Relevant

Security Assessment Findings Report

Business Confidential

Date: January 2th, 2023

Project: 897-19

Version 1.0

# Table of Contents

[Table of Contents 2](#_Toc9866461)

[Confidentiality Statement 3](#_Toc9866462)

[Disclaimer 3](#_Toc9866463)

[Contact Information 3](#_Toc9866464)

[Assessment Overview 4](#_Toc9866465)

[Assessment Components 4](#_Toc9866466)

[External Penetration Test 4](#_Toc9866467)

Internal [Penetration Test](#_Toc9866467) 5

[Finding Severity Ratings 5](#_Toc9866468)

[Scope 6](#_Toc9866469)

[Scope Exclusions 6](#_Toc9866470)

[Client Allowances 6](#_Toc9866471)

[Executive Summary 7](#_Toc9866472)

[Attack Summary 7](#_Toc9866473)

[Security Strengths 8](#_Toc9866474)

[SIEM alerts of vulnerability scans 8](#_Toc9866475)

[Security Weaknesses 8](#_Toc9866476)

[Missing Multi-Factor Authentication 8](#_Toc9866477)

[Weak Password Policy 8](#_Toc9866478)

[Unrestricted Logon Attempts 8](#_Toc9866479)

[Vulnerabilities by Impact 9](#_Toc9866480)

[External Penetration Test Findings 10](#_Toc9866481)

[Insufficient Lockout Policy – Outlook Web App (Critical) 10](#_Toc9866482)

[Additional Reports and Scans (Informational) 13](#_Toc9866483)

# Confidentiality Statement

This document is the exclusive property of Relevant and Demo Security (Demo-Sec). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Relevant and Demo-Sec.

Demo-Sec may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Demo-Sec prioritized the assessment to identify the weakest security controls an attacker would exploit. Demo-Sec recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

|  |  |
| --- | --- |
|  |  |

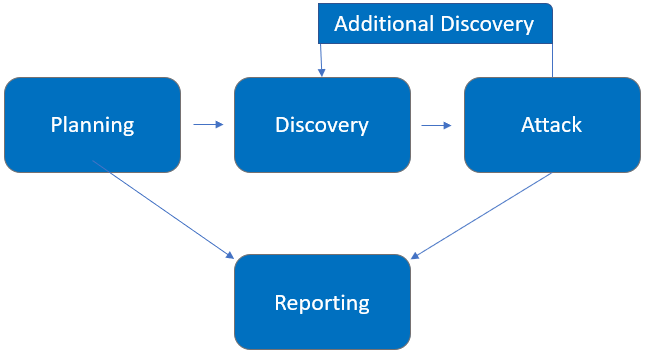
|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| **Relevant** | | |
| John Smith | VP, Information Security (CISO) | Office: (555) 555-5555  Email: [john.smith@](mailto:john.smith@demo.com)relevant.thm |
| Jim Smith | IT Manager | Office: (555) 555-5555  Email: [jim.smith@relevant](mailto:jim.smith@demo.com).thm |
| Joe Smith | Network Engineer | Office: (555) 555-5555  Email: [joe.smith@relevant.](mailto:joe.smith@demo.com)thm |
| **Demo Security** | | |
| Demo Guy | Lead Penetration Tester | Office: (555) 555-5555  Email: demo@demo-sec.com |

# Assessment Overview

From January 2th, 2023 to January 9th, 2023, Relevant engaged Demo-Sec to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Demo-Sec engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

## Internal Penetration Test

An internal penetration test emulates the role of an attacker gained access to the internal network. A Demo-Sec engineer attempts to escalate their privileges, spread malware, steal credentials, leak information, perform man-in-the-middle attacks (MITM) and more to take advantage of their access to internal resources. Although it was prohibited in this assesment, the engineer may also attempt to pivot in the network to gain access to other machines.

## Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| External Black Box Penetration Test | 10.10.54.39 |
| Internal Black Box Penetration Test | 10.10.54.39 |

## Scope Exclusions

Per client request, Demo-Sec did not perform any Denial of Service attacks during testing.

## Client Allowances

Relevant did not provide any allowances to assist the testing.

# Executive Summary

Demo-Sec evaluated Relevant’s external security posture through an external network penetration test from January 2th, 2023 to January 9th, 2023. By leveraging a series of attacks, Demo-Sec found critical level vulnerabilities that allowed full internal access to the Relevant’s provided server. It is highly recommended that Relevant address these vulnerabilities as soon as possible as the vulnerabilities require really low effort to get System access to the machine

## Attack Summary

**First compromise path:**

The following table describes how Demo-Sec gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Got SMB access with anonymous (null) authentication. | Relevant should disable anonymous login to the SMB shares. |
| 2 | Enumerated the files in the SMB server, found a passwords.txt file under //relevant/nt4wrksv/ which had base64 encoded (easily reversible to clear text) credentials (name - password | Relevant should remove the passwords.txt or restrict access to it. |
| 3 | Knowing that nt4 is relevant to windows servers and this is a web server, Demo-Sec tried to find a directory that has the same name as the smb share (nt4wrksv). Demo-Sec found the directory under http://$ip:49663/. Demo-Sec tried to upload a .aspx reverse shell (not obfuscated) via smb (anonymous login) and was successful. | Relevant should disable the write access of the anonymous user to this share and/or disable access to the web directory at port 49663 unless it’s necessary.  Relevant should also configure their Antivirus so that reverse shells can be detected. |
| 4 | After uploading a webshell and navigating to it, Demo-Sec got access to the server as “iis apppool\defaultapppool”.  Further enumeration showed that the user has “SeImpersonatePrivilege”. With this privilege, a potato attack has been tried with “sweet potato” (not obfuscated) and got “nt authority\system”. Further enumeration showed that SweetPotato used its PrintSpoofer mod to escalate privileges. | Demo-Sec recommend Relevant to configure their Antivirus to catch potato attacks and update their system to the latest version. |

