SCOTT
MACLEAN

NOVEMBER 2024

VULNERABILITY ASSESSMENT REPORT

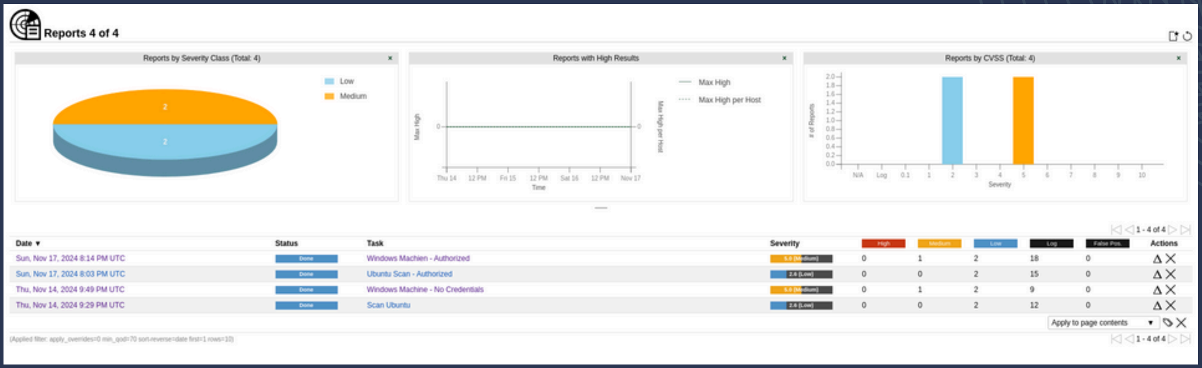
TABLE OF CONTENTS

EXECUTIVE SUMMARY

This assessment was conducted to evaluate the organization's current security posture and identify potential vulnerabilities that could expose the organization to cyber threats. By analyzing system configurations, network traffic, and security policies, and leveraging frameworks like CVSS, MITRE ATT&CK, and NIST RMF, we aimed to assess the organization's ability to protect sensitive data and critical systems.

To mitigate these vulnerabilities, we recommend prioritizing remediation efforts based on CVSS scores and correlating them to common attack vectors outlined in MITRE ATT&CK. Additionally, we propose implementing security controls aligned with NIST RMF to strengthen the organization's overall security posture.

SCAN RESULTS



Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sun, Nov 17, 2024 8:14 PM UTC	Done	Windows Machien - Authorized	5.0 (Medium)	0	1	2	18	0	Δ ✕
Sun, Nov 17, 2024 8:03 PM UTC	Done	Ubuntu Scan - Authorized	2.6 (Low)	0	0	2	15	0	Δ ✕
Thu, Nov 14, 2024 9:49 PM UTC	Done	Windows Machine - No Credentials	5.0 (Medium)	0	1	2	9	0	Δ ✕
Thu, Nov 14, 2024 9:29 PM UTC	Done	Scan Ubuntu	2.6 (Low)	0	0	2	12	0	Δ ✕

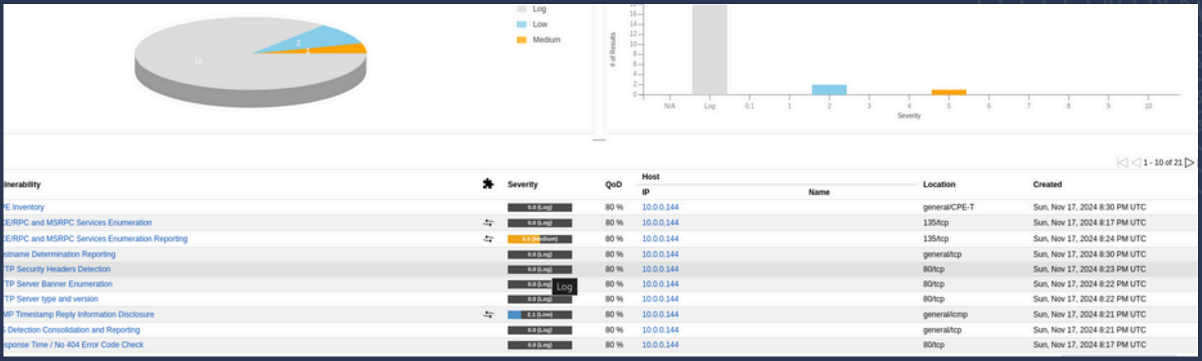
(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

