Metasploitable

Setting Up a Practice Target Machine

Last Updated 3/18/12

RAPID7

TABLE OF CONTENTS

About This Guide

Setting Up Metasploitable

Getting Started with Metasploitable

About This Guide

This guide provides instructions for you to set up the Metasploitable virtual machine as a target machine. The following sections describe the audience, organization, and conventions used within this guide.

Target Audience

This guide is for IT and security professionals who use the Metasploit Framework or Metasploit commercial editions as a penetration testing solution.

Organization

This guide includes the following chapters:

- About this Guide
- Setting Up Metasploitable
- Getting Started with Metasploitable

Document Conventions

The following table describes the conventions and formats that this guide uses:

Convention	**Description**
Command	Indicates buttons, UI controls, and fields. For example, "**Click Projects > New Project**."
Code	Indicates command line, code, or file directories. For example, "Enter the following: `chmod +x Desktop/metasploit-3.7.1-linux-x64-installer`."
Title	Indicates the title of a document or chapter name. For example, "For more information, see the *Metasploit Pro Installation Guide*."
Note	Indicates there is additional information about the topic.

Support

You can visit the Customer Center or e-mail the Rapid7 support team to submit questions and receive support for Metasploit Pro and Metasploit Express. To log in to the Customer Center, use the e-mail and password provided by Rapid7.

The following table describes the methods you can use to contact the Rapid7 support team.

Support Method	Contact Information
Customer Center	http://www.rapid7.com/customers/customer-login.jsp
E-mail	support@rapid7.com

There is not an official support team dedicated to the Metasploit Framework or Metasploit Community. If you are a Metasploit Community or Framework user, you can visit the Metasploit Community for support.

Product Name Usage

The following table describes how this guide uses product names:

Product Name	Description
Metasploit	Refers to the Metasploit commercial editions, such as Metasploit Pro, Express, and Community, and the Metasploit Framework.
Metasploit Pro	Refers to Metasploit Pro, Express, and Community, unless noted otherwise.
Metasploit Framework	Refers to the Metasploit Framework only.

Required Credentials

The following table describes the credentials that you need to log in to Metasploitable:

Account	Credentials
Ubuntu VM	msfadmin:msfadmin

Setting Up Metasploitable

This chapter covers the following topics:

Before You Begin

Before you can begin, you must perform the following tasks:

- Download and install VMware Workstation or VMware Player.
- Download and install Metasploit on either your local system or on a virtual machine.
- Download the Metasploitable zip file.
- Verify that your local system meets the minimum system requirements.

Download and Install VMware Workstation

For information on how to download and install VMware Workstation or VMware Player, visit the VMware website.

Download and Install Metasploit

To download the Metasploit installer, visit the Metasploit website. Choose the installer that is appropriate for your operating environment.

For information on how to install Metasploit, visit the Metasploit Pro Installation Guide. You can use the instructions for Metasploit Pro to install all Metasploit products. The steps do not vary between products.

Download Metasploitable

1. Visit Rapid7 to download the BitTorrent file.
2. Open the Metasploitable BitTorrent file in a BitTorrent client.
3. Download and unzip the contents of the Metasploitable zip file.

System Requirements

- Intel Core 2 Quad @2.66 GHz
- 8 GB Crucial DDR3 RAM
- 500 GB WD HD
- VMware Workstation

Resources

For additional information on Metasploit products and VMware, visit the following resources:

- VMware Online Help
- Metasploit Community

About Metasploitable

Metasploitable is an Ubuntu 8.04 server that runs on a VMware image. The Metasploitable virtual machine contains a number of vulnerable services and an install of Apache Tomcat 5.5, DistCC, Tiki Wiki, and MySQL.

The purpose of Metasploitable is to provide you with a vulnerable target machine that you can use to work with Metasploit Pro, Metasploit Express, Metasploit Community, and the Metasploit Framework. Your goal is to discover the services and vulnerabilities that exist on Metasploitable and to exploit them to learn more information about the virtual machine. For example, you can run a bruteforce attack against the Metasploitable virtual machine to collect passwords from the system.

Resetting Metasploitable

Metasploitable runs in non-persistent disk mode, so you do not need to worry about destroying the box. The non-persistent disk mode does not save changes to the virtual machine. Instead, the non-persistent disk mode restores the virtual machine to the initial state each time you reset or power off the machine.

To reset the Metasploitable virtual machine, you can choose one of the following options:

- VM > Power > Reset
- VM > Power > Restart Guest
- VM > Power > Power off

Active Services

Metasploitable contains the following active services:

- FTP
- SSH

- Telnet
- SMTP
- DNS
- HTTP
- NetBIOS
- SMB
- MySQL
- distcc
- PostgreSQL

Credentials

The following table describes the credentials for the services on Metasploitable:

Service	Credentials
SSH	user:user
MySQL	root:root
PostgreSQL	postgres:postgres
HTTP	tomcat:tomcat

Setting Up Metasploitable

The following sections describe how to launch and log in to Metasploitable.

