Group2:

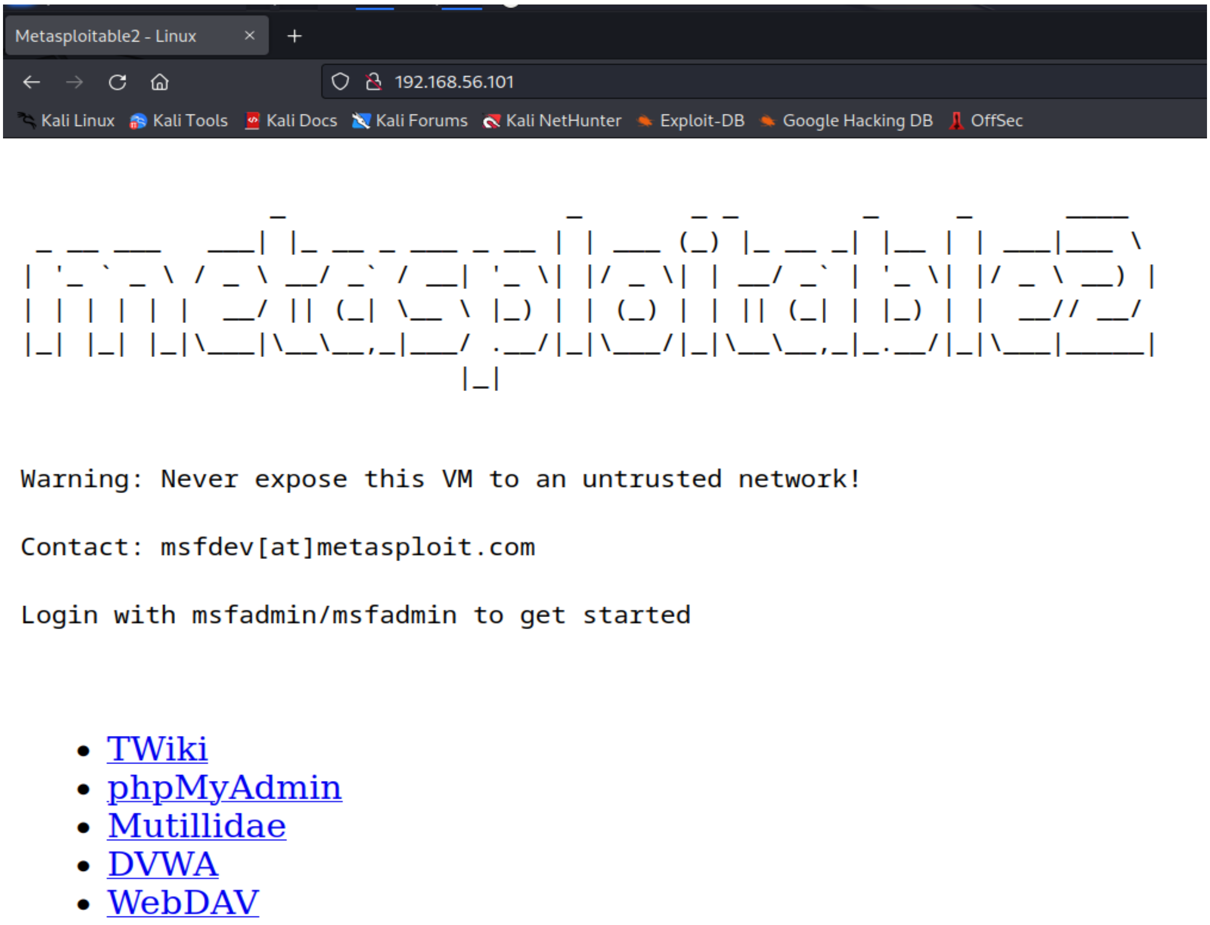
1. Perform exploiting DVWA

a) Perform SQL injection on DVWA

b) Perform Cross-site scripting on DVWA

c) Perform File upload DVWASQL injection, Cross site scripting:

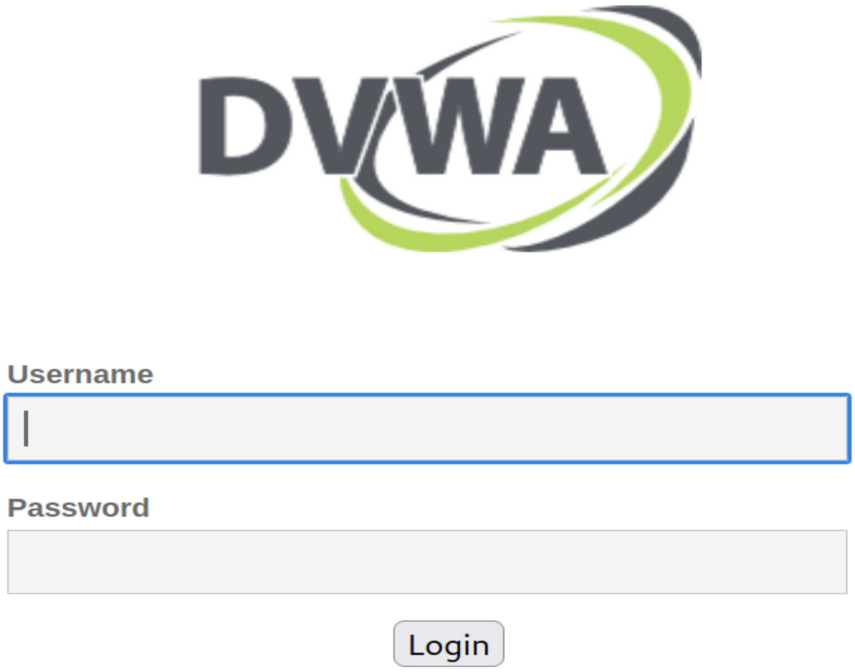
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.



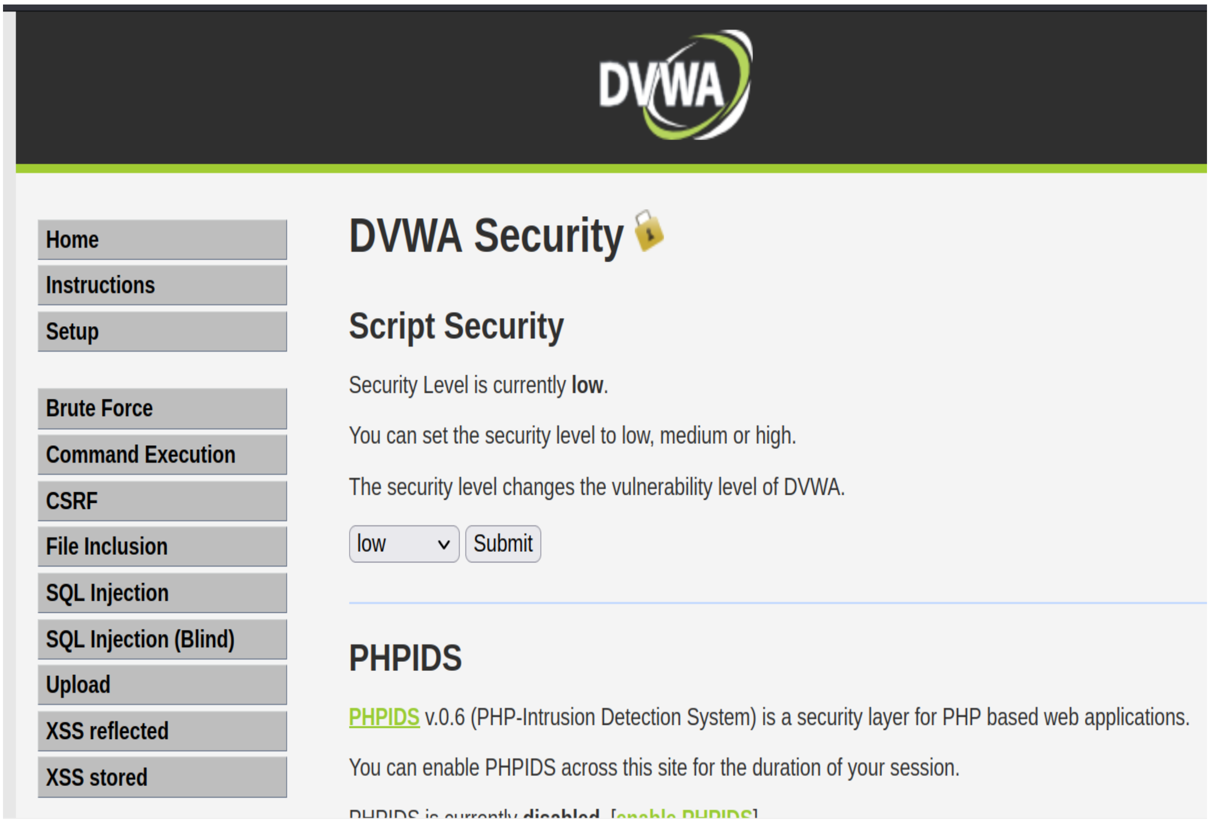
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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.



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 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.

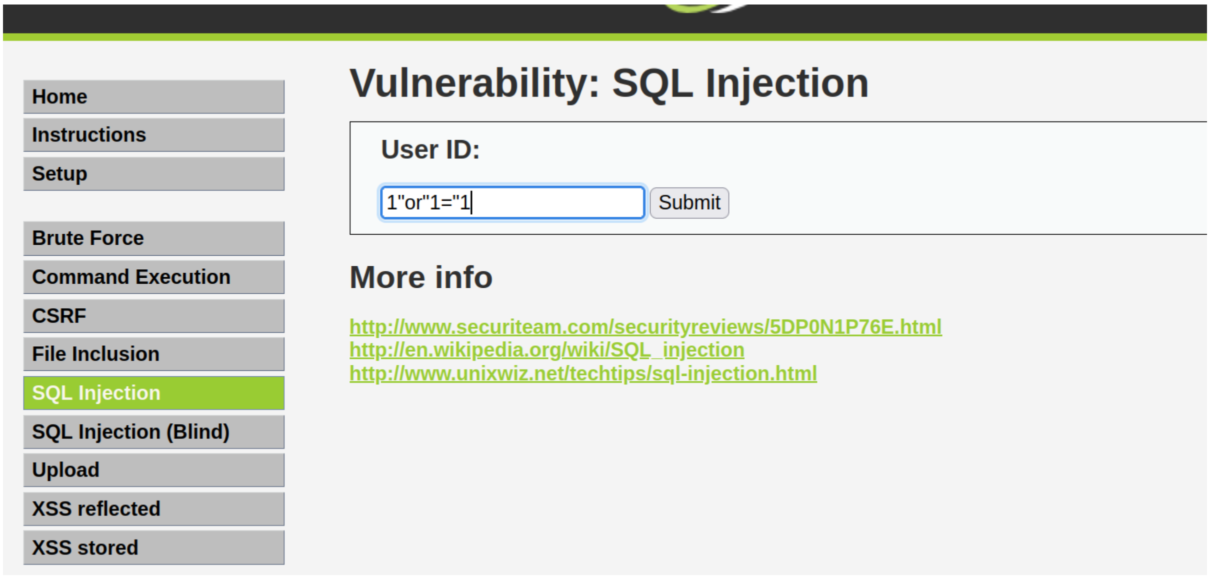
low

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]



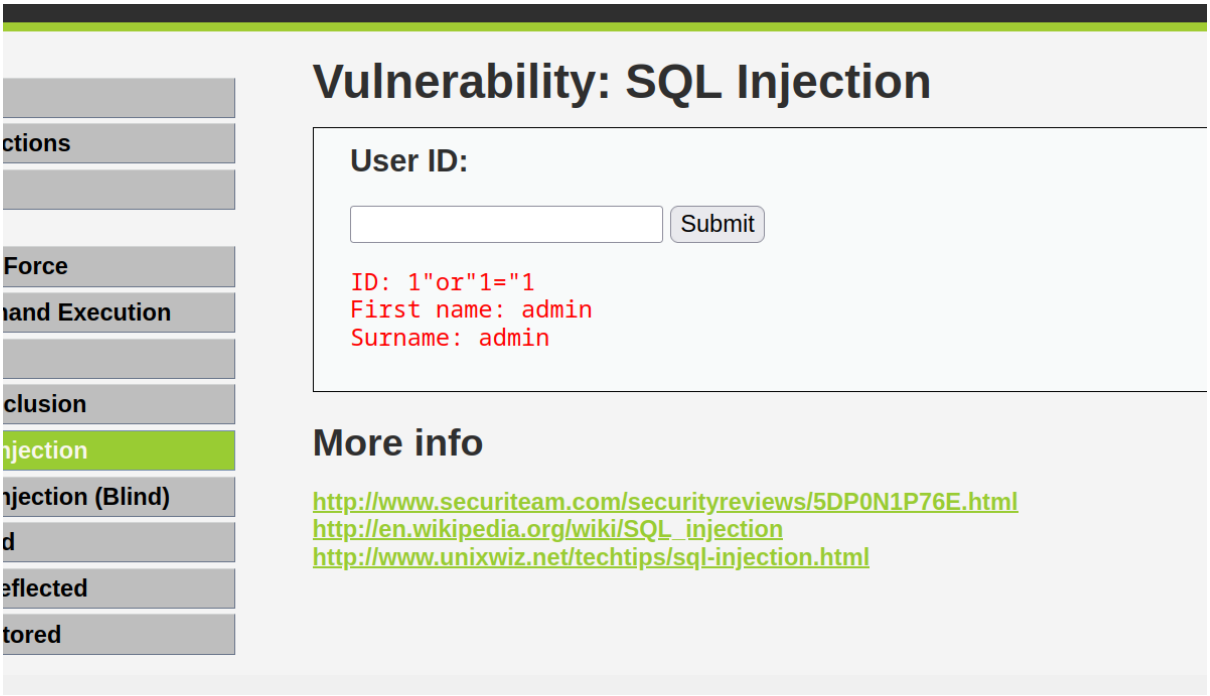
Vulnerability: SQL Injection

User ID:

1"or"1="1

More info

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



Vulnerability: SQL Injection

User ID:

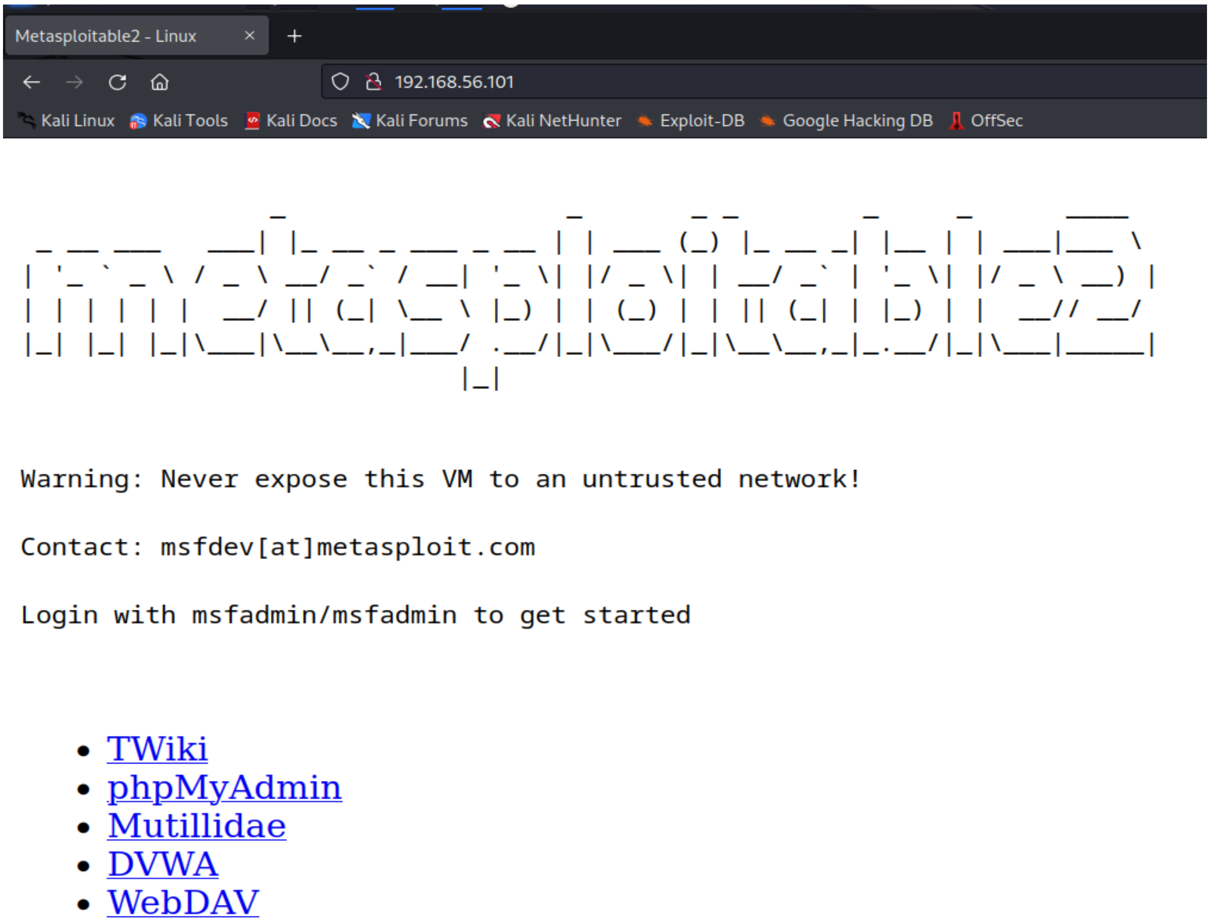
```
ID: 1"or"1="1
First name: admin
Surname: admin
```

More info

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

Perform Cross-site scripting on DVWA

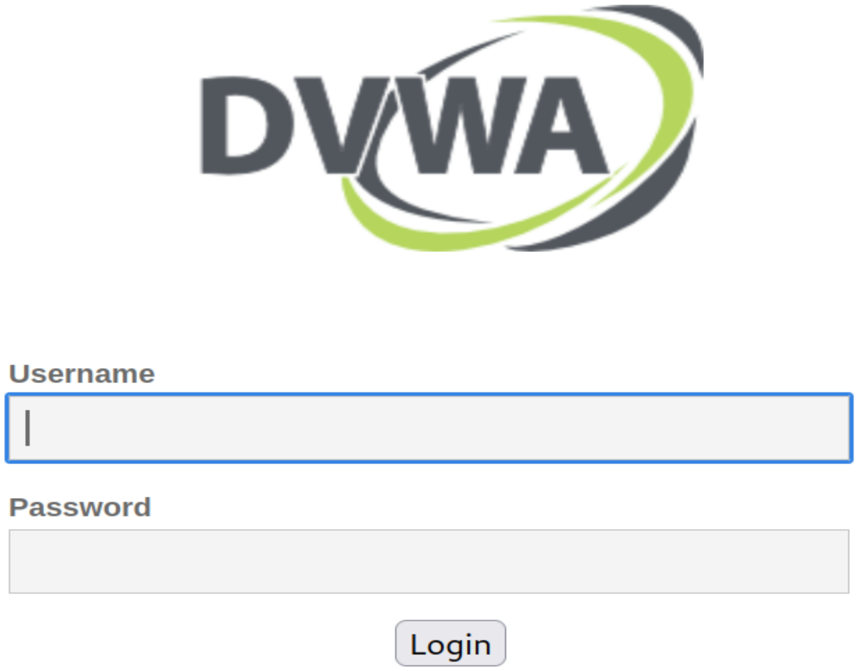
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.



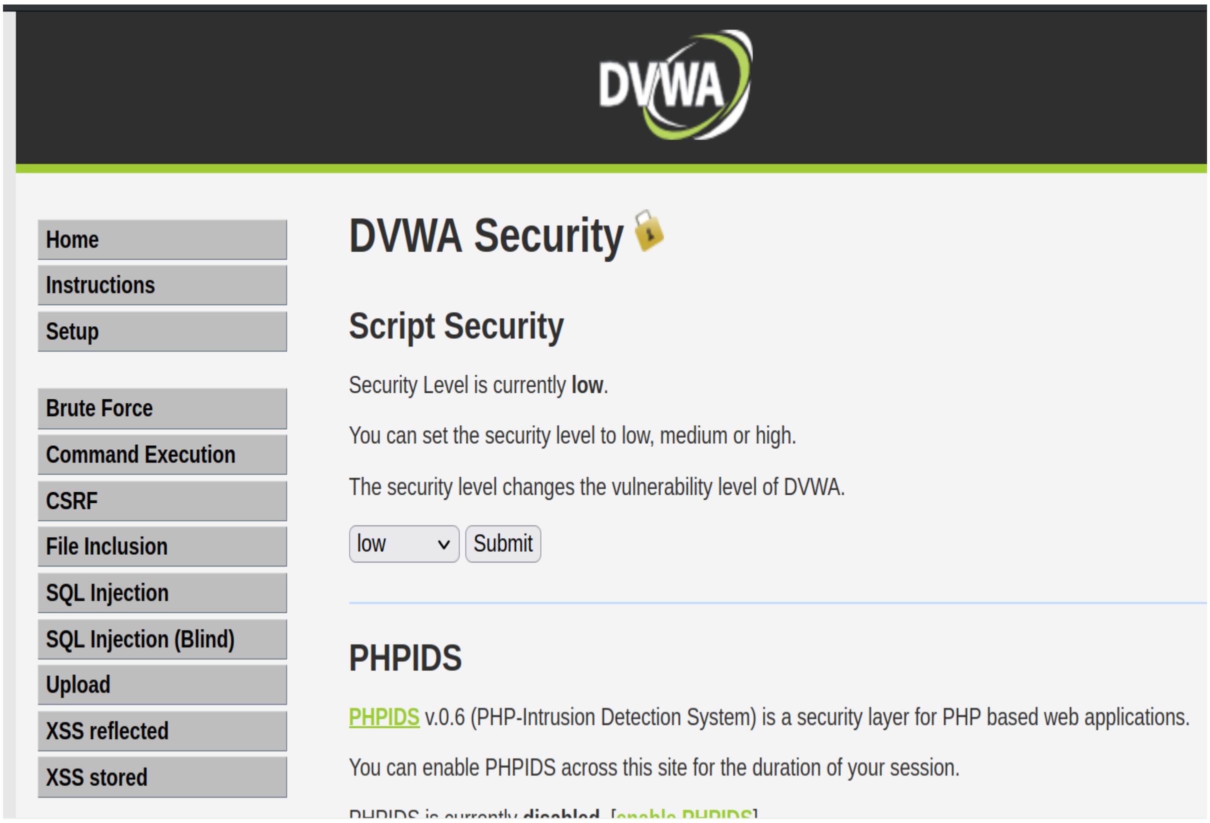
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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.



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



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.

low ⌄ Submit

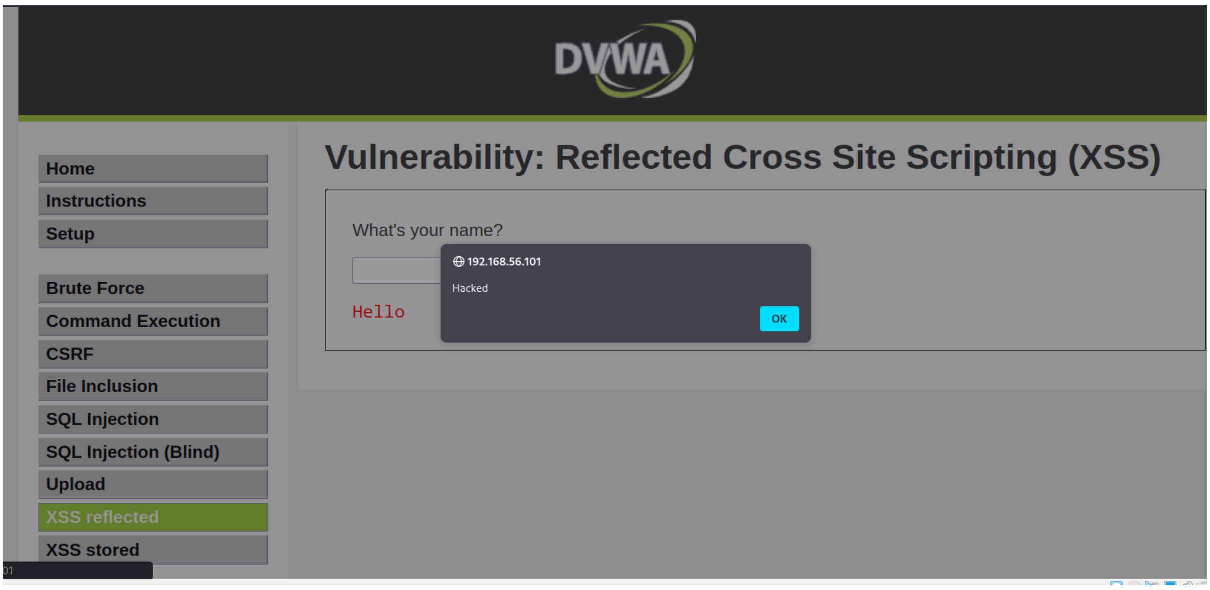
PHPIDS

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]

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.



