Teacher Guide

|  |  |  |
| --- | --- | --- |
| Kali linux Icon | Simpleicons Brands Iconpack | Simpleicons Team | Podman - Wikipedia | Hacking Metasploitable 2: Installation and Escalation |

**Please Complete All Four Sections Below in Sequential Order!**

**Section 1 - Guided + Independent Practice  
Engineer and network a Docker ethical hacking lab using containers (Kali, Metasploitable2)**Suggested Solution at Bottom

Podman containers, not to be confused with virtual machines, are process configurations that rely on a host operating system (OS). In the case of running Podman Desktop on Windows, users typically install the Windows Subsystem for Linux (WSL v2), which consists of a bare bones Linux OS (Fedora) that serves as the container(s) host system on which they run. Docker may also be configured to run Windows containers, which would utilize the host system’s OS but open up your Windows system to a plethora of security vulnerabilities. (**Insert Image 1**)

Podman Desktop provides a graphical user interface (GUI) management window that enables users to pull images and manage containers and applications. The Podman Desktop installation also prompts the user to install the Podman engine on which the container processes operate.

Let’s assume for this foundational unit lesson that we’re going to stick with Linux containers and utilize WSL 2 within the Windows environment.

Step 1.1 – Turn on Windows Features Virtual Machine Platform and Windows Subsystem for Linux and restart your computer.

A screenshot of a computer

AI-generated content may be incorrect.

Update WSL and set to version 2 in PowerShell or Command Prompt (admin):

> wsl.exe --update

> wsl --set-default-version 2

Do a status check to confirm everything is fine:

> wsl –status

Step 1.2 – Install Podman Desktop and Docker Engine.

Podman Desktop downloads can be found at <https://podman-desktop.io/downloads>. We are interested in [Podman Desktop for Windows (x64)](https://github.com/podman-desktop/podman-desktop/releases/download/v1.19.1/podman-desktop-1.19.1-setup-x64.exe). You will be automatically prompted to install the Podman Engine.



Step 1.3 – In Podman Desktop, select Images in the left menu and Pull in the top menu. Search for and pull the following images: *kalilinux/kali-rolling*, *tleemcjr/metasploitable2*

A screenshot of a computer

AI-generated content may be incorrect.

Step 1.4 – Open a PowerShell terminal as administrator. In the first terminal, create your network to be shared by the containers and assign an IP range and subnet. I created a network called “podnetwork” using bridge mode to host and an IP range beginning at 4.3.2.0 on /27 (cidr notation) or subnet 255.255.224.0.

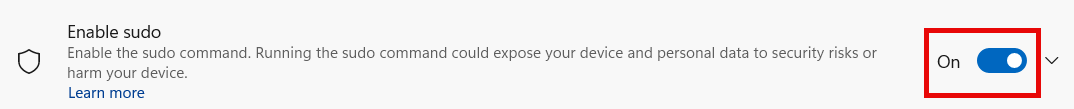


After creation, check to make sure “podnetwork” is listed following the PowerShell command >podman network list

A screenshot of a computer

AI-generated content may be incorrect.

Step 1.5 – Before running the sudo (super user do) command, enable “sudo” in Windows - Developer Settings – Enable sudo when needed and disable it when not in use.



Open two PowerShell terminals and separately run both containers on the hackwork network. Here are the terminal commands for each:





Once ready, you should have two terminal windows open to each of the containers’ file systems:

A screenshot of a computer

AI-generated content may be incorrect.

**What happens if I restart or boot Windows?**  
To start Podman and your containers on Windows, first open Podman and click on the run symbol next to each container:

A screenshot of a chat

AI-generated content may be incorrect.

Then open two PowerShell terminals as administrator on Windows and enter the following commands:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Step 1.6 – Update, upgrade, and install the requisite Kali Linux binaries:

At the Kali terminal, you are logged in as root and will see a # symbol prompt. Install the necessary binaries using the Advanced Packet Tool (APT):

Update and upgrade:  
# apt update

# apt full-upgrade -y

Install plocate (locate command) and update the database:

# apt install -y plocate

# updatedb

Test the locate command by locating the binary for Lynx:

A screen shot of a computer program

AI-generated content may be incorrect.

Install Kali Net-tools, Cewl, and Medusa:  
# apt install -y net-tools

# apt install -y netcat

# apt install -y wordlists

# apt install -y maskprocessor (hint: use “mp64” to run from terminal)

# apt install -y lynx

# apt install -y medusa

# apt install -y hydra

Install Netcat (IP and Port Scanning):

# apt install -y netcat-traditional

A screen shot of a computer

AI-generated content may be incorrect.