Running Metasploitable in an Isolated Network

To ensure that you do not unintentionally damage your local system, you should configure Metasploitable to use the host only mode. The host only mode restricts the virtual machine to an isolated virtual network.

To configure Metasploitable to use the host only mode in VMware Workstation:

1. Open the Metasploitable virtual machine in VMware Workstation.
2. Choose **VM > Settings** from the main menu bar.
3. From the **Hardware** tab, choose **Network Adapter** from the **Device** list.
4. Select the **Host-only mode** from the **Network Connection** options.
5. Click **OK** to apply your changes.

Launching Metasploitable in VMware Workstation

To launch Metasploitable for the first time, open the location that contains the unzipped Metasploitable folder and double-click the Metasploitable VMware virtual machine configuration file.

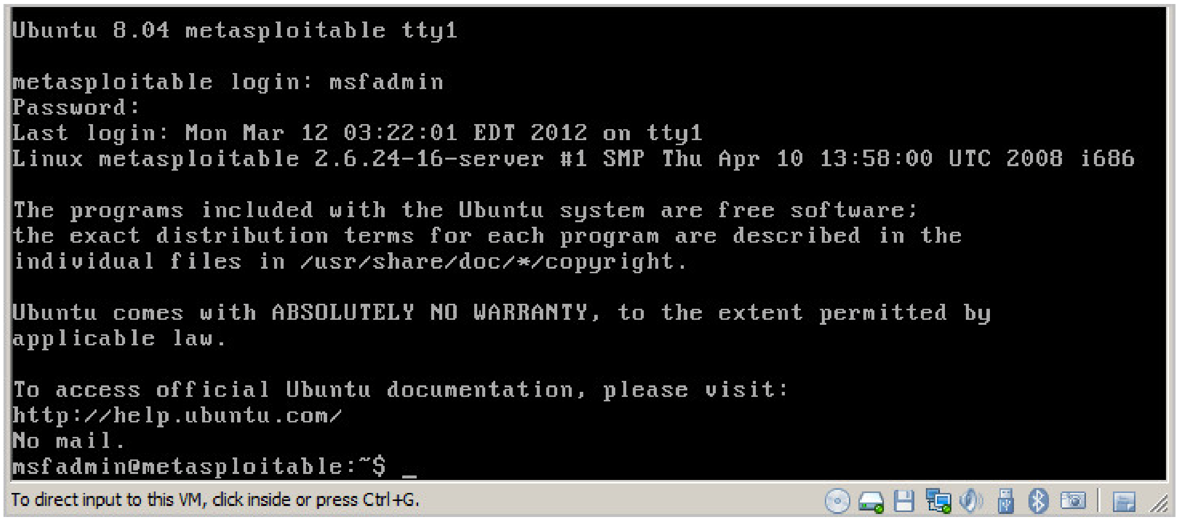
Before the virtual machine boots up, VMware prompts you to choose whether you copied or moved the virtual machine. Select the copied option. The Metasploitable VM will boot up and install all the necessary services and applications.

Logging In to Metasploitable

When Metasploitable boots up, the system prompts you for the Metasploitable login. To log in to Metasploitable, use the following credentials: `msfadmin:msfadmin`.

After you successfully log in to Metasploitable, the terminal drops to a command line prompt.

The following image shows the screen after you log in to Metasploitable:



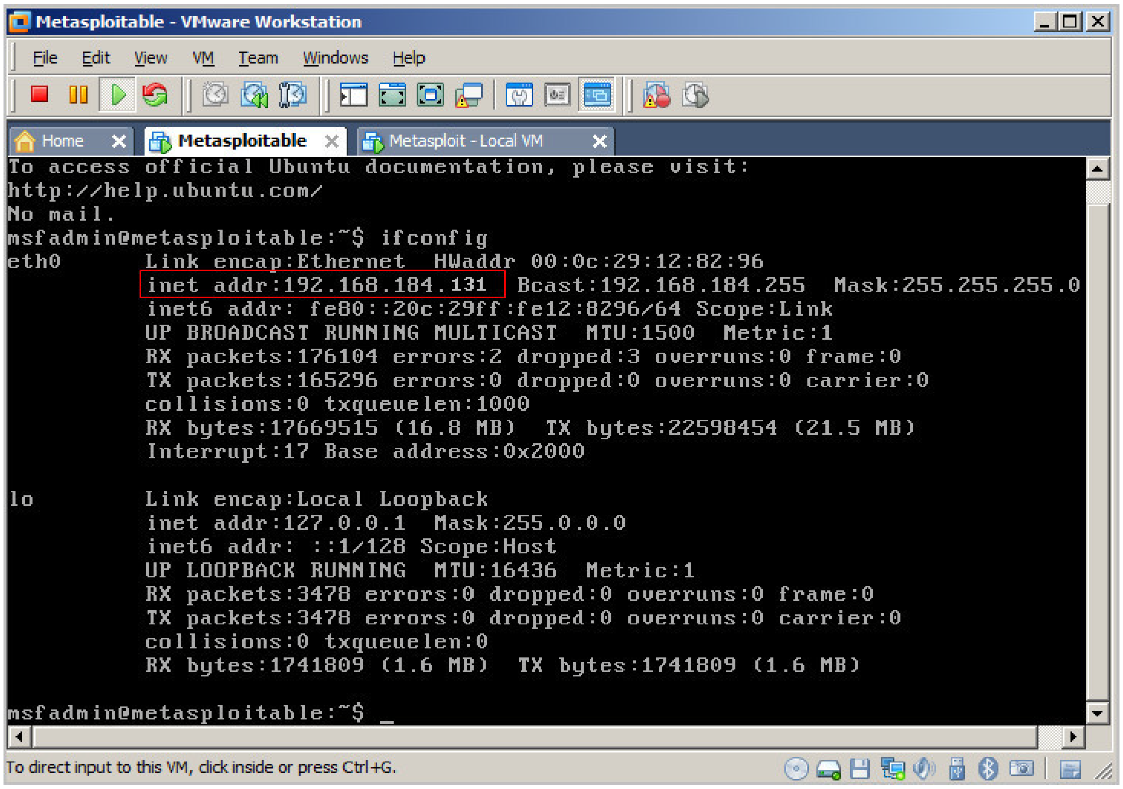
```
Ubuntu 8.04 metasploitable tty1

metasploitable login: msfadmin
Password:
Last login: Mon Mar 12 03:22:01 EDT 2012 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Identifying the IP Address for Metasploitable

After you log in to Metasploitable, you must identify the IP address that has been assigned to it. This is the target host address that you use to scan for vulnerable services and exploit vulnerabilities in Metasploit.

To identify the IP address for Metasploitable, type `ifconfig` at the command prompt.

The following image shows the results that `ifconfig` returns:



Metasploitable - VMware Workstation
File Edit View VM Team Windows Help
Home
Metasploitable
Metasploit - Local VM
To direct input to this VM, click inside or press Ctrl+G.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:12:82:96
          inet addr:192.168.184.131  Bcast:192.168.184.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe12:8296/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:176104 errors:2 dropped:3 overruns:0 frame:0
          TX packets:165296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17669515 (16.8 MB)  TX bytes:22598454 (21.5 MB)
          Interrupt:17 Base address:0x2000

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:3478 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1741809 (1.6 MB)  TX bytes:1741809 (1.6 MB)

msfadmin@metasploitable:~$ _
```

Based on the results, the IP address for the Metasploitable virtual machine is `192.168.184.131`.

GETTING STARTED WITH METASPLOITABLE

This chapter covers the following topics:

Host Discovery

Host discovery is the process of identifying the ports, services, and operating systems that are in use by hosts on a particular network. You run a scan to find the hosts that are accessible on a network and to help you identify vulnerabilities based on the open ports and services that the scan finds.

Scanning Metasploitable with Metasploit Pro

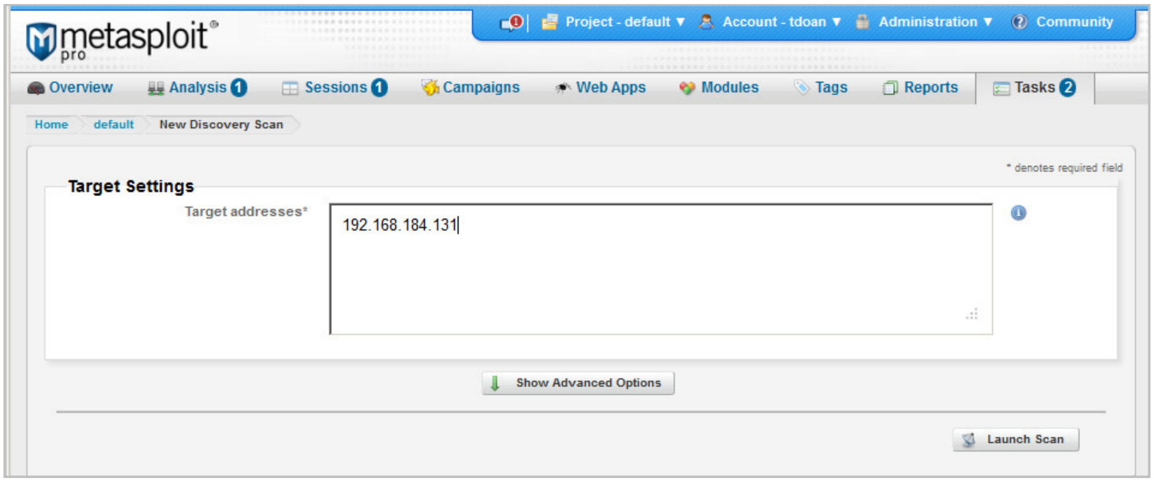
As a Metasploit Pro user, you can launch a discovery scan to enumerate services and ports on the Metasploitable machine. A discovery scan performs host discovery, port scanning, and OS fingerprinting.

