SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

DIGITAL ASSIGNMENT 5 - WINTER SEMESTER 2022-23

Course : Information Security Management

Course Code : CSE3502

Slot : L29+30

Name : Chavan Mukul Manish

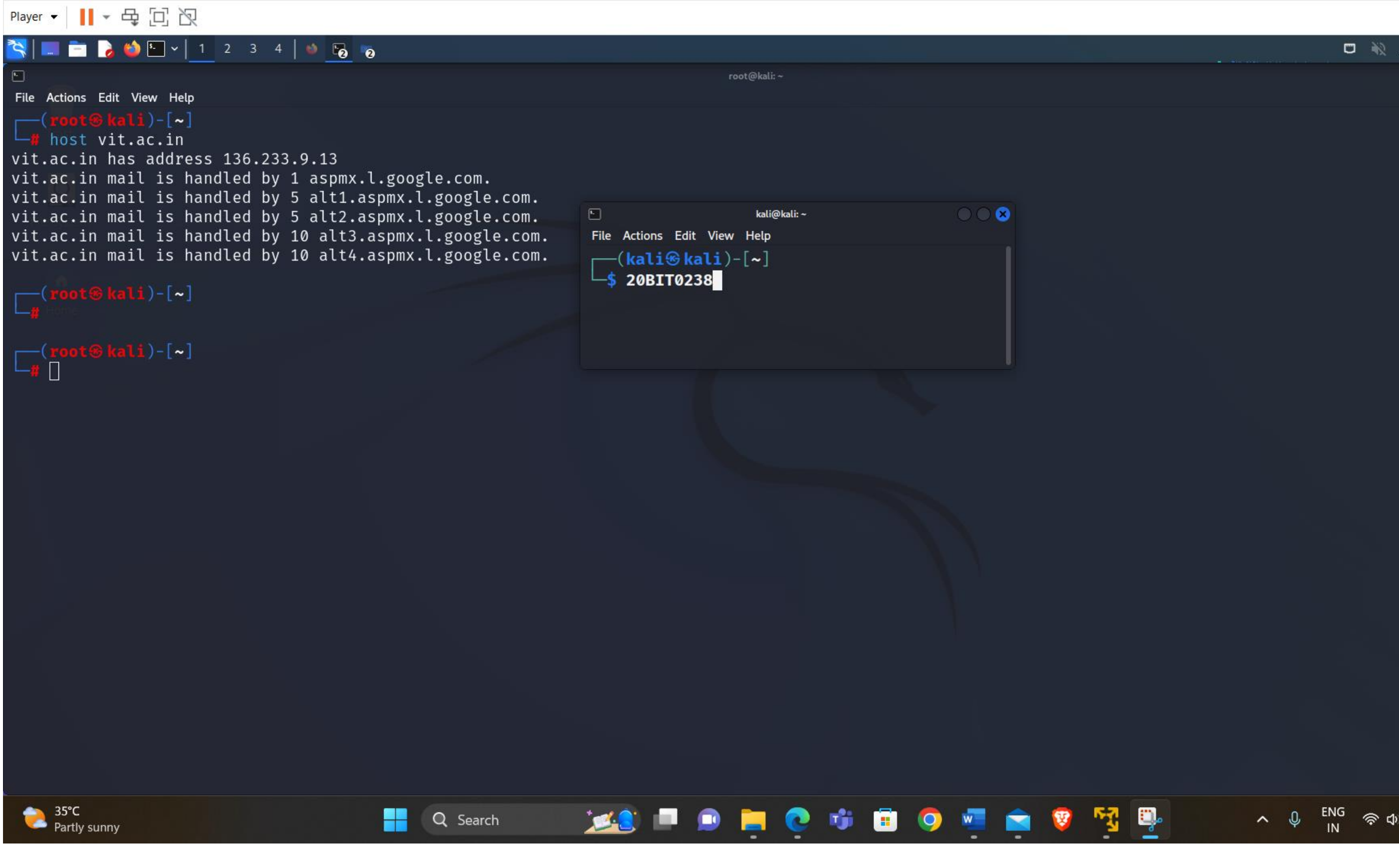
Reg no : 20BIT0238

1.Perform the various types of DNS enumeration by referring the video link given below on any website other than the given in the video which is also not a popular website.

https://www.youtube.com/watch?v=rQ-dc5kwRtU

Snapshot of host,nslookup and dig commands (3 marks)

