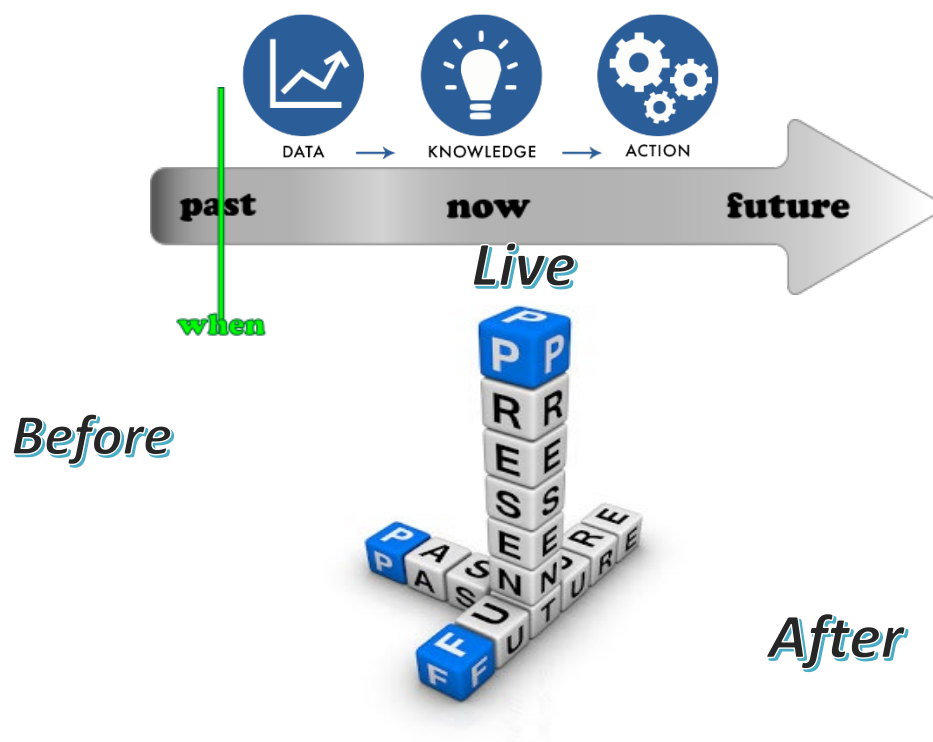




Ethical Hacking (ACCA7033)

Understanding Web Attacks – Part 1



Lab Activities are based on **EC Council – CEH Curriculum**

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you insights about web attacks.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

*** This LAB is adopted from EC Council**

Task 1: Footprint a web server using various information-gathering tools and inbuilt commands

Task 2: Crack remote passwords

Task 3: Exploiting parameter tampering vulnerability
--

ICONS Used in this document:



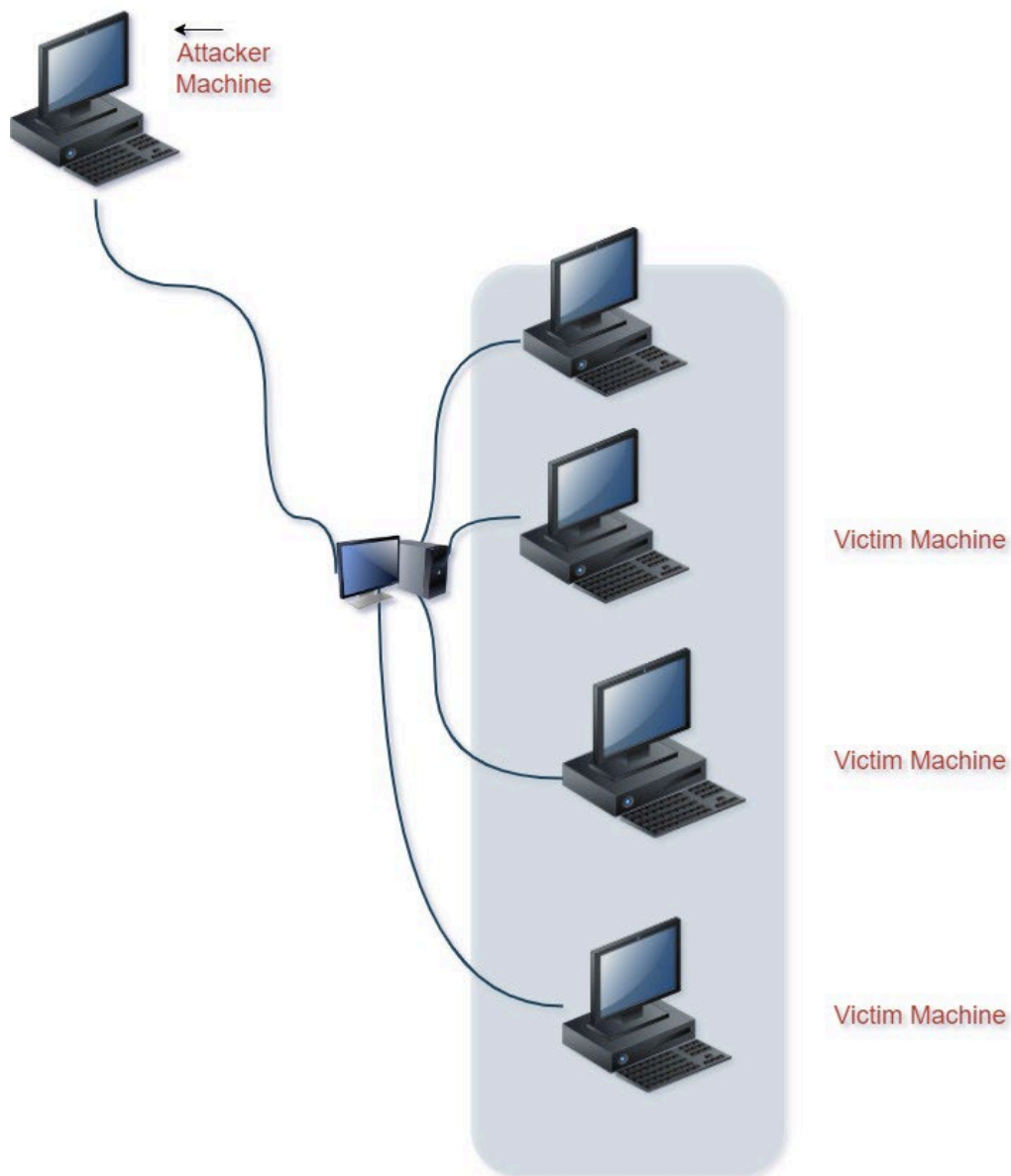
Find out the outcome/ Answers/ Solution/ Discussion via Forum



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Lab Topology

Guide to Setup
your Lab



- **Attacker Machines:** *Kali Linux, Parrot, Ubuntu (It's your Choice)*
- **Victim Machines:** *Combination of Win 10, 11, Win Server 2019, 22, Linux (CentOS, Debian), bee-box v1.6*
- **Web Servers:** DVWA, Good Shopping, Moviescope etc

Task 1: Footprint a web server using various information-gathering tools and inbuilt commands

Use your knowledge and understanding gained from this course so far, to document the relevant steps to footprint a web server by gathering information manually and by using tools. List the tools and their functionality.

This task is pretty much an open task/ activity. Depending on your interest, time and knowledge gained so far, you could do a very detailed work here. I strongly recommend you to use this work in your coursework as well, where appropriate.

Assuming that, you are clear and have a better understanding of footprinting methods, we move to the next task.

Task 2: Perform a Web Server Attack to Crack FTP Credentials

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system.

An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method.

Most password cracking techniques are successful, because of weak or easily guessable passwords.

We are trying to identify an open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool. Here, we will use a sample password file (samp_pass.txt) containing a list of passwords to crack the FTP credentials on the target machine.

1. Assume that you are an attacker, and you have observed that the FTP service is running on the Windows 10 machine. *(Configure your environment accordingly to enable FTP service running in the target machine)*
2. Perform an Nmap scan on the target machine (Windows 10) to check if the FTP port is open.
3. From the attackers machine, run the programs as a root user and jump to the root directory.
4. In the terminal window, type `nmap -p 21 [IP Address of target machine]`. For reference to this lab, the IP address of Windows 10 (target machine) is 10.10.1.10.

```

Nmap scan report for 10.10.1.10
Host is up (0.00078s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:01 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

```

(You must get an output like the above)

5. Check if an FTP server is hosted on the Windows 10 machine by typing `ftp 10.10.1.10`. You will be prompted to enter user credentials. *The need for credentials implies that an FTP server is hosted on the machine.*
6. Try entering random usernames and passwords in an attempt to gain FTP access.
7. Are you able to login with random guesses? You might or not be able to log in to the FTP server.
8. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
9. For this lab, the username and password lists will be made available in the shared folder. *(If you can't find them, create one)*
10. In the terminal window, type `hydra`. *(The IP address of Windows 10 in this lab exercise is 10.10.1.10. This IP address might vary in your lab environment.)*
`Hydra -L / "the path"/username.txt -P / "the path"/ password.txt ftp://10.10.1.10`
 Hydra tries various combinations of usernames and passwords (present in the Unames.txt and Passwords.txt files) on the FTP server and outputs cracked usernames and passwords.