A discovery scan starts with an Nmap scan to detect available systems and scan ports. Next, the discovery scan sweeps the target network with UDP probes to identify additional systems. After the discovery scan identifies available ports, the discovery scan sweeps the ports with service specific modules to identify active services.

To perform a discovery scan with Metasploit Pro:

1. Create a new project or open an existing project.
2. Click the **Analysis** tab.
3. Click **Scan**.
4. Enter the IP address for Metasploitable in the **Target Addresses** field.
5. Click **Show Advanced Options** to view a list of additional options that you can configure. You may want to change the portscan speed, depending on your network connection. The default setting is **Insane**, but you should use this setting only if you are on a fast LAN. You can use **Normal** for most network connections.

The following image shows a basic discovery scan configuration:

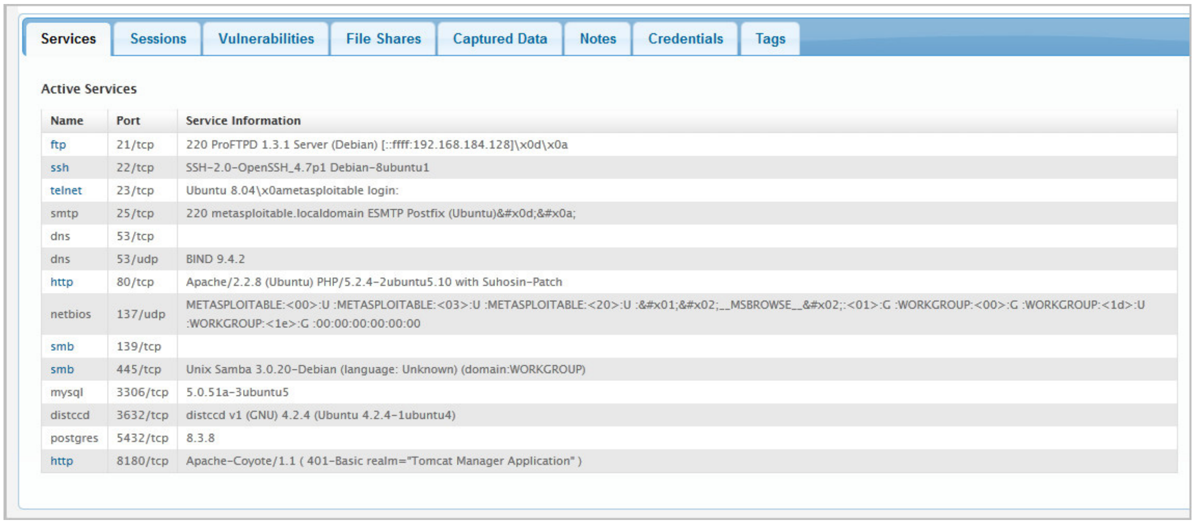


* denotes required field

Target Settings

Target addresses*: 192.168.184.131

After the scan completes, the Host page displays a list of all active services discovered by the scan:



Active Services

Name	Port	Service Information
ftp	21/tcp	220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.184.128]\x0d\x0a
ssh	22/tcp	SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
telnet	23/tcp	Ubuntu 8.04\x0ametasploitable login:
smtp	25/tcp	220 metasploitable.localdomain ESMTP Postfix (Ubuntu)&#x0d;&#x0a;
dns	53/tcp	
dns	53/udp	BIND 9.4.2
http	80/tcp	Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
netbios	137/udp	METASPLOITABLE:<00>:U :METASPLOITABLE:<03>:U :METASPLOITABLE:<20>:U :&#x01;&#x02;__MSBROWSE__&#x02;:<01>:G :WORKGROUP:<00>:G :WORKGROUP:<1d>:U :WORKGROUP:<1e>:G :00:00:00:00:00:00
smb	139/tcp	
smb	445/tcp	Unix Samba 3.0.20-Debian (language: Unknown) (domain:WORKGROUP)
mysql	3306/tcp	5.0.51a-3ubuntu5
distccd	3632/tcp	distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
postgres	5432/tcp	8.3.8
http	8180/tcp	Apache-Coyote/1.1 (401-Basic realm="Tomcat Manager Application")