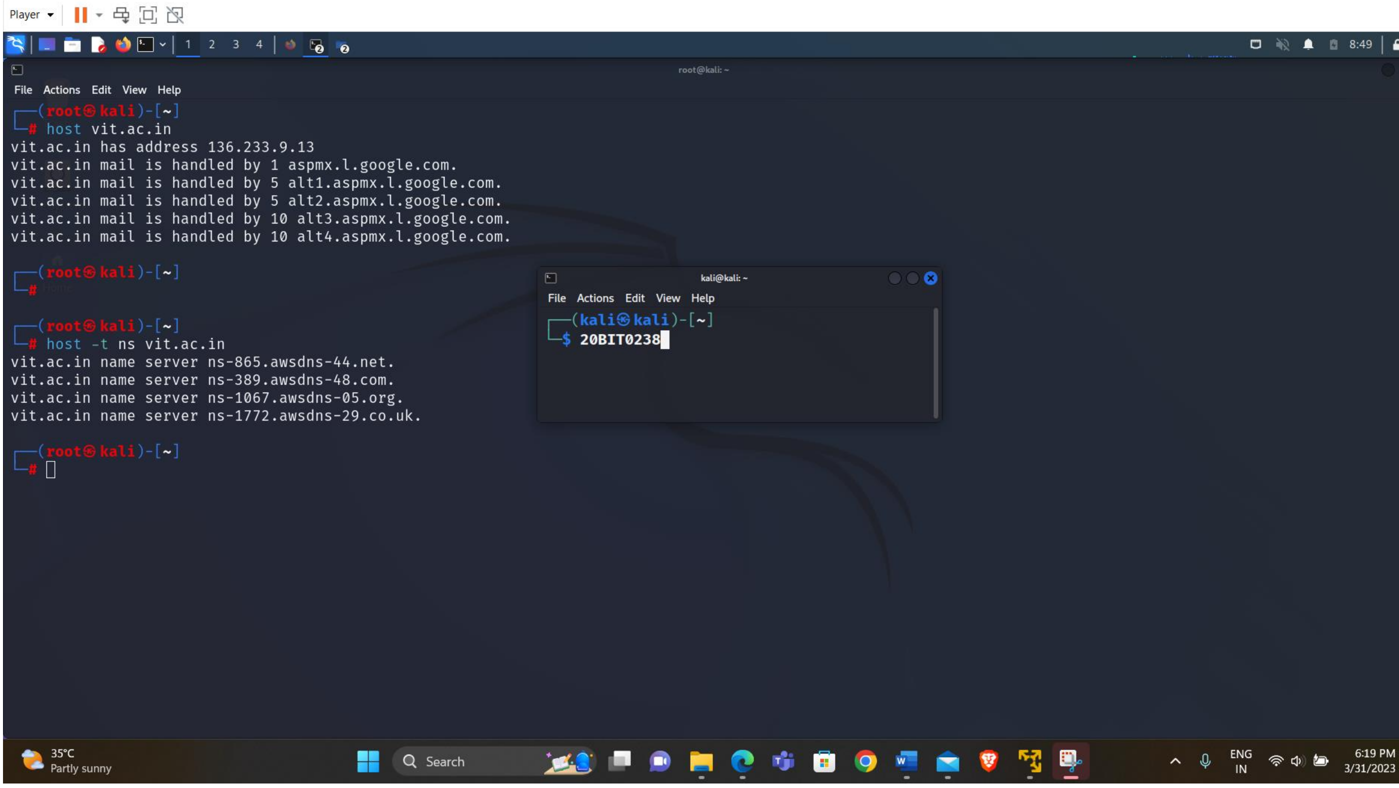
host vit.ac.in



```
┌──(root㉿kali)-[~]
└─# host vit.ac.in
vit.ac.in has address 136.233.9.13
vit.ac.in mail is handled by 1 aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt1.aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

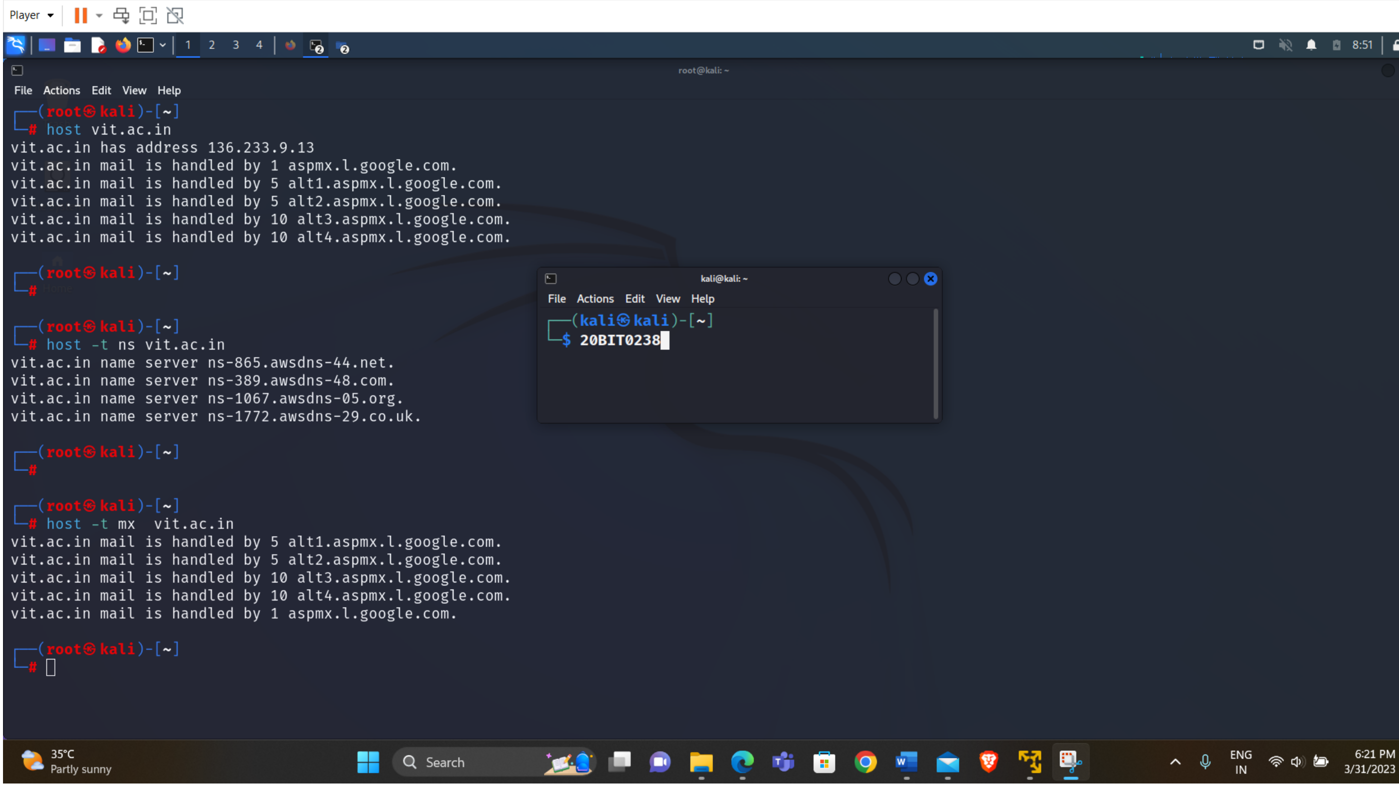
host -t ns vit.ac.in



```
┌──(root㉿kali)-[~]
└─# host vit.ac.in
vit.ac.in has address 136.233.9.13
vit.ac.in mail is handled by 1 aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt1.aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# host -t ns vit.ac.in
vit.ac.in name server ns-865.awsdns-44.net.
vit.ac.in name server ns-389.awsdns-48.com.
vit.ac.in name server ns-1067.awsdns-05.org.
vit.ac.in name server ns-1772.awsdns-29.co.uk.