Fig 1.1

Figure 1.1 provides a visual representation of the vulnerability scans conducted on two target machines: Ubuntu and Windows. A total of four scans were performed, utilizing OpenVAS, a comprehensive vulnerability assessment tool. To ensure accurate results, the firewall on both machines was temporarily disabled, and network connectivity was verified using a ping test.

The scans were executed using the full and fast operation modes, with and without authentication credentials. The results indicate the presence of five vulnerabilities across both machines. By employing this systematic approach, we were able to gain valuable insights into the security posture of the target systems.

SCAN RESULTS



lnerability		Severity	QoD	Host		Location	Created
				IP	Name		
PE Inventory		0.0 (Log)	80 %	10.0.0.144		general/CPE-T	Sun, Nov 17, 2024 8:30 PM UTC
CE/RPC and MSRPC Services Enumeration	⇆	0.0 (Log)	80 %	10.0.0.144		135/tcp	Sun, Nov 17, 2024 8:17 PM UTC
CE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.0.0.144		135/tcp	Sun, Nov 17, 2024 8:24 PM UTC
stname Determination Reporting		0.0 (Log)	80 %	10.0.0.144		general/tcp	Sun, Nov 17, 2024 8:30 PM UTC
TP Security Headers Detection		0.0 (Log)	80 %	10.0.0.144		80/tcp	Sun, Nov 17, 2024 8:23 PM UTC
TP Server Banner Enumeration		0.0 (Log)	80 %	10.0.0.144		80/tcp	Sun, Nov 17, 2024 8:22 PM UTC
TP Server type and version		0.0 (Log)	80 %	10.0.0.144		80/tcp	Sun, Nov 17, 2024 8:22 PM UTC
MP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	10.0.0.144		general/icmp	Sun, Nov 17, 2024 8:21 PM UTC
Detection Consolidation and Reporting		0.0 (Log)	80 %	10.0.0.144		general/tcp	Sun, Nov 17, 2024 8:21 PM UTC
sponse Time / No 404 Error Code Check		0.0 (Log)	80 %	10.0.0.144		80/tcp	Sun, Nov 17, 2024 8:17 PM UTC

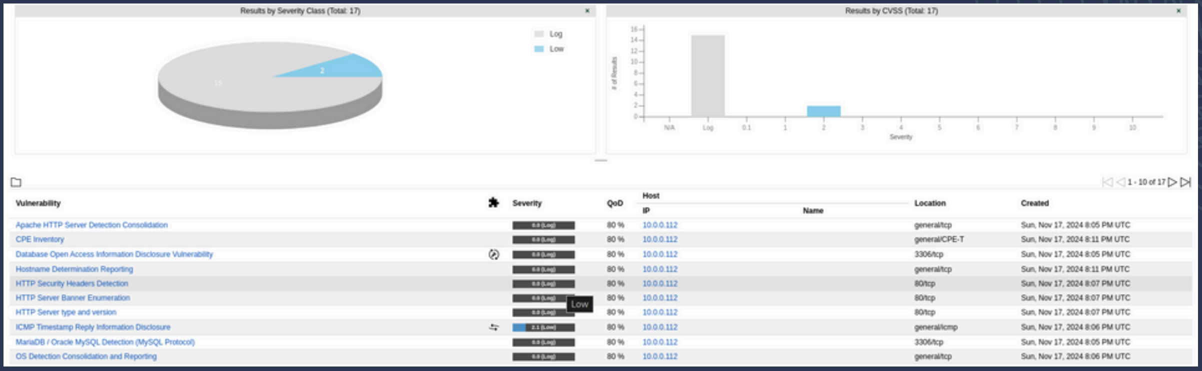
Fig 1.2

Fig 1.2 shows a list of vulnerabilities identified in the vulnerability scan using OpenVAS on the windows machine using full login credentials. The results are categorized primarily by severity level.

