

PENETRATION TEST REPORT

Prepared by Protecly

Prepared for: Microsoft, Windows Server 2012

V1.0 November | 16 | 2024



Windows Server® 2012

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



No warranties, express or implied are given by Proteclly respect to accuracy, reliability, quality, correctness, or freedom from error or omission of this work product, including any implied warranties of merchantability, fitness for a specific purpose or non-infringement. This document is delivered "as is", and Proteclly shall not be liable for any inaccuracy thereof. Proteclly does not warrant that all errors in this work product shall be corrected. Except as expressly set forth in any master services agreement or project assignment, Proteclly is not assuming any obligations or liabilities including but not limited to direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of or reliance upon any information in this document. This document does not imply an endorsement of any of the companies or products mentioned. ©2024 Proteclly. All rights reserved. No part of this document may be reproduced, copied or modified without the express written consent of the authors. Unless written permission is expressly granted for other purposes, this document shall be treated at all times as the confidential and proprietary material of Proteclly and may not be distributed or published to any third-party.



Table of Contents

Executive Summary

Methodology

Scope of Work

Findings and Observations

- **4.1 Reconnaissance and Information Disclosure**

Recommendations

Conclusion

Appendix



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

Proteclly 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 Nessus 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:

The screenshot displays the winsev12 web interface. The main section shows a table of 13 vulnerabilities, all categorized as 'Info' level. The table includes columns for Severity, CVSS, VPR, EPSS, Name, Family, and Count. The vulnerabilities listed are:

Sev	CVSS	VPR	EPSS	Name	Family	Count
Info	---	---	---	HTTP (Multiple Issues)	Web Servers	2
Info	---	---	---	Common Platform Enumeration (CPE)	General	1
Info	---	---	---	Device Type	General	1
Info	---	---	---	Ethernet Card Manufacturer Detection	Misc.	1
Info	---	---	---	Ethernet MAC Addresses	General	1
Info	---	---	---	Nessus Scan Information	Settings	1
Info	---	---	---	Nessus SYN scanner	Port scanners	1
Info	---	---	---	OS Identification	General	1
Info	---	---	---	Service Detection	Service detection	1
Info	---	---	---	TCP/IP Timestamps Supported	General	1
Info	---	---	---	Traceroute Information	General	1
Info	---	---	---	VMware Virtual Machine Detection	General	1
Info	---	---	---	WS-Management Server Detection	Web Servers	1

On the right side of the interface, the 'Scan Details' section shows:

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:46 PM
- End: Today at 11:56 PM
- Elapsed: 10 minutes

The 'Vulnerabilities' section features a donut chart showing the distribution of severity levels: 13 Info, 0 Low, 0 Medium, 0 High, and 0 Critical.

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>