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

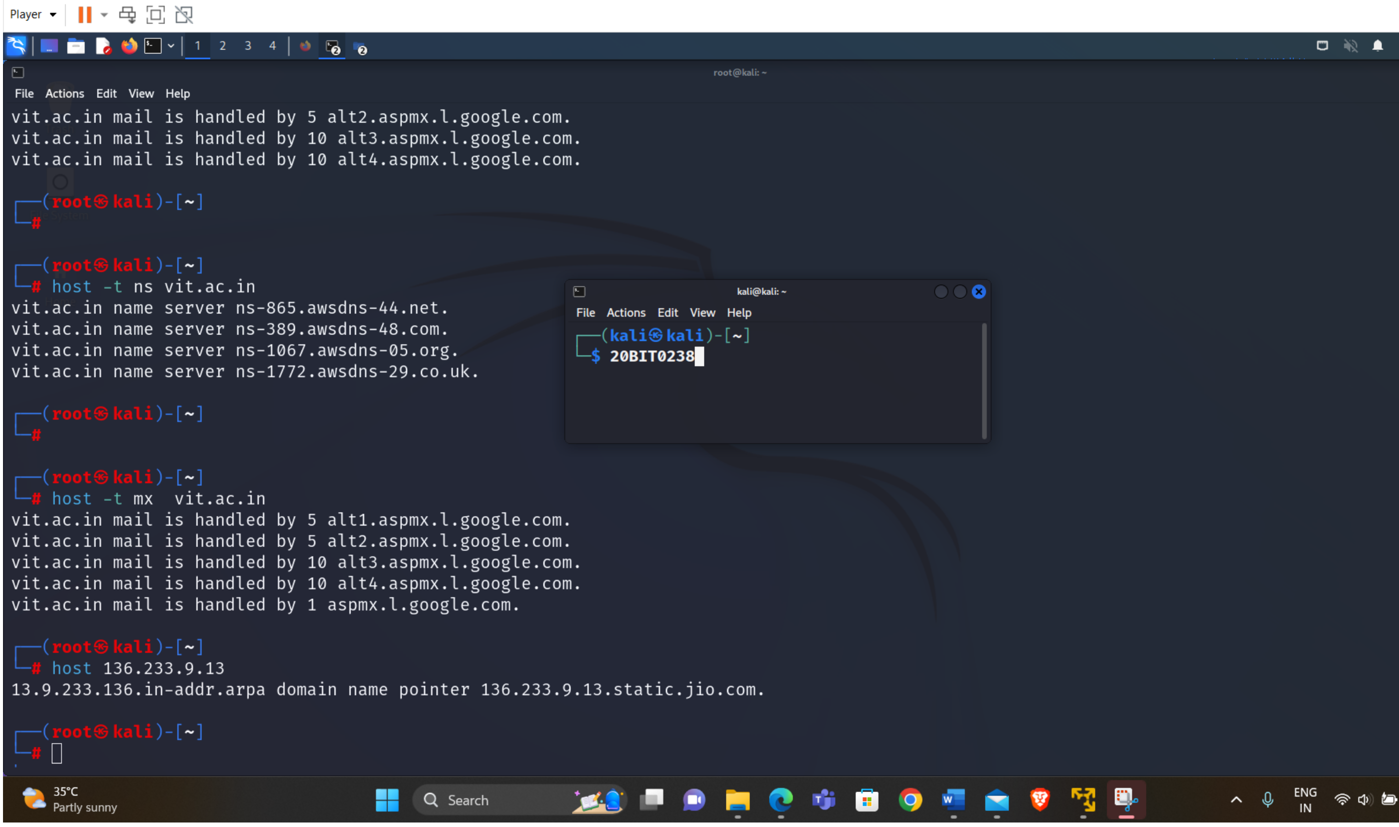
host -t mx vit.ac.in



```
┌──(root㉿kali)-[~]
└─# host vit.ac.in
vit.ac.in has address 136.233.9.13
vit.ac.in mail is handled by 1 aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt1.aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# host -t ns vit.ac.in
vit.ac.in name server ns-865.awsdns-44.net.
vit.ac.in name server ns-389.awsdns-48.com.
vit.ac.in name server ns-1067.awsdns-05.org.
vit.ac.in name server ns-1772.awsdns-29.co.uk.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# host -t mx  vit.ac.in
vit.ac.in mail is handled by 5 alt1.aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.
vit.ac.in mail is handled by 1 aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

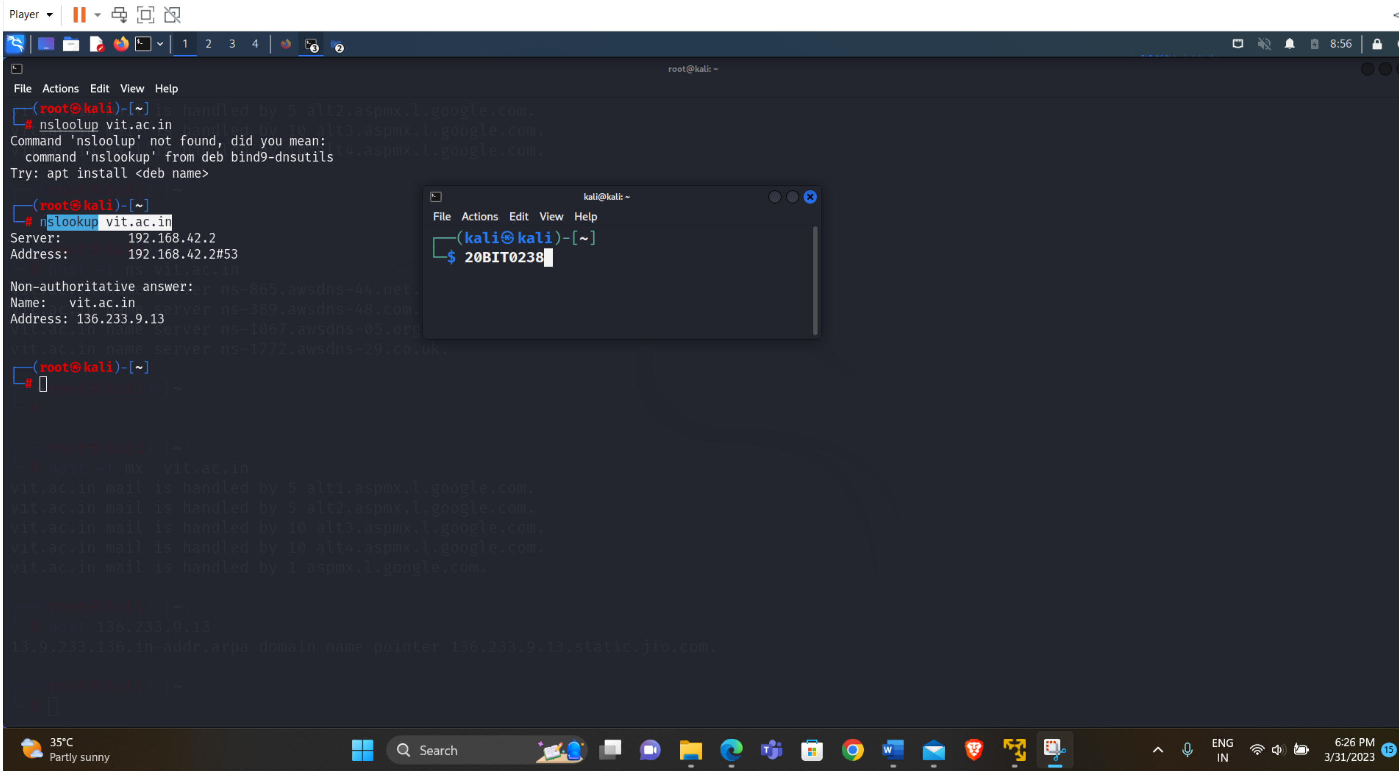
host 136.233.9.13