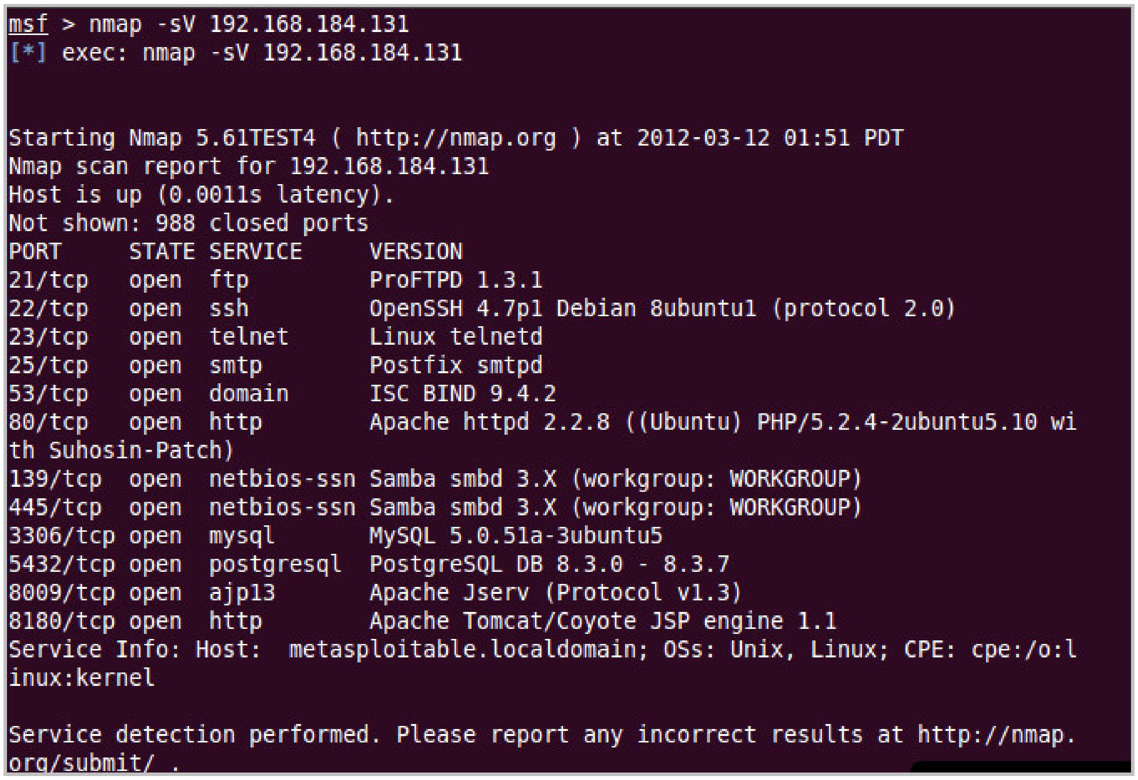
Scanning Metasploitable with the Metasploit Framework

If you are a Metasploit Framework user, you can run an Nmap scan directly from msfconsole to enumerate services and ports.

Use a command, like the following, to perform an Nmap scan through msfconsole:

```
msf > nmap -sV 192.168.184.131
```

The following image shows the results of the Nmap scan:



```
msf > nmap -sV 192.168.184.131
[*] exec: nmap -sV 192.168.184.131


Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-12 01:51 PDT
Nmap scan report for 192.168.184.131
Host is up (0.0011s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 wi
th Suhosin-Patch)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:l
inux:kernel

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
```

Bruteforce Attacks

A bruteforce attack tries a large number of common user name and password combinations in order to open a session on the target machine. After the bruteforce attack successfully guesses a credential, the system stores the user name and password in the project or workspace.

Running a Bruteforce Attack with Metasploit Pro

In Metasploit Pro, the bruteforce attack launches service specific modules to attempt to crack the credentials for the service. You choose the services that you want to target, and the bruteforce attack chooses modules that target those services.

If the bruteforce attack successfully cracks a credential and opens a session, you can use the session to gain further access and information for the system.