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

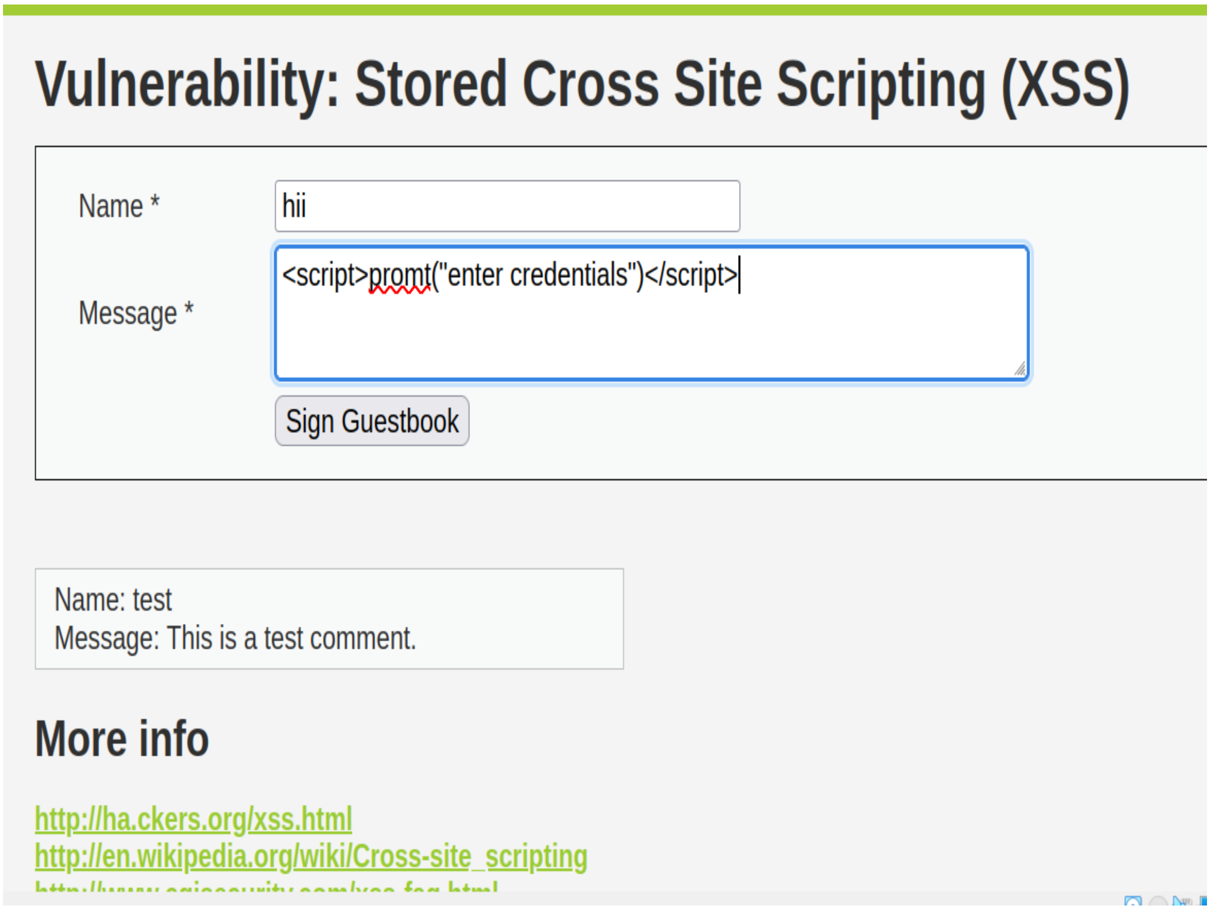
Hello

192.168.56.101

Hacked

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)

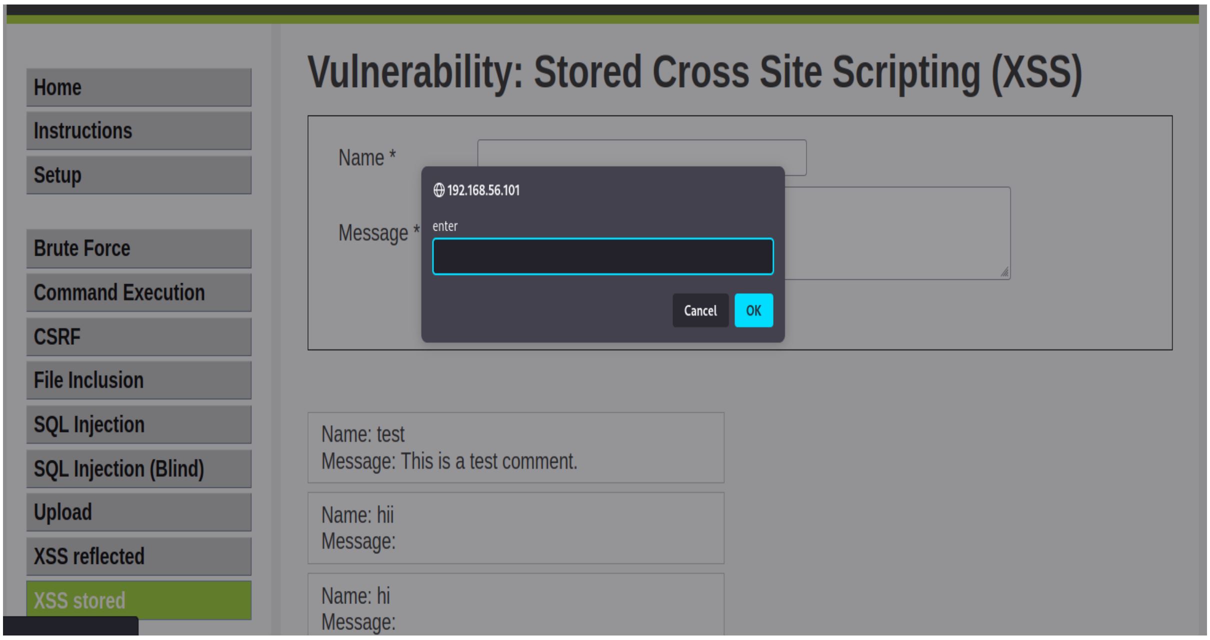
Name * hii

Message * <script>promt("enter credentials")</script>

Name: test
Message: This is a test comment.

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

192.168.56.101

enter

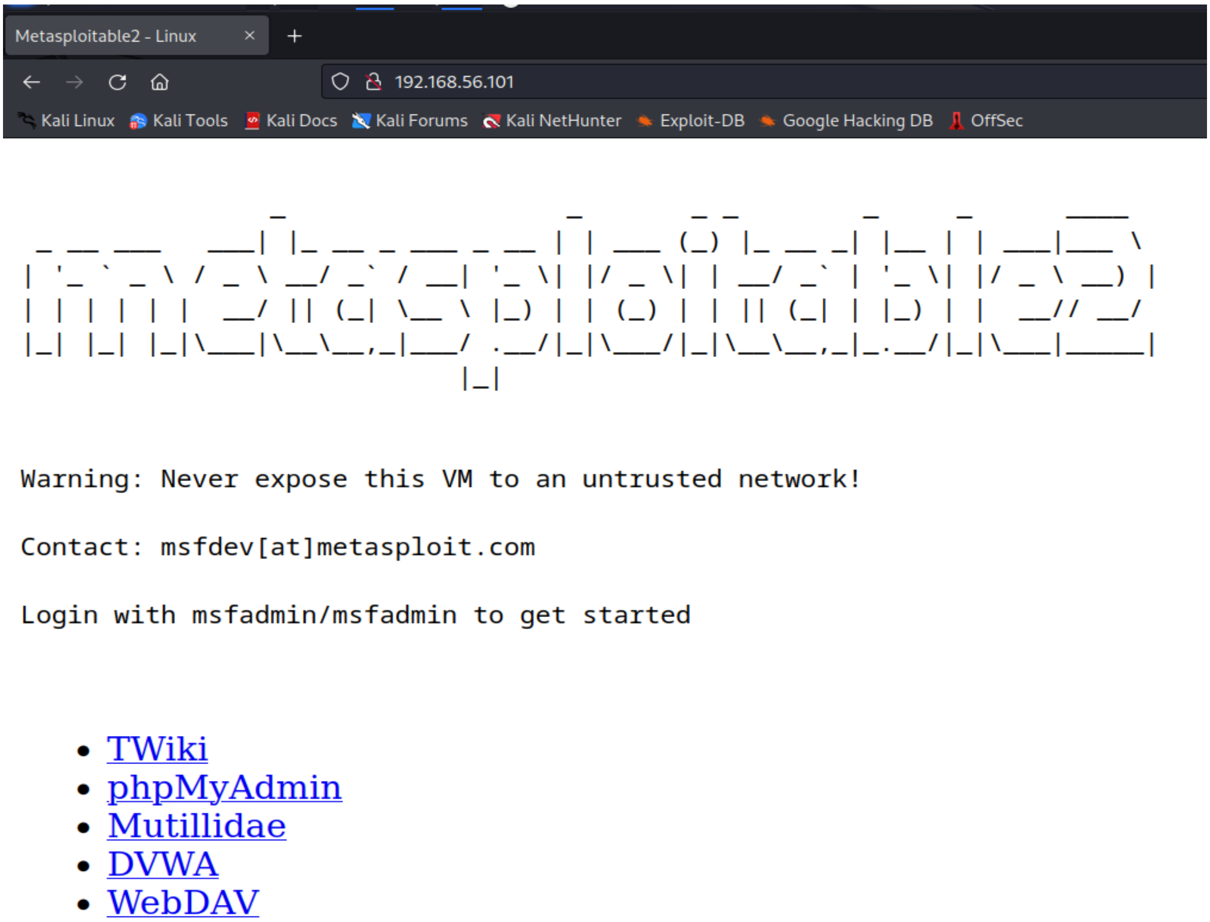
Name: test
Message: This is a test comment.

Name: hii
Message:

Name: hi
Message:

Perform File upload DVWA

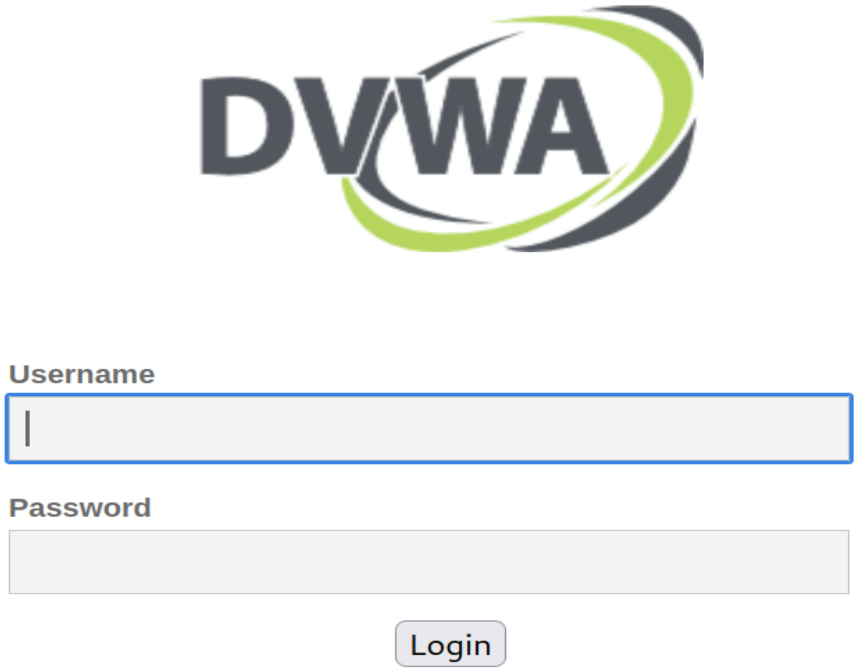
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.



