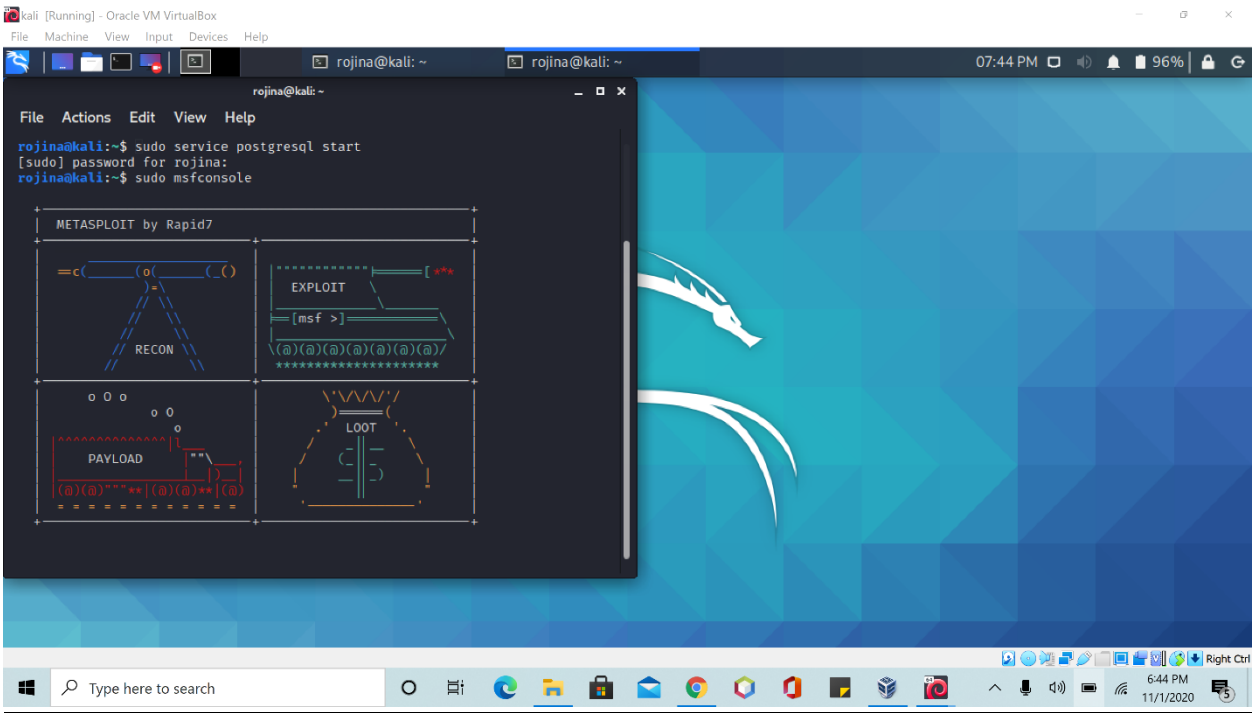
Attack on Windows

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.

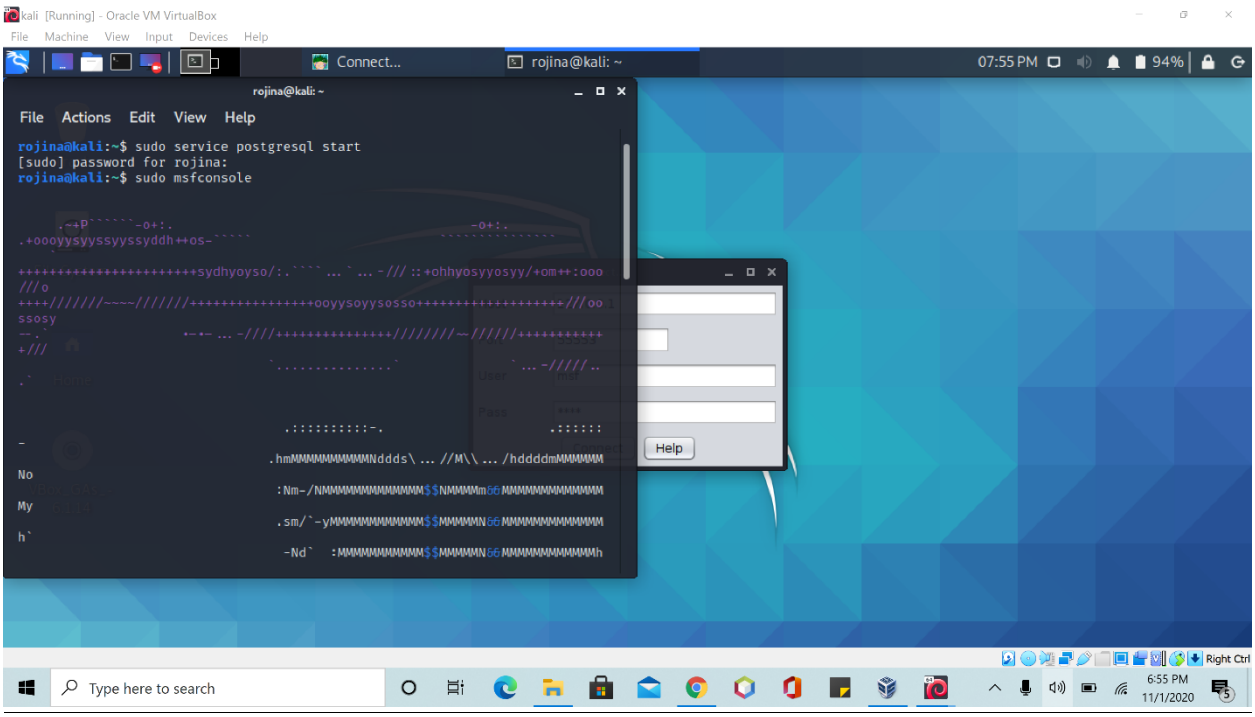
We are using Armitage to attack Windows XP from Linux. Armitage is a tool that visualizes the target that we want to attack, recommends exploits and exposes the advanced post-exploitation features in framework.

All the steps with their screenshots are shown below.

