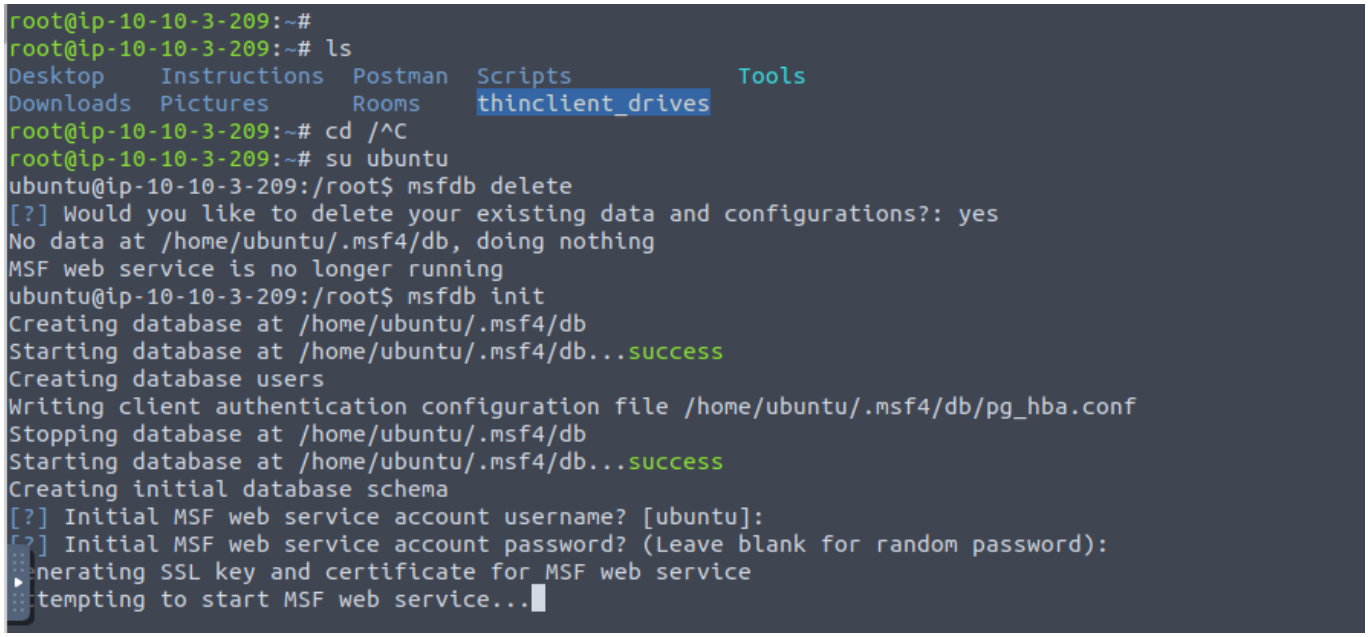
Intro to C2 - VM Compromise Guide

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.

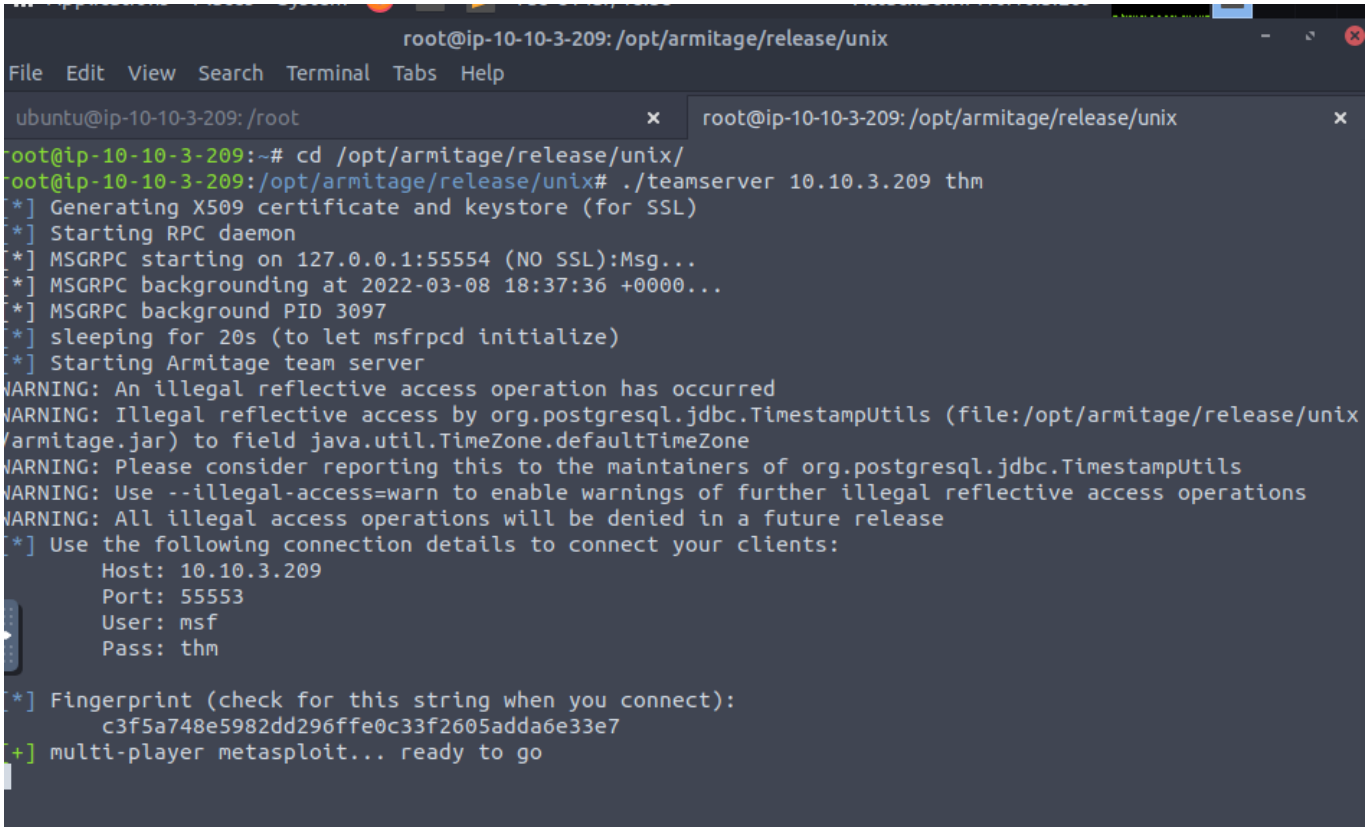
Re-initializing PostgreSQL