To perform a bruteforce attack against Metasploitable:

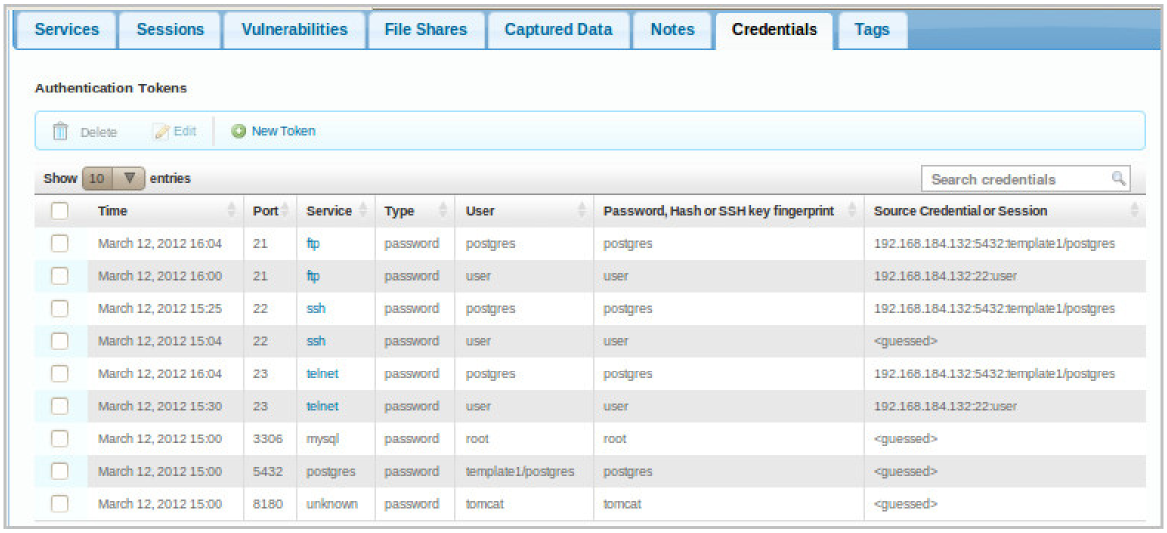
1. In your project, click the **Analysis** tab.
2. Select the Metasploitable machine.
3. Click **Bruteforce**.
4. When the Bruteforce configuration page appears, choose the services that you

want to target and the depth of the bruteforce attack. For example, if you want the bruteforce attack to only try default user name and passwords combinations, you can choose the **defaults only** depth. Additionally, you can set any of the advanced settings to further customize the bruteforce attack.

5. Launch the bruteforce attack.

After the bruteforce finishes, you can view the cracked passwords, exposed file shares, collected hashes, system notes, and active sessions from the host page.

The following image shows the list of credentials that the bruteforce attack looted from Metasploitable.



Authentication Tokens

□	Time	Port	Service	Type	User	Password, Hash or SSH key fingerprint	Source Credential or Session
□	March 12, 2012 16:04	21	ftp	password	postgres	postgres	192.168.184.132:5432:template1/postgres
□	March 12, 2012 16:00	21	ftp	password	user	user	192.168.184.132:22:user
□	March 12, 2012 15:25	22	ssh	password	postgres	postgres	192.168.184.132:5432:template1/postgres
□	March 12, 2012 15:04	22	ssh	password	user	user	<guessed>
□	March 12, 2012 16:04	23	telnet	password	postgres	postgres	192.168.184.132:5432:template1/postgres
□	March 12, 2012 15:30	23	telnet	password	user	user	192.168.184.132:22:user
□	March 12, 2012 15:00	3306	mysql	password	root	root	<guessed>
□	March 12, 2012 15:00	5432	postgres	password	template1/postgres	postgres	<guessed>
□	March 12, 2012 15:00	8180	unknown	password	tomcat	tomcat	<guessed>

Running a Bruteforce Attack with the Metasploit Framework

Before you can run a bruteforce attack, you need to review the list of services discovered by the Nmap scan. Use the service information to determine the modules that you want to run as part of the bruteforce attack. You can search for modules that target specific services.

For example, since the scan identified SMB and MySQL, you can run the smb_login module (auxiliary/scanner/smb/smb_login) and the mysql_login module (auxiliary/scanner/mysql/mysql_login).