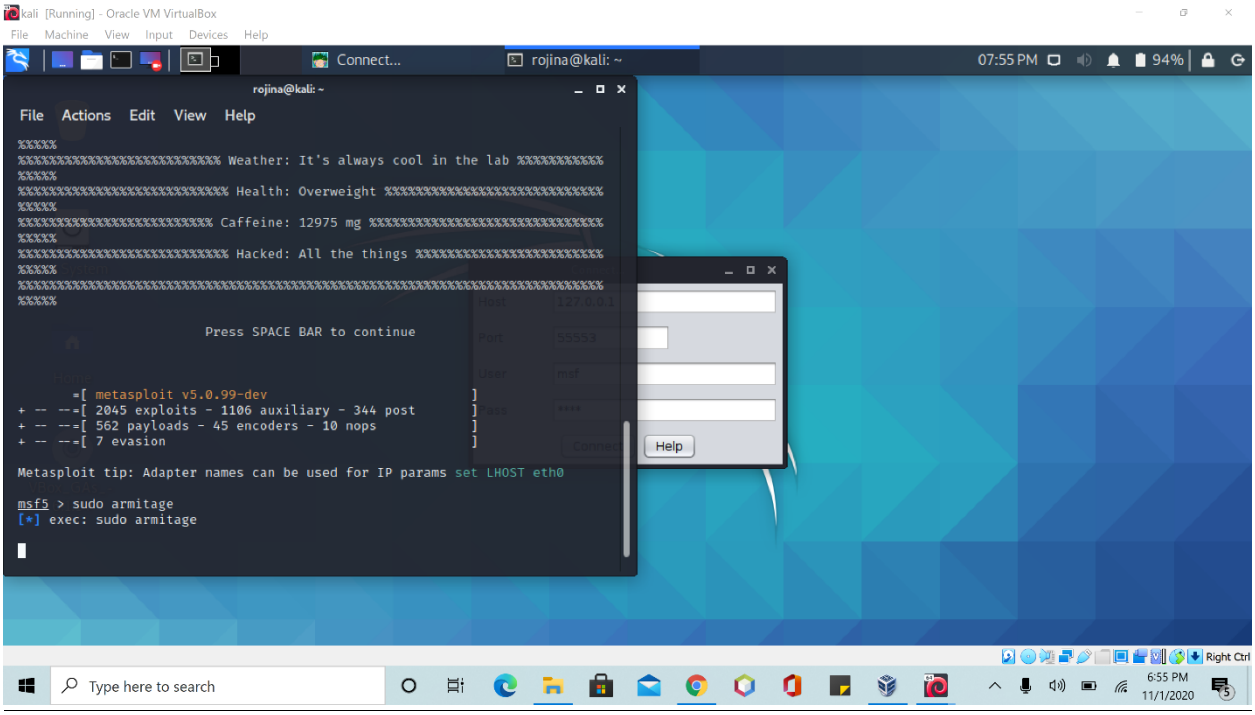
First we run the Metasploit database server. The Metasploit allows hacker to safely simulate attacks. It also makes hacking and attacking easier. Metasploit has a built in database system which makes scanning information and importing, exporting easier and quick.

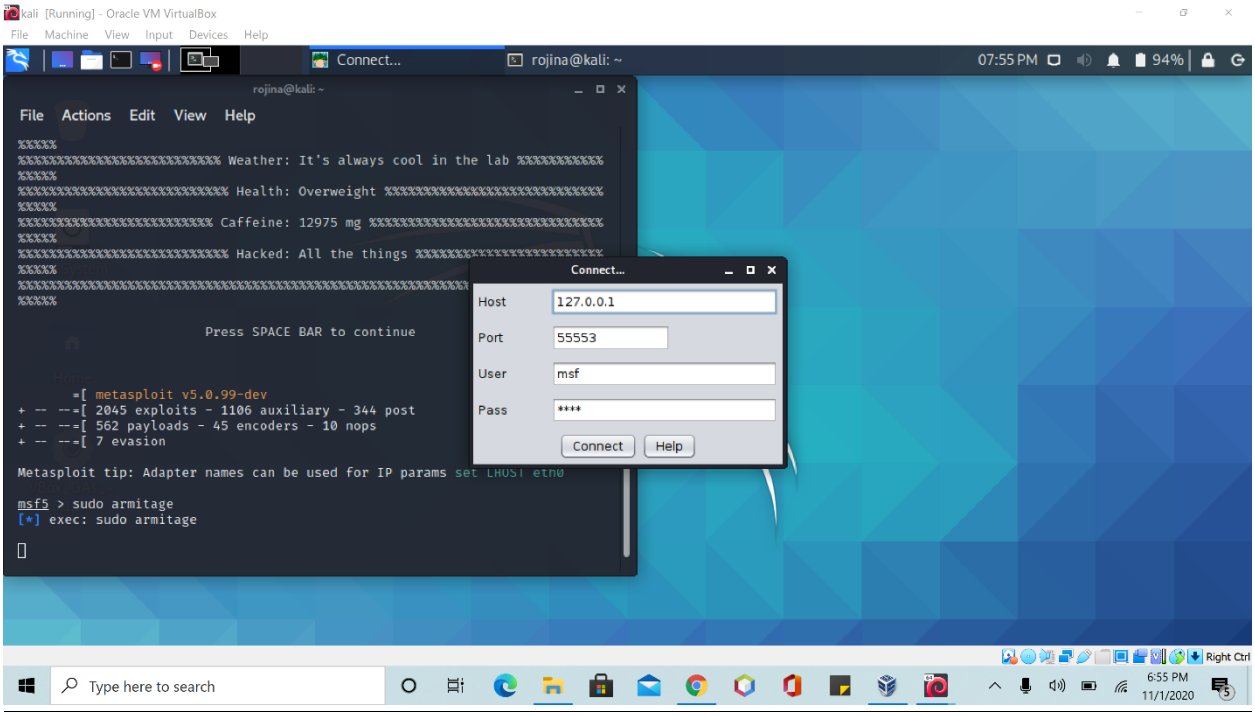


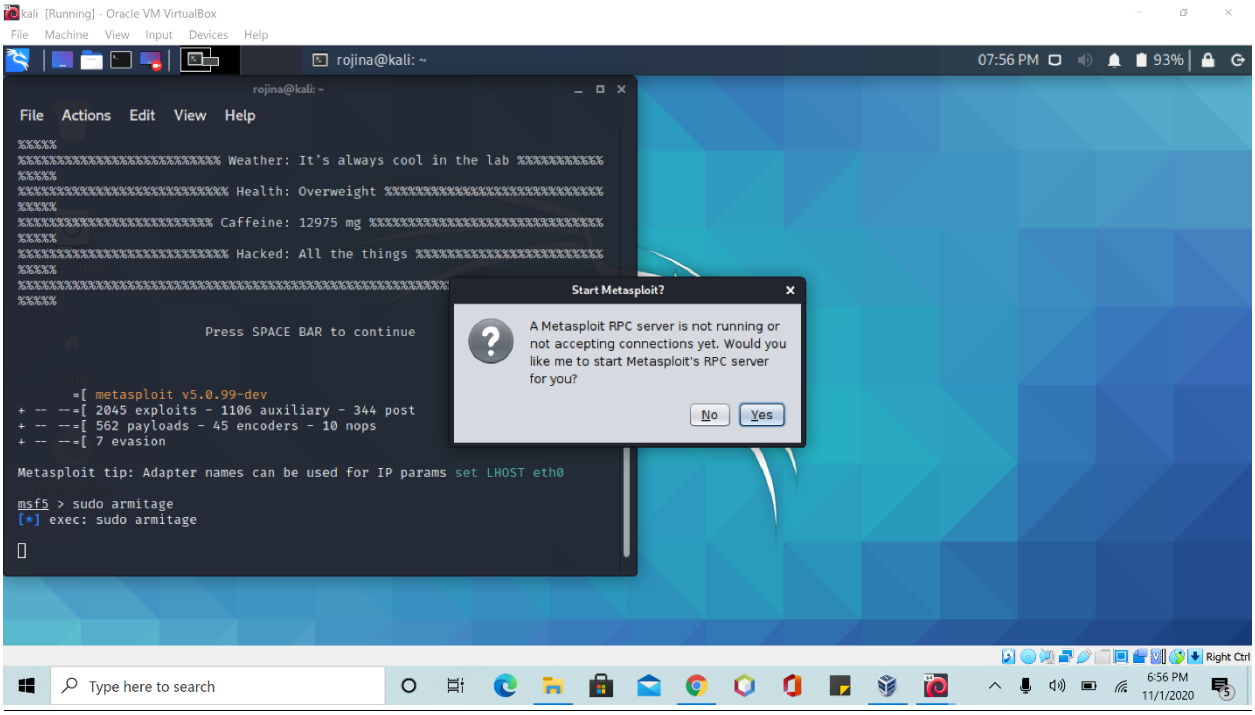
Then, we entered the required password.