```
su ubuntu

msfdb delete

msfdb init
```

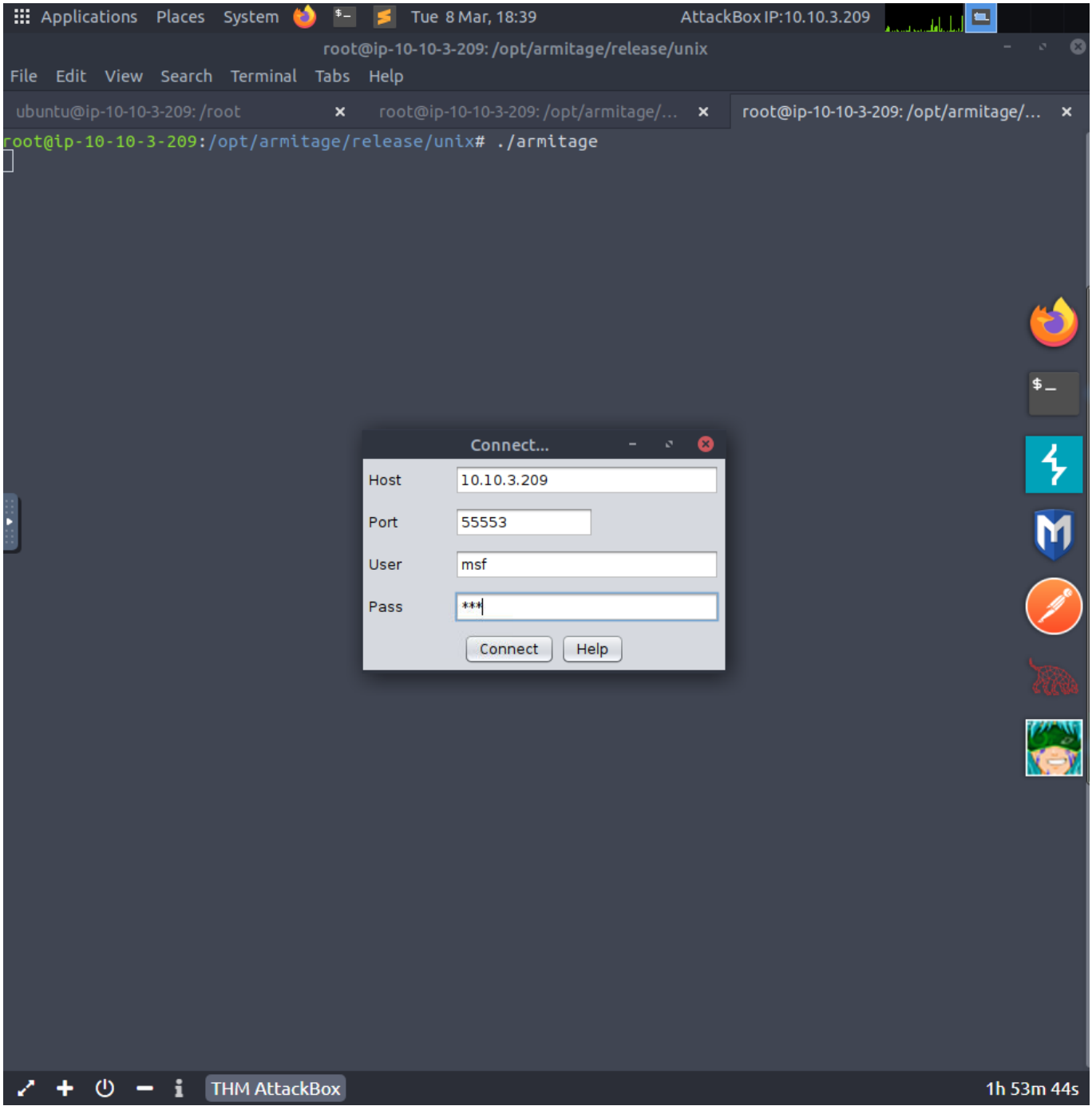
Starting Armitage's Team Server

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