Run the locate command to make sure Net-tools, Netcat, Lynx, Wordlists, Maskprocessor, and Medusa are installed. Here is an example using the locate function to search for instances of Netcat:

A screen shot of a computer screen

AI-generated content may be incorrect.

The “bin” in the Linux file path */usr/bin/netcat* stands for “binary”, which are scripts or applications.

**Step 1.7 –** **Independent Practice**  
The core binary used in Kali for targeting exploits in systems is called Metasploit (Framework). Your task is to research how to install Metasploit on Kali. Then use your Kali PowerShell terminal to install Metasploit and its database. Finish by starting up Metasploit and providing a screenshot of the graphic, version, and the msf6 > prompt with a search result for the vsftpd exploit.

(Suggested Solution):

Install Metasploit  
# apt install -y Metasploit-framework

Start Metasploit and initialize database

# msfconsole

**Step 1.8 – Independent Practice**

Look up the vsftpd exploit on the Rapid7 Exploit Database:   
<https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor>

Print out the Metasploit solution guide for exploiting the vsftpd 2.3.4 backdoor vulnerability.

msf6 > search vsftpd

A computer screen shot of a black screen

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

**A blue and white cat face

AI-generated content may be incorrect.**

**Section 2 - Guided + Independent Practice**

**Network Reconnaissance and Assessing Target Vulnerabilities**Suggested Solution at Bottom

Our podnetwork uses the IP range 4.3.2.0/27. What that means is that both Kali and Metasploitable2 were assigned IP addresses on a first-come, first-served basis via the Domain Host Control Protocol (DHCP). Think of an IP address as like a key to joining a network. The /27 part is CIDR notation for the subnet 255.255.224.0. Subnets are a means toward creating local area networks (LANs). A router usually sits at the heart of a LAN and is the instrument that assigns new devices IP addresses via DHCP. (**Insert Image 2**)

A good tool for looking up CIDR notation is Subnet Ninja’s Cheat Sheet:

<https://subnet.ninja/subnet-cheat-sheet>

There is a networking model known as the OSI 7 layers of networking. It breaks down the networking layers into seven groups to help with understanding. Routers, LANs, and IP addresses fall under Layer 3 (Network).

See: <https://www.geeksforgeeks.org/open-systems-interconnection-model-osi>

Systems that are assigned IP addresses on a LAN communicate with one another via ports and services. Firewalls are used to manage open and closed ports and allow/disallow traffic.

For this guided practice, we are going to use Netcat to analyze and output a list of the target system’s open ports and services.

Step 2.1 – In the separate PowerShell terminals, look up the Kali and Metasploitable2’s IP addresses with ifconfig:

A screenshot of a computer program

AI-generated content may be incorrect.

We can see that both Kali and Metasploitable2 have been assigned IP addresses from the 4.3.2.0/27 range we specified when we created our “podnetwork”. That’s good. We are going to focus on the target Metasploitable2’s IP address of 4.3.2.3.

Step 2.2 – Let’s run Netcat against our target system’s IP of 4.3.2.3 and ports 1 thru 443. We are going to use the arguments *-z* (report connection status) and *-v* (verbose output):

A screen shot of a computer

AI-generated content may be incorrect.

We are going to focus on the Secure Shell (SSH) service “open” on port 22.

Port 22/tcp ssh (Secure Shell)

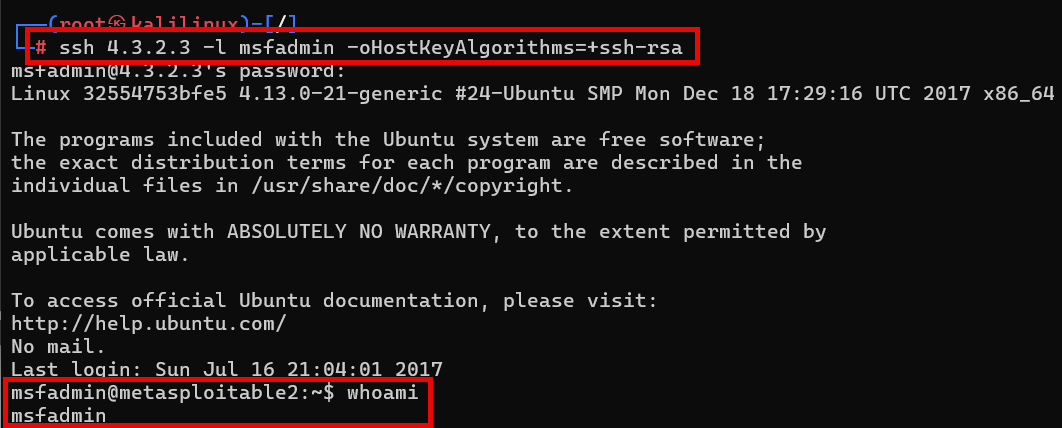
Services like “ssh” listen for like connections from other hosts. We are going to connect to the target system via SSH port 22 and then, at the conclusion of this lesson, utilize the same service/port to password crack with Medusa.