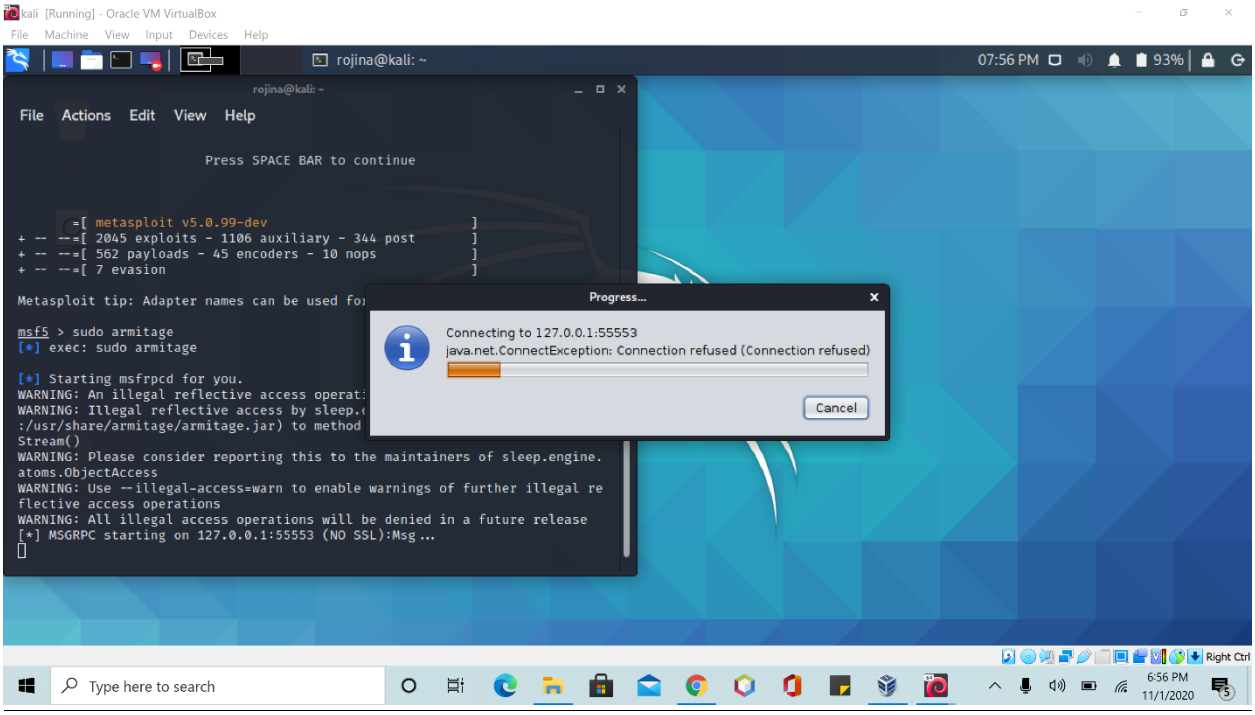


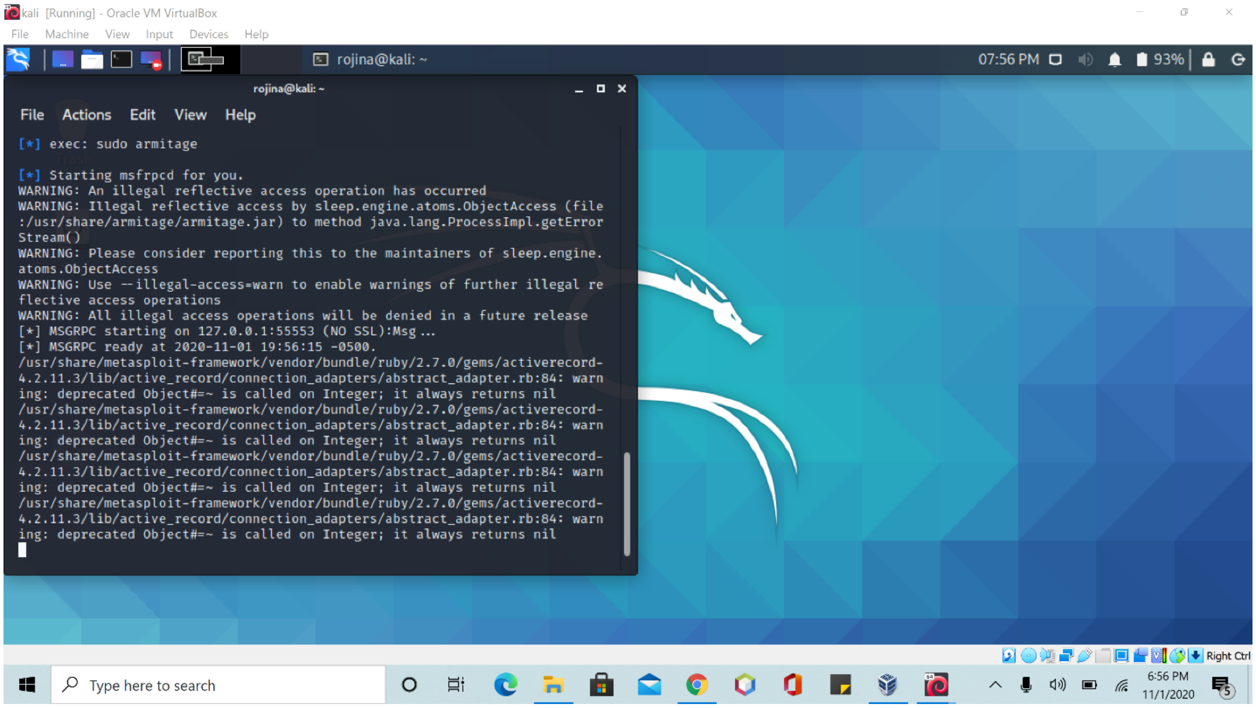
Opened armitage through console to launch attack process. Armitage makes attacking lot easier and faster.


