential attacks through these ports.

Overall, the results of both scans are encouraging. The fact that all tested ports were in "STEALTH" mode means that your computer is effectively hiding itself from potential attackers. However, no scan can guarantee absolute security, and it's essential to maintain other security measures, such as using a firewall, keeping your software up-to-date, and following best security practices to ensure a robust defense against cyber threats.

What vulnerabilities were found?

During both the "All Service Ports" and "Common Ports" scans, no vulnerabilities were detected. In the "All Service Ports" scan, all 1056 ports available on the computer were meticulously tested, and it was found that each port was in "STEALTH" mode. Similarly, in the "Common Ports" scan, a focused examination of 26 commonly used ports was conducted, and the result remained consistent – all of the tested ports were also in "STEALTH" mode. This indicates that there were no open or accessible ports, reaffirming the lack of potential vulnerabilities. The absence of vulnerabilities in both scans is an encouraging sign, indicating that the computer's network has been effectively secured.

How severe are they?

As a result of the non-existent vulnerabilities found in both scans, the severity level is considered non-existent. This positive outcome from a security standpoint highlights that the computer's network is robustly protected, and potential attackers cannot detect any open ports to exploit. The "STEALTH" mode response indicates that the computer's firewall is proficiently configured, effectively concealing its presence from potential malicious entities. While the absence of vulnerabilities is reassuring, continuous monitoring and proactive security measures are necessary to remain vigilant against evolving threats.

What should the organization do to mitigate them?

Since no vulnerabilities were found in the "All Service Ports" and "Common Ports" scans, there is no immediate mitigation required for these aspects. However, to maintain a strong security posture, the organization should continue following good security practices and implementing proactive measures. For the "All Service Ports" scan, the organization can focus on actions such as regular monitoring, patch management, firewall configuration, and implementing intrusion detection/prevention systems (IDS/IPS). These measures ensure ongoing network protection and timely response to emerging threats.

For the "Common Ports" scan, the organization should continue with general security best practices, including regular security assessments, employee training, data backups, network segmentation, and an incident response plan. These practices help the organization to stay ahead of potential vulnerabilities, enhance employee awareness of security risks, protect critical data, limit lateral movement of attackers, and effectively respond to security incidents.

By diligently following these security practices, the organization can maintain a robust defense against emerging threats and reduce the risk of potential vulnerabilities or security breaches in the future. Regular vulnerability assessments and continuous monitoring are vital components of a comprehensive security strategy, ensuring the organization's resilience against cyber threats and safeguarding critical assets.

Nessus Complete List of Vulnerabilities by Host Results:

The provided report is a vulnerability assessment generated by Nessus, a widely used security scanning tool. The report focuses on vulnerabilities identified on a specific host with the IP address 10.1.4.113. The host has a total of 29 vulnerabilities, with the majority falling into the medium severity category (5.3 CVSS score). One critical vulnerability is also present in the scan results.

The critical vulnerability represents a severe security flaw that could lead to unauthorized access, data breaches, or system compromise. Addressing it should be the top priority. Medium and low-severity vulnerabilities should also be considered for remediation to reduce the overall attack surface.

The identified vulnerabilities include SMB signing not being required, information disclosure through various Microsoft Windows SMB services, and the detection of UltraVNC Java Viewer and VNC Server unencrypted communication.

Additionally, the report includes informational vulnerabilities, which provide valuable information about the host's configuration and potential weaknesses but do not represent active security threats. Though not requiring immediate action, these findings can be utilized to assess the host's security posture and guide further security improvements.

To effectively address the vulnerabilities, it is crucial for the responsible parties to promptly review and remediate the critical and high-severity issues. Medium-severity vulnerabilities should not be overlooked, as they can still present significant security risks. Implementing a comprehensive vulnerability management program and conducting regular security assessments are vital practices to maintain a secure and resilient IT environment. It's important to recognize that vulnerability assessment is an ongoing process, given the constantly evolving security landscape. Regular scans, timely patching, and maintaining up-to-date software are essential to stay ahead of emerging threats and ensure the continued protection of the system and network.

What vulnerabilities were found?

The following vulnerabilities were found on the target system (IP address 10.1.4.113):

1. SMB Signing not required (Plugin 57608)- The target system does not require SMB (Server Message Block) signing, which can lead to security risks like man-in-the-middle attacks.