- Low: Less serious vulnerabilities that may not pose an immediate threat.
- Medium: Moderate-severity vulnerabilities that could potentially be exploited.
- High: Critical vulnerabilities that could lead to significant security breaches.

We have found that there is a medium severity risk having to do with the open 135 port with the vulnerability being DCE/RPC and MSRPC Services Enumeration Reporting. This vulnerability indicates that the system is vulnerable to enumeration attacks, where an attacker can gather information about the services running on the system and can expose sensitive information about the system. This was given a score of 5.0 which directly relates to the CVSS[1] score given by NIST.

SCAN RESULTS



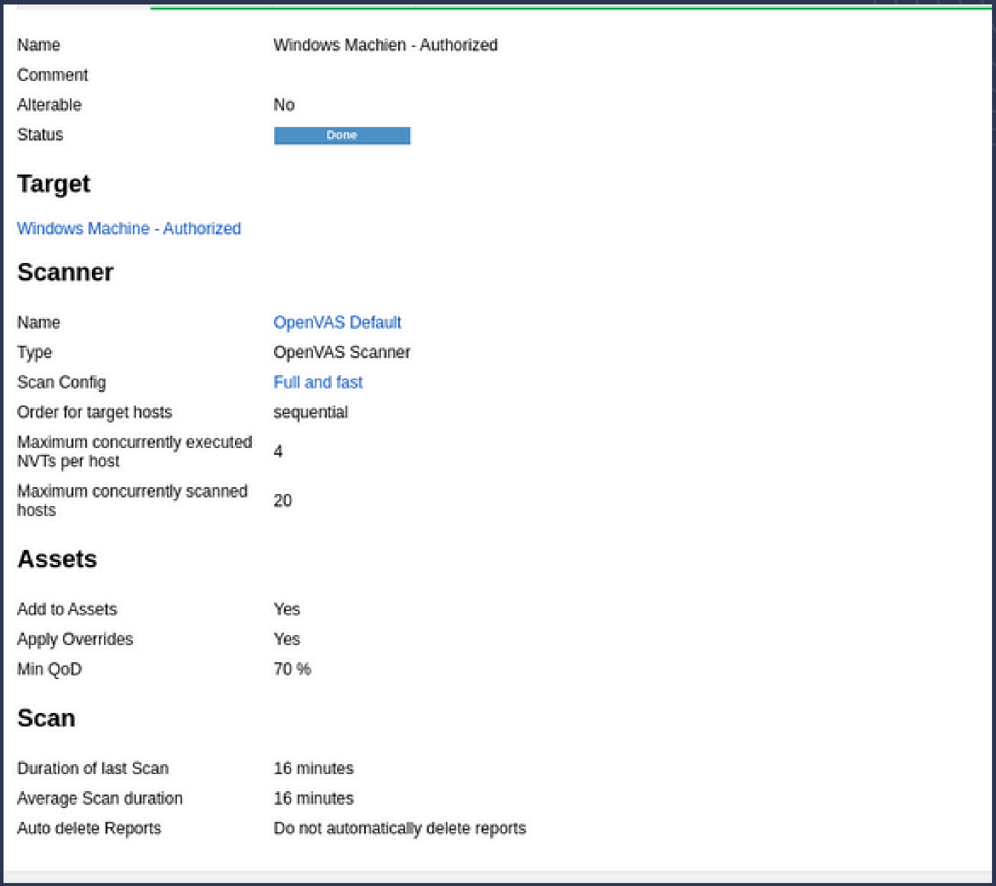
1 - 10 of 17

Vulnerability		Severity	QoD	Host		Location	Created
				IP	Name		
Apache HTTP Server Detection Consolidation		0.0 (Log)	80 %	10.0.0.112		general/tcp	Sun, Nov 17, 2024 8:05 PM UTC
CPE Inventory		0.0 (Log)	80 %	10.0.0.112		general/CPE-T	Sun, Nov 17, 2024 8:11 PM UTC
Database Open Access Information Disclosure Vulnerability		0.0 (Log)	80 %	10.0.0.112		3306/tcp	Sun, Nov 17, 2024 8:05 PM UTC
Hostname Determination Reporting		0.0 (Log)	80 %	10.0.0.112		general/tcp	Sun, Nov 17, 2024 8:11 PM UTC
HTTP Security Headers Detection		0.0 (Log)	80 %	10.0.0.112		80/tcp	Sun, Nov 17, 2024 8:07 PM UTC
HTTP Server Banner Enumeration		0.0 (Log)	80 %	10.0.0.112		80/tcp	Sun, Nov 17, 2024 8:07 PM UTC
HTTP Server type and version		0.0 (Log)	80 %	10.0.0.112		80/tcp	Sun, Nov 17, 2024 8:07 PM UTC
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	10.0.0.112		general/icmp	Sun, Nov 17, 2024 8:06 PM UTC
MariaDB / Oracle MySQL Detection (MySQL Protocol)		0.0 (Log)	80 %	10.0.0.112		3306/tcp	Sun, Nov 17, 2024 8:05 PM UTC
OS Detection Consolidation and Reporting		0.0 (Log)	80 %	10.0.0.112		general/tcp	Sun, Nov 17, 2024 8:06 PM UTC

Fig 1.3