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Connect...
rojina@kali: ~
07:55 PM
94%
rojina@kali: ~
File Actions Edit View Help
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%
%%%%%
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 IP params set LHOST eth0
msf5 > sudo armitage
[*] exec: sudo armitage
Help
Right Ctrl
Type here to search
6:55 PM
11/1/2020

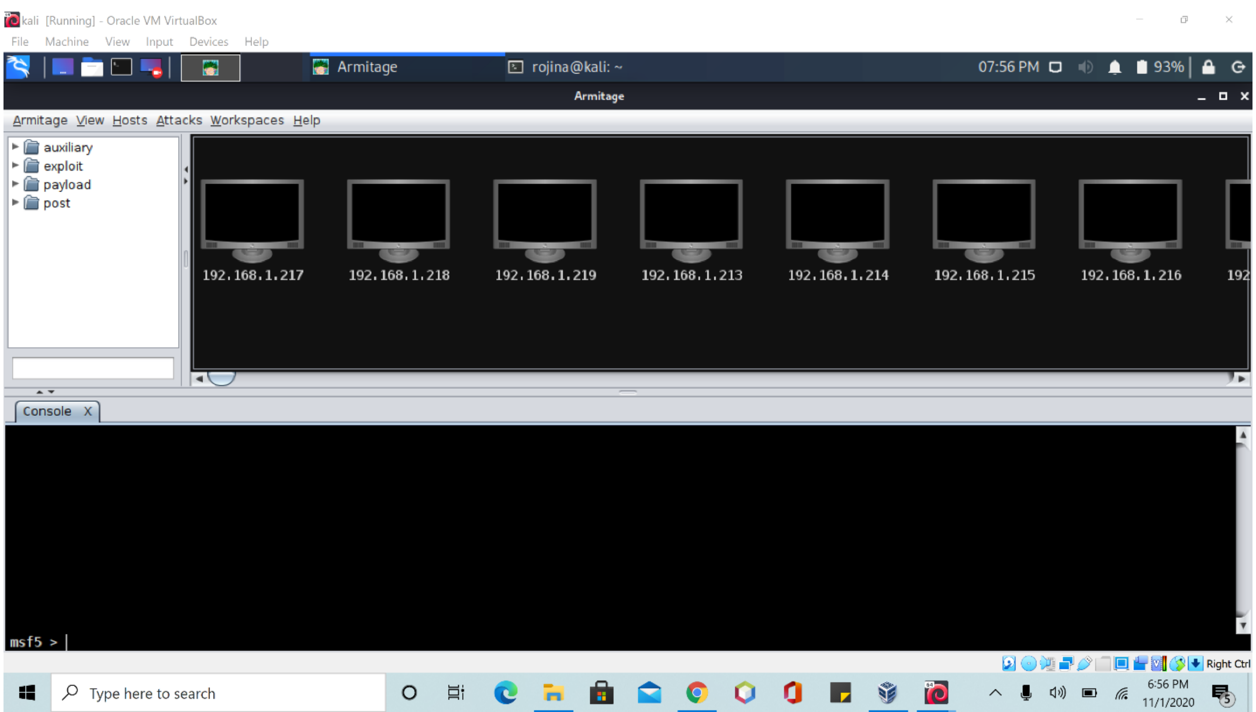

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Connect...
rojina@kali: ~
07:55 PM
94%
rojina@kali: ~
File Actions Edit View Help
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%
%%%%%
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 IP params set LHOST eth0
msf5 > sudo armitage
[*] exec: sudo armitage
Connect...
Host 127.0.0.1
Port 55553
User msf
Pass ****
Connect
Help
Right Ctrl
Type here to search
6:55 PM
11/1/2020


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
rojina@kali: ~
07:56 PM
93%
rojina@kali: ~
File Actions Edit View Help
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%
%%%%%
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 IP params set LHOST eth0
msf5 > sudo armitage
[*] exec: sudo armitage
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
Right Ctrl
Type here to search
6:56 PM
11/1/2020

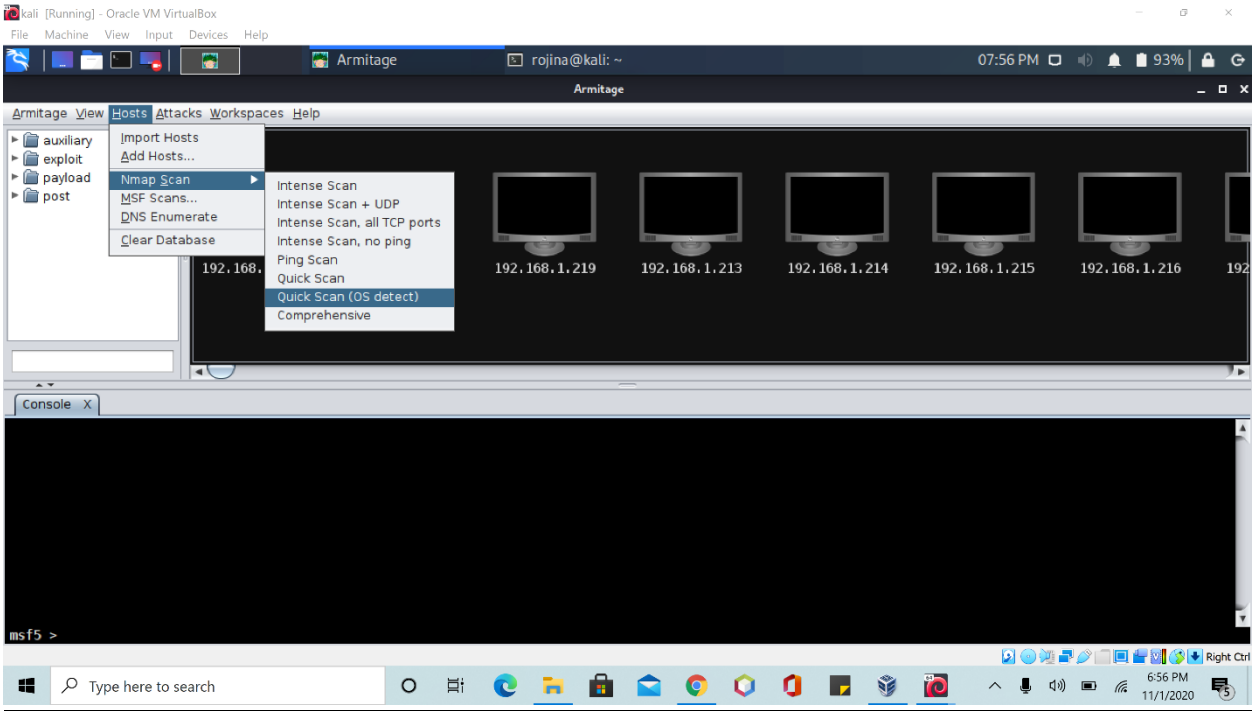

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
rojina@kali: ~
07:56 PM
93%
rojina@kali: ~
File Actions Edit View Help
Press SPACE BAR to continue
=[metasploit v5.0.99-dev
+ -- --=[2045 exploits - 1106 auxiliary - 344 post
+ -- --=[562 payloads - 45 encoders - 10 nops
+ -- --=[7 evasion
Metasploit tip: Adapter names can be used fo
msf5 > sudo armitage
[*] exec: sudo armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operat
WARNING: Illegal reflective access by sleep.
:/usr/share/armitage/armitage.jar) to method
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 re
flective 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...
Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)
Cancel
Right Ctrl
Type here to search
6:56 PM
11/1/2020