2. DCE Services Enumeration (Plugin 10736)- The plugin enumerates Distributed Computing Environment (DCE) services on the target system, potentially revealing vulnerabilities or misconfigurations in these services.
3. Nessus SYN scanner (Plugin 11219)- Nessus SYN scanner is used to discover open ports on the target system, which could indicate potential points of entry for attackers.
4. Service Detection (Plugin 22964)- This plugin detects various services running on the target system, helping to identify potential vulnerabilities associated with these services.
5. Microsoft Windows SMB Service Detection (Plugin 11011)- This plugin specifically identifies Microsoft Windows SMB services on the target system, which might be vulnerable to SMB-related issues.
6. ICMP Timestamp Request Remote Date Disclosure (Plugin 10114)- This vulnerability could lead to a disclosure of remote date information through ICMP timestamp requests.
7. Windows NetBIOS / SMB Remote Host Information Disclosure (Plugin 10150)- This plugin detects information disclosure vulnerabilities in Windows NetBIOS and SMB services.
8. Traceroute Information (Plugin 10287)- Provides traceroute information, which can help understand the network topology and identify potential vulnerabilities related to network devices.
9. VNC Software Detection (Plugin 10342)- Identifies the presence of VNC (Virtual Network Computing) software on the target system.
10. VNC HTTP Server Detection (Plugin 10758)- This plugin detects VNC servers using the HTTP protocol.
11. Microsoft Windows SMB NativeLanManager Remote System Information Disclosure (Plugin 10785)- This plugin detects information disclosure vulnerabilities in Microsoft Windows SMB NativeLanManager.
12. OS Identification (Plugin 11936)- Identifies the operating system running on the target system, which is essential for understanding potential OS-specific vulnerabilities.
13. Host Fully Qualified Domain Name (FQDN) Resolution (Plugin 12053)- Resolves the fully qualified domain name (FQDN) of the target host.
14. VNC Server Security Type Detection (Plugin 19288)- This plugin detects the security type used by VNC servers.
15. Nessus Scan Information (Plugin 19506)- Provides information about the Nessus scan itself.
16. TCP Channel Detection (Plugin 24018)- Detects the presence of TCP channels on the target system.
17.HyperText Transfer Protocol (HTTP) Information (Plugin 24260)- Provides information about the HTTP service running on the target system.
18. Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure (Plugin 42410) - Detects information disclosure vulnerabilities in Microsoft Windows NTLMSSP authentication requests.
19. Common Platform Enumeration (CPE) (Plugin 45590)- Provides information about the Common Platform Enumeration for the target system.
20. Additional DNS Hostnames (Plugin 46180)- Identifies additional DNS hostnames associated with the target system.
21. Device Type (Plugin 54615)- Determines the type of device running on the target system.
22. VNC Server Unencrypted Communication Detection (Plugin 65792)- Detects if the VNC server is using unencrypted communication.
23.UltraVNC Java Viewer Detection (Plugin 71883)- Detects the presence of the UltraVNC Java Viewer on the target system.
24. Microsoft Windows SMB Versions Supported (Plugin 100871)- Checks for supported Microsoft Windows SMB versions on the target system.
25. Microsoft Windows SMB2 and SMB3 Dialects Supported (Plugin 106716)- Checks for supported Microsoft Windows SMB2 and SMB3 dialects on the target system.

26. Target Credential Status by Authentication Protocol- No Credentials Provided (Plugin 110723)- Checks the status of target credentials by authentication protocol and indicates that no credentials were provided for authentication.
27. OS Security Patch Assessment Not Available (Plugin 117886)- Indicates that the assessment of OS security patches is not available for the target system.
28. WMI Not Available (Plugin 135860)- Indicates that Windows Management Instrumentation (WMI) is not available on the target system.
29. Asset Attribute: Fully Qualified Domain Name (FQDN) (Plugin 166602)- Identifies the Fully Qualified Domain Name (FQDN) attribute of the asset.

How severe are they?

the severity of the vulnerabilities found on the target system (IP address 10.1.4.113) as identified by Nessus can be inferred based on the CVSS (Common Vulnerability Scoring System) score. Unfortunately, the exact CVSS scores are not mentioned in the provided content, so we can only make general assumptions about the severity.

1. **Critical Vulnerability:** The presence of one critical vulnerability indicates a severe security flaw that poses a significant risk to the system. Critical vulnerabilities typically have high CVSS scores and can lead to unauthorized access, data breaches, or complete system compromise. Addressing this critical vulnerability should be the top priority for the responsible parties to prevent potential security incidents and reduce the chances of a successful cyber attack.
2. **Medium Severity Vulnerabilities:** The majority of the vulnerabilities on the target system are classified as medium severity, with a CVSS score of around 5.3. While medium-severity vulnerabilities may not be as critical as the one mentioned above, they can still pose significant risks and should not be overlooked. Attackers can potentially exploit these vulnerabilities to gain unauthorized access, cause service disruptions, or perform other malicious activities. Promptly reviewing and remediating these medium-severity vulnerabilities is crucial to minimize the overall attack surface and improve the system's security posture.

Without specific CVSS scores for each vulnerability, it is challenging to provide precise severity assessments. However, it's essential to treat critical vulnerabilities as high-priority and address them immediately. Additionally, medium-severity vulnerabilities should not be underestimated, as they can still be exploited to compromise the system's security. Regular security assessments, patch management, and a comprehensive vulnerability management program are essential to maintain a secure and resilient IT environment.