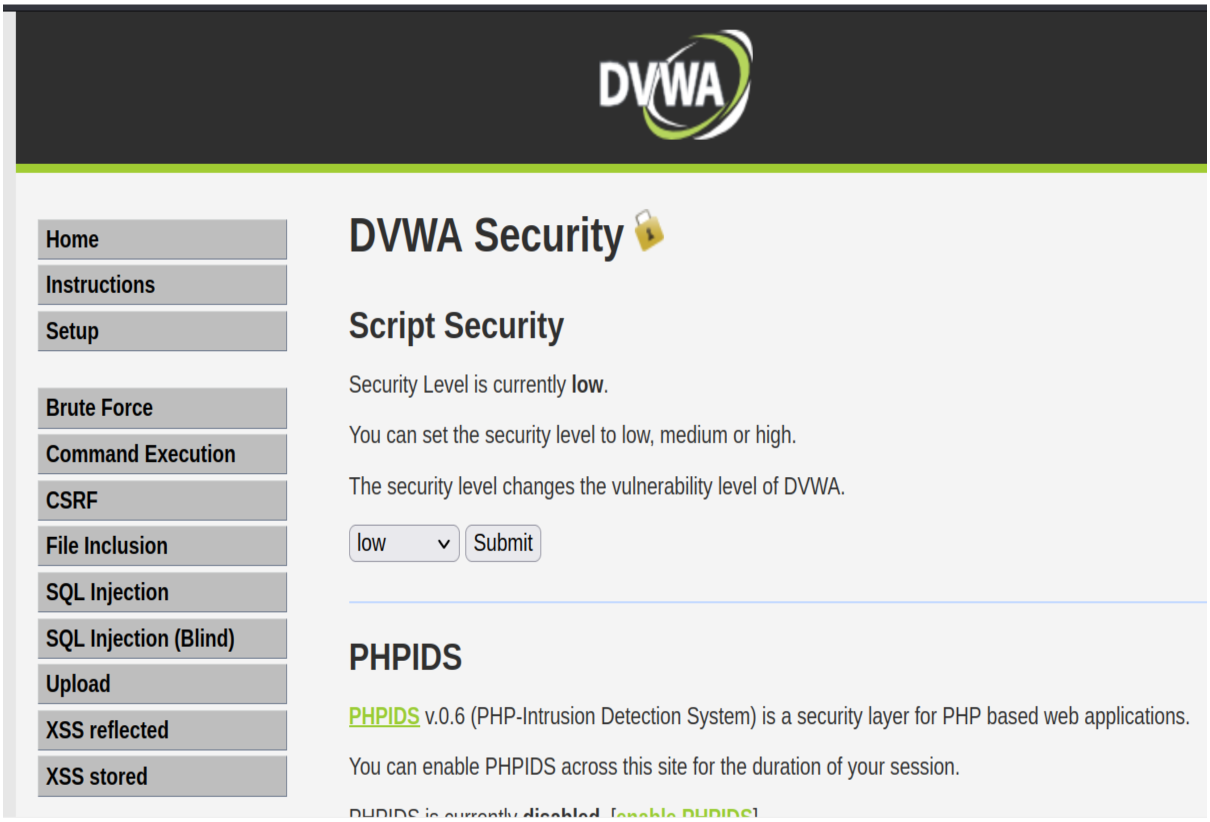
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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.



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



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.

low ⌄ Submit

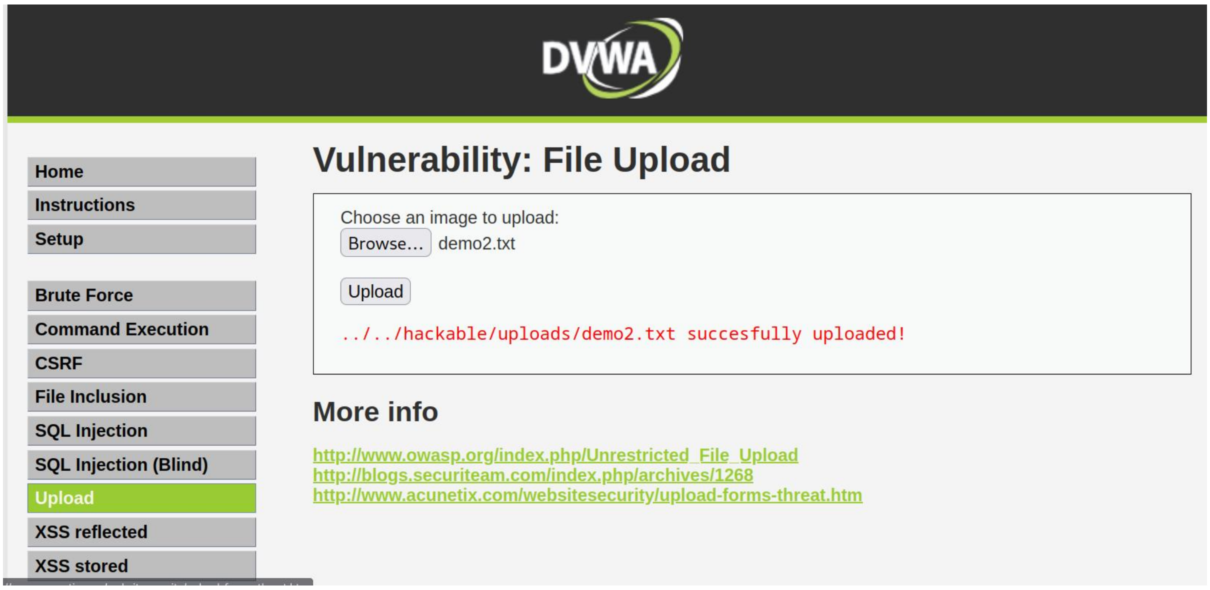
PHPIDS

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]

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.



Vulnerability: File Upload

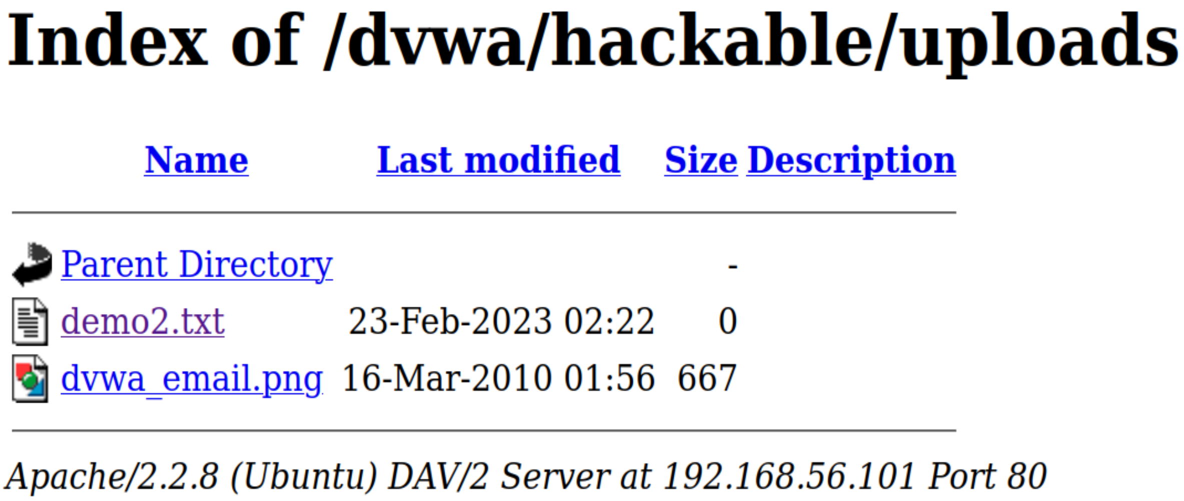
Choose an image to upload:

demo2.txt

```
../../hackable/uploads/demo2.txt succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm



Index of /dvwa/hackable/uploads

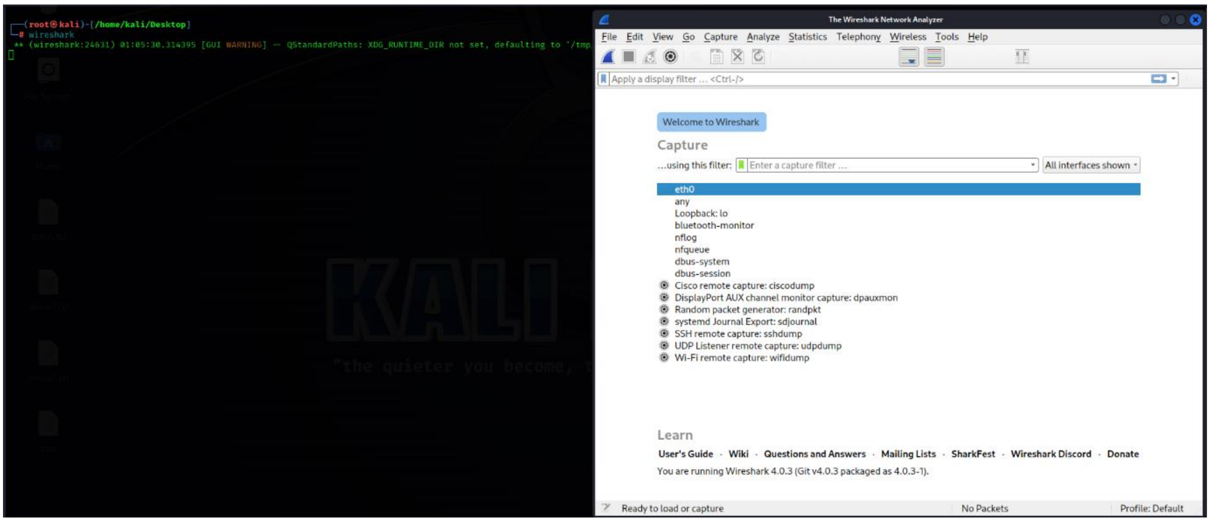
Name	Last modified	Size	Description
Parent Directory		-	
demo2.txt	23-Feb-2023 02:22	0	
dvwa_email.png	16-Mar-2010 01:56	667	

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.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# wireshark
 ** (wireshark:24631) 01:05:30.314395 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp
```

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

- eth0
- any
- Loopback: lo
- bluetooth-monitor
- nflog
- nfqueue
- dbus-system
- dbus-session
- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump
- Wi-Fi remote capture: wifidump

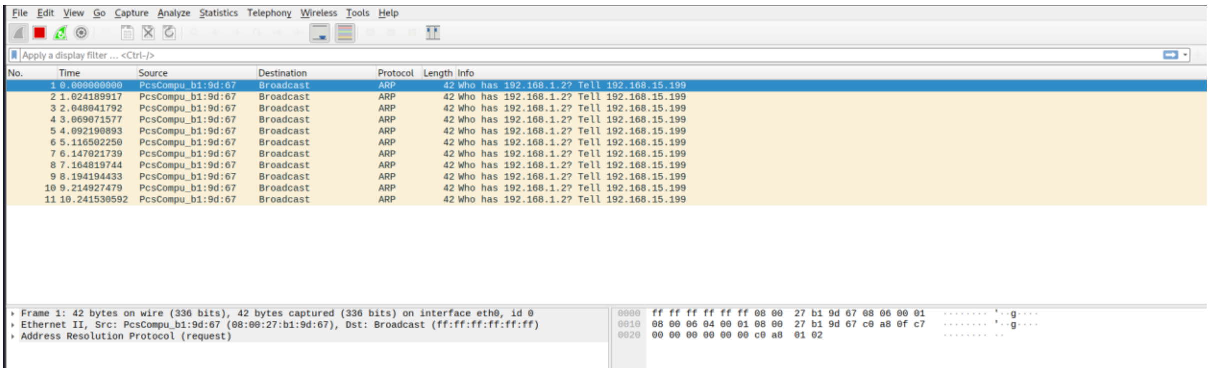
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (Git v4.0.3 packaged as 4.0.3-1).

Ready to load or capture | No Packets | Profile: Default

Step 2: double click on the eth0 option.



