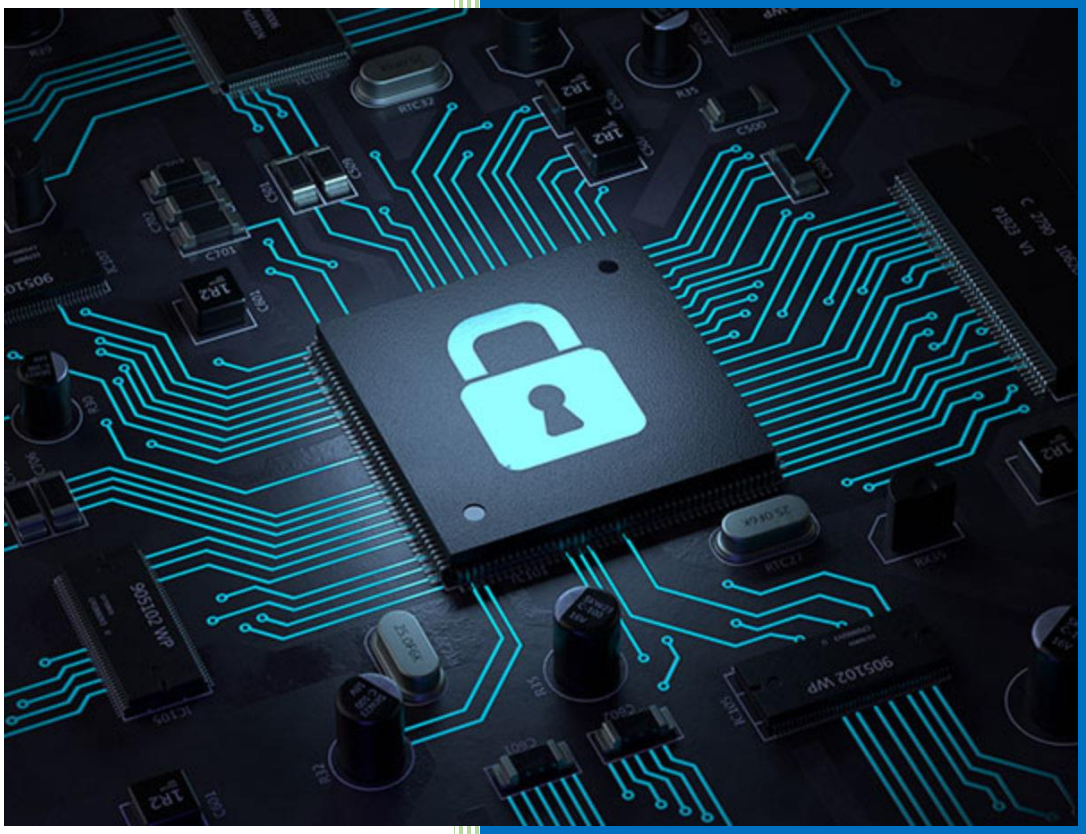
FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY



Lab 7: Web Application Security (Part 1)

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of the virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) *The lab report must be submitted within the time given using the provided link in the eLearning platform.*

`

TASK 1: EXPLORING VULNERABLE WEBSITES IN METASPLOITABLE

OBJECTIVE

To explore vulnerable websites in Metasploitable Virtual Machine.

TASK DESCRIPTION

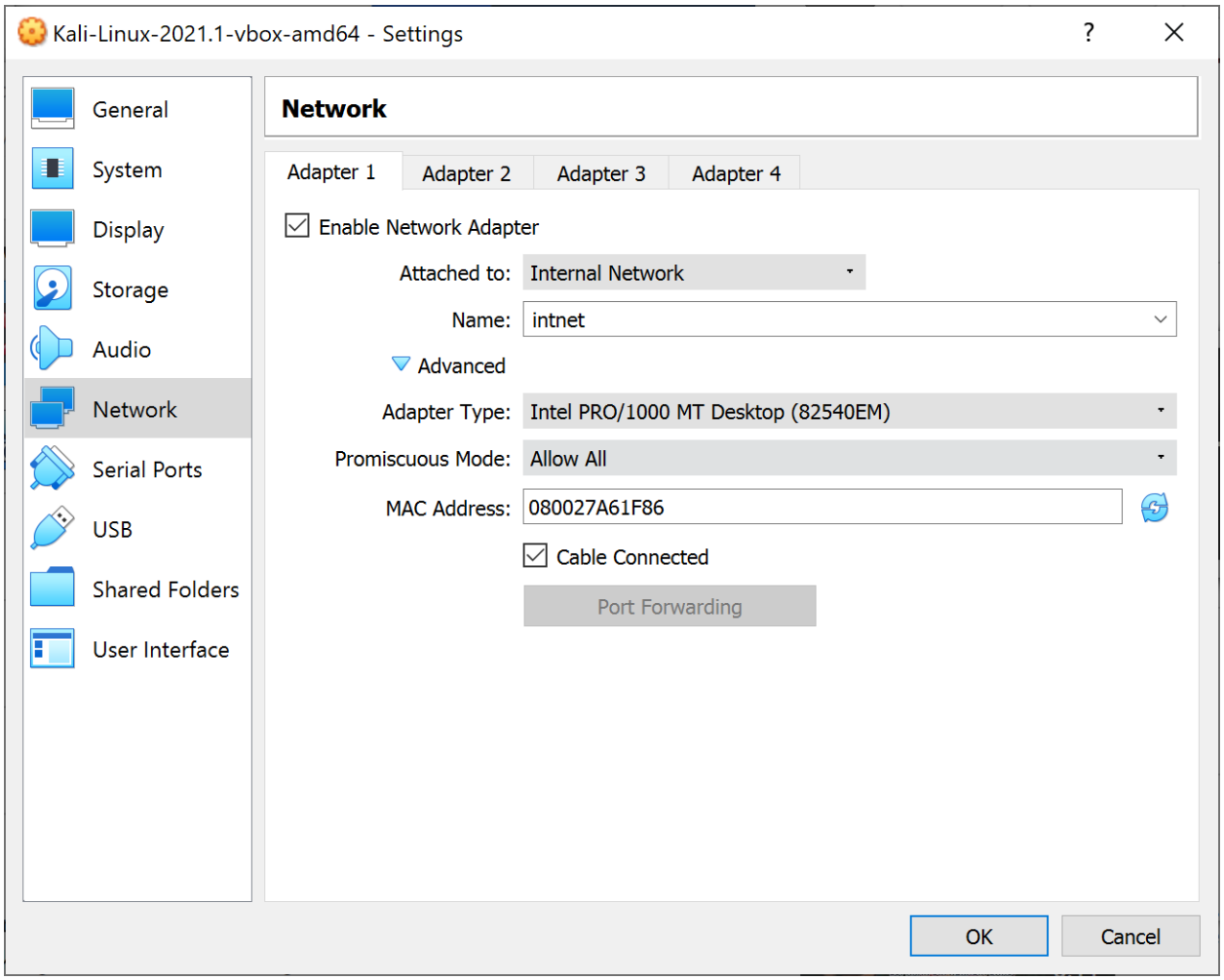
For this task, the student will explore two vulnerable websites in Metasploitable. These include DVWA and Mutillidae where both will be tested in the following task.