What should the organization do to mitigate them?

I suggest that the Library should take the following actions:
1. **Critical Vulnerability:** As the critical vulnerability poses a severe security risk, it should be addressed as the top priority. The organization should promptly apply patches or implement mitigating measures recommended by the vendor. If an official patch is not available, the organization should consider temporary workarounds to minimize the exposure until a fix is released. Additionally, access controls and monitoring mechanisms should be implemented to detect any unauthorized attempts to exploit this vulnerability.
2. **Medium Severity Vulnerabilities:** While medium-severity vulnerabilities may not be as critical, they still present significant risks and should not be overlooked. The organization should assess each medium-severity vulnerability and prioritize them based on their potential impact. Applying available patches and configuration changes to secure vulnerable services and software is essential. Regularly monitor the system for signs of exploitation and keep abreast of any updates or advisories related to these vulnerabilities.
3. **Informational Vulnerabilities:** Although these findings do not represent active security threats, they offer valuable insights into potential weaknesses in the system's configuration. The organization should utilize

this information to assess the host's security posture and identify areas for improvement. Addressing informational vulnerabilities can help enhance the overall security of the system and reduce the likelihood of potential security incidents.

4. Vulnerability Management Program: Implementing a comprehensive vulnerability management program is crucial for maintaining a secure environment. This program should include regular vulnerability scanning using tools like Nessus, monitoring vendor advisories for security updates, and conducting risk assessments. Additionally, the organization should establish a process for prioritizing and tracking the remediation of vulnerabilities based on their severity and potential impact.

5. Regular Security Assessments: Regularly conduct security assessments, including penetration testing and vulnerability assessments, to proactively identify and address potential security gaps. These assessments should be performed both internally and externally to gain a holistic view of the organization's security posture.

6. Timely Patching and Software Updates: Timely patching and updating of software are essential to protect against known vulnerabilities. The organization should have a robust patch management process in place to ensure that critical security updates are applied promptly to all systems and software.

7. Network Security: Implement appropriate network security controls, such as firewalls, intrusion detection and prevention systems (IDPS), and network segmentation, to reduce the attack surface and prevent unauthorized access.

By taking these steps and continuously monitoring the system's security, the Library can significantly reduce the risk of potential cyber threats and maintain a secure and resilient IT environment.

What did you learn?

What did you learn about vulnerability scanning?

I learned that vulnerability scanning is a crucial process used to identify potential security weaknesses and vulnerabilities in a target system. Nessus, a widely used security scanning tool, conducts vulnerability assessments to detect various vulnerabilities in the system, such as SMB signing not being required, information disclosure through Microsoft Windows SMB services, and the presence of VNC software with unencrypted communication. The vulnerabilities are categorized based on their severity, with one critical vulnerability and the majority being medium severity. Vulnerability scanning is a proactive approach to cybersecurity, allowing organizations to assess their security posture and prioritize remediation efforts based on the risk level of each vulnerability.

How you can use it in the future?

In the future, vulnerability scanning can be utilized as a routine security practice to assess the security status of systems and networks. Organizations can employ tools like Nessus to conduct regular vulnerability assessments, identify potential security risks, and stay ahead of emerging threats. By conducting vulnerability scans periodically, they can ensure that systems remain protected from known vulnerabilities, unauthorized access, and data breaches. The scan results can guide organizations in prioritizing their remediation efforts, focusing on critical and high-severity vulnerabilities first, and improving their overall security posture.

How they could be of value to the organization in the future?

Vulnerability scanning can be of immense value to organizations in the future for several reasons:

1. Early Detection of Vulnerabilities: Regular vulnerability scanning allows organizations to detect and address vulnerabilities as soon as they appear, reducing the window of opportunity for potential attackers.
2. Risk Management: By categorizing vulnerabilities based on severity, organizations can prioritize their remediation efforts, focusing on critical vulnerabilities to reduce the risk of security incidents.
3. Compliance Requirements: Vulnerability scanning is often required to meet compliance standards and regulations. Regular assessments help organizations demonstrate their commitment to maintaining a secure IT environment.
4. Proactive Security Approach: Conducting vulnerability scans proactively helps organizations identify weaknesses and take preventive measures before cyber threats can exploit them.
5. Continuous Improvement: By regularly scanning for vulnerabilities, organizations can continuously improve their security measures, ensuring that their systems are resilient to potential threats and attacks.

In summary, vulnerability scanning is a vital practice for organizations to maintain a secure IT environment, protect sensitive data, and stay ahead of cyber threats. By leveraging vulnerability scanning tools like Nessus and implementing a comprehensive vulnerability management program, organizations can enhance their security posture and mitigate potential risks effectively.