Step 2.3 – Use your Kali terminal to install Secure Shell (SSH) and connect to the target system:

A screen shot of a computer

AI-generated content may be incorrect.

Next, we’ll connect to the target from Kali using SSH, the administrative user “msfadmin” and the ssh-rsa algorithm override for Kali to communicate to the target system:



The *-l* argument is for entering the username.

Hint: We’ll pretend that we don’t know the exact username and password for the Maskprocessor wordlists part of the lesson; however, we’ll use the knowledge gained that both the username and password of the target system are eight characters in length and use the letters (a, d, f, I, m, n, s).

**2.4 - Independent Practice**  
Open your Kali PowerShell terminal and perform the following tasks:

1. Install FTP and connect to the Metasploitable2 target over port 21. You may need to use the “msfadmin” user and password to log in.
2. Install Telnet and connect to the Metasploitable2 target over port 22. You may notice a clue on the initial screen specifying the username and password!
3. Do some internet research and explain why it was necessary to use the *-oHostKeyAlgorithms=+ssh-rsa* argument in the SSH connection above. What does “ssh-rsa” stand for? Why does this argument allow us to connect our Kali system to the target Metasploitable2?

(Suggested Solution)

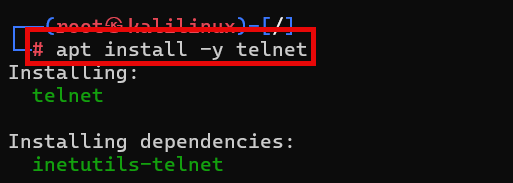
1. Install FTP and connect to Metasploitable2.

# apt install -y ftp

A screen shot of a computer

AI-generated content may be incorrect.

2. Telnet and connect to Metasploitable2 (reveals “msfadmin” username/password).



A screenshot of a computer screen

AI-generated content may be incorrect.

3. Why is the argument *-oHostKeyAlgorithms=+ssh-rsa* necessary to connect Kali Linux to Metasploitable2 via SSH?

The key to this task is modifying the SSH connection string to allow Kali to communicate with an outdated cipher on Metasploitable2 (RSA): *-oHostKeyAlgorithms=+ssh-rsa*

A blue circle with a white gear and a black dragon

AI-generated content may be incorrect.

**Section 3 - Guided + Independent Practice  
Build Strategic User and Password Lists with Maskprocessor**

Suggested Solution at Bottom

Maskprocessor (“mp64”) is a powerful Kali Linux tool to install. This open-source tool is used for creating custom wordlists from scanned websites. Wordlists are giant delimited lists of username and/or password possibilities. (**Insert Image 3**)

With Maskprocessor, users may generate custom wordlists based on criteria such as character sets, length, patterns, and combinations. Maskprocessor wordlists may be used with password cracking tools such as Hashcat, Hydra, Medusa, and John the Ripper. The more accurate the wordlist, the less time it takes to crack passwords.

Of note is that at the heart of password cracking lies hashes. Hashes are strings of random-looking characters that are generated by a system to mask the original username or password. This process of masking is called a cipher. For example, a password such as “iL0v3U” will not be visible in the system to a threat actor. What will be available upon deep inspection is the hash generated from the password iL0v3U.

You can use a converter tool such as dCode (<https://www.dcode.fr/hash-function>) to play around with hashes like md5 and sha1. Here is an example output of the password iL0v3U hashed with md5:

A close-up of a tool

AI-generated content may be incorrect.

Step 3.1 – Check to see if Maskprocessor is installed on the system:

A screen shot of a computer

AI-generated content may be incorrect.

Step 3.2 – Learn some Maskprocessor syntax with help.

A screenshot of a computer program

AI-generated content may be incorrect.

Practice using the syntax with this example:

* Generate a wordlist that is three characters using only lower-case alpha (a – z).
* Output the wordlist to *mp64\_wordlist3.txt*.
* Show the first and last five words generated in the wordlist using head and tail functions.
* Use the chmod command to change the file permissions to 775 (Read, Write).
* List the folder contents.