```
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# host -t ns vit.ac.in
vit.ac.in name server ns-865.awsdns-44.net.
vit.ac.in name server ns-389.awsdns-48.com.
vit.ac.in name server ns-1067.awsdns-05.org.
vit.ac.in name server ns-1772.awsdns-29.co.uk.

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# host -t mx  vit.ac.in
vit.ac.in mail is handled by 5 alt1.aspmx.l.google.com.
vit.ac.in mail is handled by 5 alt2.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt3.aspmx.l.google.com.
vit.ac.in mail is handled by 10 alt4.aspmx.l.google.com.
vit.ac.in mail is handled by 1 aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─# host 136.233.9.13
13.9.233.136.in-addr.arpa domain name pointer 136.233.9.13.static.jio.com.

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

nslookup vit.ac.in



```
┌──(root㉿kali)-[~]
└─# nsloolup vit.ac.in
Command 'nsloolup' not found, did you mean:
  command 'nslookup' from deb bind9-dnsutils
Try: apt install <deb name>

┌──(root㉿kali)-[~]
└─# nslookup vit.ac.in
Server:         192.168.42.2
Address:        192.168.42.2#53

Non-authoritative answer:
Name:   vit.ac.in
Address: 136.233.9.13

┌──(root㉿kali)-[~]
└─# 
```