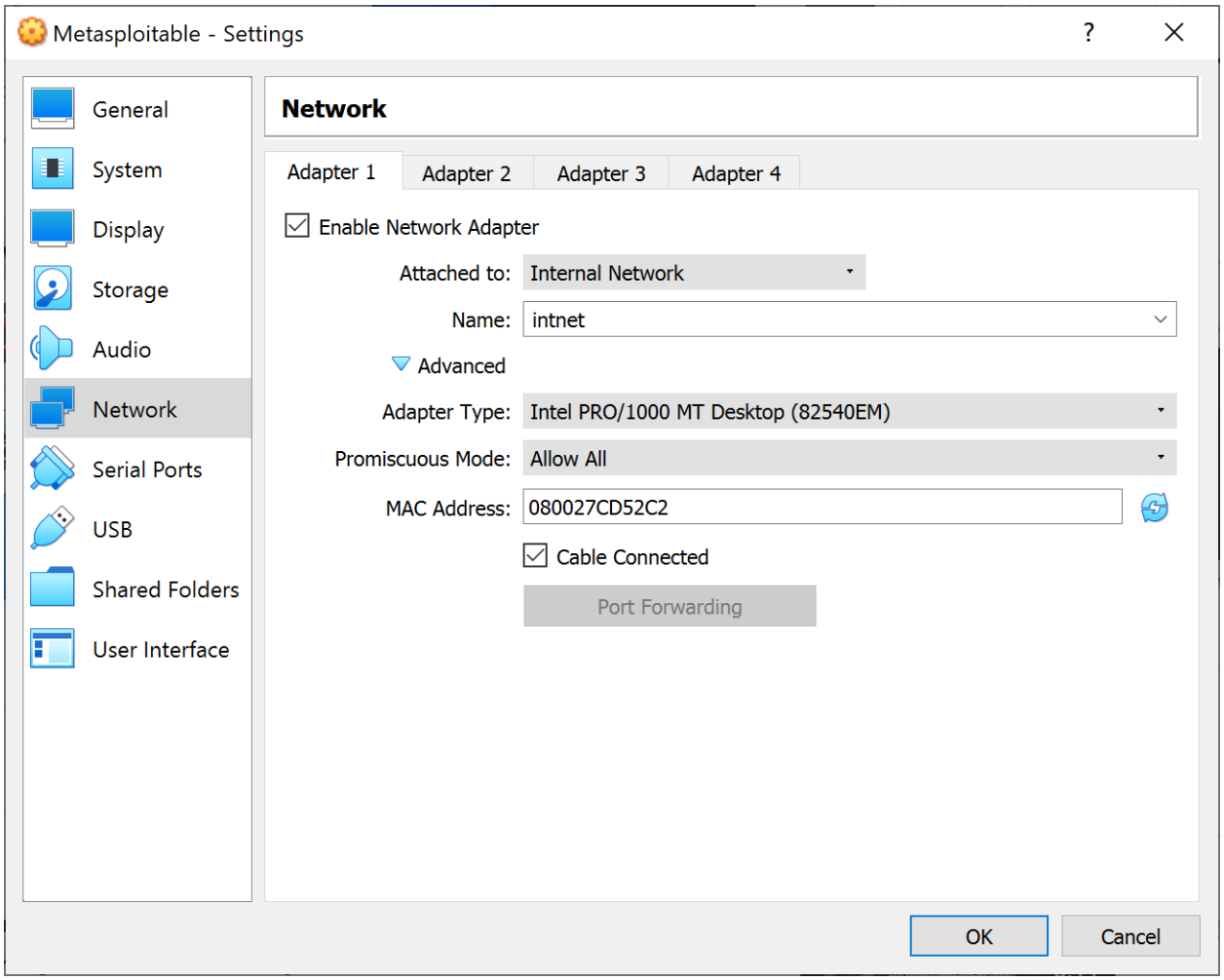
ESTIMATED TIME

60 Minutes

STEPS:

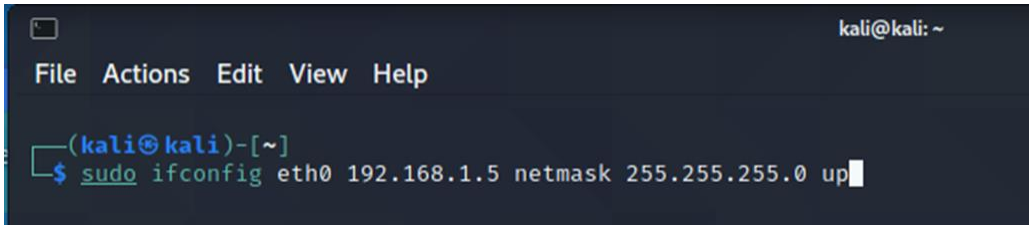
1. First of all, we begin with setting up the network to allow the communication between Metasplotaible and Kali Linux virtual machine. This time we will use the internal network as the network type for both virtual machines.


Kali-Linux-2021.1-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
intnet
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Allow All
MAC Address:
080027A61F86
Cable Connected
Port Forwarding
OK
Cancel



2. After you have set the correct network configuration, click **Start** for Kali Linux followed by Metasploitable virtual machine.

3. Log in to Kali Linux and open a terminal. Type the following command to set the IP Address as **192.168.1.5**, subnet and turn on the network adapter.