A screen shot of a computer

AI-generated content may be incorrect.

Step 3.3 – Create a wordlist directory in Kali (*/root/wordlists*), change its permissions recursively, and generate three sample wordlists with Maskprocessor.

Create a wordlist directory and change its permissions to 775. The *-R* stands for recursive, meaning that the 775 directory permissions flow down to all the directories and files therein.

A computer code on a black background

AI-generated content may be incorrect.

Example 1: Generate a wordlist titled *wordlist-1.txt* with lowercase alpha (a-z) of length 3 to 4 characters:

A black and red background with white text

AI-generated content may be incorrect.

Use the head command to view the first 10 list items (three characters in length):

A screen shot of a computer

AI-generated content may be incorrect.

And the tail command to check the last 10 list items (four characters in length):  
A screen shot of a computer

AI-generated content may be incorrect.

Example 2: Generate a wordlist called *wordlist2.txt* with alphanumeric characters (a-z, 0-9) of length 2-3 characters and use the head (two characters) and tail (three characters) to verify results:

A screenshot of a computer program

AI-generated content may be incorrect.

**3.4 Independent Practice**

We know from the Netcat network reconnaissance guided practice that the Kali username and password consists of eight alpha characters and the letters a, d, f, i, m, n s. However, pretend we are not sure of the order of those characters except for the first four characters (msfa. . . .). Use Maskprocessor to generate both your user and password wordlists in the */root/wordlists* folder. The more accurate your wordlist, the better the time savings.

(Suggested Solution)

Given that we know the order of the first six lower case characters (msfadm \_ \_), the total characters (adfimns), and the length (8 characters) of the Metasploitable2 username and password, we can use Maskprocessor to output the following strategic wordlist:



A screenshot of a computer program

AI-generated content may be incorrect.

The outputs begin with “msfad” and all eight-character possibilities are completed. The user and password wordlists will be the same.

A screen shot of a computer

AI-generated content may be incorrect.

A green mask with yellow eyes and a black background

AI-generated content may be incorrect.

**Section 4 - Guided + Independent Practice**

**Exploit Target System Vulnerability and Brute Force Crack with Medusa**

Suggested Solution at Bottom

Medusa is an amazing password cracking tool available for Kali Linux. It is a parallel, modular, brute-force login username and password cracker that supports numerous protocols for target entry to commence its attack.

See: <https://www.kali.org/tools/medusa>

Step 4.1 - For a list of the Medusa function’s arguments (options), open your Kali PowerShell terminal and type in:

# medusa -h

A screenshot of a computer program

AI-generated content may be incorrect.

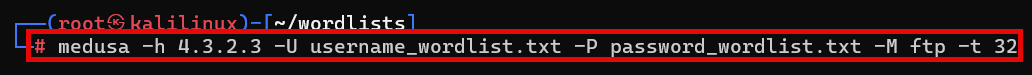
Step 4.2 - For example, if we were to type in a Medusa command to brute-force attack a target’s usernames and passwords, we would use the following:

# medusa -h [target IP] -U [username list] -P [password list] -M [module] -t [threads default 16]

**4.3 Independent Practice**Step - 4.3.1- FTP - Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the FTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete.

Suggested Solution

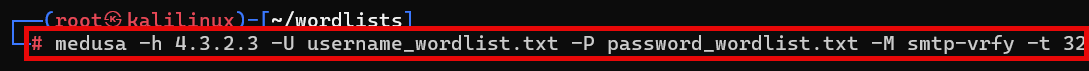
(Answers may vary based on students’ IP addresses, Maskprocessor-generated wordlists, and protocols):



Step - 4.3.2- SMTP - Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the SMTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete. Medusa may take quite some time, based on your computing resources. I recommend using 32 threads. Graphics card processors are far superior to CPUs in hash/password cracking exercises!

Suggested Solution – Hint: “smtp” is not the correct Medusa module name!

(Answers may vary based on student’s IP addresses, Maskprocessor-generated wordlists, and protocols):



Step - 4.3.3 - SSH - Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the FTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete.

Suggested Solution

(Answers may vary based on student’s IP addresses, Maskprocessor-generated wordlists, and protocol):



A logo with a cat and text

AI-generated content may be incorrect.A green dragon with white teeth

AI-generated content may be incorrect.

**Section 5 - Guided + Independent Practice**

**Exploit Target System’s Web Server (“DVWA”) Vulnerability and Brute-Force Crack with Hydra**

Suggested Solution at Bottom

Hydra is a parallel, mult-threaded brute-force username and password cracking tool. Hydra can be configured to crack website login pages (username and password input fields). However, let’s first get acquainted with the text-based Linux web browser Lynx. The Lynx browser will prove useful when using either Docker or Podman to build and work with your container-based ethical hacking lab.