The following example shows how you can run the mysql_login module in msfconsole:

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(smb_login) > show options
msf auxiliary(smb_login) > set RHOSTS 192.168.184.131
msf auxiliary(smb_login) > set THREADS 1000
msf auxiliary(smb_login) > run
```

Evidence

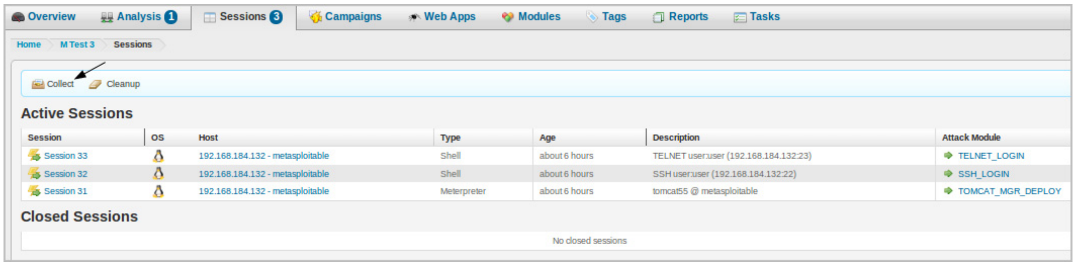
During evidence collection, Metasploit Pro gathers system passwords, system information, screenshots, SSH keys, and system files.

The purpose of evidence collection is to obtain sensitive information and to use that information to gain further access to the network or as evidence of compromise. For example, you can use screenshots to show that you were able to gain access to a targeted system.

Note: Metasploit Community does not provide access to evidence collection. You must use Metasploit Pro or Metasploit Express to use this feature.

Collecting Evidence with Metasploit Pro

1. In your project, click the **Sessions** tab.
2. Click **Collect**.



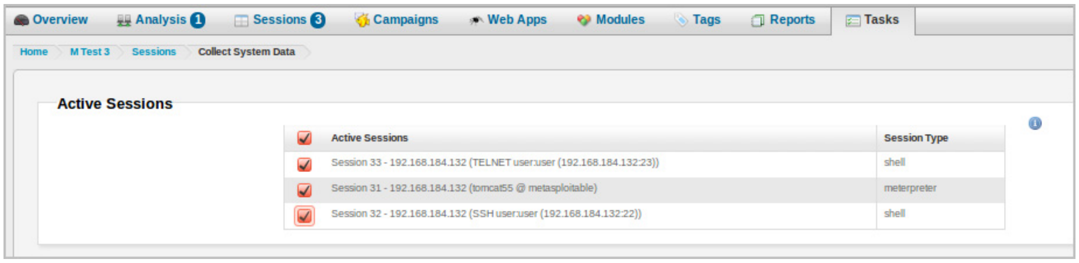
Active Sessions

Session	OS	Host	Type	Age	Description	Attack Module
Session 33		192.168.184.132 - metasploitable	Shell	about 6 hours	TELNET user:user (192.168.184.132:23)	TELNET_LOGIN
Session 32		192.168.184.132 - metasploitable	Shell	about 6 hours	SSH user:user (192.168.184.132:22)	SSH_LOGIN
Session 31		192.168.184.132 - metasploitable	Meterpreter	about 6 hours	tomcat55 @ metasploitable	TOMCAT_MGR_DEPLOY

Closed Sessions

No closed sessions

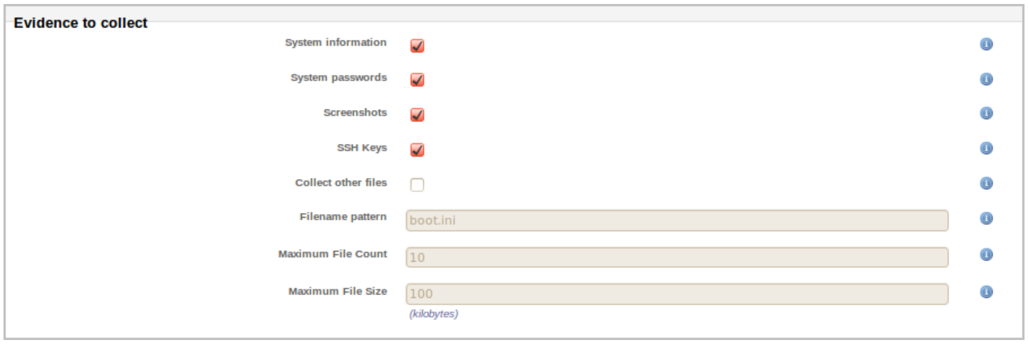
3. When the **Collect System Data** window appears, select the sessions that you want to use to collect evidence.



Active Sessions

☑	Active Sessions	Session Type
☑	Session 33 - 192.168.184.132 (TELNET user:user (192.168.184.132:23))	shell
☑	Session 31 - 192.168.184.132 (tomcat55 @ metasploitable)	meterpreter
☑	Session 32 - 192.168.184.132 (SSH user:user (192.168.184.132:22))	shell

4. Select the information that you want to collect.



Evidence to collect

System information	☑
System passwords	☑
Screenshots	☑
SSH Keys	☑
Collect other files	□
Filename pattern	boot.ini
Maximum File Count	10
Maximum File Size	100 (kilobytes)

5. Run the data collection.

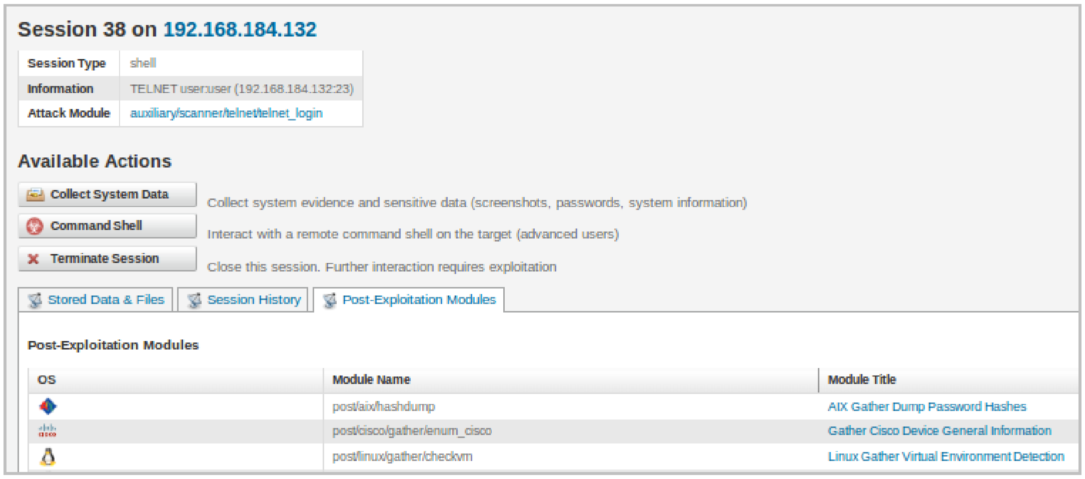
Post-Exploitation

If you ran a bruteforce attack against Metasploitable, then you should have a few open sessions that you can use to gather additional information and further exploit the machine. For example, you may have an SSH, telnet, and Tomcat session open. The session type, Meterpreter or shell, determines what kind of actions you can perform within the session.

During post-exploitation, your goal is to determine the value of information stored on the target machine and to find a way to maintain access to the exploited system.

Running a Post-Exploitation Module with Metasploit Pro

1. In your project, click the **Sessions** tab.
2. Click on a session name to open the session's details page.