**Second compromise path:**

The following table describes how Demo-Sec gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Tested the server against MS17-10 (EternalBlue) with Metasploit’s “windows/smb/ms17\_010\_psexec” module.  The target was vulnerable and Demo-Sec got “nt authority\system” | Demo-Sec recommends Relevant to update the SMB version to the latest and make sure to disable SMBv1. |

# Security Strengths

## SIEM alerts of vulnerability scans

During the external part of the assessment, the Relevant security team was not able to detect Demo-Sec engineers’ vulnerability scans against their systems.

During the internal part of the assessment, the Relevant security team was able to detect malicious PowerShell activities. (AMSI)

# Security Weaknesses

## Unrestricted Logon Attempts

During the assessment, Demo-Sec performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed. Demo-Sec could not get any access with their brute force attempts, but it’s best practice to restrict the number of requests in case someone with more time and resource tries to bruteforce.

## Antivirus is not properly configured

During the assessment, Demo-Sec tried to upload non-obfuscated reverse shells, webshells, exploit and enumeration scripts. Other than PowerShell (which is blocked by AMSI) Demo-Sec was able to run everything with no problem.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

z

## Blackbox Penetration Test Findings

Writable web directory (Critical)

|  |  |
| --- | --- |
| Description: | Relevant allows anonymous SMB users to write to nt4wrksv directory at port 49663 |
| Impact: | Critical |
| System: | 10.10.54.39 |
| References: |  |

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: Users have write access to nt4wrksv via SMB anonymous login. Demo-Sec was able to upload a reverse shell and get access to internal network of Relevant. Demo-Sec recommends Relevant to restrict access to the nt4wrksv directory or disable access to the web directory at port 49663 unless it’s necessary.  Item 2: Demo-Sec was able to upload a non-obsucated reverse shell. Relevant should configure their anti-virus to detect reverse shells. |

MS17-10 – Eternal Blue (Critical)

|  |  |
| --- | --- |
| Description: | Relevant had SMBv1 enabled on their server which allowed Demo-Sec to run “Eternal Blue” and get a shell as “nt authority\system” (full access) |
| Impact: | Critical |
| System: | 10.10.54.39 |
| References: | https://nvd.nist.gov/vuln/detail/cve-2017-0144 – Eternal Blue |

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: SMBv1 is enabled. Demo-Sec recommends Relevant to update their SMB version to the latest.  Item 2: No anti-virus is in place. Demo-Sec was able run non-obfuscated meterpreter shell. Demo-Sec recommends Relevant to configure their anti-virus. |

CVE-2022-21999 Print Spoofer (High)

|  |  |
| --- | --- |
| Description: | Relevant has not patched their server for the “Print Spoofer” vulnerability which allowed Demo-Sec to run “PrintSpoofer.exe” and get a shell as “nt authority\system” (full access) |
| Impact: | High |
| System: | 10.10.54.39 |
| References: | https://nvd.nist.gov/vuln/detail/CVE-2021-36970 – Print Spoofer |

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: The server is not patched. Demo-Sec recommends Relevant to update their Windows version to the latest.  Item 2: No anti-virus was in place. Demo-Sec was able run non-obfuscated PrintSpoofer.exe. Demo-Sec recommends Relevant to configure their anti-virus. |

Insufficient Lockout Policy – SMB/RDP (Moderate)

|  |  |
| --- | --- |
| Description: | Relevant allowed unlimited logon attempts against their SMB and RDP services. Demo-Sec could not get any access with their brute force attempts, but it’s best practice to restrict the number of requests in case someone with more time and resource tries to bruteforce. |
| Impact: | Moderate |
| System: | 10.10.54.39 |
| References: | [NIST SP800-53r4 AC-17](https://nvd.nist.gov/800-53/Rev4/control/AC-17) - Remote Access  [NIST SP800-53r4 AC-7(1)](https://nvd.nist.gov/800-53/Rev4/control/AC-7" \l "enhancement-1) - Unsuccessful Logon Attempts |Automatic Account Lock |

**Remediation**

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: RDP and SMB permitted unlimited login attempts. Demo-Sec recommends Relevant to restrict logon attempts against their service. |

Base64 encoded passwords at world readable smb (Moderate)

|  |  |
| --- | --- |
| Description: | Demo-Sec was able log into SMB and find a passwords.txt file //$ip/nt4wrksv/ directory. One of the passwords was an easy to crack password.  The credentials didn’t lead anywhere, but it’s best to take action in case someone with more time and resource takes advantage of them. |
| Impact: | Moderate |
| System: | 10.10.54.39 |
| References: | https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf – Print Spoofer |

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: The SMB service had base64 encoded credentials. Demo-Sec recommends Relevant to restrict access to the share or remove the password file unless necessary.  Item 2: Weak passwords were found. Demo-Sec noticed one of the passwords was easy to crack. Demo-Sec recommends Relevant to check their password policy. |

Last Page