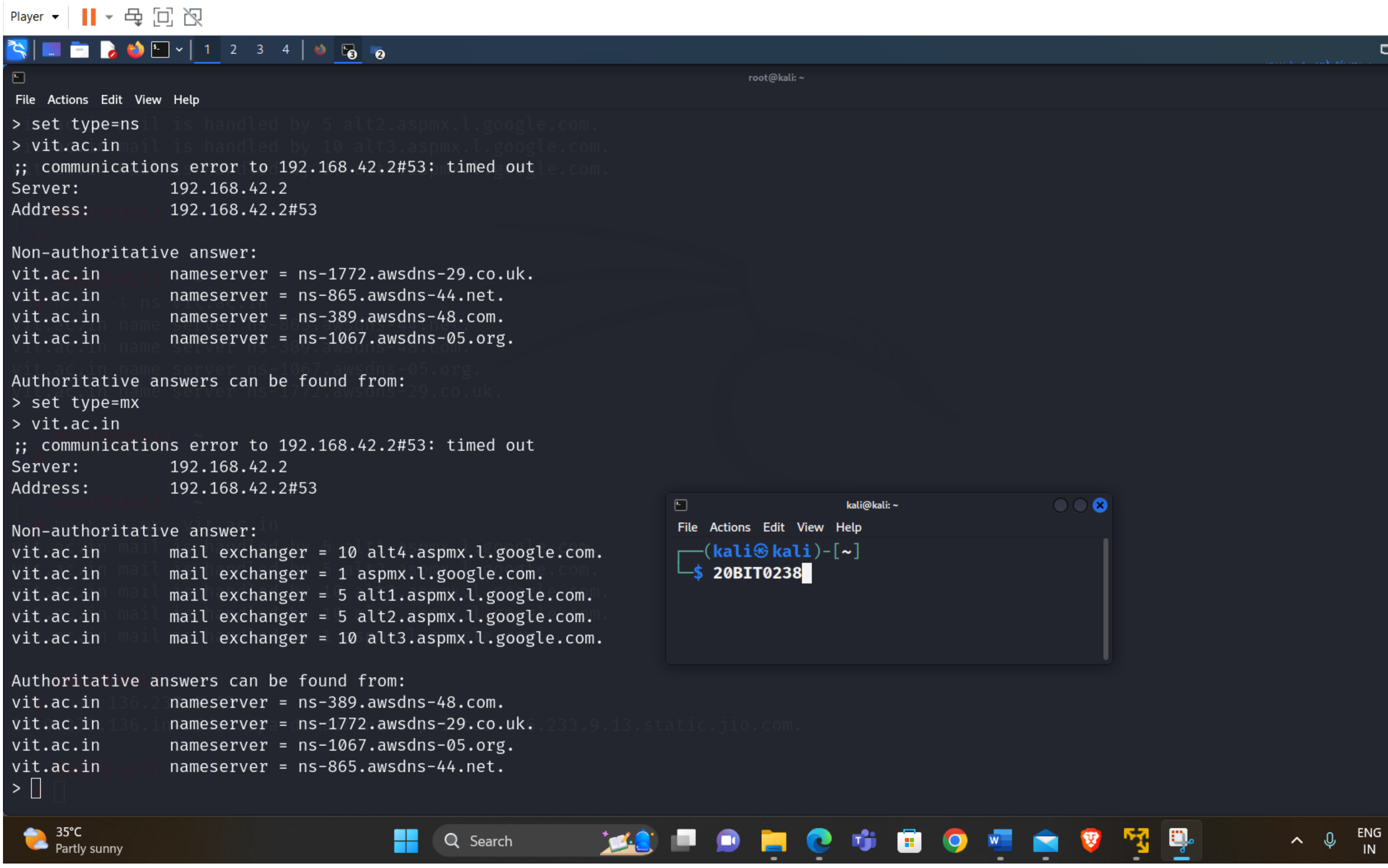
```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

set type=ns

> vit.ac.in

set type=mx

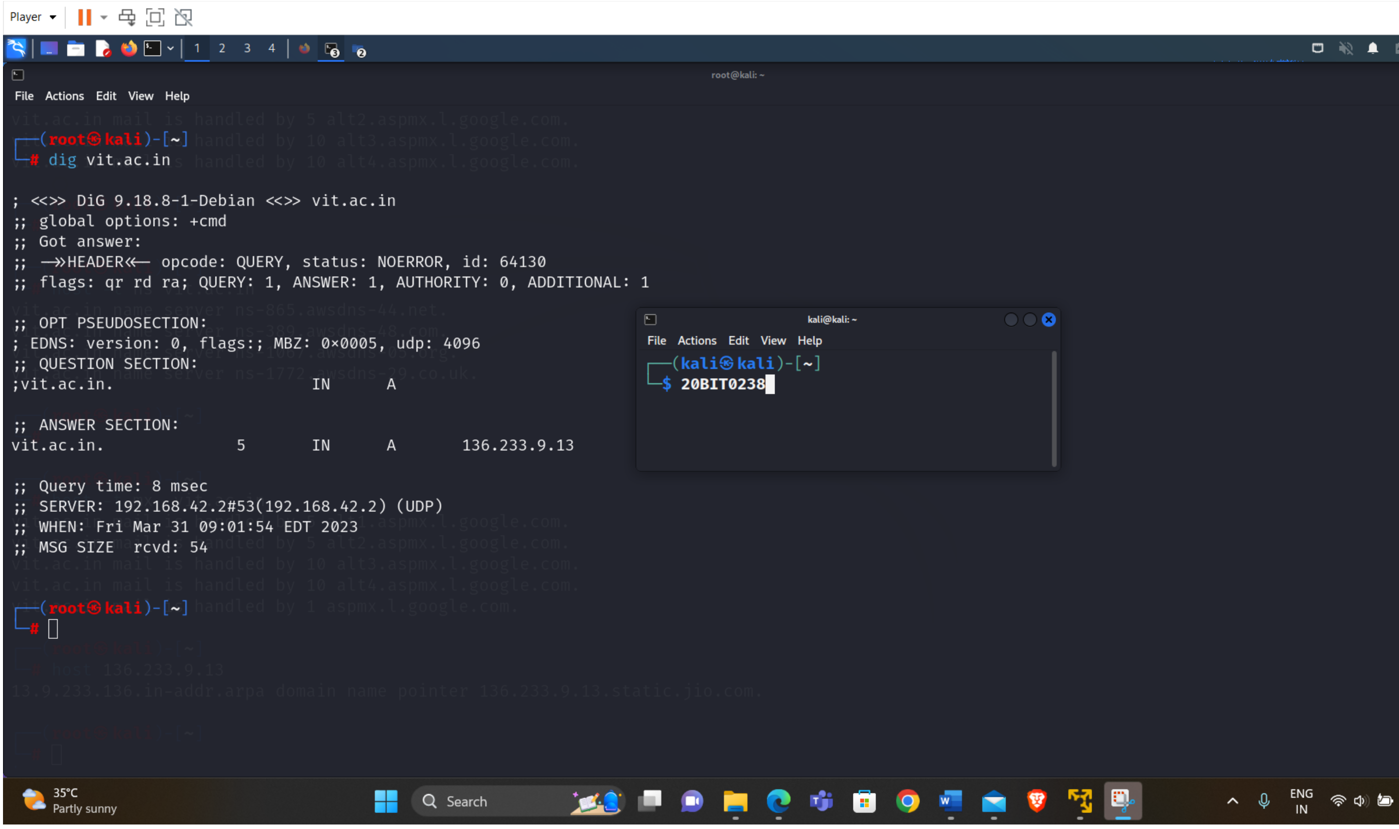
> vit.ac.in



```
> set type=ns
> vit.ac.in
;; communications error to 192.168.42.2#53: timed out
Server:         192.168.42.2
Address:        192.168.42.2#53

Non-authoritative answer:
vit.ac.in       nameserver = ns-1772.awsdns-29.co.uk.
vit.ac.in       nameserver = ns-865.awsdns-44.net.
vit.ac.in       nameserver = ns-389.awsdns-48.com.
vit.ac.in       nameserver = ns-1067.awsdns-05.org.