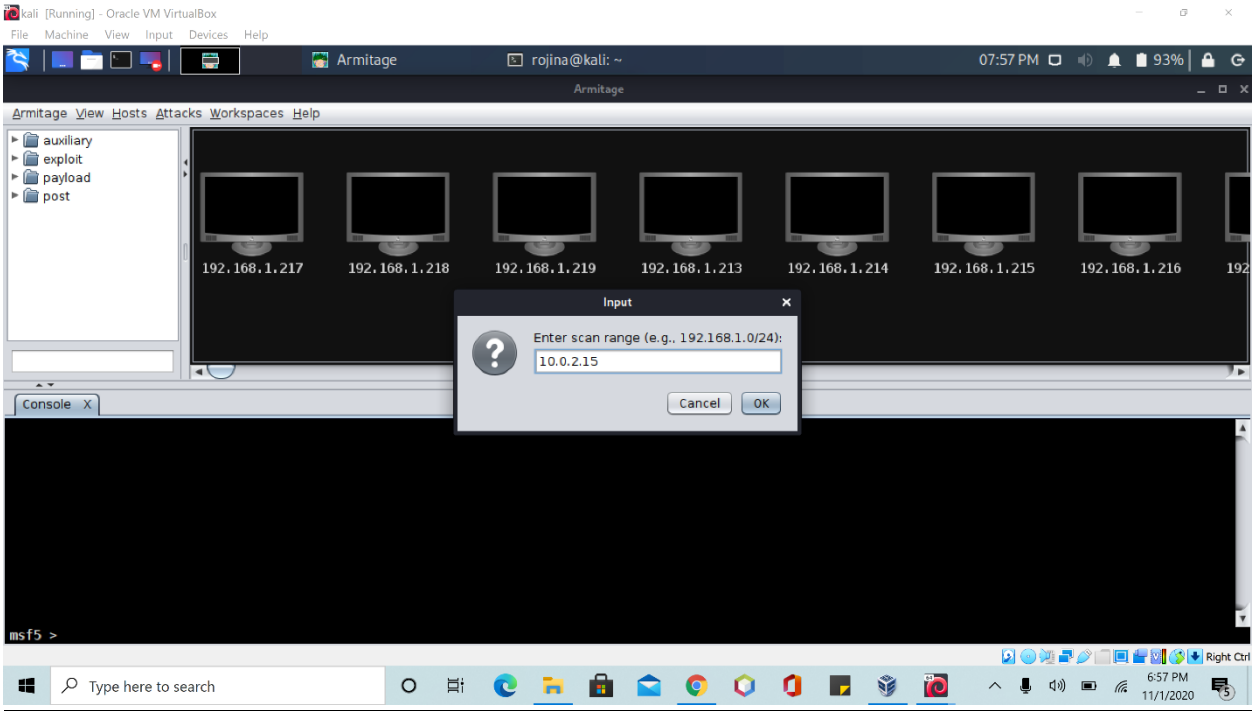
Shown are all the IP address available.



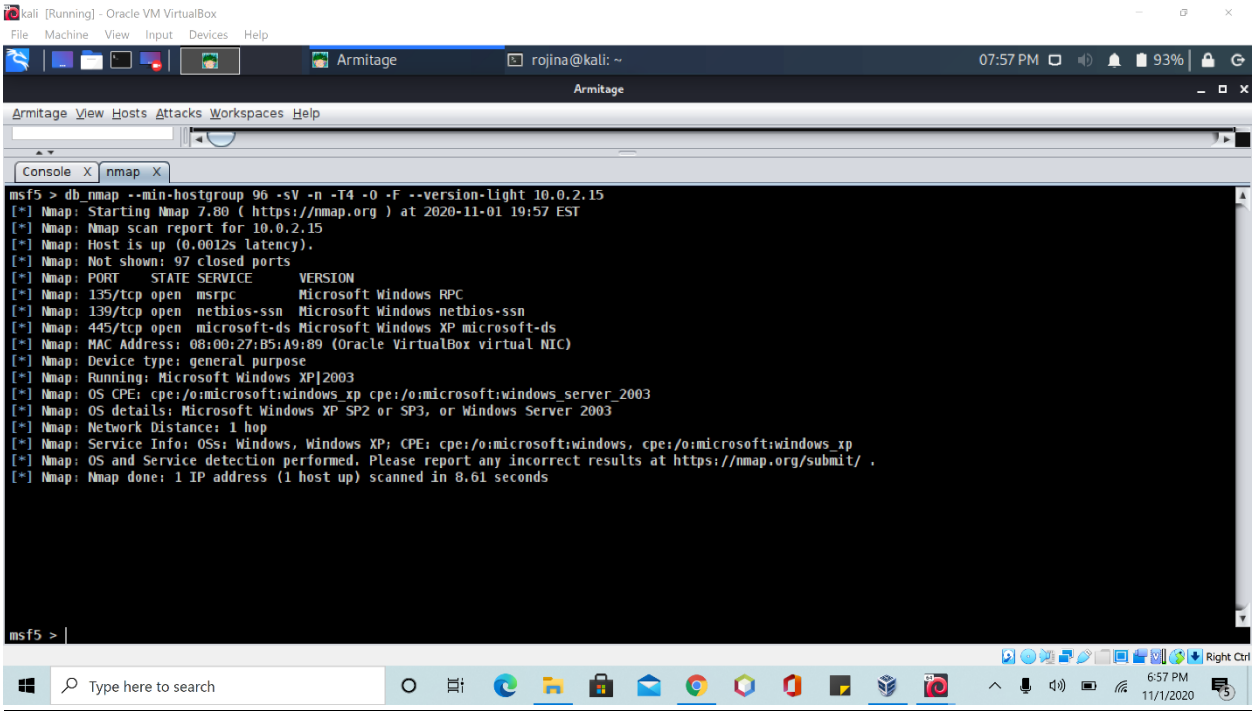
Searching for our Winows XP IP address.



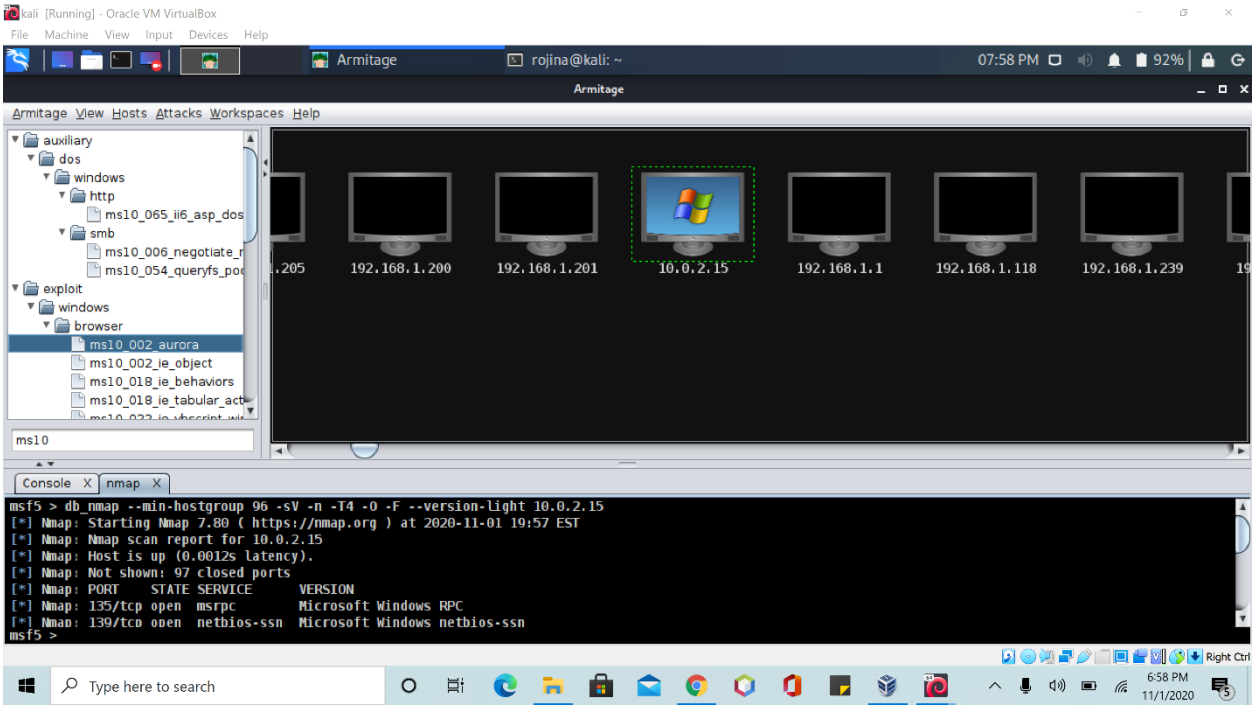
Manually typing in the IP address.