Fig 1.3 shows the report for the full and fast scan done on the Ubuntu system using full login credentials. It shows that we have 1 low severity vulnerability with a CVSS score of 2.1. This vulnerability has been identified as ICMP Timestamp Reply Information Disclosure. This vulnerability exposes system information, such as the system's timestamp, which could be used in timing attacks or other forms of reconnaissance.

METHODOLOGY



Name	Windows Machien - Authorized
Comment	
Alterable	No
Status	Done

Target

Windows Machine - Authorized

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	sequential
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	16 minutes
Average Scan duration	16 minutes
Auto delete Reports	Do not automatically delete reports

Fig 1.4

Fig 1.4 Shows the scan settings that were conducted on each machine using OpenVAS software. The settings used for both the windows and ubuntu machine were the same with the only difference being the IP address for the target. We could have done both the Ubuntu and Windows machine under the same scan using the IP range tool in OpenVAS as the login credentials are the same, but we opted to separate them to give a better view of what vulnerability was on each machine. We used the full and fast scan to give us a comprehensive view of each machine. We made sure to temporarily disable each target systems firewall for the test and sending a ping to each target to make sure they could receive packets which would also verify we could conduct a scan on them.

FINDINGS

We successfully conducted vulnerability scans on both the Windows and Ubuntu systems using OpenVAS. The Windows scan, which took approximately 16 minutes, and the Ubuntu scan, which took approximately 7 minutes, yielded consistent results. Both authorized and unauthorized scans revealed the same number of vulnerabilities. However, the authorized scans provided additional information, including a few low-severity log files that were not identified in the unauthorized scans.