Note: This might take some time to complete.

```

[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.10:21/
[21][ftp] host: 10.10.1.10  login: Martin  password: apple
[STATUS] 4730.00 tries/min, 4730 tries in 00:01h, 36444 to do in 00:08h, 16 active
[STATUS] 4715.33 tries/min, 14146 tries in 00:03h, 27028 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.10  login: Jason  password: qwerty
[STATUS] 4721.29 tries/min, 33049 tries in 00:07h, 8125 to do in 00:02h, 16 active
[STATUS] 4719.88 tries/min, 37759 tries in 00:08h, 3415 to do in 00:01h, 16 active
1 of 1 target successfully completed, 2 valid passwords found

```

11. Try to log in to the FTP server using one of the cracked username and password combinations.

12. On entering the credentials, you will successfully be able to log in to the server.

```

l → #ftp 10.10.1.10
Connected to 10.10.1.10.
220 Microsoft FTP Service
Name (10.10.1.10:attacker): Martin
331 Password required
Password: Attacks
230 User logged in.

```

13. Now you can remotely access the FTP server hosted on the Windows 10 machine.

14. Type `mkdir Hacked` and press Enter to remotely create a directory named Hacked on the Windows 10 machine through the ftp terminal.

```

Name (10.10.1.10:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.

```

15. Login to Windows/ Target Machine. Navigate to the FTP folder to see the directory named Hacked is created, showing that you have successfully gained remote access to the FTP server by obtaining the appropriate credentials. Type help command to look for other options as well.

```

ftp> help
Commands may be abbreviated.  Commands are:

!      dir      mdelete      qc          site
$      disconnect mdir         sendport    size
account exit      mget         put          status
append form     mkdir        pwd          struct
ascii  get      mls          quit         system
bell   glob     mode         quote        sunique
binary hash    modtime      recv         tenex
bye    help     mput         reget        tick
case   idle    newer        rstatus      trace
cd      image   nmap         rhelp        type
cdup    ipany    nlist        rename       user
chmod   ipv4     ntrans       reset        umask
close   ipv6     open         restart      verbose
cr      lcd     prompt       rmdir        ?
delete ls       passive      runique
debug  macdef   proxy        send

```

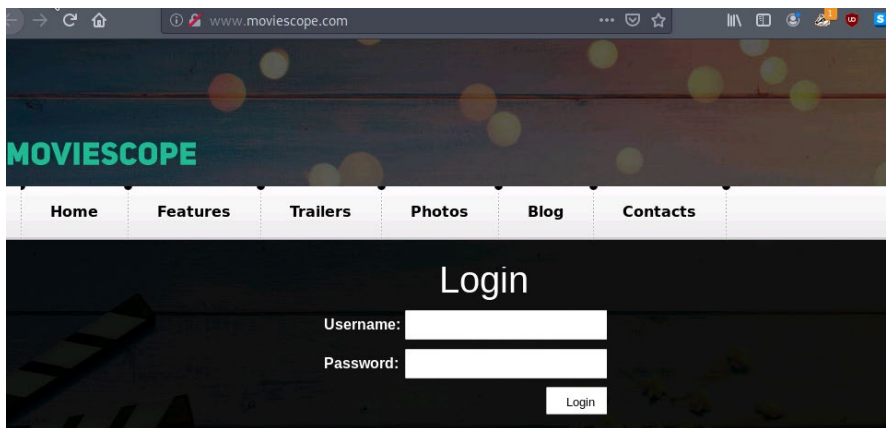
Task 3: Perform a Web Application Attack to Compromise the Security of Web Applications to Steal Sensitive Information

The task in this lab will assist in performing attacks on web applications using various techniques and tools.

1. Perform Parameter Tampering using Burp Suite: A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions,

price, and quantity of products. Here, we will use the Burp Suite tool to perform parameter tampering.