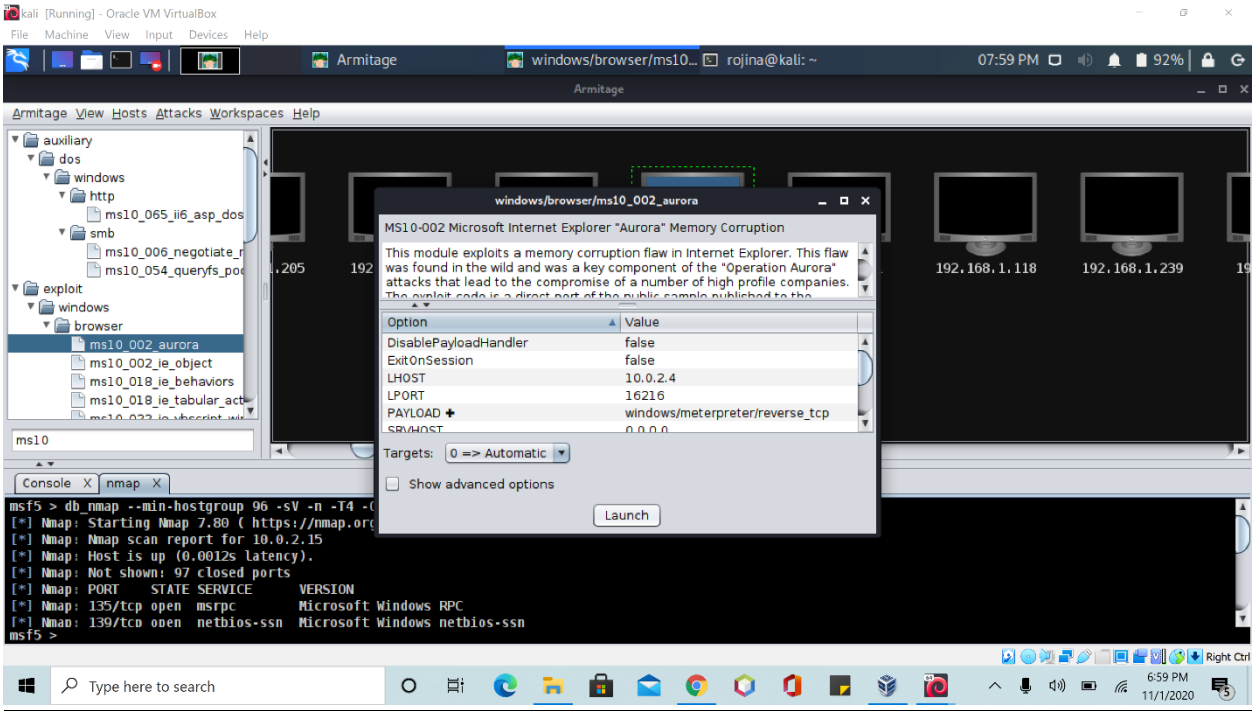


We can see that our Windows XP has been detected.

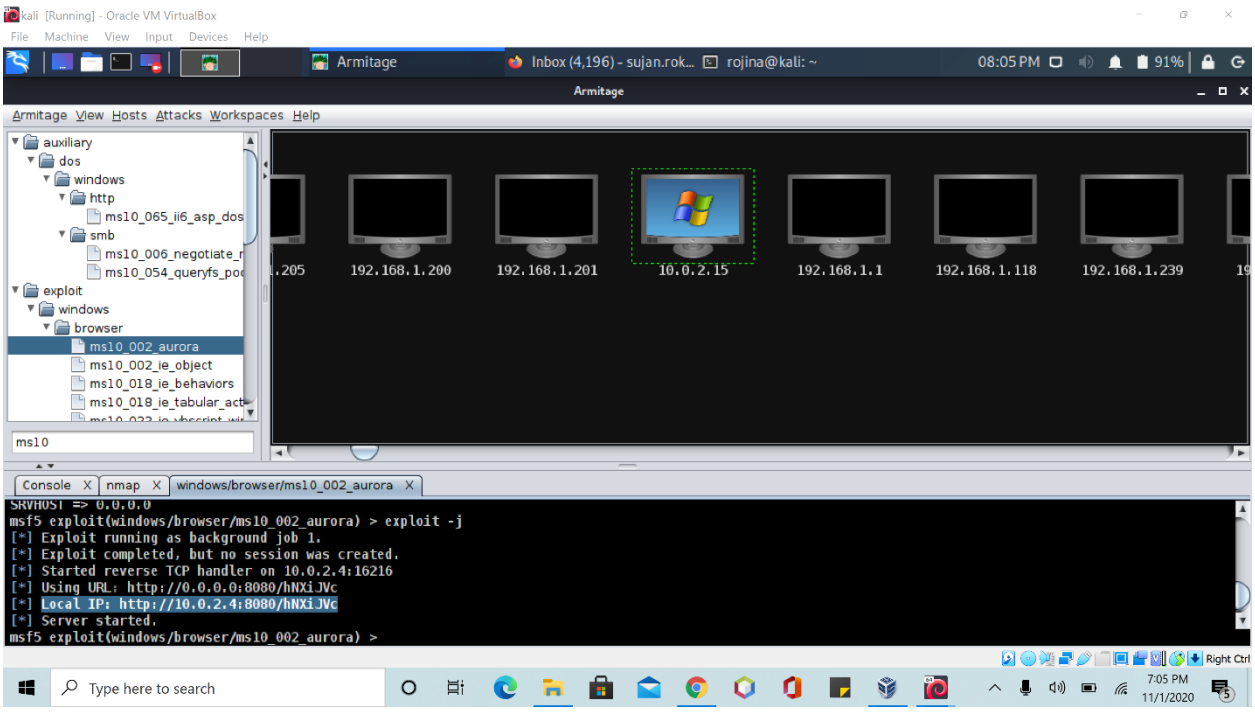


Windows XP found. Now attack the system using ms10_002_aurora.