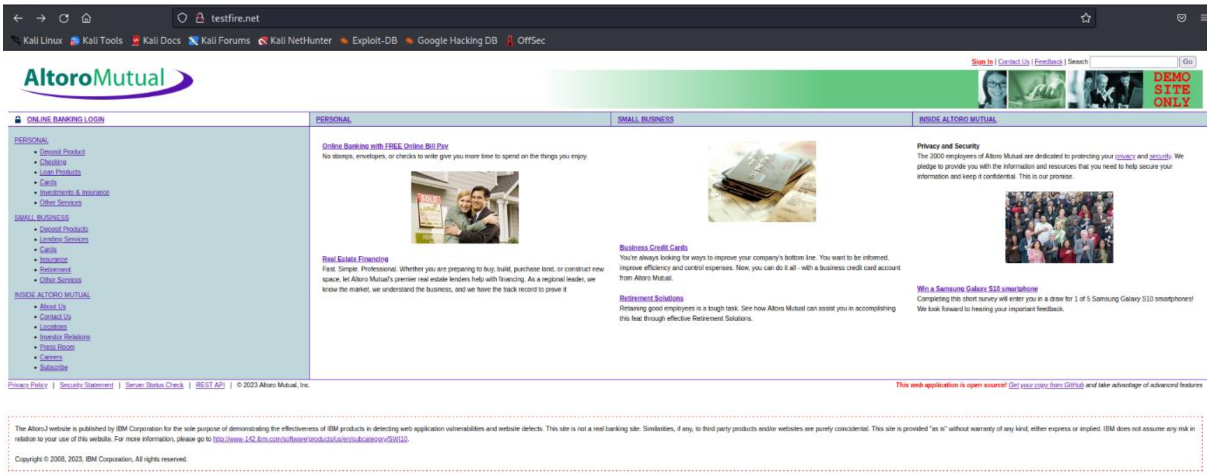
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source              Destination     Protocol  Length Info
    1 0.000000000   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    2 1.024189917   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    3 2.048041792   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    4 3.069071577   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    5 4.092190893   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    6 5.116502250   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    7 6.147021739   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    8 7.164819744   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
    9 8.194194433   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
   10 9.214927479   PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
   11 10.241530592  PcsCompu_b1:9d:67   Broadcast       ARP       42 Who has 192.168.1.2? Tell 192.168.15.199
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 08 00  27 b1 9d 67 08 06 00 01   ········ '··g····
0010  08 00 06 04 00 01 08 00  27 b1 9d 67 c0 a8 0f c7   ········ '··g····
0020  00 00 00 00 00 00 c0 a8  01 02                     ········ ··
```

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



testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- 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.

Real Estate Financing

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.

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone

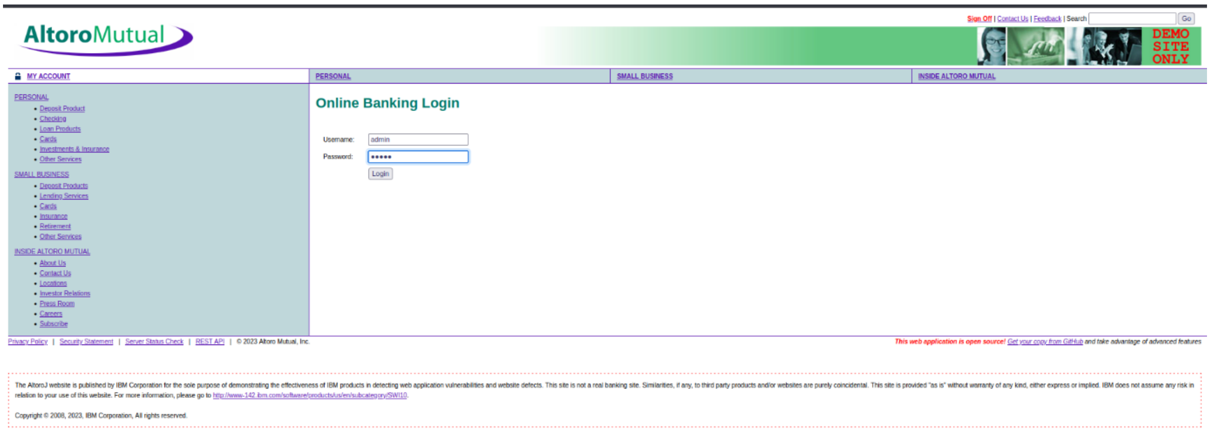
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

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

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

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 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-142.ibm.com/software/products/us/en/subcategory/SWI10.

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



Sign Off | Contact Us | Feedback | Search Go

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: admin

Password: •••••

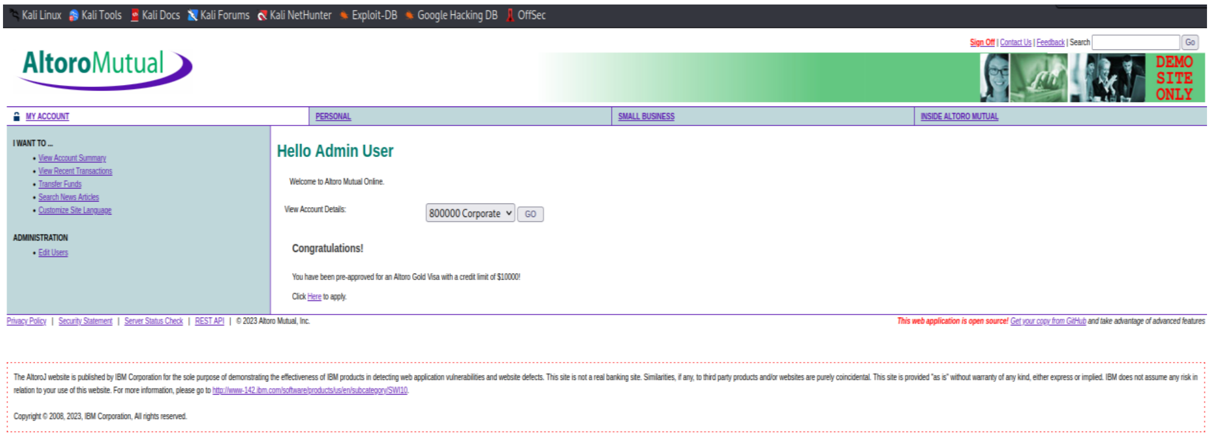
Login

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

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

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 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-142.ibm.com/software/products/us/en/subcategory/SWI10.

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



Sign Off | Contact Us | Feedback | Search Go

DEMO SITE ONLY

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 GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

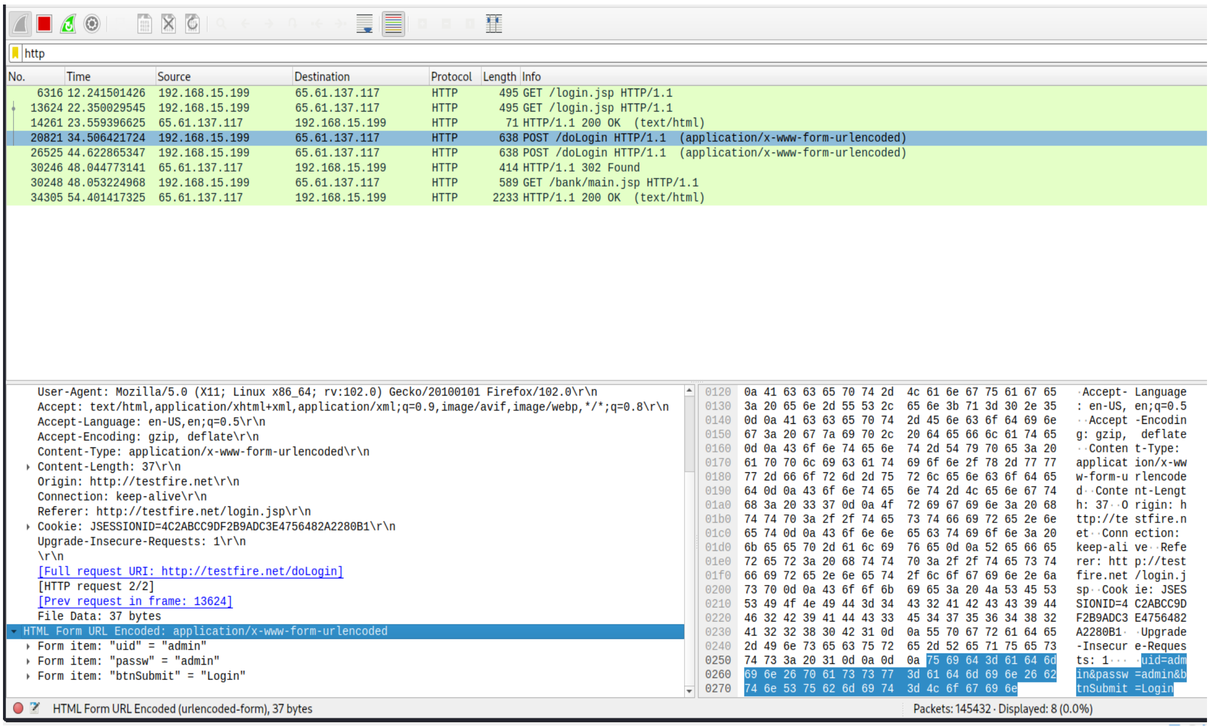
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

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

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 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-142.ibm.com/software/products/us/en/subcategory/SWI10.

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.



```
http

No.   Time          Source          Destination     Protocol Length Info
 6316 12.241501426  192.168.15.199  65.61.137.117   HTTP      495 GET /login.jsp HTTP/1.1
13624 22.350029545  192.168.15.199  65.61.137.117   HTTP      495 GET /login.jsp HTTP/1.1
14261 23.559396625  65.61.137.117   192.168.15.199  HTTP       71 HTTP/1.1 200 OK  (text/html)
20821 34.506421724  192.168.15.199  65.61.137.117   HTTP      638 POST /doLogin HTTP/1.1  (application/x-www-form-urlencoded)
26525 44.622865347  192.168.15.199  65.61.137.117   HTTP      638 POST /doLogin HTTP/1.1  (application/x-www-form-urlencoded)
30246 48.044773141  65.61.137.117   192.168.15.199  HTTP      414 HTTP/1.1 302 Found
30248 48.053224968  192.168.15.199  65.61.137.117   HTTP      589 GET /bank/main.jsp HTTP/1.1
34305 54.401417325  65.61.137.117   192.168.15.199  HTTP     2233 HTTP/1.1 200 OK  (text/html)
```