`

4. To test whether the configuration works as expected, use type **ifconfig** to confirm it.

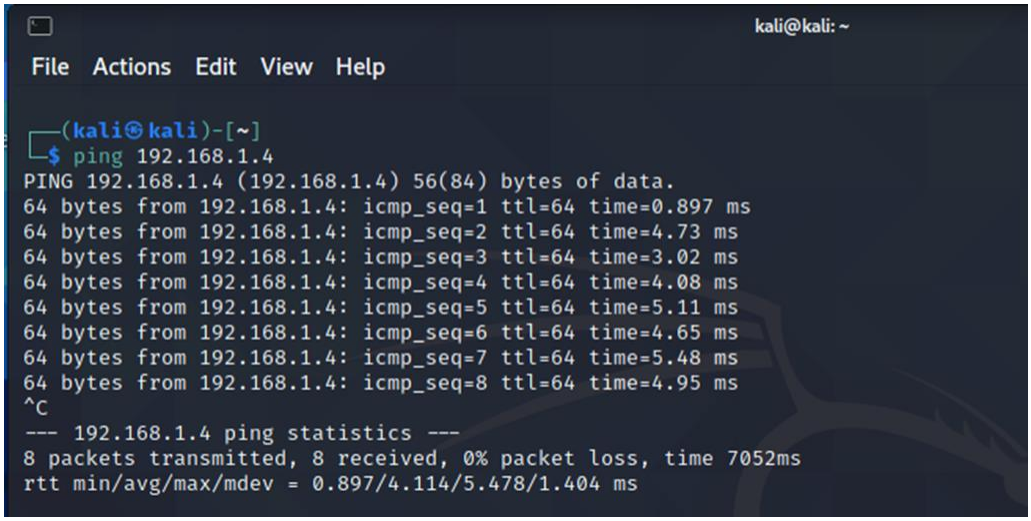
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fea6:1f86  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a6:1f:86  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2394 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 10508 (10.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. Next, switch to Metasploitable virtual machine. We are going to repeat a similar configuration step as we have done previously. This time, we put the IP Address as **192.168.1.4** for Metasploitable. Again, confirm the new setting with the **ifconfig** command.

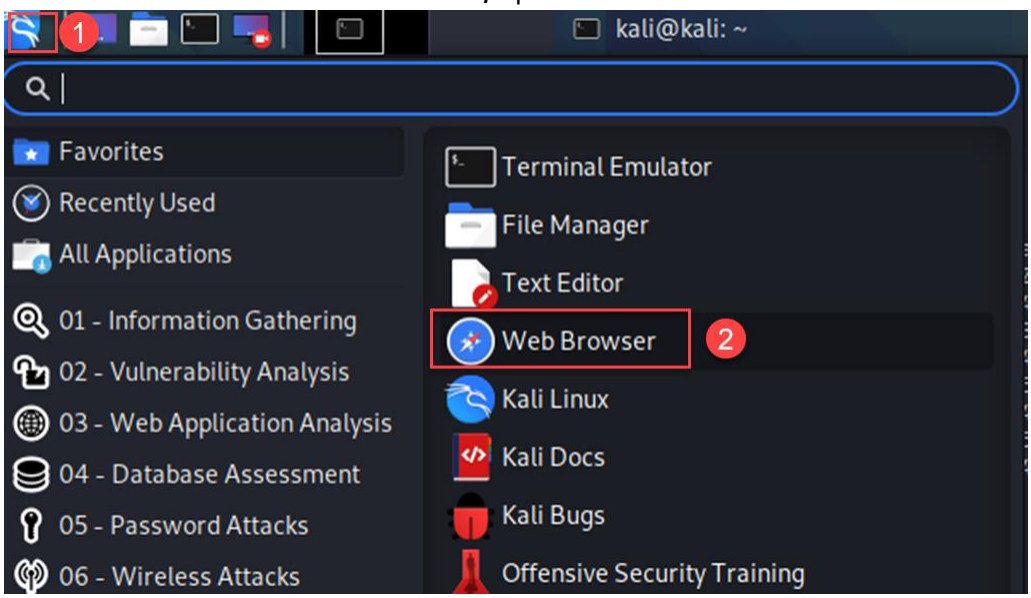
```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.4 netmask 255.255.0 up
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:52:c2
          inet addr:192.168.1.4  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fecd:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8016 (7.8 KB)  TX bytes:5348 (5.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31841 (31.0 KB)  TX bytes:31841 (31.0 KB)
```

`

6. After both virtual machines got their IP Address, now let's test the communication between the two by using the **ping** command. At the Kali Linux virtual machine, follow the command on the screenshot below. If we get the reply from 192.168.1.4 (Metasploitable) then we are ready for the next step.