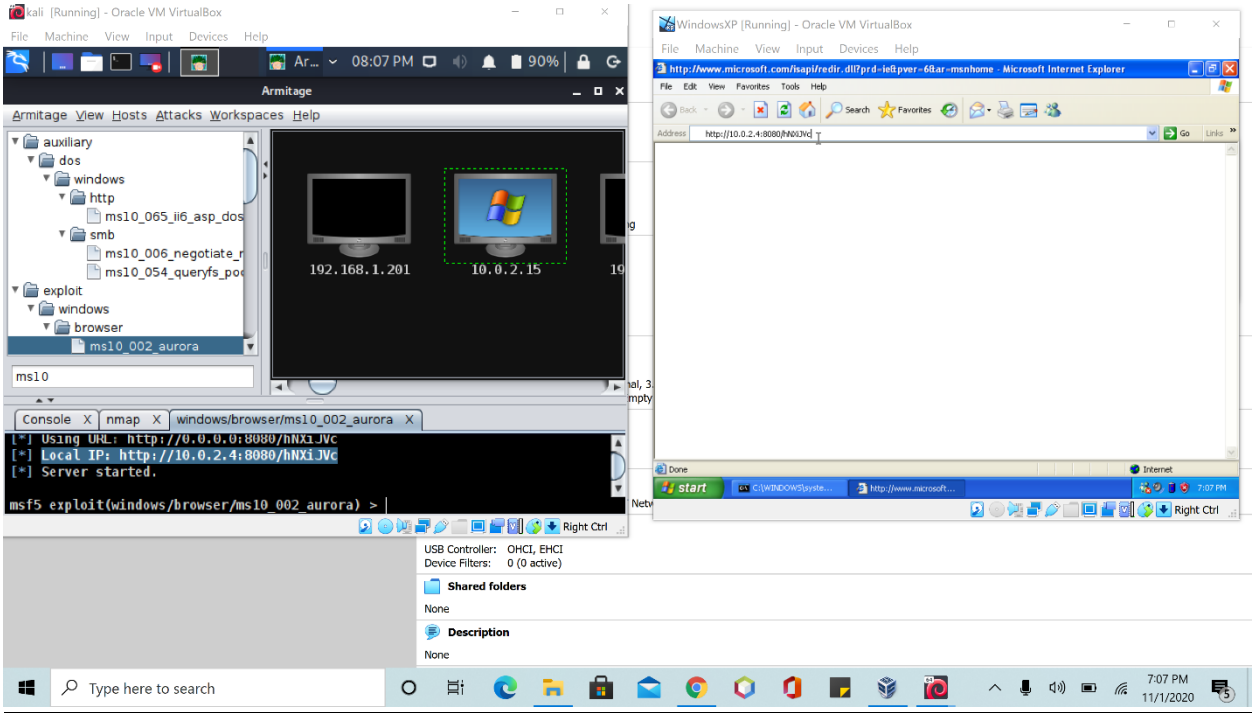


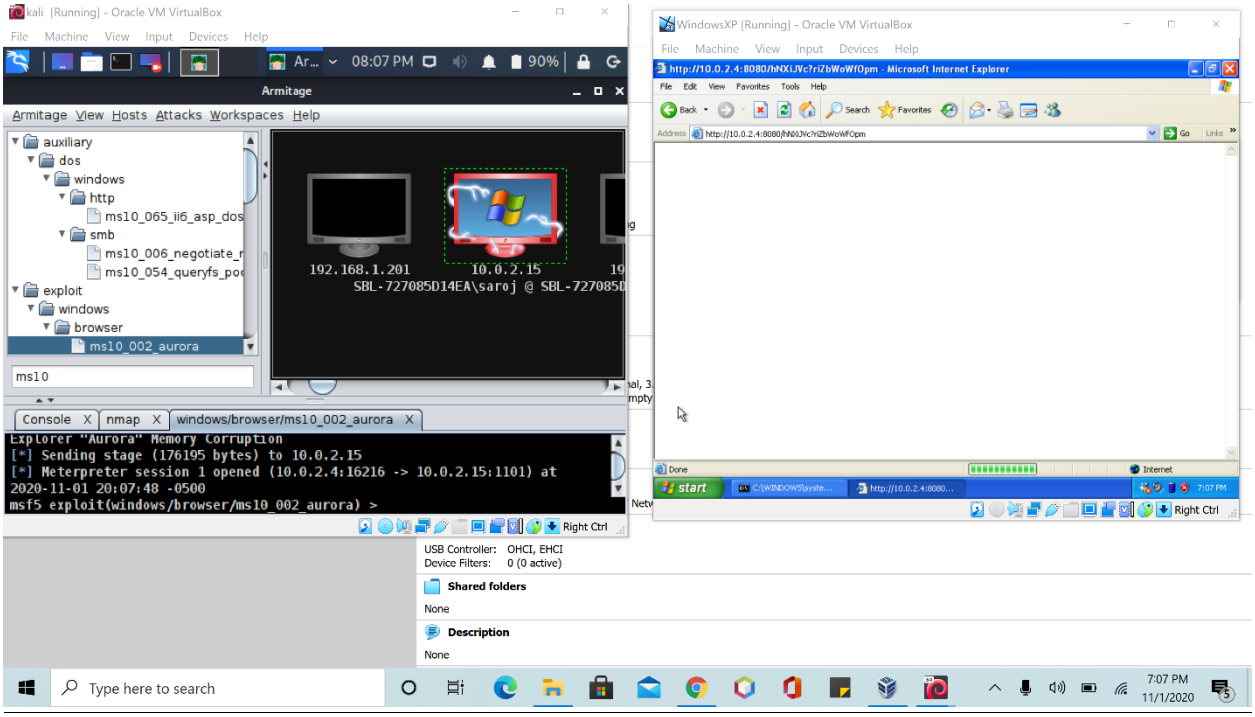


A link under Local IP has been generated which will be the medium to attack the system.