```
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  › Content-Length: 37\r\n
    Origin: http://testfire.net\r\n
    Connection: keep-alive\r\n
    Referer: http://testfire.net/login.jsp\r\n
  › Cookie: JSESSIONID=4C2ABCC9DF2B9ADC3E4756482A2280B1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testfire.net/doLogin]
    [HTTP request 2/2]
    [Prev request in frame: 13624]
    File Data: 37 bytes
˅ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uid" = "admin"
  › Form item: "passw" = "admin"
  › Form item: "btnSubmit" = "Login"
```

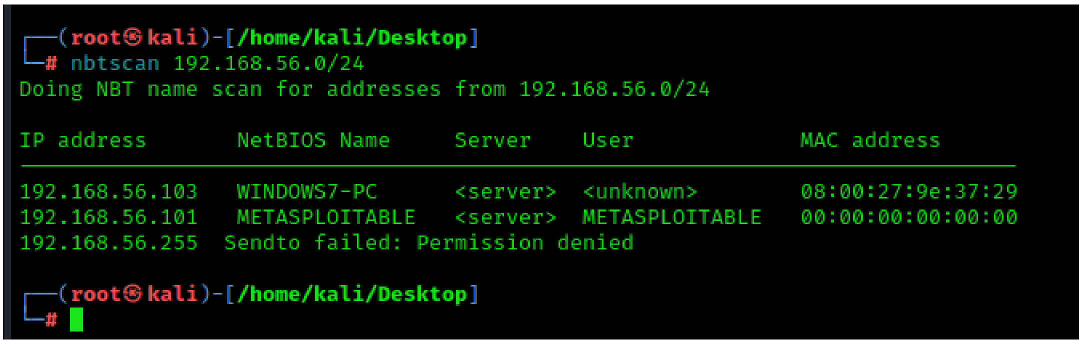
```
0120  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0130  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0140  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0150  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0160  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type:
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
0180  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
0190  64 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   d··Conte nt-Lengt
01a0  68 3a 20 33 37 0d 0a 4f  72 69 67 69 6e 3a 20 68   h: 37··O rigin: h
01b0  74 74 70 3a 2f 2f 74 65  73 74 66 69 72 65 2e 6e   ttp://te stfire.n
01c0  65 74 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   et··Conn ection:
01d0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 52 65 66 65   keep-ali ve··Refe
01e0  72 65 72 3a 20 68 74 74  70 3a 2f 2f 74 65 73 74   rer: htt p://test
01f0  66 69 72 65 2e 6e 65 74  2f 6c 6f 67 69 6e 2e 6a   fire.net /login.j
0200  73 70 0d 0a 43 6f 6f 6b  69 65 3a 20 4a 53 45 53   sp··Cook ie: JSES
0210  53 49 4f 4e 49 44 3d 34  43 32 41 42 43 43 39 44   SIONID=4 C2ABCC9D
0220  46 32 42 39 41 44 43 33  45 34 37 35 36 34 38 32   F2B9ADC3 E4756482
0230  41 32 32 38 30 42 31 0d  0a 55 70 67 72 61 64 65   A2280B1· ·Upgrade
0240  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0250  74 73 3a 20 31 0d 0a 0d  0a 75 69 64 3d 61 64 6d   ts: 1··· ·uid=adm
0260  69 6e 26 70 61 73 73 77  3d 61 64 6d 69 6e 26 62   in&passw =admin&b
0270  74 6e 53 75 62 6d 69 74  3d 4c 6f 67 69 6e         tnSubmit =Login
```

HTML Form URL Encoded (urlencoded-form), 37 bytes

Packets: 145432 · Displayed: 8 (0.0%)

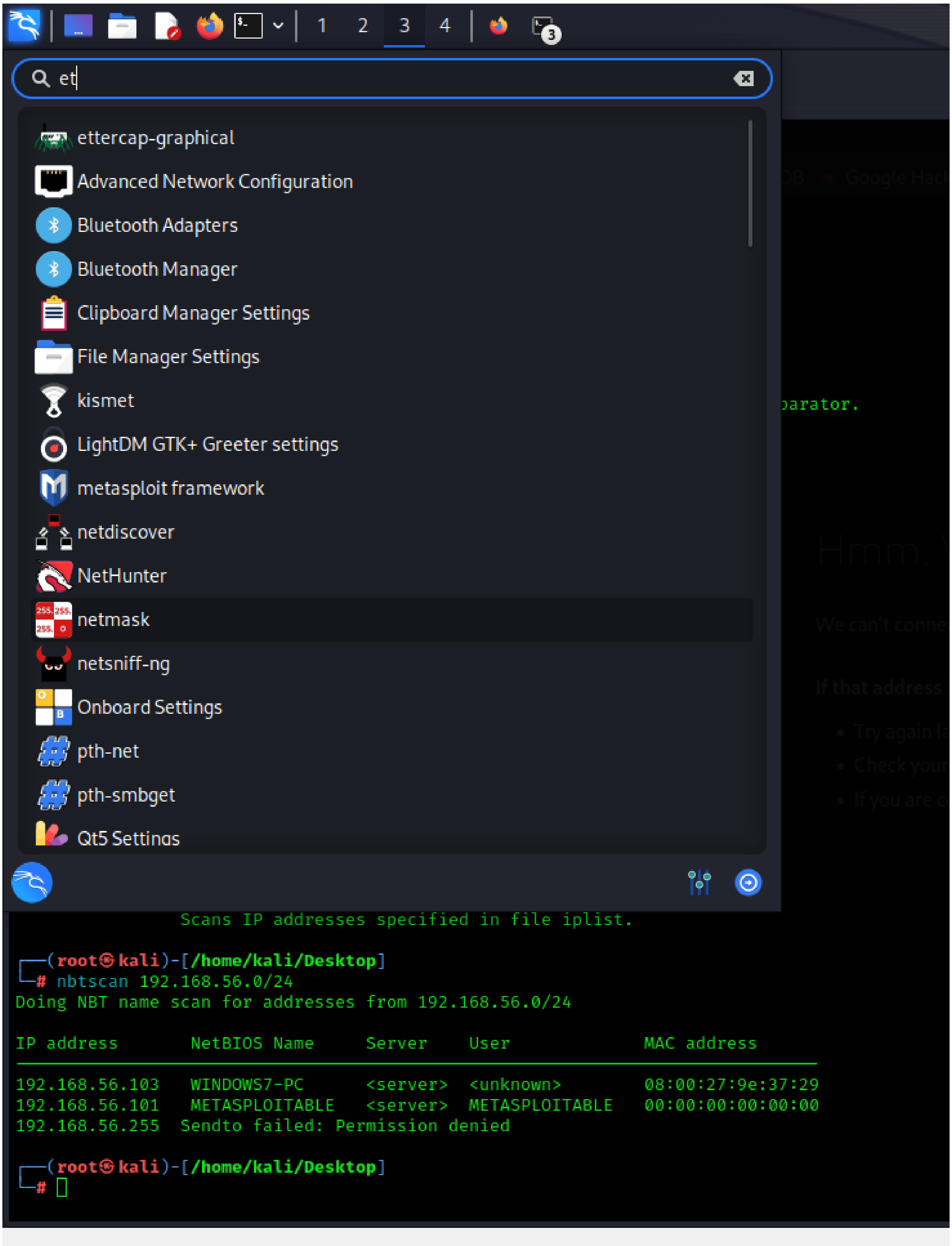
Perform Sniffing using Ettercap in kali linux

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.



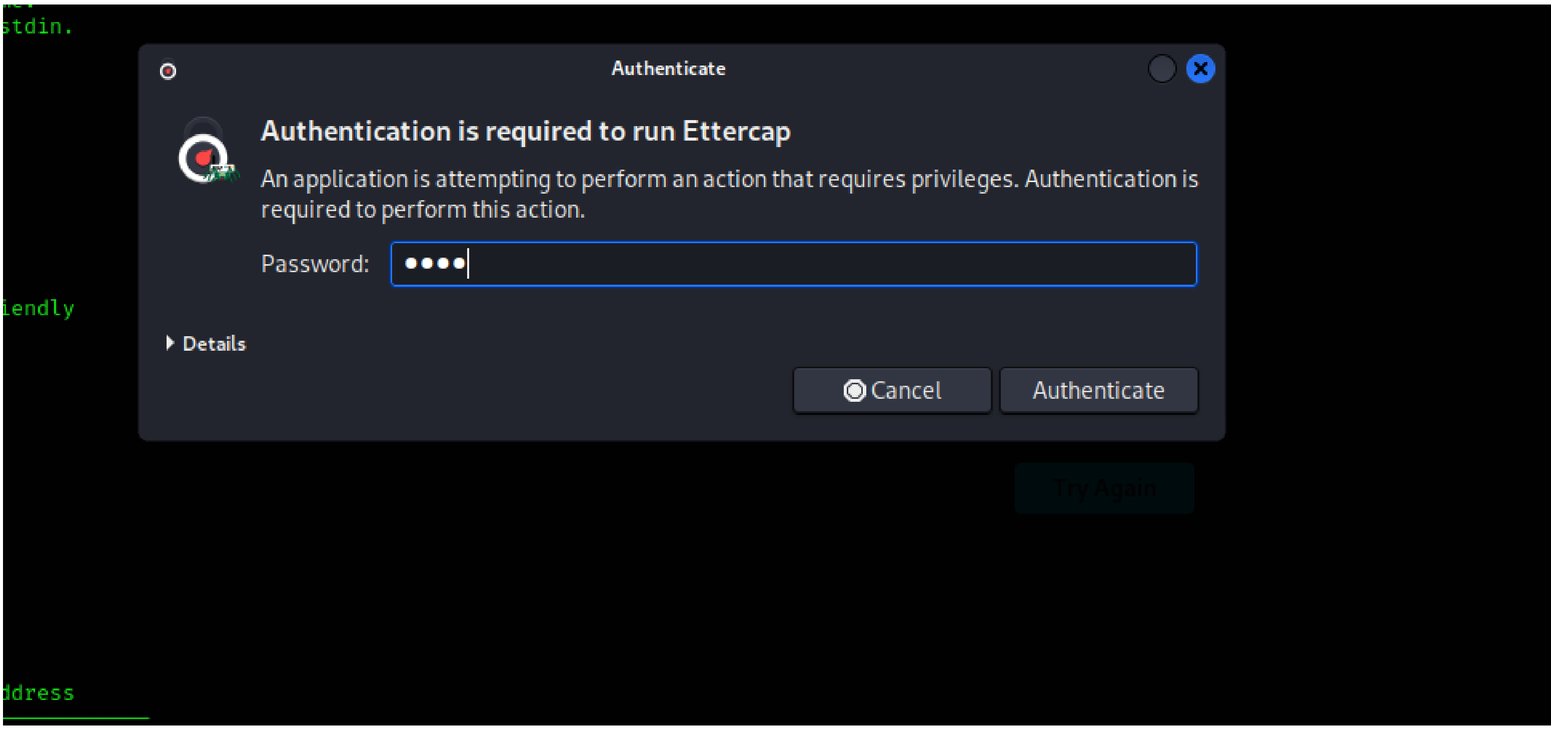
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

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.



```
                 Scans IP addresses specified in file iplist.

┌──(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 3: Enter the password of root that is kali and authenticate it.



