PENETRATION TEST REPORT

Prepared by Protecly

Prepared for: Microsoft, Windows Server 2012

V1.0 November | 16 | 2024

Protecly
www.Protecly.com

Windows server 2012, Microsoft
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2

Protecly
Email: Contact@protecly.com - Web: www.protecly.com

Table of Contents

DOCUMENT CONTROL

Issue Control			
Document Reference	N/A	**Project #**	N/A
Issue	1.0	**Date**	November 16, 2024
Classification	Public	**Author**	Lucas Audette
Document Title	Windows server 2012 Penetration Test		
Approved by			
Released by	Lucas Audette		

Owner Details	
Name	**Lucas Audette**
Office/Region	**Worcester MA, USA**
Contact Number	**000-000-0000**
E-mail Address	**Lucas.Audette@assumption.edu**

Revision History			
Issue	**Date**	**Author**	**Comments**
1.0	November 16, 2024	Lucas Audette	N/A

Executive Summary

Protecly conducted a comprehensive security assessment of Microsoft's Windows Server 2012 in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use. The purpose of this penetration test is to identify vulnerabilities on a Windows Server 2012 environment using Nessus vulnerability scanning. This assessment evaluates the server's security posture and provides actionable recommendations to mitigate identified risks.

Key Findings:

- Total of 13 informational-level findings identified
- Vulnerabilities primarily are service, system enumeration and information disclosure
- No other severity vulnerabilities other than information types were revealed.

Although no directly exploitable issues were found, the disclosure of system and network information could assist attackers in recon. Efforts.

Methodology:

1. Tools used:
    a. Nessus Essentials (Advanced Scan)
2. Steps Taken:
    a. Configured Nesus to conduct an advanced scan of Windows Server 2012
    b. Collected vulnerability information that focused on open ports, services, and system details
3. Limitations:
4. Conducted an authentication scan since I am unable to remember the credentials to the Windows server VM. However, I think a credential scan would give more closure into more insights.

Scope of work:

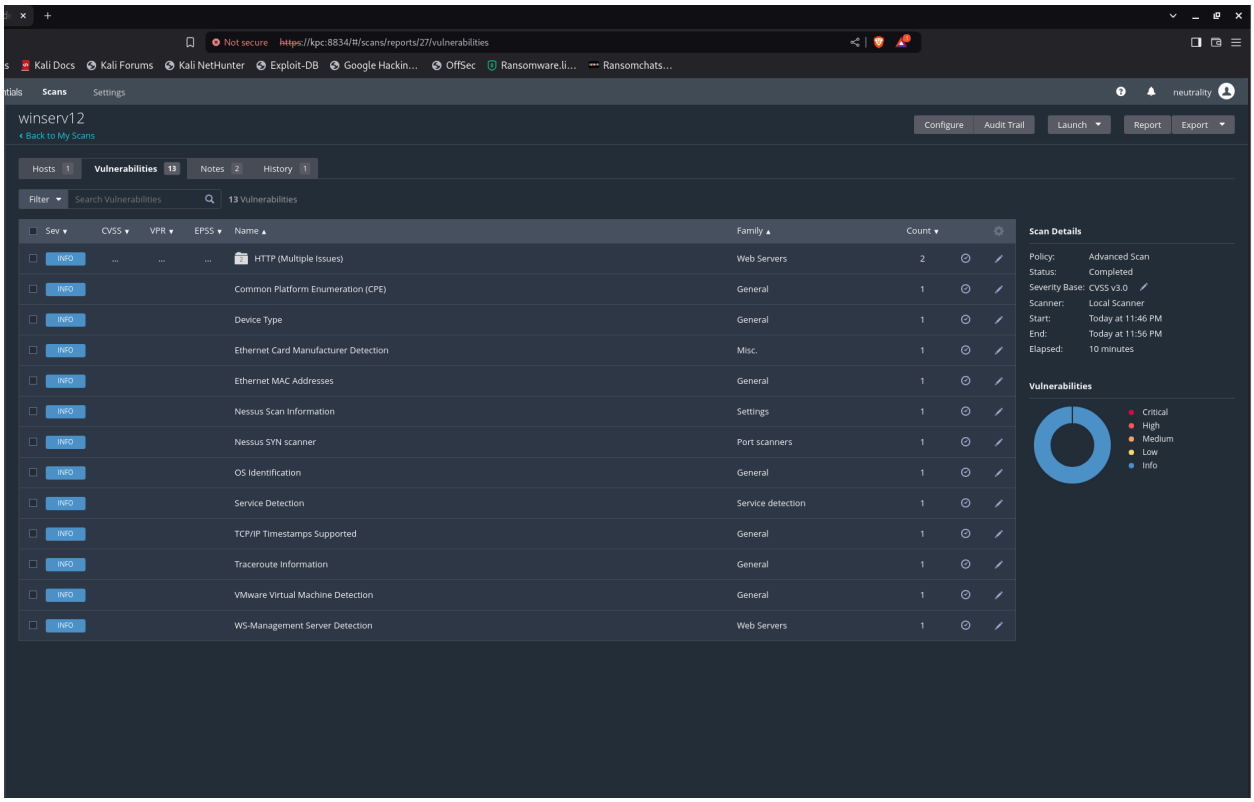
- Target: Windows server 2012
- Target IP: 192.168.23.5
- Environment: PenTesting Sandbox locally hosted through VMWare
- Scan type: Nessus Advanced Scan
- Assessment Period: Single session (10 minutes time elapsed)

Findings and Information Disclosure:

Reconnaissance and information disclosure

The advanced scan detected 13 information level findings. While the scan did not indicate any exploitable vulnerabilities, they reveal crucial system and service details that could assist attackers during recon.

The screenshot below provides what the scan found:



Recommendations

Mitigate information disclosure risks

In order to minimize the risk of attackers being able to leverage disclosed information, implement the following measures:

1. Disable TCP/IP Timestamps
    a. Risk: Timestamps allow threat actors to estimate system uptime and fingerprint the operating system
    b. Solution: Disable timestamps by modifying the systems tcp stack settings
2. Restrict HTTP Information Disclosure
    a. Risk: HTTP headers reveal server and software information.
    b. Solution: Configure the HTTP Server to minimize headers

3. Enhance service configuration:
    a. Risk: Open services provide information about the systems environment
    b. Solution: Disable unnecessary services and limit access to critical ones using firewalls or ip allow lists
4. Harden network interfaces:
    a. Risk: Exposed MAC addresses and network card details provide attackers with device information.
    b. Solution. Limit network exposure and monitor interface configurations.

Conclusion:

The Nessus Advanced Scan provided valuable insights into the system's exposure. Although no critical or exploitable vulnerabilities were identified, the presence of information disclosure issues highlight areas for security improvement:

- Implement recommended steps to limit information disclosure.
- Conduct a follow-up credentialed scan for deeper analysis.

Enhancing system configuration and minimizing exposed information will significantly improve the security posture of the Windows Server 2012.

7. Appendix

Scan Summary:

- **Scan Type:** Nessus Advanced Scan
- **Tool Used:** Nessus Essentials
- **Scan Duration:** 10 minutes
- **Findings Summary:**
    - **Critical:** 0
    - **High:** 0
    - **Medium:** 0
    - **Low:** 0
    - **Info:** 13

References:

- Nessus Documentation: https://www.tenable.com