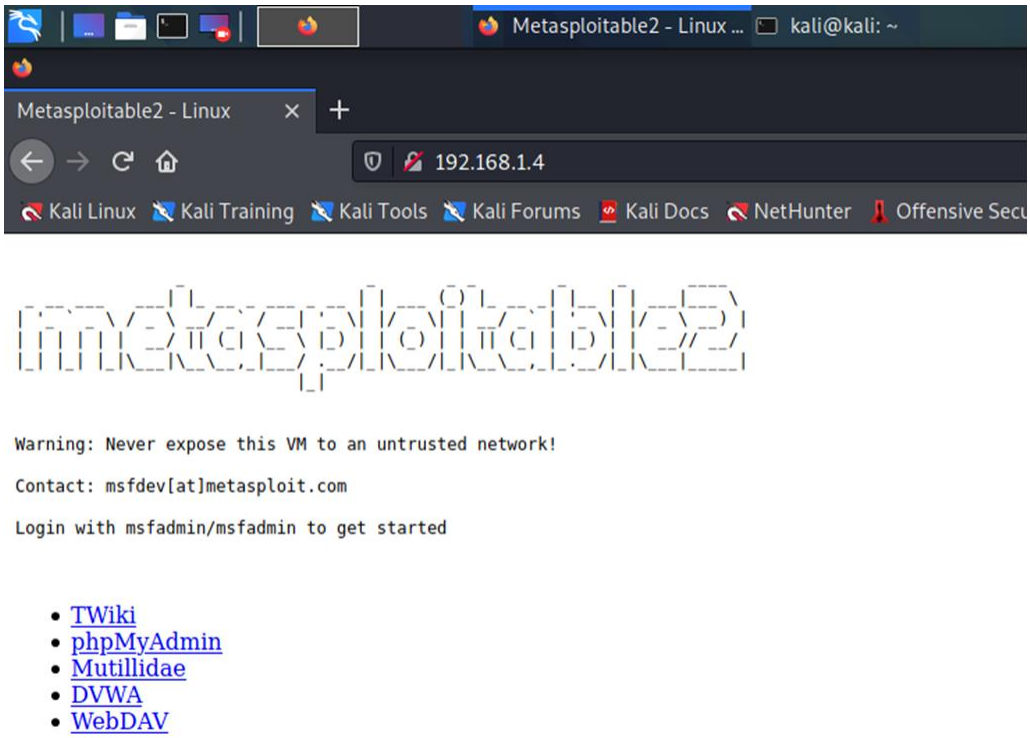


7. Still at the Kali Linux virtual machine, open the web browser.

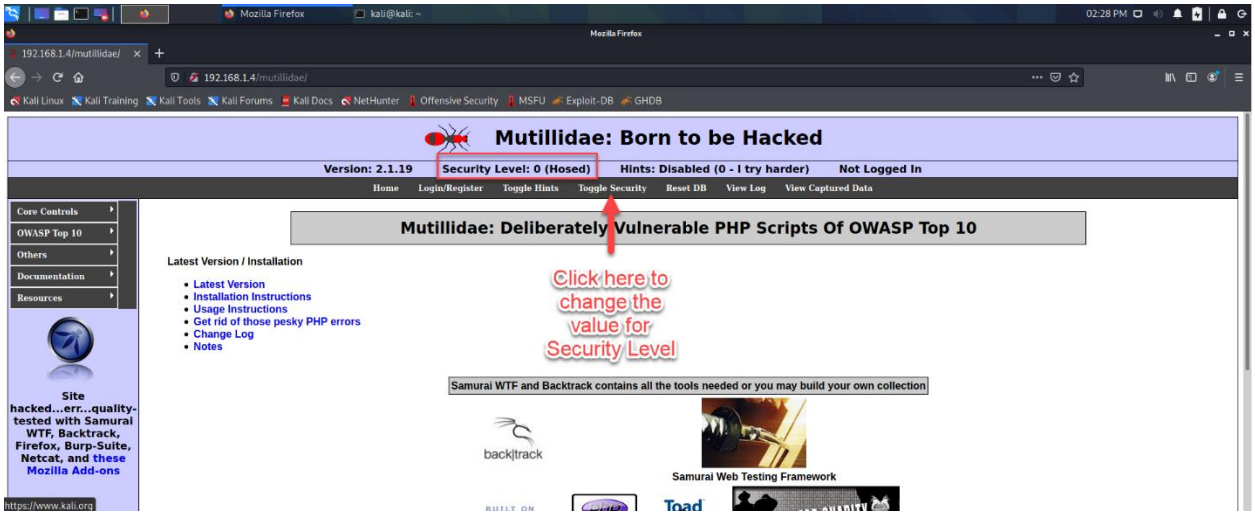


`

8. At the URL bar, type **http://192.168.1.4** and hit **Enter**. You will see a screen similar to the following. This is the list of vulnerable websites available in Metasploitable virtual machine. We are going to test two of them later. This includes Mutillidae and DVWA.



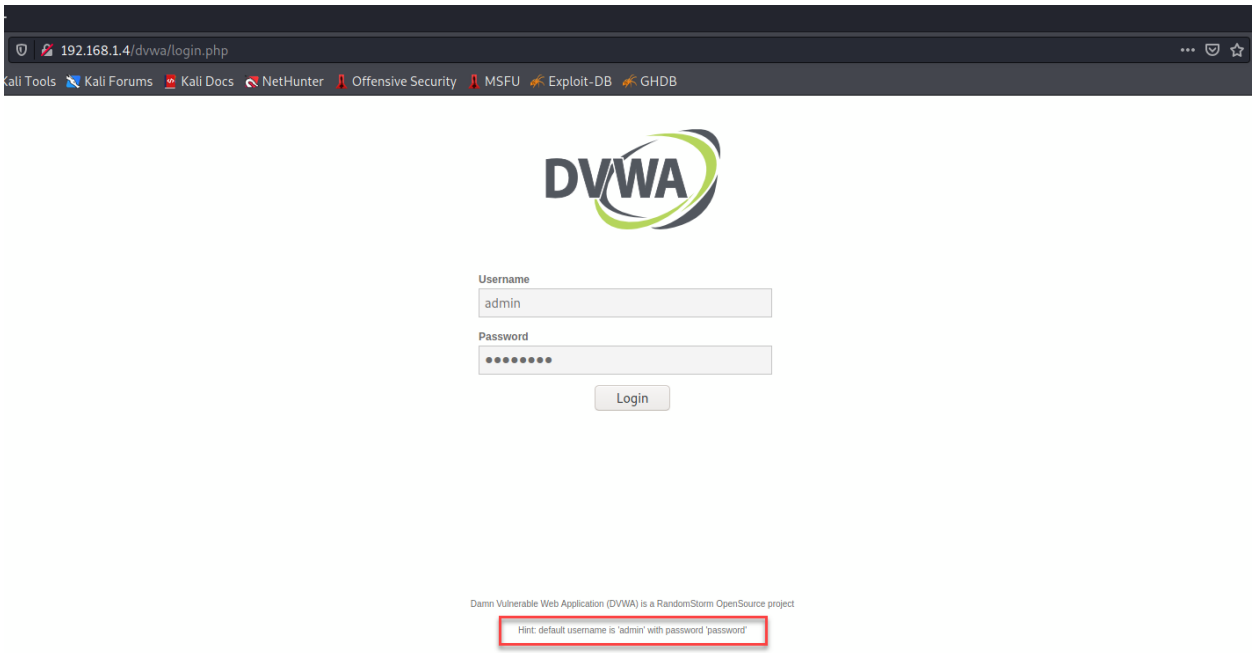
9. Next, click on the Mutillidae link. You will see the home page of the Mutillidae website. You may click on **Toggle Security** to change the value for Security Level. At this time, we only need the Security Level to be **0**.



`

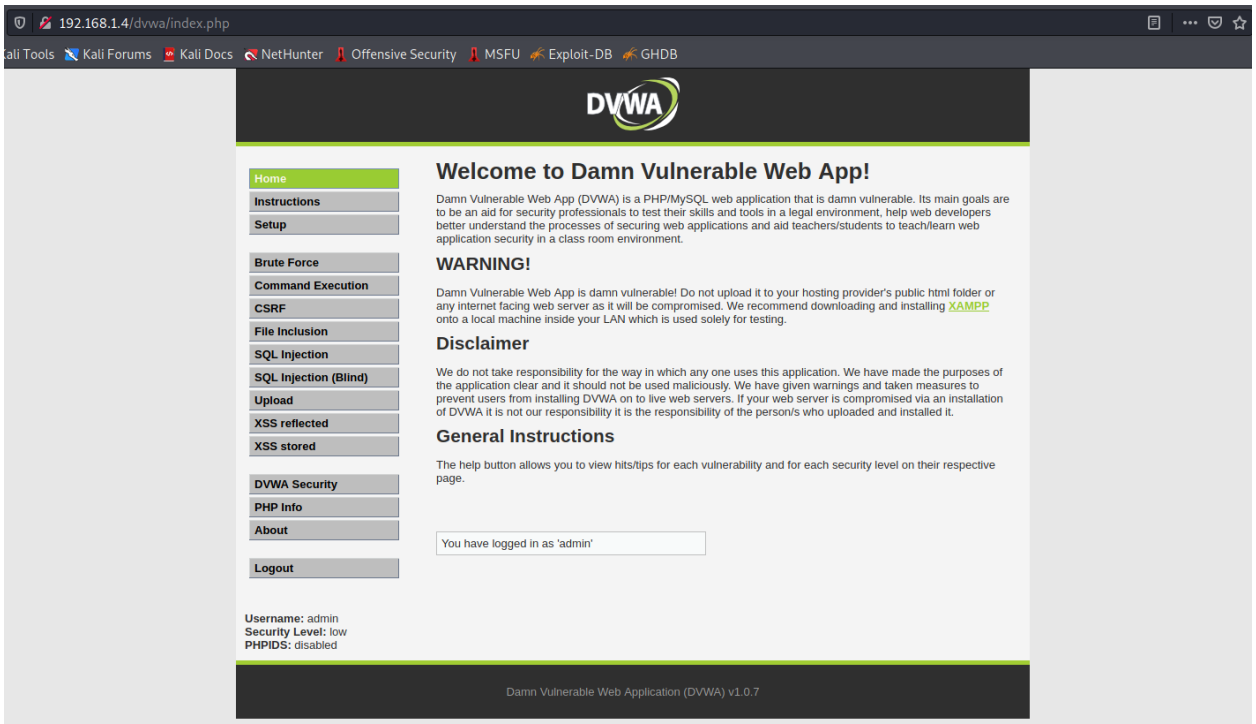
10. Now, click the browser back button a few times to go back to the screen as shown in Step 8. This time click on the **DVWA** link. The DVWA is also a vulnerable website that we are going to test later.