RISK ASSESSMENT

Name	Newest Result	Severity ▼	QoD	Results	Hosts
DCE/RPC and MSRPC Services Enumeration Reporting	Sun, Nov 17, 2024 8:24 PM UTC	5.0 (Medium)	80 %	2	1
TCP Timestamps Information Disclosure	Sun, Nov 17, 2024 8:22 PM UTC	2.6 (Low)	80 %	4	2
ICMP Timestamp Reply Information Disclosure	Sun, Nov 17, 2024 8:21 PM UTC	2.1 (Low)	80 %	4	2
Services	Sun, Nov 17, 2024 8:16 PM UTC	0.0 (Log)	80 %	5	2
SSH Authorization Check	Sun, Nov 17, 2024 8:17 PM UTC	0.0 (Log)	80 %	2	2
Unknown OS and Service Banner Reporting	Sun, Nov 17, 2024 8:23 PM UTC	0.0 (Log)	80 %	3	1
HTTP Server Banner Enumeration	Sun, Nov 17, 2024 8:22 PM UTC	0.0 (Log)	80 %	3	2
HTTP Security Headers Detection	Sun, Nov 17, 2024 8:23 PM UTC	0.0 (Log)	80 %	3	2
CPE Inventory	Sun, Nov 17, 2024 8:30 PM UTC	0.0 (Log)	80 %	4	2
HTTP Server type and version	Sun, Nov 17, 2024 8:22 PM UTC	0.0 (Log)	80 %	3	2
Hostname Determination Reporting	Sun, Nov 17, 2024 8:30 PM UTC	0.0 (Log)	80 %	4	2
DCE/RPC and MSRPC Services Enumeration	Sun, Nov 17, 2024 8:17 PM UTC	0.0 (Log)	80 %	2	1
Database Open Access Information Disclosure Vulnerability	Sun, Nov 17, 2024 8:05 PM UTC	0.0 (Log)	80 %	2	1
Response Time / No 404 Error Code Check	Sun, Nov 17, 2024 8:17 PM UTC	0.0 (Log)	80 %	1	1
MariaDB / Oracle MySQL Detection (MySQL Protocol)	Sun, Nov 17, 2024 8:05 PM UTC	0.0 (Log)	80 %	2	1
OS Detection Consolidation and Reporting	Sun, Nov 17, 2024 8:21 PM UTC	0.0 (Log)	80 %	4	2
SSH Login Failed For Authenticated Checks	Sun, Nov 17, 2024 8:22 PM UTC	0.0 (Log)	80 %	2	2
Apache HTTP Server Detection Consolidation	Sun, Nov 17, 2024 8:05 PM UTC	0.0 (Log)	80 %	2	1
Web Application Scanning Consolidation / Info Reporting	Sun, Nov 17, 2024 8:24 PM UTC	0.0 (Log)	80 %	2	2
SMB Remote Version Detection	Sun, Nov 17, 2024 8:22 PM UTC	0.0 (Log)	80 %	2	1
SMB/CIFS Server Detection	Sun, Nov 17, 2024 8:17 PM UTC	0.0 (Log)	80 %	4	1
HTTP Server type and version	Sun, Nov 17, 2024 8:22 PM UTC	0.0 (Log)	80 %	3	2

Fig 1.5

RISK ASSESSMENT

Fig 1.5 gave a list of all the scanned vulnerabilities on your companies systems. From these scans, we have determined that there are 3 vulnerabilities that should be patched and we will give our recommendations on why.

Highest Priority

DCE/RPC and MSRPC Services Enumeration Reporting:

This Vulnerability had a CVSS score of 5.0 making it the highest severity vulnerability in our scan. What this vulnerability means is that a system (Windows) is exposing information about its running services. This information can be valuable to attackers as it can reveal potential vulnerabilities and attack vectors.

We have identified that this vulnerability commonly is used by threat actors to pinpoint running applications and services on a system to tailor an attack as specified in Mitre Technique T1010[2]- Application Window Discovery.

Medium Priority

TCP Timestamps Information Disclosure:

This vulnerability occurs when a system is configured to send timestamps in TCP packets. While timestamps can be useful for certain network diagnostics, they can also expose sensitive information about the system such as system uptime, network round trip time and system clock synchronization.

The MITRE ATT&CK technique most closely associated with this vulnerability is also T1010. While this technique primarily focuses on discovering running applications and services on a system, it can also be used to gather information about the system's configuration, including network parameters like TCP timestamps.