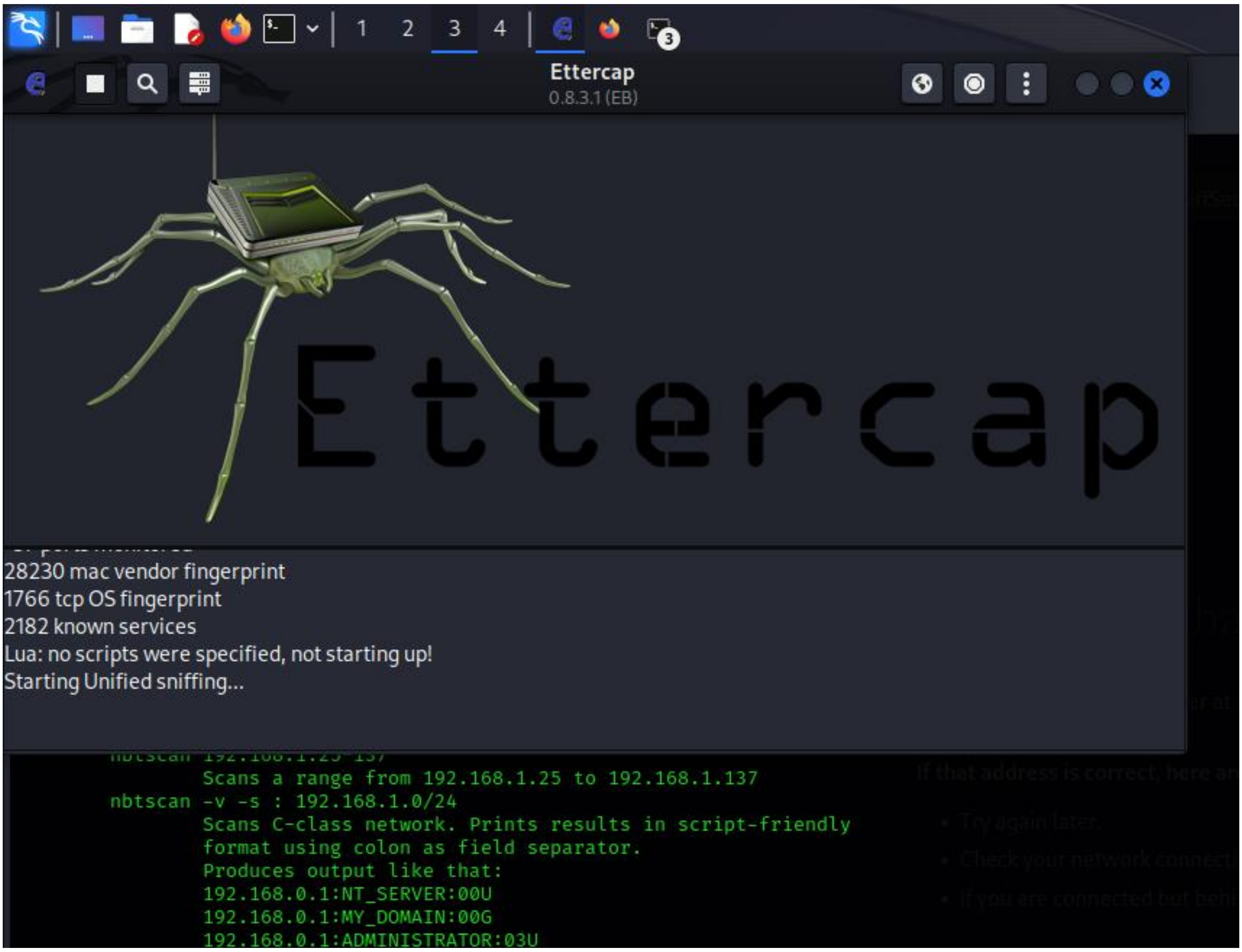
```
stdin.
iendly
ddress
```

Authenticate

Authentication is required to run Ettercap

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

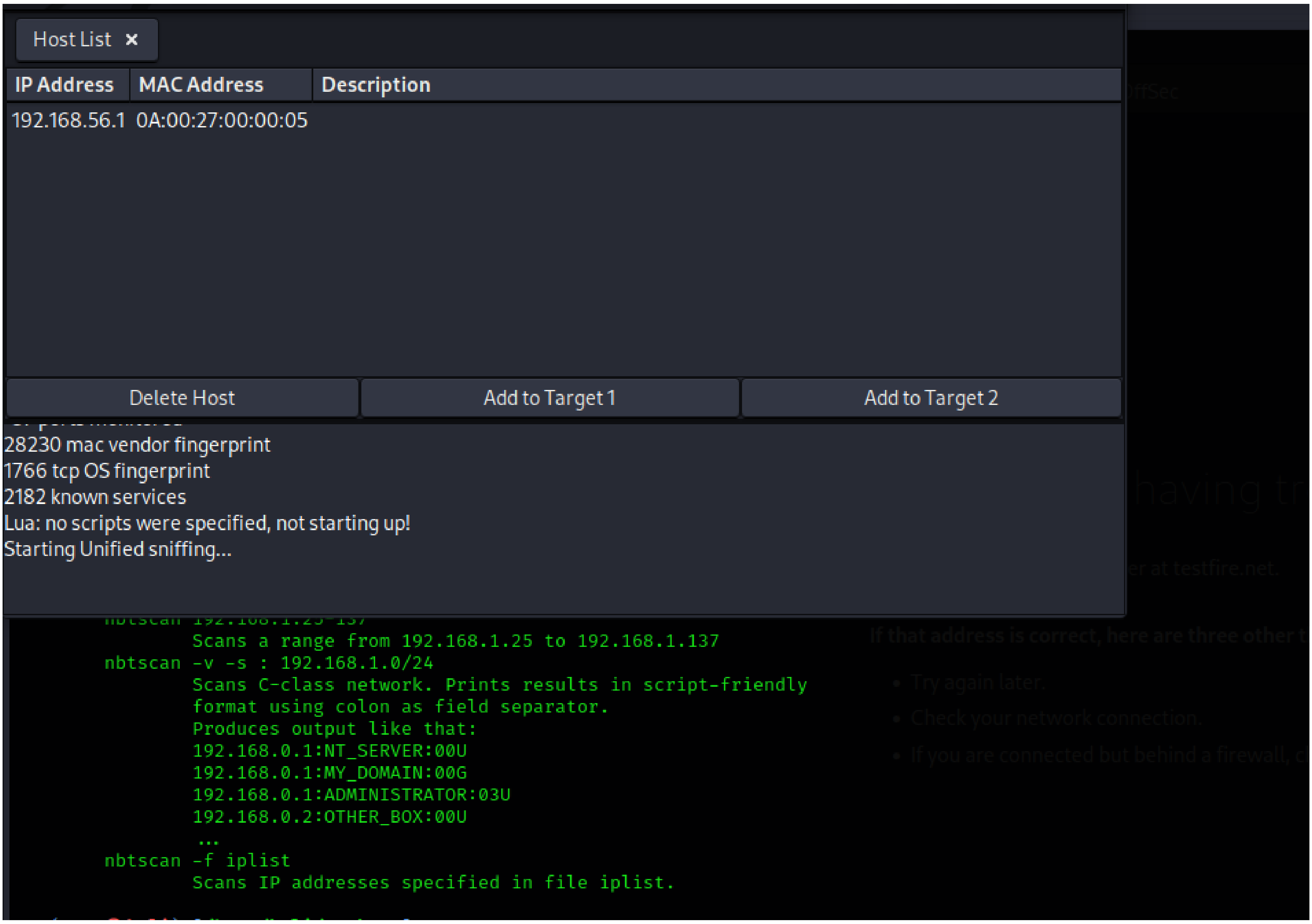
Password: ●●●●



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

```
                 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
```

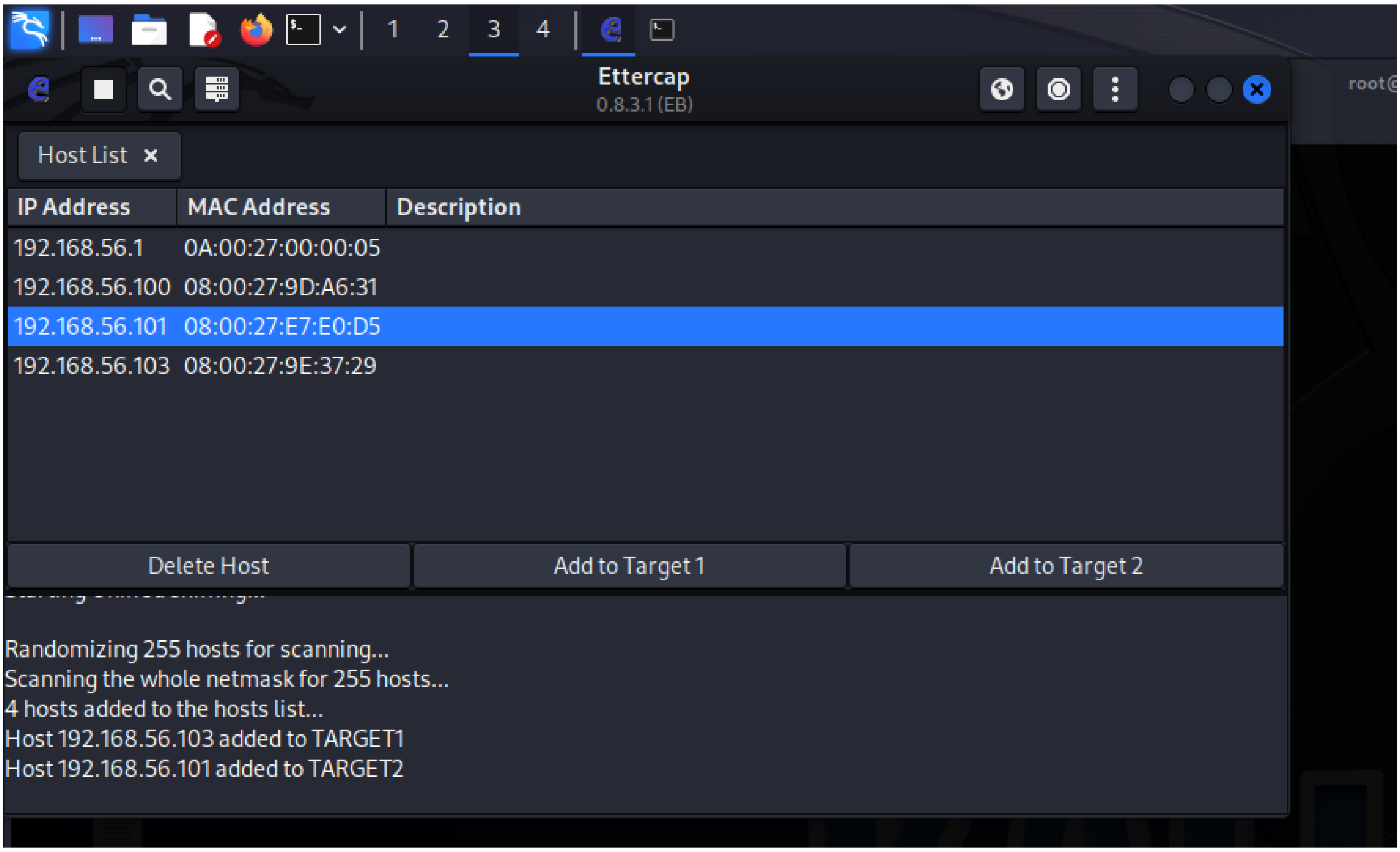
Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto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



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

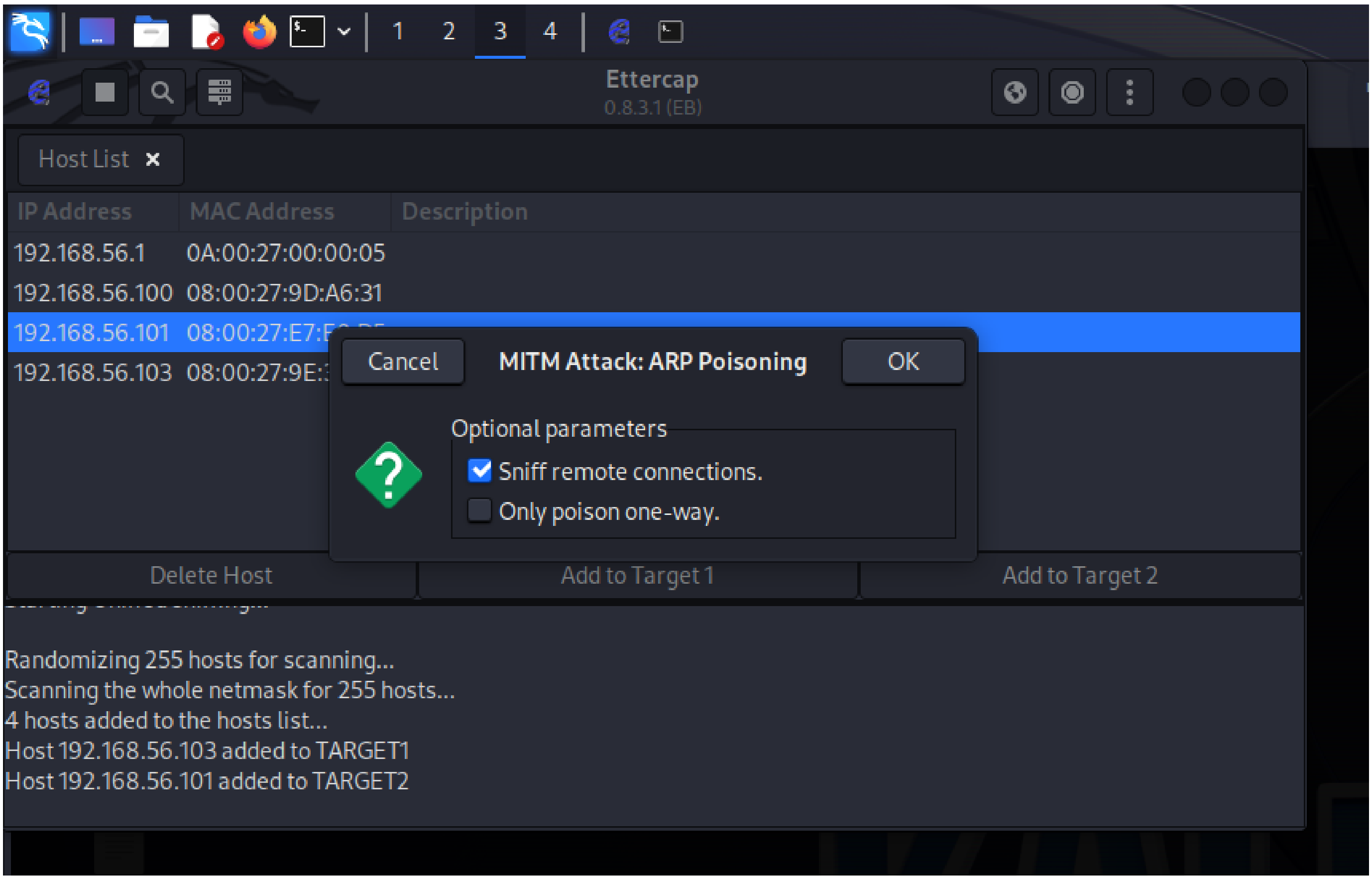
```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

```
        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.
```



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	

```
Starting Unified sniffing...