./teamserver 10.10.3.209 thm
```

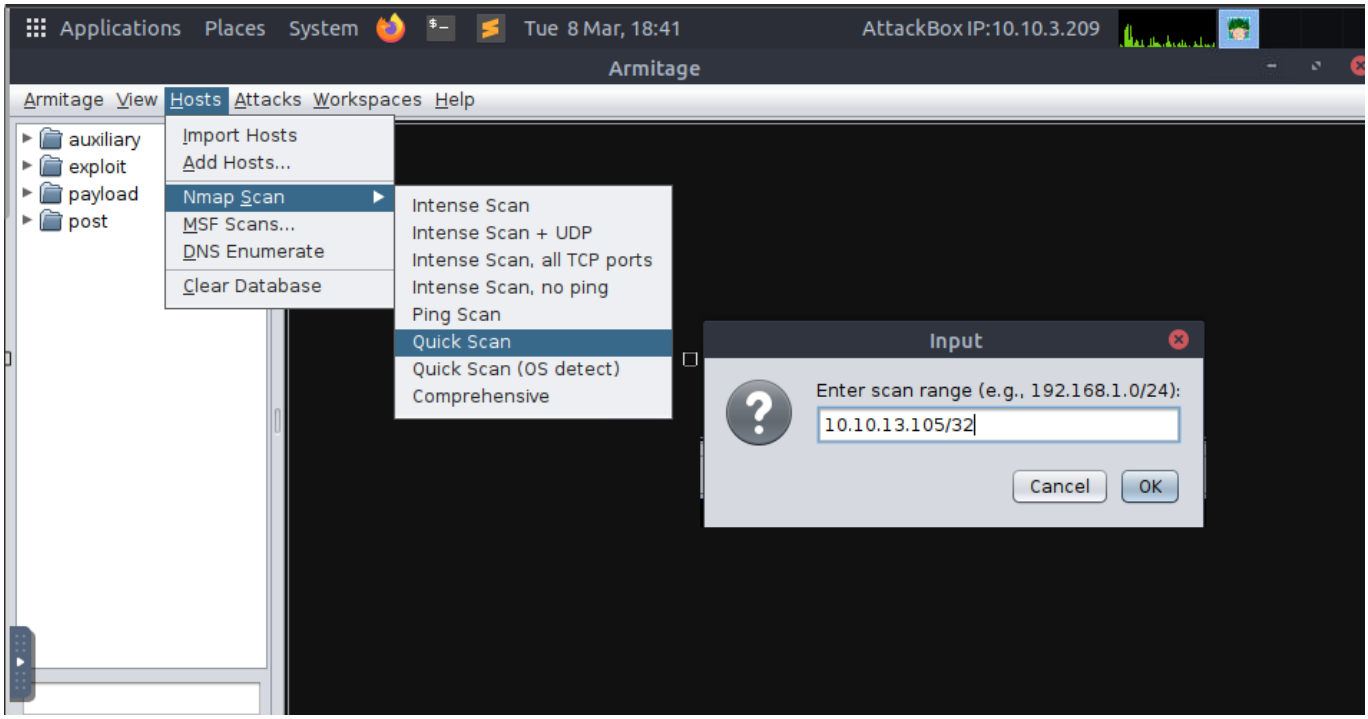


Launching Armitage

```
./armitage
```

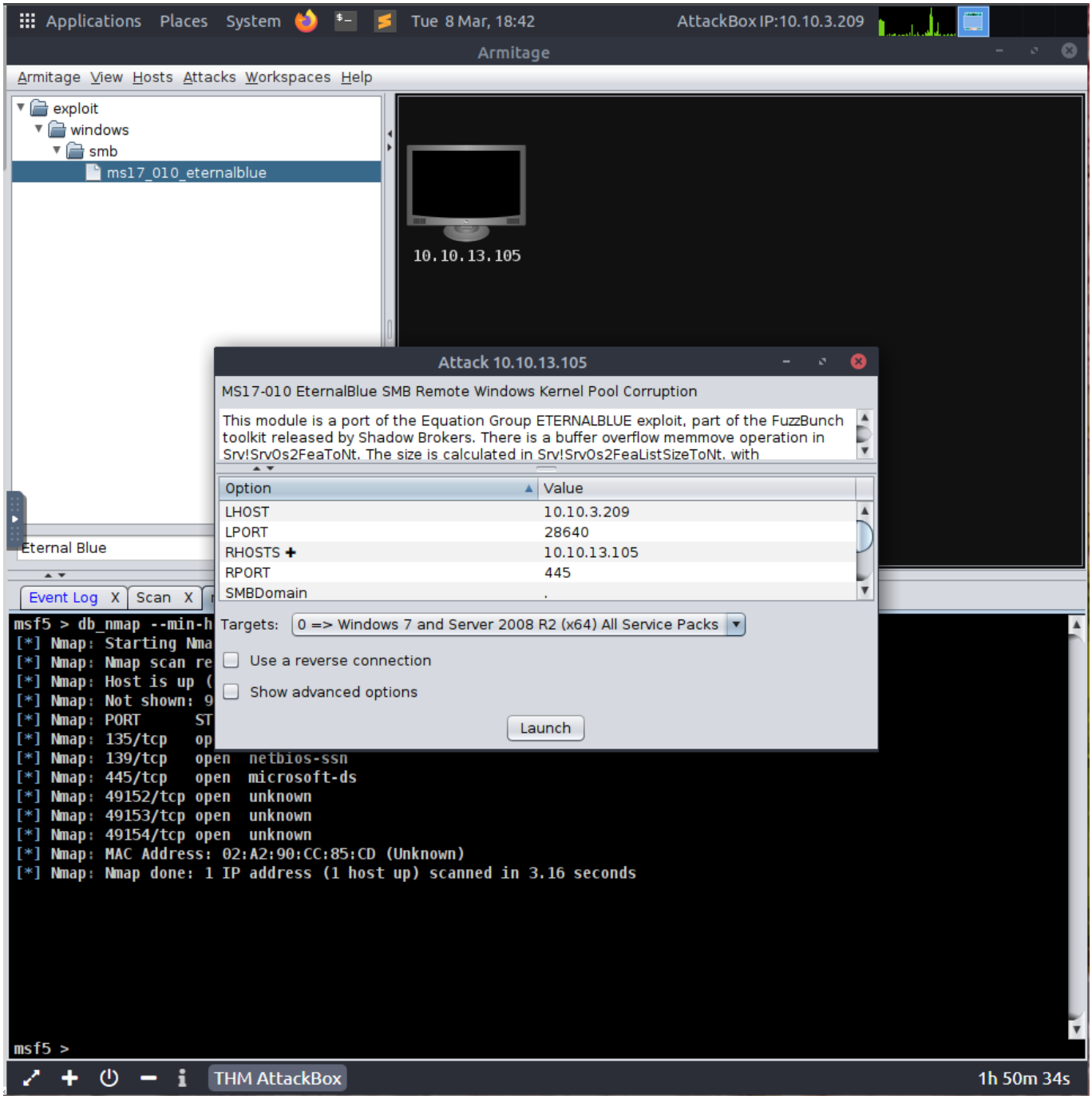

Applications Places System Tue 8 Mar, 18:39 AttackBox IP:10.10.3.209
root@ip-10-10-3-209: /opt/armitage/release/unix
File Edit View Search Terminal Tabs Help
ubuntu@ip-10-10-3-209: /root
root@ip-10-10-3-209: /opt/armitage/...