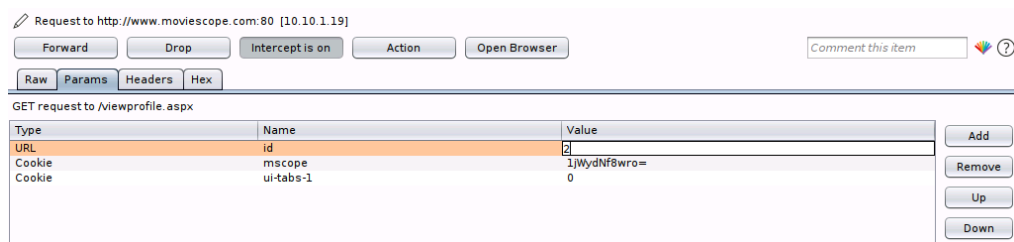
2. For this task, the target website (**www.moviescope.com**) need to be configured/ hosted in the victim machine, (possibly a **Windows Server 2022 or 2019**) depending on your environment. The moviescope setup files are available in the shared folder.
3. Check if the target website is working fine in your attacker machine (Kali – for me).



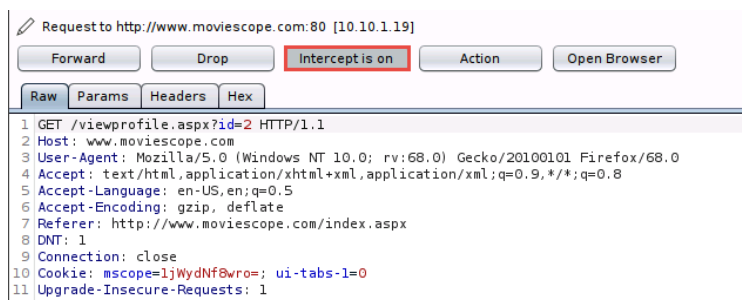
4. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser. In the browser, go to Proxy Settings.
5. Turn on the Manual Proxy Settings and configure the HTTP Proxy as **127.0.0.1** and the Port as **8080**. Click **Save**.
6. Launch the **Burp Suite** application. If needed, accept the terms and conditions.
 - a. **Burp Suite** initializes.
 - b. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected
 - c. Select the **Use Burp defaults** radio-button and click the **Start Burp** button.
 - d. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.
 - e. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running. Turn the interception on if it is off.
 - f. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**.

Click the **Login** button. *Here, we are logging in as a registered user on the website.*

- g. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application. You can observe that the entered login credentials were intercepted by the Burp Suite.
- h. Now, keep clicking the **Forward** button until you are logged into the user account.
- i. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.
- j. Now, click the **View Profile** tab from the menu bar to view the user information.
- k. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request.
- l. Now, navigate to the **Params** tab under the **Intercept** tab to view the captured parameters.
- m. Under the **Params** tab, observe a table with captured values such as **URL** and **Cookie**.
- n. In the **URL** type with the name **id**, double-click the **Value** column to change it from **1** to **2**.



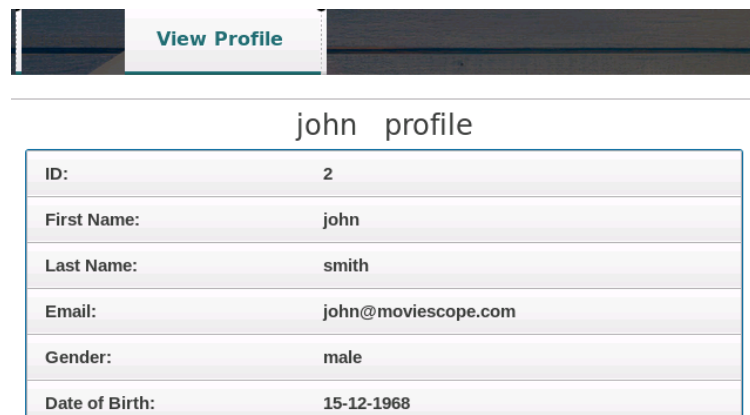
- o. After changing the value, navigate back to the **Raw** tab and click the **Intercept is on** button to turn off the interception.



- p. After switching off the interception, navigate back to the browser window and observe that the user account
- q. What did you observe?

associated with ID=2 appears with the name John

Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.



- r. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.
- s. Switch to the browser and remove the browser proxy set up by selecting the **No proxy** radio-button.
- t. This concludes the demonstration of how to perform parameter tampering using Burp Suite.

Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Any other Troubleshooting Steps, you need to share?
6. Rate yourself: How confident are you to mitigate such tampering attacks? What are the countermeasures would you take/ recommend to overcome/ avoid such attacks?
7. Did you try any other Web Server attacks? I strongly recommend you to try other Web Server Attacks discussed during the lectures. Document them.

-----End of Activity 6 -----