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
```



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:	
192.168.56.103	08:00:27:9E:	

MITM Attack: ARP Poisoning

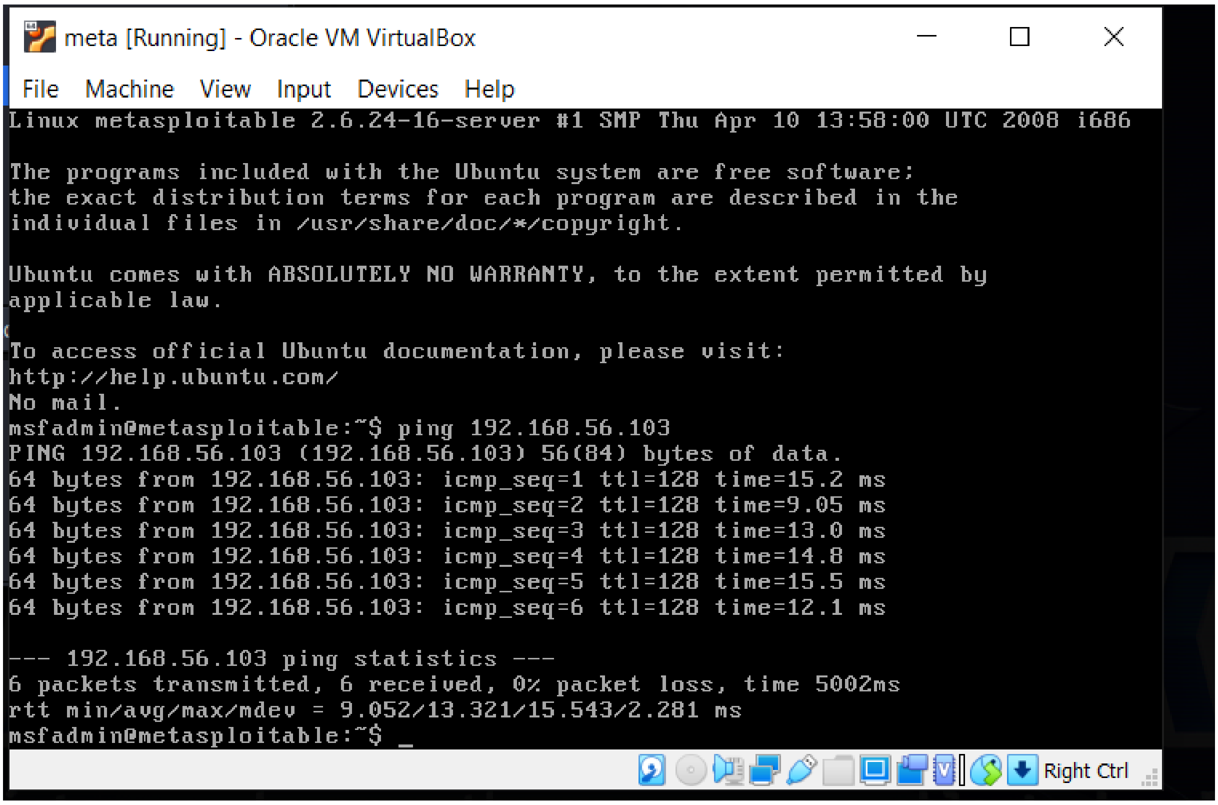
Optional parameters

☑ Sniff remote connections.

☐ Only poison one-way.

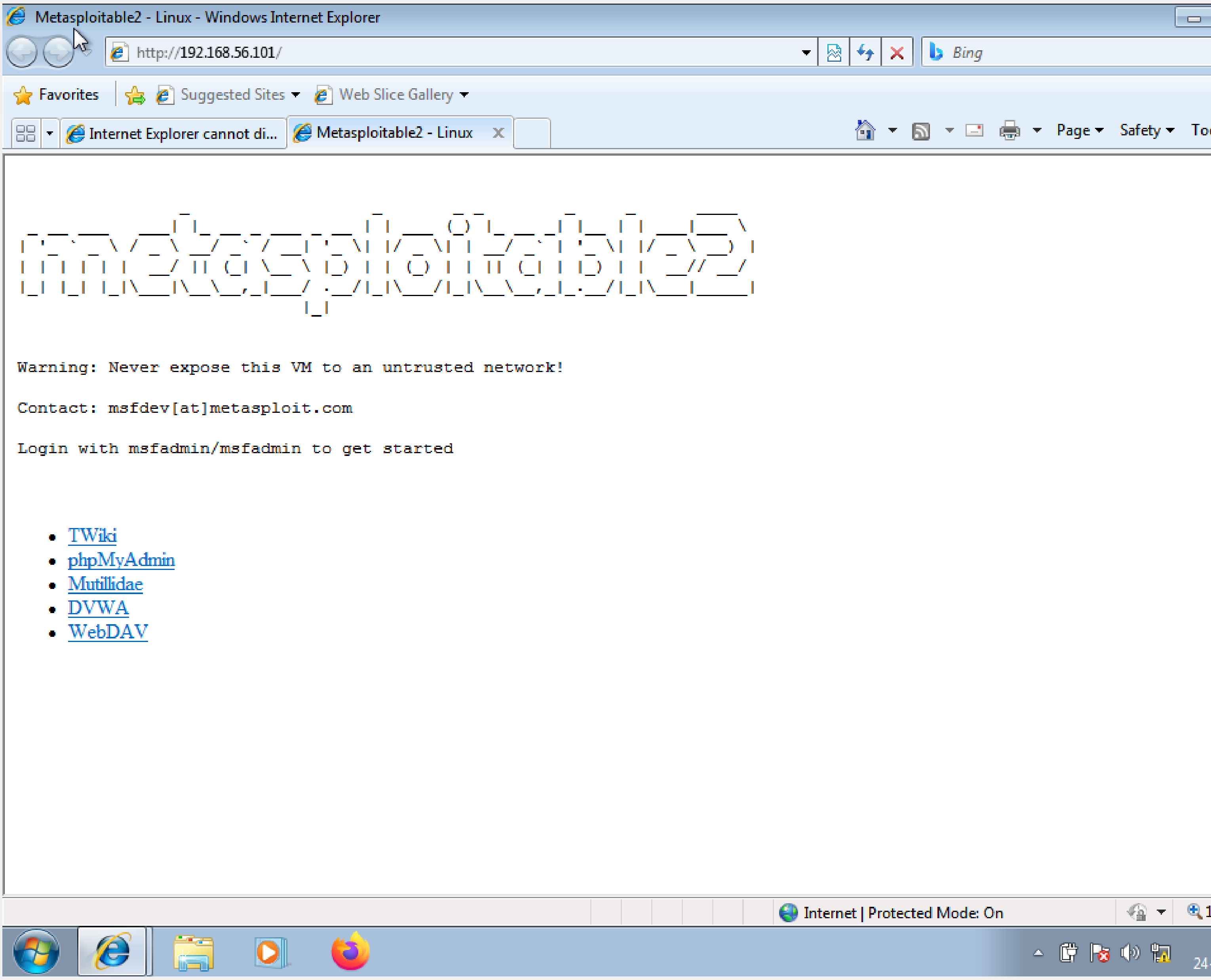
```
Starting Unified sniffing...

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
Right Ctrl

```
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:~$ _
```


Metasploitable2 - Linux - Windows Internet Explorer
http://192.168.56.101/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot di...
Metasploitable2 - Linux
Page
Safety
To
Internet | Protected Mode: On
24

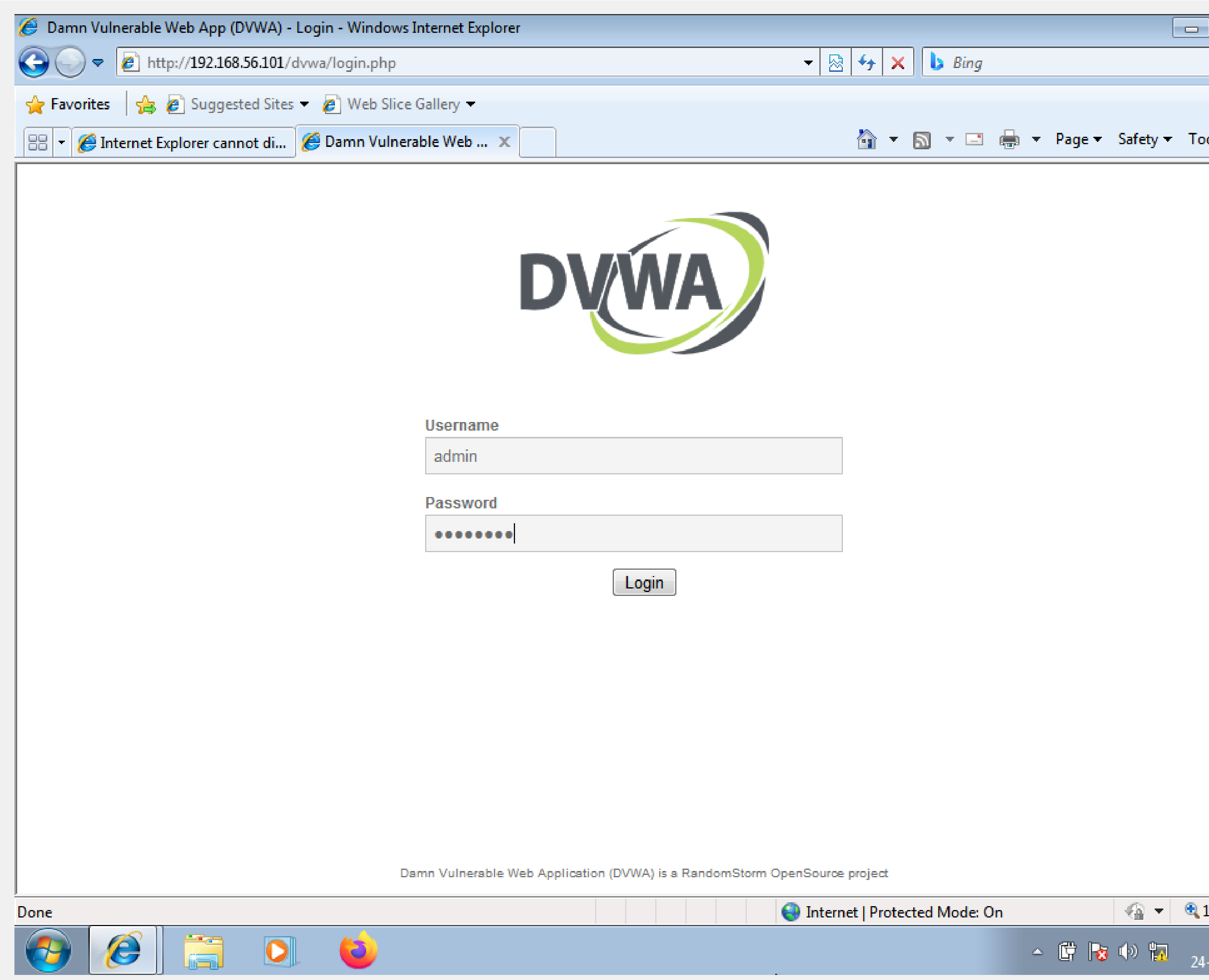
```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          
```

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


Damn Vulnerable Web App (DVWA) - Login - Windows Internet Explorer
http://192.168.56.101/dvwa/login.php
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot di...
Damn Vulnerable Web ...
Page
Safety
Toc
DVWA

Username

admin

Password

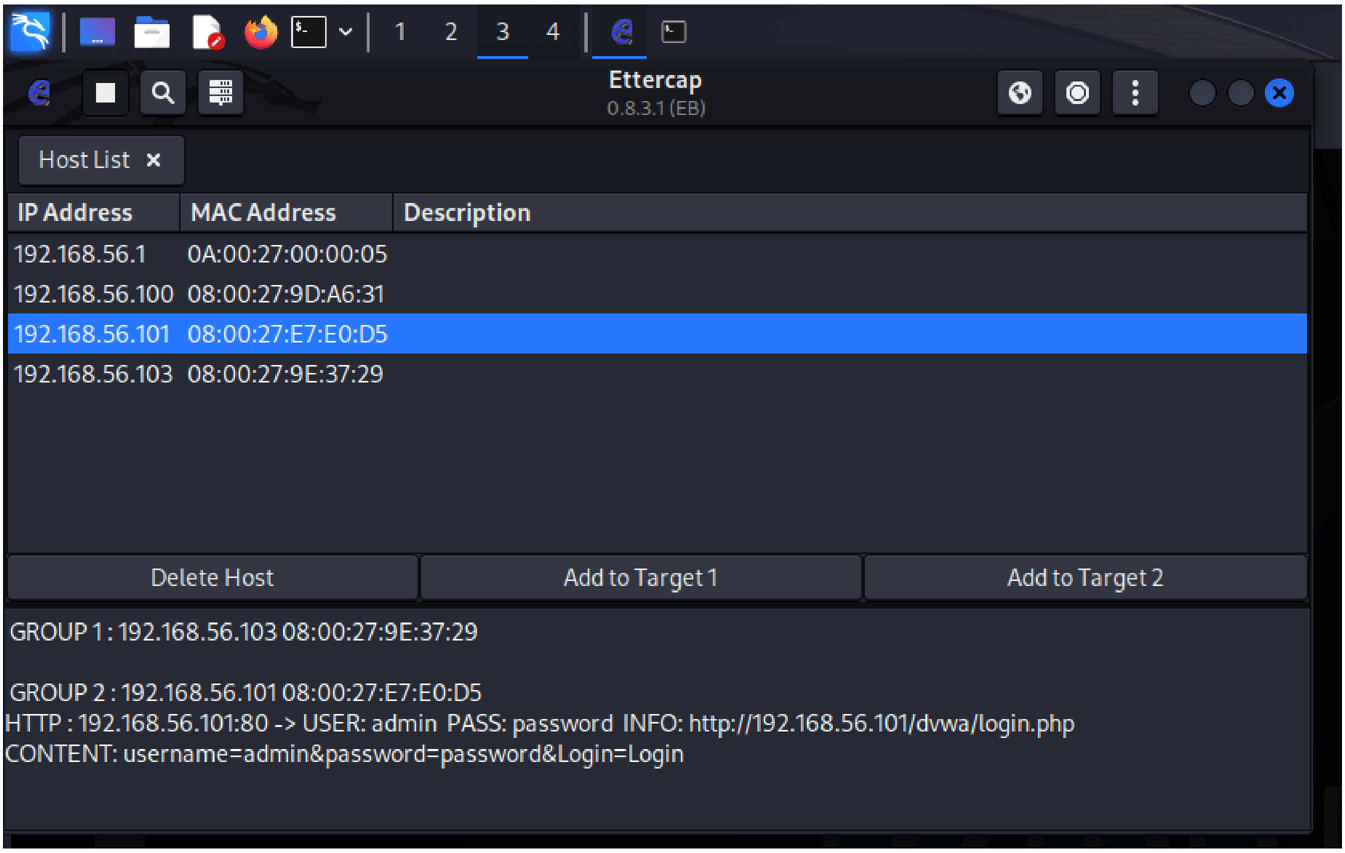
••••••••

Login

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

Done
Internet | Protected Mode: On

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



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	

```
 GROUP 1 : 192.168.56.103 08:00:27:9E:37:29

 GROUP 2 : 192.168.56.101 08:00:27:E7:E0:D5
HTTP : 192.168.56.101:80 -> USER: admin  PASS: password  INFO: http://192.168.56.101/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login
```