root@ip-10-10-3-209: /opt/armitage/...
root@ip-10-10-3-209:/opt/armitage/release/unix# ./armitage
Connect...
Host 10.10.3.209
Port 55553
User msf
Pass ***
Connect Help
THM AttackBox
1h 53m 44s

Scan the VM -



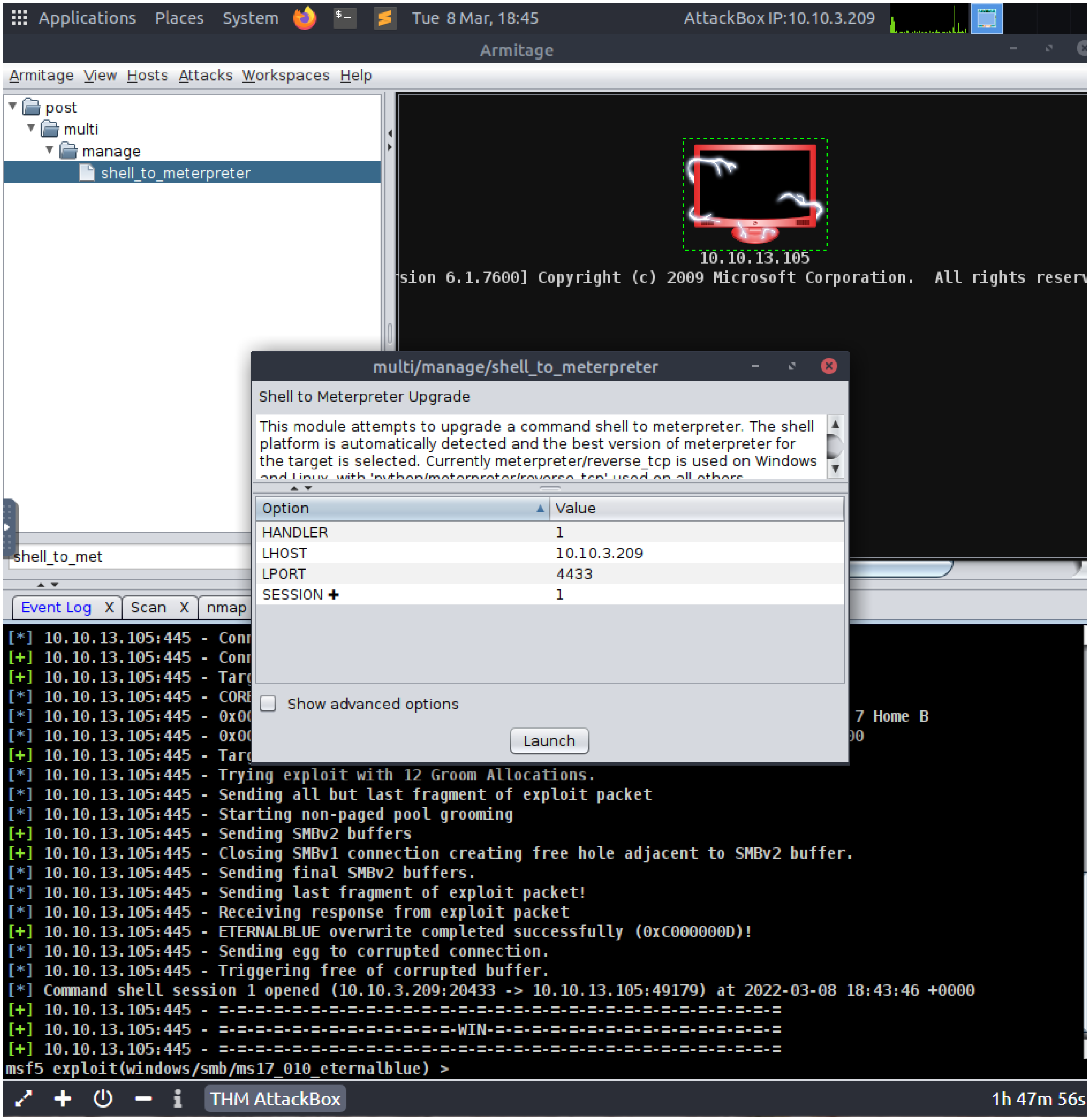