3. Click the **Post-Exploitation Modules** tab. A list of post-exploitation modules that you can run against the session displays. Metasploit Pro compiles the list of post-exploitation modules based on the service and system information that is available for the session.



Session 38 on 192.168.184.132

Session Type	shell
Information	TELNET user:user (192.168.184.132:23)
Attack Module	auxiliary/scanner/telnet/telnet_login

Collect system evidence and sensitive data (screenshots, passwords, system information)

Interact with a remote command shell on the target (advanced users)

Close this session. Further interaction requires exploitation

Post-Exploitation Modules

OS	Module Name	Module Title
◆	post/aix/hashdump	AIX Gather Dump Password Hashes
cisco	post/cisco/gather/enum_cisco	Gather Cisco Device General Information
🐧	post/linux/gather/checkvm	Linux Gather Virtual Environment Detection

4. Scroll through the list of post-exploitation modules and click on the module title for the exploit that you want to run.
5. When the post-exploitation details page displays, select any additional sessions that you want to run the post-exploitation module against.
6. Configure any options that you need in order to obtain the results that you want.
7. Run the module.

Reports

Metasploit Pro offers several report types that you can use to categorize your findings and test results. The report type that you select depends on the information that you want to present. For example, to show the data that you collected from Metasploitable, you can generate a collected evidence report. Or to present a high-level overview of the test results, you can generate an audit report.

Ultimately, reports help you to clearly assess and identify the vulnerabilities and risks that exist on the target system. Use this information to provide support and to outline the tactics that an organization can implement to improve its security posture.

Note: Metasploit Community does not provide access to reports. You must use Metasploit Pro or Metasploit Express to use this feature.

Generating a Report with Metasploit Pro

1. In your project, click the **Reports** tab. The **Saved Reports and Data Exports** page appears.
2. Click **Standard Report**. The **New Reports** page appears.
3. Select a report type. For example, if you want a detailed report of the evidence collected by Metasploit Pro, choose the collected evidence report.
4. Select the report format that you want to use to generate the report. You can choose multiple report formats. For example, you can generate a PDF and a Word report.
5. Enter a name for the report.
6. Select the sections that you want to include in the report. The sections that are available vary between report types. For example, a services report can contain a network services table, and a collected evidence report can contain a complete evidence table.
7. Choose whether you want to include graphics and charts in the report.
8. Generate the report.

After Metasploit Pro generates the report, you can view the completed report from the Reports page. Review the reports to analyze and assess your findings.