Authoritative answers can be found from:
> set type=mx
> vit.ac.in
;; communications error to 192.168.42.2#53: timed out
Server:         192.168.42.2
Address:        192.168.42.2#53

Non-authoritative answer:
vit.ac.in       mail exchanger = 10 alt4.aspmx.l.google.com.
vit.ac.in       mail exchanger = 1 aspmx.l.google.com.
vit.ac.in       mail exchanger = 5 alt1.aspmx.l.google.com.
vit.ac.in       mail exchanger = 5 alt2.aspmx.l.google.com.
vit.ac.in       mail exchanger = 10 alt3.aspmx.l.google.com.

Authoritative answers can be found from:
vit.ac.in       nameserver = ns-389.awsdns-48.com.
vit.ac.in       nameserver = ns-1772.awsdns-29.co.uk.
vit.ac.in       nameserver = ns-1067.awsdns-05.org.
vit.ac.in       nameserver = ns-865.awsdns-44.net.
> 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

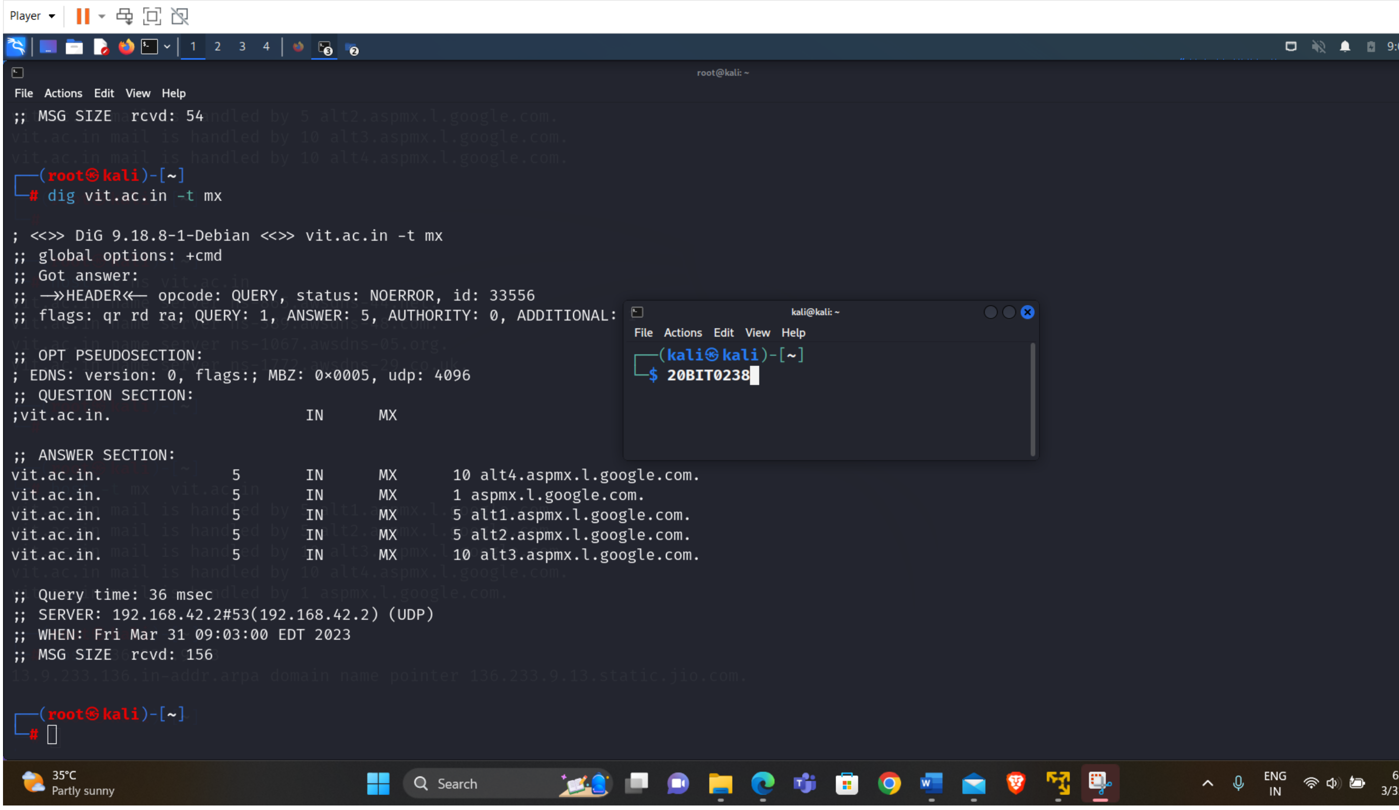
dig vit.ac.in



```
┌──(root㉿kali)-[~]
└─# dig vit.ac.in

; <<>> DiG 9.18.8-1-Debian <<>> vit.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64130
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;vit.ac.in.                     IN      A

;; ANSWER SECTION:
vit.ac.in.              5       IN      A       136.233.9.13

;; Query time: 8 msec
;; SERVER: 192.168.42.2#53(192.168.42.2) (UDP)
;; WHEN: Fri Mar 31 09:01:54 EDT 2023
;; MSG SIZE  rcvd: 54

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

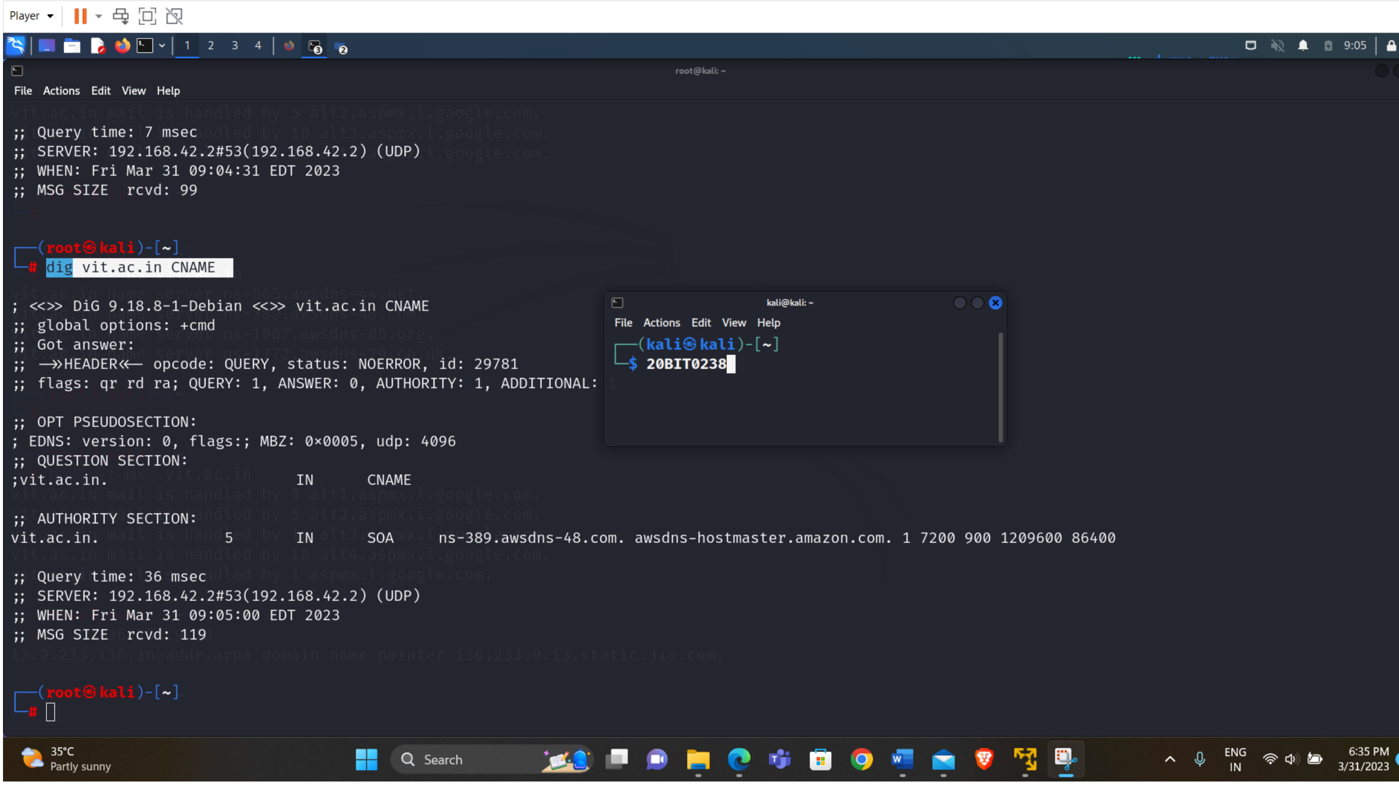
dig vit.ac.in -t mx