Exploit the VM -

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”

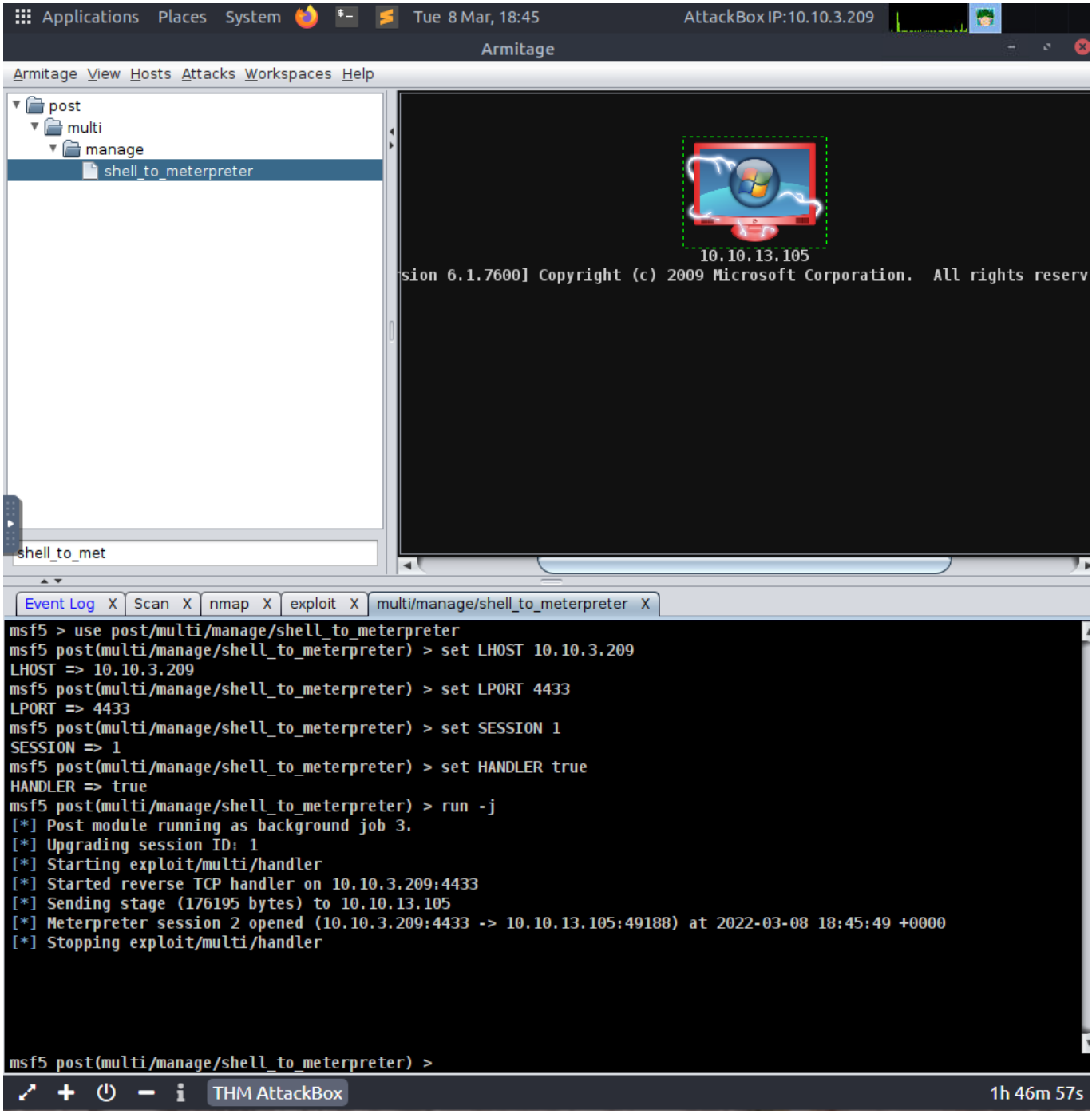


Upgrade Shell to Meterpreter

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”

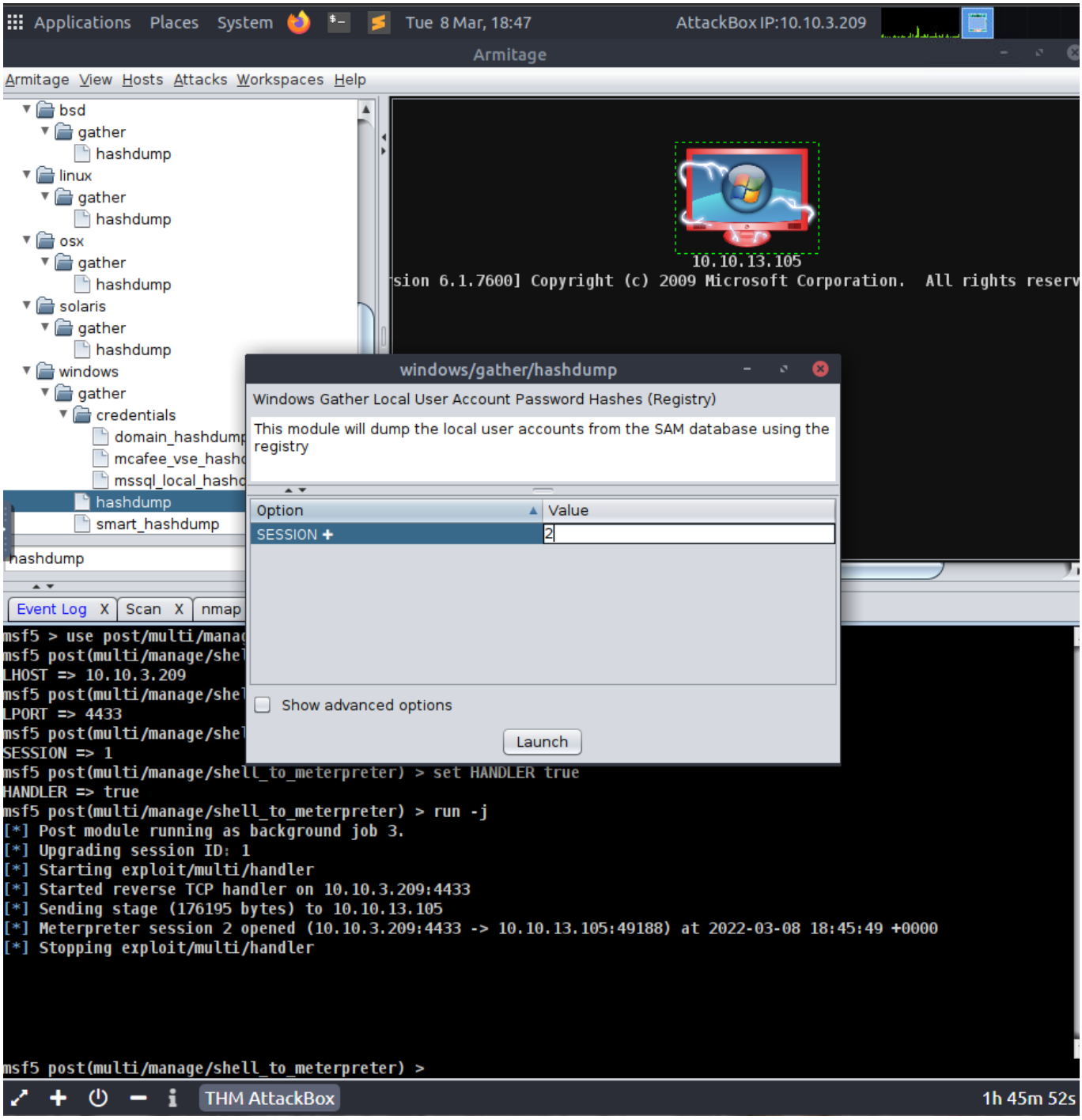


You can verify the migration to meterpreter completed successfully by verifying the machine icon has changed and the “Meterpreter Session 2 Opened” has appeared.



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”



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