11. Login to the DVWA website with **admin** as the username and **password** as the password.

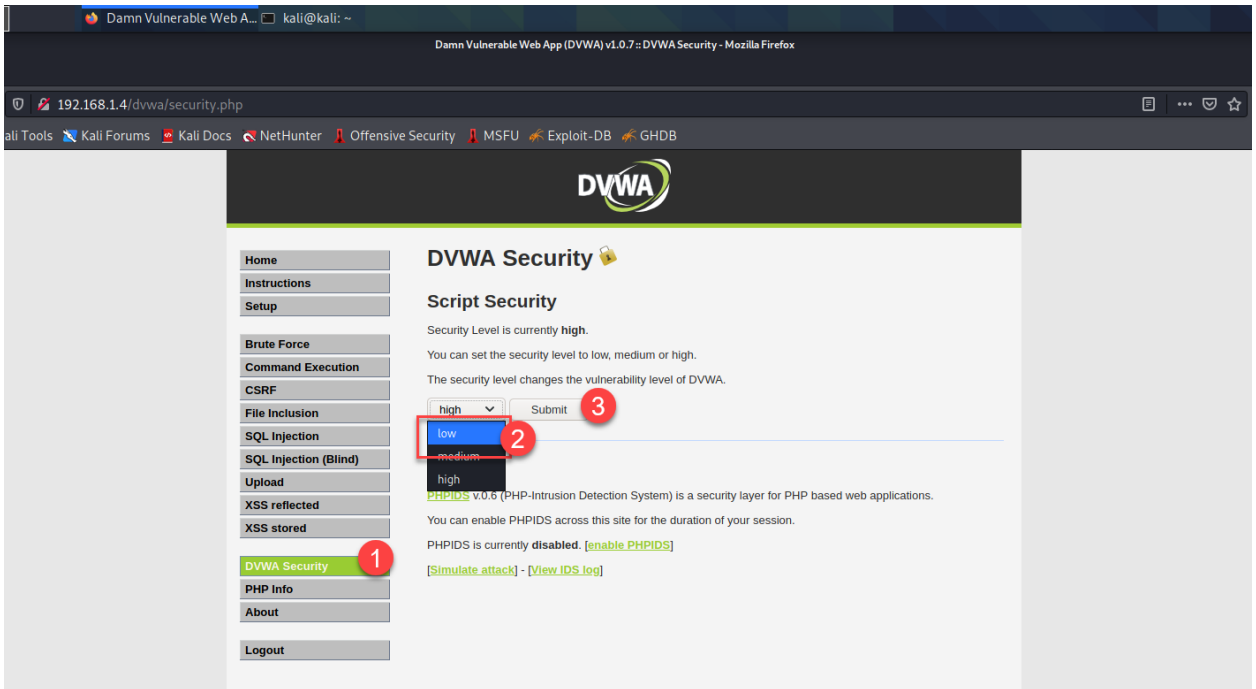


`

12. After successful login, you will see the homepage of the DVWA website. At the left menu, you will find a list of common website attacks. We are not going to test that yet but will change the DVWA security level first.

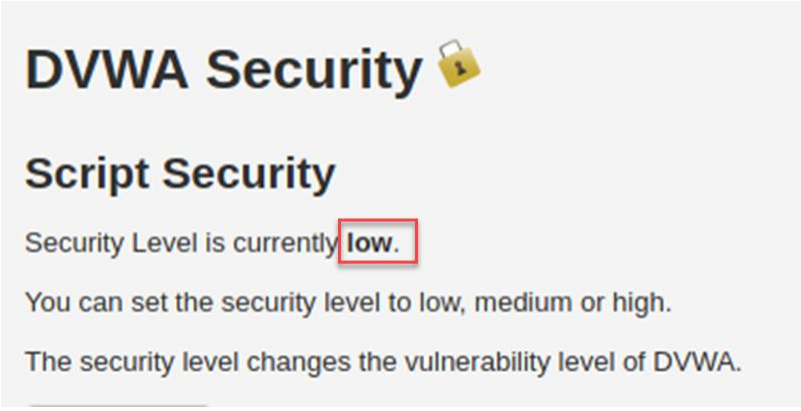


13. To change the security level, click on the **DVWA Security** at the left menu. Then, select **low** from the dropdown box and click **Submit** button.



`

14. We can confirm the configuration has been affected by looking at the following section.



15. That's all the steps for the configuration of vulnerable websites. Do not turn off the virtual machines yet because we will use them again in Task 3. Next, we will carry with the first step for web security testing which is information gathering.

`

TASK 2: INFORMATION GATHERING OF A WEBSITE

OBJECTIVE

To use tools to gather information about a certain website.

TASK DESCRIPTION

During this task, the student will use Netcraft and whois domain tools to gain some information about a website.