Step 5.1 – Verify install of Lynx performed earlier in the lesson:

A red square with white text

AI-generated content may be incorrect.

Step 5.2 – Let’s open the Damn Vulnerable Web Application (“DVWA”) that comes packaged with Metasploitable2:

A screenshot of a computer

AI-generated content may be incorrect.

Now we can see above the DVWA comes packaged with TWiki, phpMyAdmin, Mutillidae, DVWA, and WebDAV. The admin username and password “msfadmin” is also provided; ignore that for now. The Commands at the bottom utilize the arrow keys to move and lowercase and uppercase letters and symbols for menu options.

Step 5.3 – Use the arrow keys to highlight “DVWA” and surf to that page:

A screenshot of a computer

AI-generated content may be incorrect.

Notice the Username and Password entry fields and a Login option. Please ignore the supplied admin username and password.

**5.4 – Independent Practice**  
Check out the screenshot of the DVWA login page above. What is the URL for this page?

5.5 – Suggested Solution

The URL for the page is http://4.3.2.3/dvwa/login.php

**5.6 – Independent Practice**   
Log in to the DVWA web server and in the Security menu section change the security level to “Low”.

5.7 – Suggested Solution  
A screenshot of a computer

AI-generated content may be incorrect.

**5.8 – Independent Practice**  
Remember how to build a Massprocessor username list and password list? Let’s assume you know the first three lower alpha letters of the user password. Build the list *username\_wordlist2.txt* and display the first and last 10 character strings.

Suggested Answer:A screenshot of a computer

AI-generated content may be incorrect.

Now assume you know the first six letters of the lower alpha password. Use Massprocessor to build the list *password\_wordlist2.txt* and show the first and last 10 character strings:

Suggested Answer:

A screen shot of a computer

AI-generated content may be incorrect.

A green dragon with white teeth

AI-generated content may be incorrect.

**5.9 Independent Practice**  
Hydra is an amazing password cracking tool available for Kali Linux. It is a parallelized login multi-thread capable password cracker that supports numerous protocols for target entry to commence its attack. Let’s use Hydra to brute-force attack the DVWA login page (/dvwa/login.php).

See: <https://www.kali.org/tools/hydra>

Step 5.10 - For a list of Hydra’s arguments (options), open your Kali PowerShell terminal and type in:

# hydra -h

A screenshot of a computer screen

AI-generated content may be incorrect.

Step 5.11 - For example, if we were to type in a Hydra command to brute-force attack a target’s usernames and passwords, we would use the following:

# hydra -L usernames.txt -P wordlist.txt <targetIP> <protocol>

**Step 5.12 – Independent Practice**  
Please use the two wordlists (*username\_wordlist2.txt*, *password\_wordlist2.txt*) you recently generated with Maskprocessor (mp64). Do some AI searching with Grok and Gemini on how to use Hydra to brute force the DVWA login page. Make sure you preface your searches with “ethical hacking” and “authorized” to avoid being flagged!

5.12a - Use what you’ve learned from the AI language learning models and build a successful command string to brute force the DVWA login page with hydra and your two wordlists. Submit a screenshot of your command string and successful attempt.

5.12b - Please break down the parts of the command string and explain the purpose of each part!

5.12c - Analyze and compare the differences between Grok’s and Gemini’s command string.

5.13 - Suggested Solution

Question: **“How do you use Hydra to ethically hack the DVWA login.php page?”**  
  
**AI Google Gemini solution (works):**

Unmodified from Gemini (edit to suit environment IP address, etc.)

*# hydra -L users.txt -P passwords.txt 192.168.1.100 http-post-form \*

*"/DVWA/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed" -V*

Gemini solution customized to use two Maskprocessor (mp64) wordlists and IP address of our target:

A screenshot of a computer program

AI-generated content may be incorrect.

**AI Grok 3 solution (works)**

Unmodified from Grok (edit to suit environment IP address, etc.)

*# hydra -L /root/users.txt -P /root/passwords.txt localhost http-post-form \*

*"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"*

Grok3 solution customized to use two Maskprocessor (mp64) wordlists and IP address of our target:

A screen shot of a computer

AI-generated content may be incorrect.

The elements of both Gemini’s and Grok’s command strings are:  
1. Hydra command, -L username.list -P password.list IP address of target http-post-form (URL, form fields and actions for username and password data entry) and return message for failed login attempts.