RISK ASSESSMENT

Medium Priority

ICMP Timestamp Reply Information Disclosure:

This vulnerability occurs when a system responds to ICMP Timestamp Requests with detailed timestamps. These timestamps can reveal sensitive information about the system such as system uptime and clock synchronization.

The MITRE ATT&CK most commonly associated with this is T0043[3] System Reconnaissance: This technique encompasses a wide range of activities that attackers use to gather information about a target system, including scanning for vulnerabilities, identifying running services, and collecting system information.

In the next section, we give recommendations for how we can patch these vulnerabilities and further recommendation to improve the security posture of your organization.

RECOMMENDATIONS

The identified vulnerabilities, DCE/RPC and MSRPC Services Enumeration Reporting, TCP Timestamps Information Disclosure, and ICMP Timestamp Reply Information Disclosure, pose potential security risks to the system. These vulnerabilities can be exploited by attackers to gather sensitive information about the system and potentially launch further attacks.

To mitigate these vulnerabilities and enhance the overall security posture, the following strategies should be implemented:

Patch Management:

- Prioritize Critical Patches: Prioritize the installation of security patches that address the identified vulnerabilities.
- Regular Patching Schedule: Establish a regular patching schedule to ensure timely application of security updates.
- Patch Testing: Test security patches in a controlled environment to minimize the risk of unintended consequences.

Network Segmentation:

- Isolate Critical Systems: Isolate 4 critical systems and services from the public internet if possible, into their own VLAN, to reduce the attack surface.

Firewall Configuration:

- Restrict Network Access: Configure firewalls to restrict inbound and outbound traffic to only necessary services.
- Block Unnecessary Ports: Block ports that are not required for essential services, such as those used for RPC and ICMP.

System Configuration:

- Disable Unnecessary Services: Disable or remove unnecessary services to reduce the attack surface.
- Configure Services Securely: Configure services with strong security settings, such as complex passwords and encryption.
- Disable Unnecessary Protocols: Disable protocols like ICMP timestamp replies that are not essential for system operation.

Monitoring and Logging:

- Implement Security Information and Event Management (SIEM): Use SIEM sensors such as ones provided by PRTG to monitor network traffic and system logs for signs of malicious activity.
- Enable Detailed Logging: Configure systems to log detailed information about security events, including failed login attempts, unauthorized access, and system anomalies.
- Regularly Review Logs: Regularly review logs to identify potential security incidents and threats.

RECOMMENDATIONS

Based on the identified vulnerabilities and the general security recommendations provided, here are some specific NIST RMF security controls that can be implemented to further strengthen the security posture:

AC-2: Access Control Policy and Procedures: Develop and implement comprehensive access control policies and procedures to restrict access to authorized individuals.

5

AC-3: Identification and Authentication: Implement strong authentication mechanisms, such as multi-factor authentication, to verify user identities.

SA-6: Security Testing and Assessment: Conduct regular vulnerability assessments and penetration testing to identify and address security weaknesses.

SI-10: Information Integrity: Implement measures to protect the integrity of information, such as data backups and data recovery procedures.

SI-11: System Integrity: Implement measures to protect the integrity of system software and hardware, including regular patching and configuration management.

SC-7: Boundary Protection: Implement network security controls, such as firewalls and intrusion detection systems, to protect the system from unauthorized access.

SC-8: Controlled Access and Services: Restrict network access to authorized users and services.

SC-11: Secure Configuration: Implement secure configuration practices to minimize vulnerabilities.

CITATIONS AND REFERENCES

1. Common Vulnerability Scoring System Calculator. NVD. (n.d.). https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

2. Application window discovery. Application Window Discovery, Technique T1010 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1010/

3. Reconnaissance. Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/TA0043/

4. Segment the network based on sensitivity - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2023, December 23). https://csf.tools/reference/critical-security-controls/version-7-1/csc-14/csc-14-1/

5. Access Enforcement - CSF Tools. CSF Tools - The Cybersecurity Framework for Humans. (2021, March 5). https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-3/