ESTIMATED TIME

60 Minutes

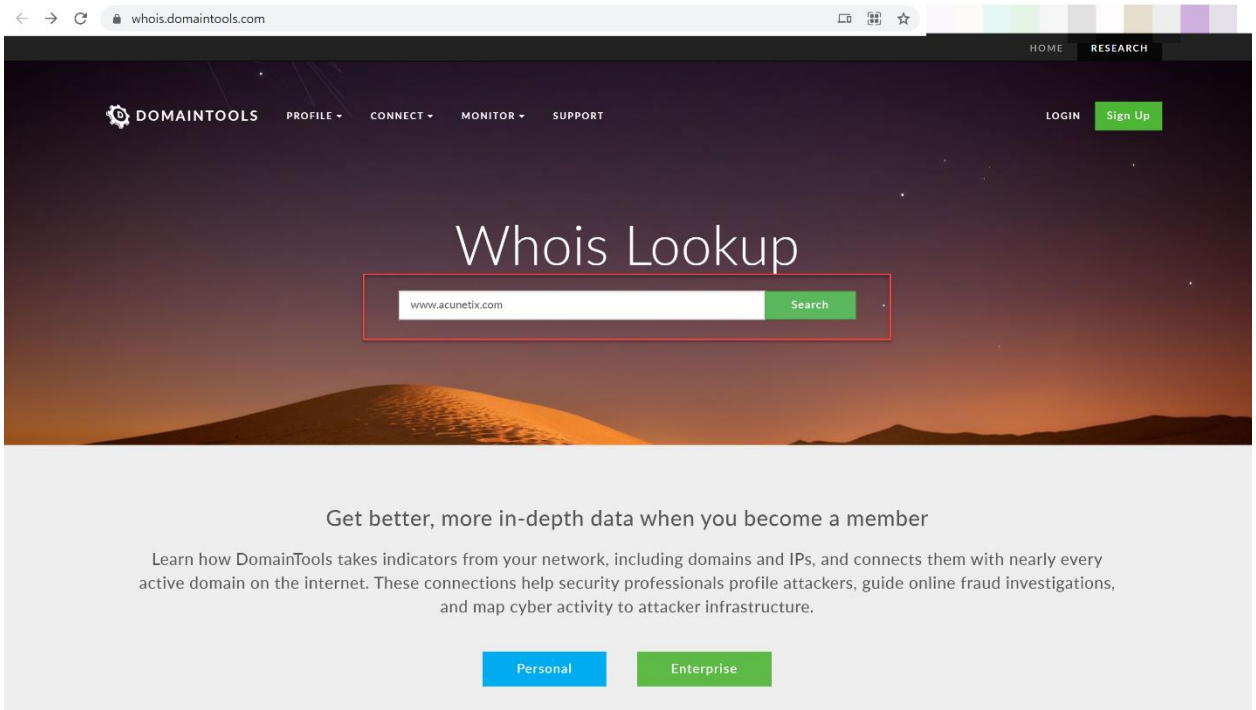
STEPS:

1. This task is carried out in the host environment. You do not need to run a virtual machine for this task.

2. At your computer, open a web browser. Type **https://whois.domaintools.com/** at the URL bar. This is a tool that can give us information about the owners of the website, an IP address, or a domain name. We are not going to attack any website by using this tool but the information returned from it might be useful for further attack.

