

**REALIZE & REACT SECURITY**

**SECURITY ASSESSMENTS FINDINGS REPORT FOR ForEver25**

**BUSINESS CONFIDENTIAL**

**Date: March 28th, 2022**

**Project: Blue**

Table of Contents

[Confidentiality Statement 2](#_Toc99409832)

[Disclaimer 3](#_Toc99409833)

[Contact Information 3](#_Toc99409834)

[1.1 Assessment Overview 3](#_Toc99409835)

[1.2 Assessment Components 4](#_Toc99409836)

[1.2.1 Internal Penetration Test 4](#_Toc99409837)

[1.3 Finding Severity Ratings 5](#_Toc99409838)

[1.4 Scope 6](#_Toc99409839)

[1.4.1 Scope Exclusions 6](#_Toc99409840)

[1.4.2 Client Allowances 6](#_Toc99409841)

[2.0 Executive Summary 7](#_Toc99409842)

[2.1 Attack Summary 7](#_Toc99409843)

[2.1.1 Vulnerability Discovery 7](#_Toc99409844)

[2.1.2 Gained Access and Exploit 8](#_Toc99409845)

[2.3 Security Weaknesses and Findings 12](#_Toc99409846)

[2.3.1 Severity ratings 12](#_Toc99409847)

# Confidentiality Statement

This document is the exclusive property of ForEver25 and REALIZE & REACT Security (REALIZE & REACTS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FOREVER25 and REALIZE & REACTS.

REALIZE & REACTS 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. REALIZE & REACTS prioritized the assessment to identify the weakest security controls an attacker would exploit. REALIZE & REACTS 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 |
| **Demo Company** | | |
| Jonathan Helmus | Instructor | Office: (555) 555-5555  Email: Jonathan.helmus@metrostate.edu |
| **REALIZE & REACT Security** | | |
| Edajei Alvine | Lead Penetration Tester | Office: (555) 555-5555  Email: vu8547fr@go.minnstate.edu |

# 1.1 Assessment Overview

From March 14th to March 28th, 2022, Realize & React engaged ForEver25 to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal penetration test. All testing performed is based on requirements stated in tryhackme room, Eternal blue.

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.

Diagram

Description automatically generated

# 1.2 Assessment Components

## 1.2.1 Internal Penetration Test

An internal penetration test is meant to identify what could be accomplished by an attacker who has internal access to your network. A Realize & React Engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# 1.3 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. |

# 1.4 Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Internal Penetration Test | 10.10.42.233 |

* Full scope information provided in “**ForEver25.. Full Findings.xslx”**

## 1.4.1 Scope Exclusions

Per client request, REALIZE & REACT Security did not perform any Denial-of-Service attacks during testing.

## 1.4.2 Client Allowances

FOREVER25 did not provide any allowances to assist the testing.

# 2.0 Executive Summary

REALIZE & REACTS evaluated FOREVER25’s internal security posture through an internal network penetration test from March 14th to March 28th. By leveraging a series of attacks, REALIZE & REACTS found some vulnerabilities that allowed full internal access to the FOREVER25 windows hosts. It is highly recommended that FOREVER25 addresses these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## 2.1 Attack Summary

## 2.1.1 Vulnerability Discovery

The following describes how REALIZE & REACT Security gained internal network access, step by step:

The first step to find the vulnerabilities here consisted of an Nmap scan following the command; **nmap -sV -sC --script vuln -oN blue.nmap 10.10.42.223**

This scan revealed some open ports with 3 ports being under 1000 and the [CVE](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0143) of the vulnerability ms17-010 found on the server.

A screenshot of a computer

Description automatically generated with medium confidence

The screenshot below confirms there is a vulnerability to eternal blue(ms17-010)

Text

Description automatically generated

Notes: This is a remote code execution vulnerability which allows an attacker to execute code remotely on the target host without being blocked or triggering any sort of alert as is done in this case with the host IP 10.10.42.233.

With access to this, an attacker could literally do as much harm as they please and this is a critical as it could lead to some further exploits as will be shown.

## 2.1.2 Gained Access and Exploit

Metasploit was used to gain access and exploit the host

Based on the following screenshots we can confirm that the host is vulnerable to eternal blue as the second screen shot shows that [**“The Host is likely vulnerable to MS17-010” .**](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)

With this information I was able to proceed with exploitation

Graphical user interface, text, application, chat or text message

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

The port didn’t need to be changed here as the internal host was accessed on port 445. This indicates a weakness as there was no trigger. I was able to background the regular shell and upgrade to a meterpreter shell.

Text

Description automatically generated

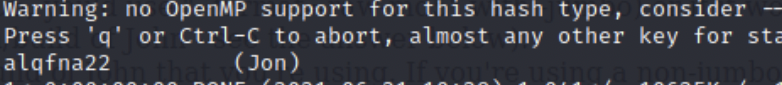
The shell was upgraded to a meterpreter shell.

Migrate was done to 704 as that’s where the service.exe process was found.

Following that upgrade, I did a hashdump which brought up some hashes and then john the ripper was used on the hash to reveal the password

A picture containing text

Description automatically generated



.

# 2.3 Security Weaknesses and Findings

Open access to shells without any level of authentication

## 2.3.1 Severity ratings

This exploit was straight forward and executable within the shortest time possible. Almost any command could be run on a host via remote execution. It could range from password harvesting up to even denial of service and more. I would consider it too straight forward for the level of harm that could potentially be caused by an attacker, thereby rating this a critical severity which should be addressed immediately.

[Eternal blue](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical  -eternalblue | 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. |