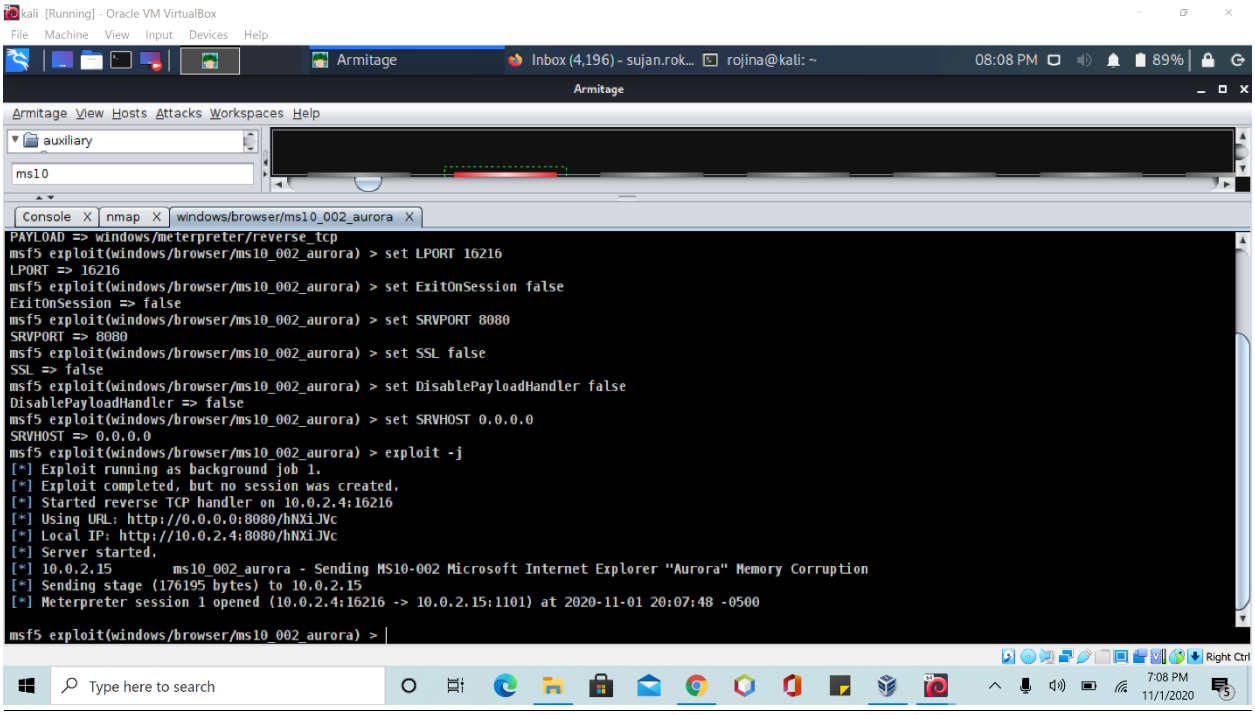


We copied the link on our Windows XP.

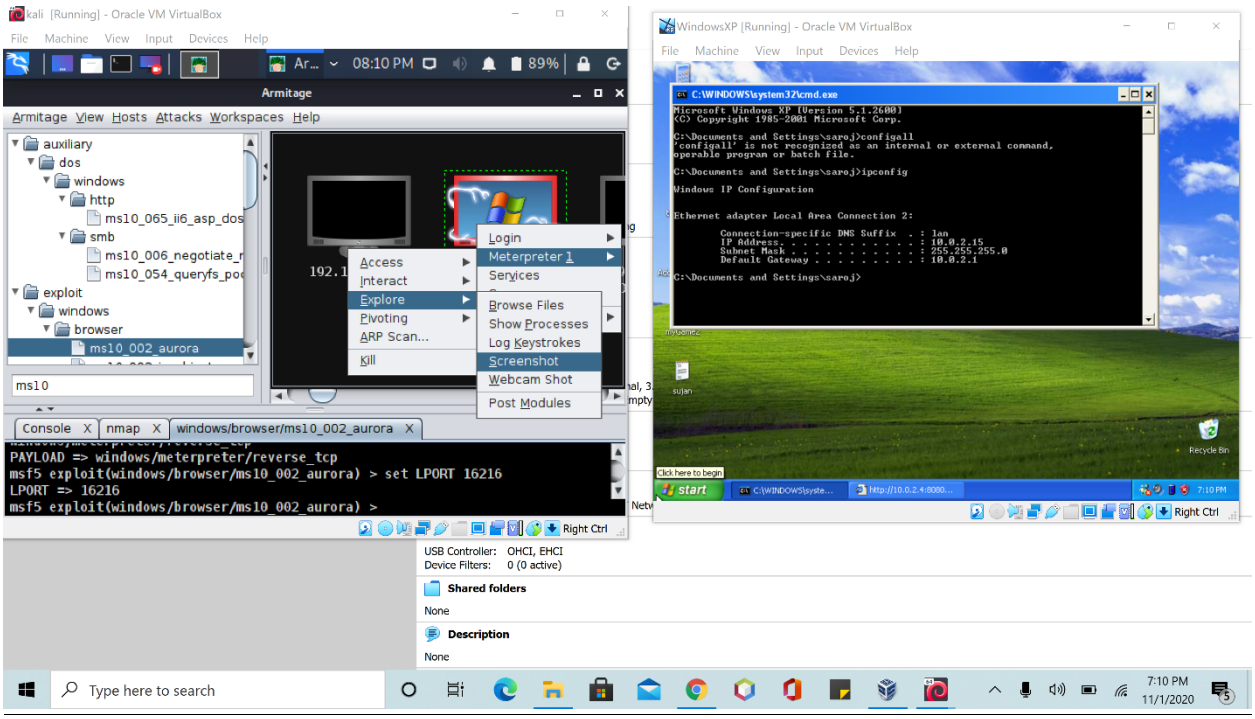




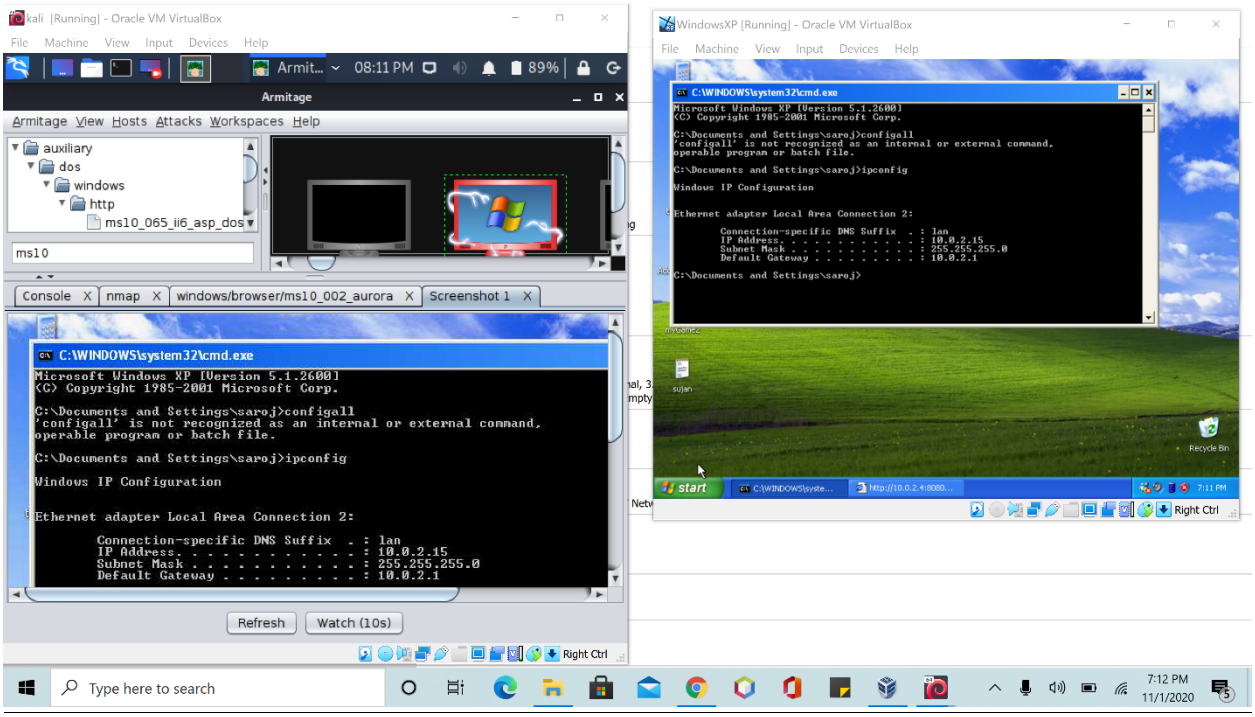
Now the attacker system has access to the Windows XP.



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.