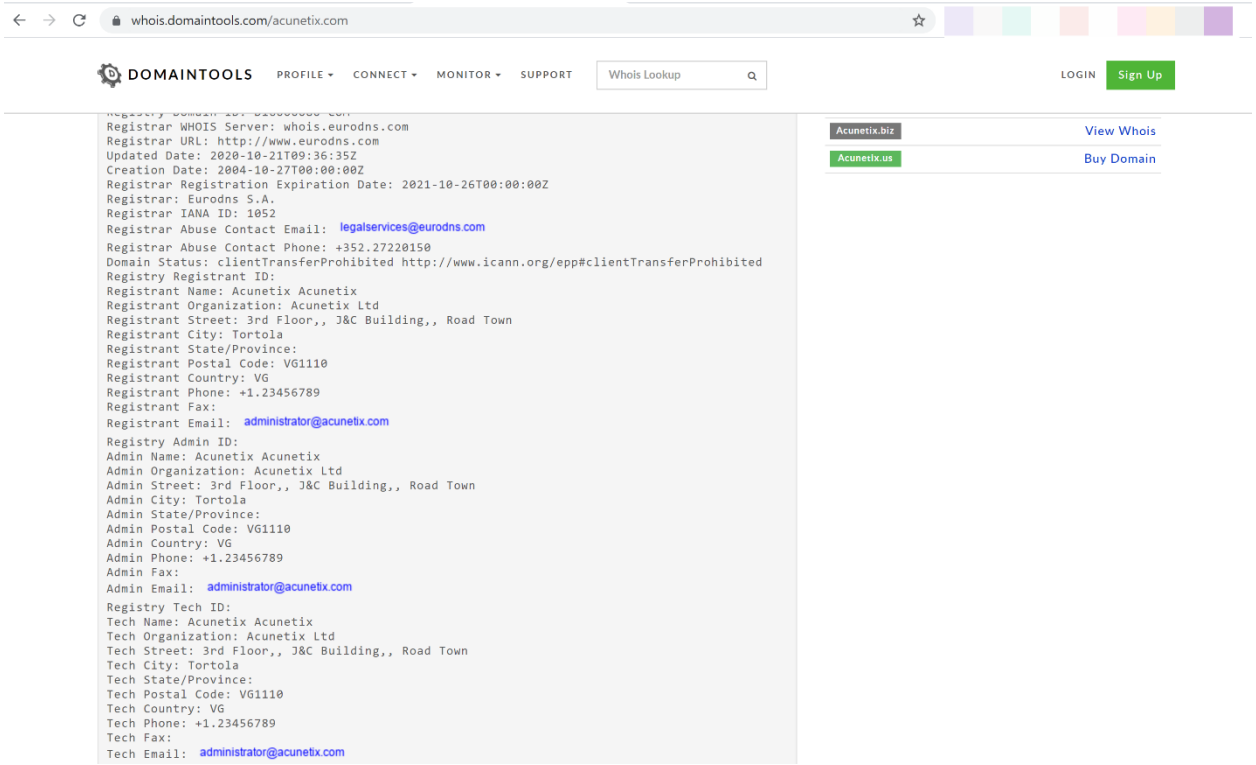
`

3. Enter a domain name **www.acunetix.com** at the search box and click the **Search** button.



`

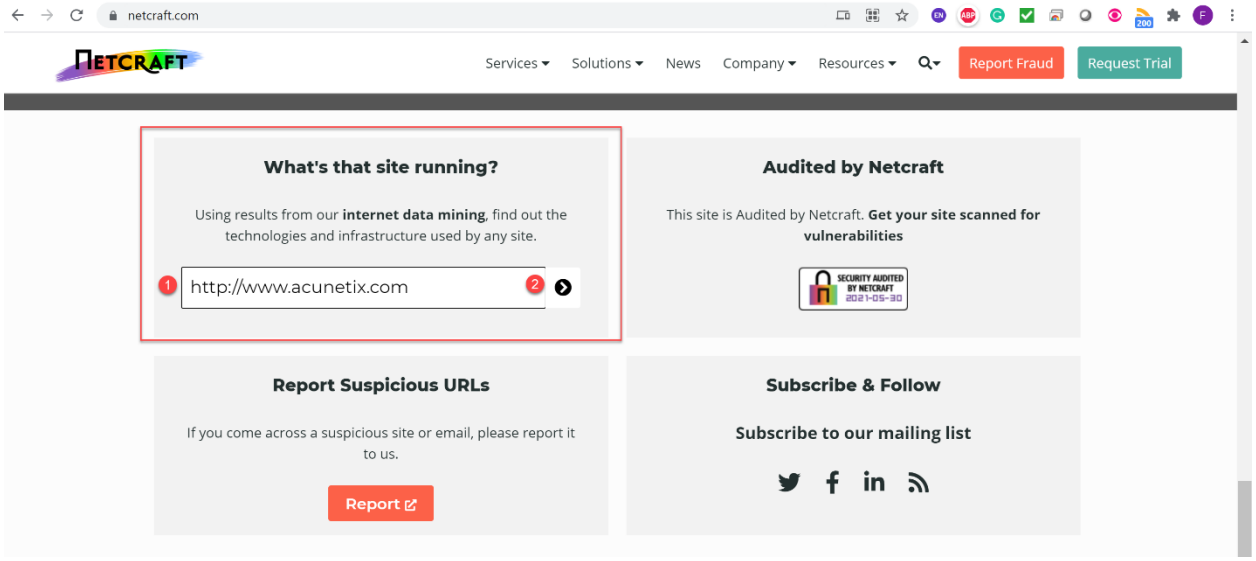
4. As a result, we can see the email address for contacting the domain name information. Usually, we will see the address of the company that registered the domain name, but sometimes a firm is using a privacy service on their domain so that we will not be able to see their address and additional information about the actual firm.



5. Find three websites of your choice, then use the whois tools to find the details behind the domain name. Get the screenshots of the results and put them into your lab report.

`

6. The second tools we are going to use is Netcraft. This tool will assist us to find the information related to certain website such as technology used, hosting history, web trackers and language used for developing the site. Type **https://www.netcraft.com/** at the URL bar and hit **Enter**. You will see the main page of the site and scroll down until you see the section as shown in the red box on the screenshot below. Type the URL as **http://www.acunetix.com** and hit the arrow button.



`

7. This will return a long result consist of many information. Scroll down to read all the information. Investigate the result to gain some useful information about the website.

sitereport.netcraft.com/?url=http://www.acunetix.com

NETCRAFT — Services — Solutions — News — Company — Resources — Report Fraud — Request Trial

Site report for http://www.acunetix.com

Look up another site?

Share:

Background

Site title	Acunetix | Web Application Security Scanner	Date first seen	March 2005
Site rank	2347	Netcraft Risk Rating	0/10
Description	Acunetix is an end-to-end web security scanner that offers a 360 view of an organization's security. Allowing you to take control of the security of all you web applications, web services, and APIs to ensure long-term protection. Acunetix's scanning engine is globally known and trusted for its unbeatable speed and precision.	Primary language	English

Network

Site	http://www.acunetix.com	Domain	acunetix.com
Netblock Owner	Amazon.com, Inc.	Nameserver	ns-1505.awsdns-60.org
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	eurodns.com
Hosting country	us	Nameserver organisation	whois.pir.org

sitereport.netcraft.com/?url=http://www.acunetix.com

NETCRAFT — Services — Solutions — News — Company — Resources — Report Fraud — Request Trial

IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ec2-54-208-84-166.compute-1.amazonaws.com		

IP delegation

IPv4 address (54.208.84.166)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
54.0.0.0-54.255.255.255	United States	NET54	American Registry for Internet Numbers
54.144.0.0-54.221.255.255	United States	AMAZON	Amazon Technologies Inc.
54.208.0.0-54.209.255.255	United States	AMAZO-ZIAD4	Amazon.com, Inc.
54.208.84.166	United States	AMAZO-ZIAD4	Amazon.com, Inc.

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the **HTTPS site report**.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Amazon.com, Inc. Amazo...	54.208.84.166	Linux	acunetix.com	14-May-2021
Amazon.com, Inc. Amazo...	54.208.84.166	Linux	nginx	20-Mar-2019

`

8. Next, repeat Step 6 and Step 7 with three of your favourite website. Then, take screenshots of the **Hosting History** and **Web Trackers** for each site. Put the screenshots into your lab report.

9. That's all the activities for information gathering for a website. Next, we will go deeper into getting more information about a website.

`

TASK 3: SCANNING CONTENT OF A WEBSITE

OBJECTIVE

To scan the content of a website to collect more information.

TASK DESCRIPTION

For this task, the student needs to run a tool known as **dirb** to scan the content of a website.

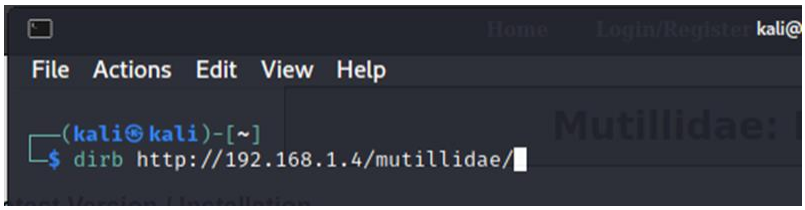
ESTIMATED TIME

60 Minutes

STEPS:

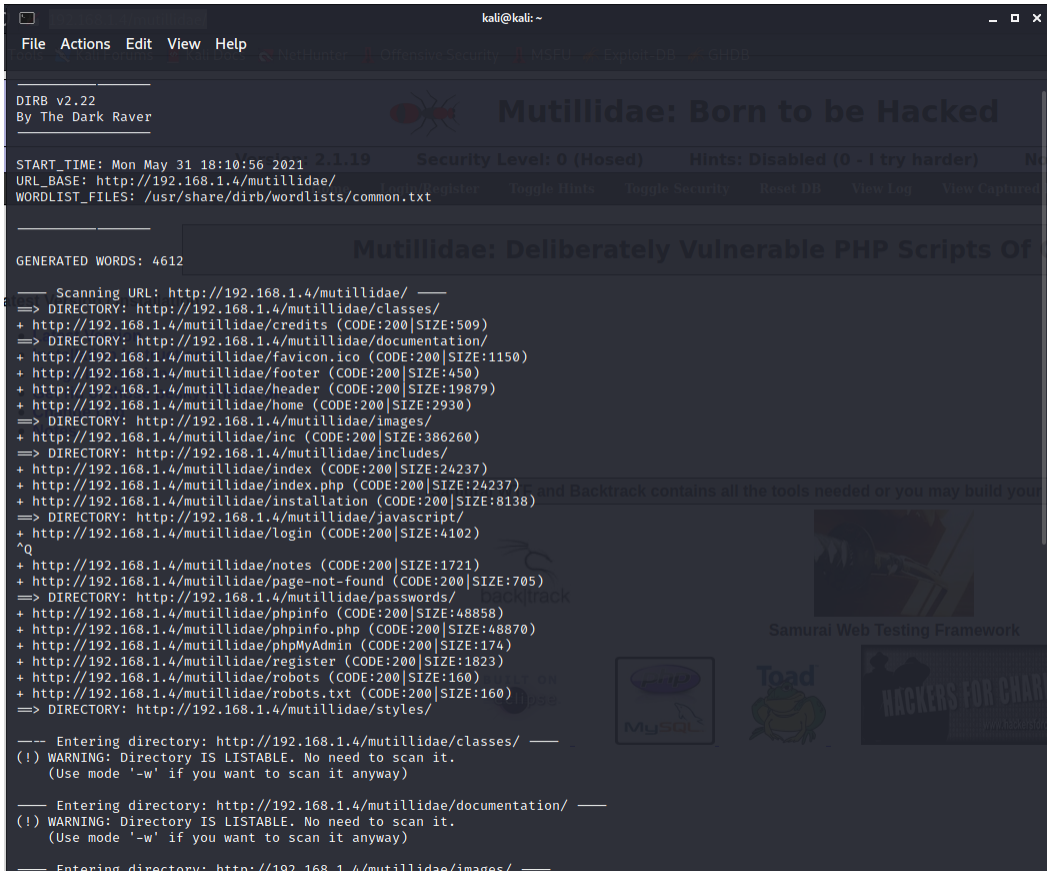
1. For this task, we need to go back to the virtual machines that we have started in Task 1.

2. First, go to Kali Linux virtual machine. For this task, we are going to scan the directory of the Mutillidae website located in the Metasploitable virtual machine. Open a terminal and type the following command and hit **Enter**:



`

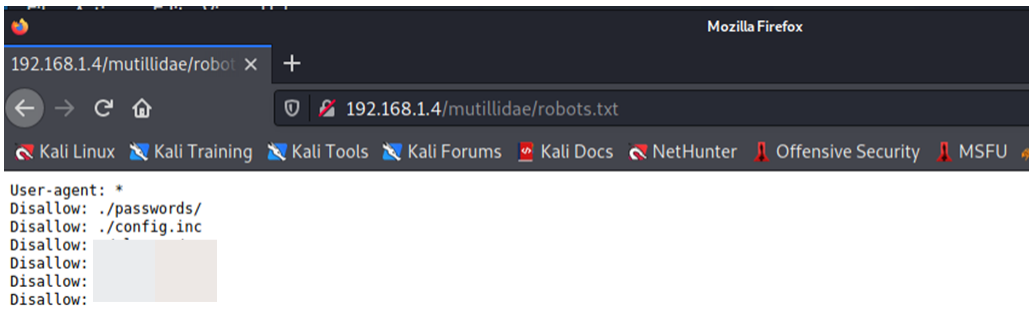
3. As a result, you will see a list of web pages on Mutillidae websites. Some of the common files are favicon.ico, header, footer, images and login. Can you find other folders or files that might be interesting and worth having a look at? List five of them. Write your answer in the lab report.



4. After finishing the previous steps, let's investigate some of the files. Usually, the **phpinfo.php** file is very useful because it shows a lot of information about the PHP interpreter running on the webserver. Go to http://192.168.1.4/mutillidae/phpinfo.php and see the information on the page. Get a screenshot of it and answer the following questions:
    a. When is the built date?
    b. What is the version of the PHP used by the Mutillidae website?
    c. What is the database server used by the Mutillidae website?

`

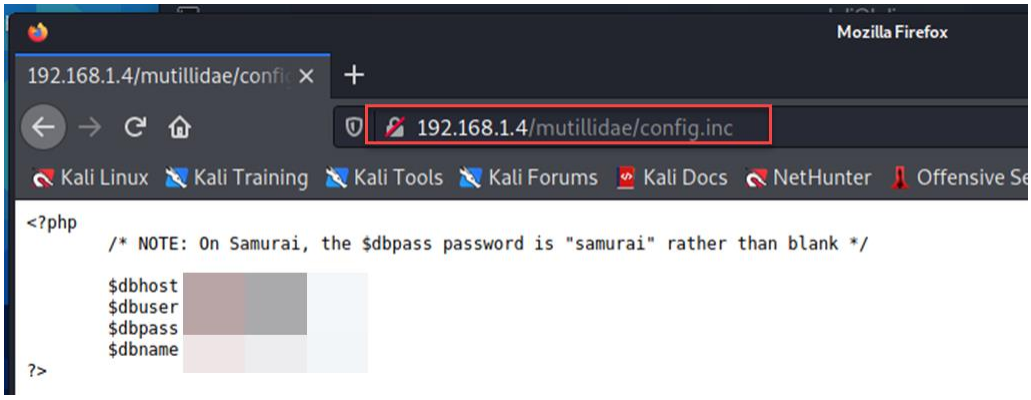
5. Besides the phpinfo file, another useful file is the **robots.txt** file. It tells the search engines, such as Google on how to deal with the website. Hence, it usually contains files that we do not want the website or Google to see or to read. Now, if we can read the robots.txt file, then we will be able to see what the web admin is trying to hide. In the following screenshot, we can see that the web administrator does not want Google to see a directory called **passwords**, and it does not want us to see a file called **config.inc** either along with some other directories. List the rest of the directories in your lab report.



6. Now we know there is a folder known as **password**. Let's go inside it and see the content. We will see an accounts.txt file. What is the content of the file? Try to click it and see the content. Grab the screenshot of it and put it into your lab report. What did you think you have obtained now? Is it useful?

`

7. Last but not least is the **config.inc** file. You should be able to realize the existence of this file during the activity in Step 5, if not, go back and investigate further. Go straight to the file and see the content by typing http://192.168.1.4/mutillidae/config.inc. Take a screenshot of the result and put it into your lab report.



8. Finally, investigate the rest of the directories in listed Step 5. Write down the findings from your observation.

REFLECTION QUESTIONS

1. Why do we need to information gathering before we can proceed with testing a website?
2. What are the common vulnerabilities of a website?
3. List tools that we can use for information gathering of a website.
4. Why does some whois information is not available to the public?
5. What tools we can use to scan a subdomain of a website domain?