```
;; MSG SIZE  rcvd: 54

┌──(root㉿kali)-[~]
└─# dig vit.ac.in -t mx

; <<>> DiG 9.18.8-1-Debian <<>> vit.ac.in -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33556
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;vit.ac.in.                     IN      MX

;; ANSWER SECTION:
vit.ac.in.              5       IN      MX      10 alt4.aspmx.l.google.com.
vit.ac.in.              5       IN      MX      1 aspmx.l.google.com.
vit.ac.in.              5       IN      MX      5 alt1.aspmx.l.google.com.
vit.ac.in.              5       IN      MX      5 alt2.aspmx.l.google.com.
vit.ac.in.              5       IN      MX      10 alt3.aspmx.l.google.com.

;; Query time: 36 msec
;; SERVER: 192.168.42.2#53(192.168.42.2) (UDP)
;; WHEN: Fri Mar 31 09:03:00 EDT 2023
;; MSG SIZE  rcvd: 156

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

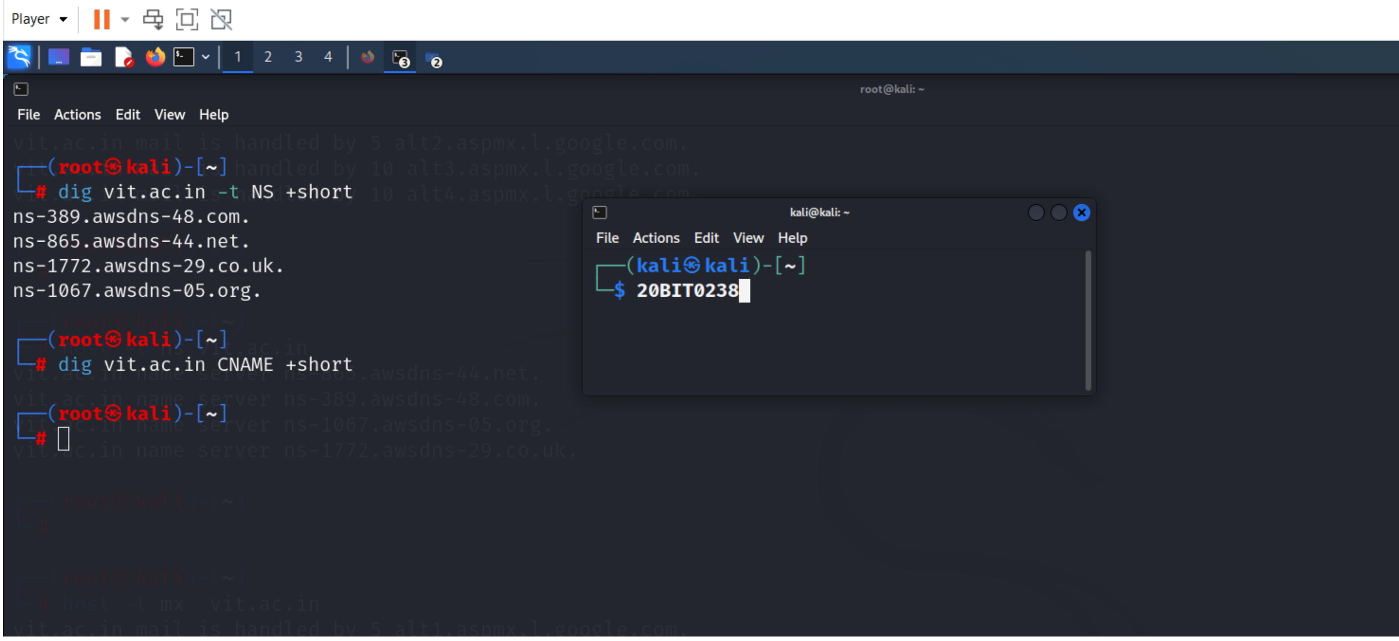
dig vit.ac.in CNAME



```
;; Query time: 7 msec
;; SERVER: 192.168.42.2#53(192.168.42.2) (UDP)
;; WHEN: Fri Mar 31 09:04:31 EDT 2023
;; MSG SIZE  rcvd: 99

┌──(root㉿kali)-[~]
└─# dig vit.ac.in CNAME

; <<>> DiG 9.18.8-1-Debian <<>> vit.ac.in CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29781
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;vit.ac.in.                     IN      CNAME

;; AUTHORITY SECTION:
vit.ac.in.              5       IN      SOA     ns-389.awsdns-48.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

;; Query time: 36 msec
;; SERVER: 192.168.42.2#53(192.168.42.2) (UDP)
;; WHEN: Fri Mar 31 09:05:00 EDT 2023
;; MSG SIZE  rcvd: 119

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

dig vit.ac.in -t NS +short

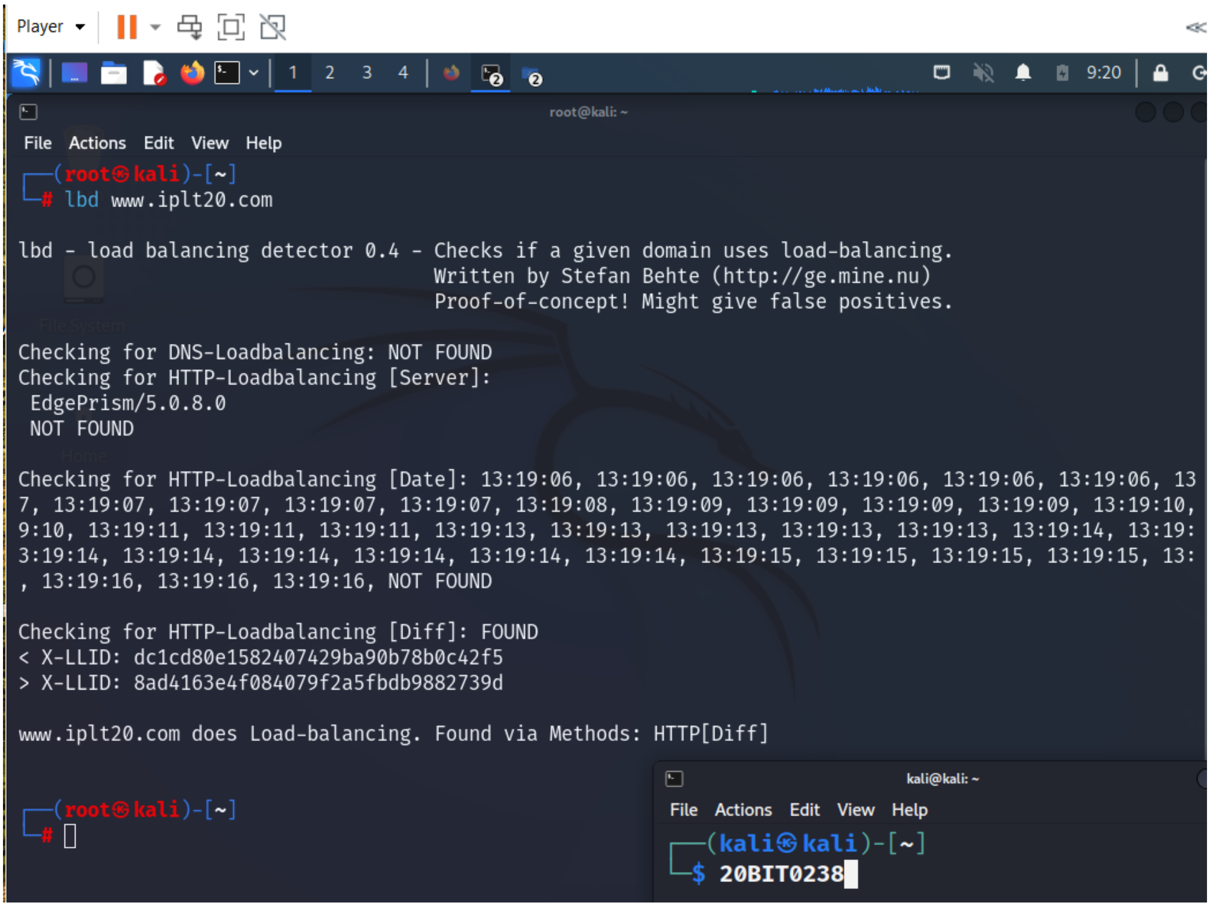


```
┌──(root㉿kali)-[~]
└─# dig vit.ac.in -t NS +short
ns-389.awsdns-48.com.
ns-865.awsdns-44.net.
ns-1772.awsdns-29.co.uk.
ns-1067.awsdns-05.org.

┌──(root㉿kali)-[~]
└─# dig vit.ac.in CNAME +short

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

2. Perform a load balancing scan by referring the video link given below on any website other than the given in the video which is also not a popular website.

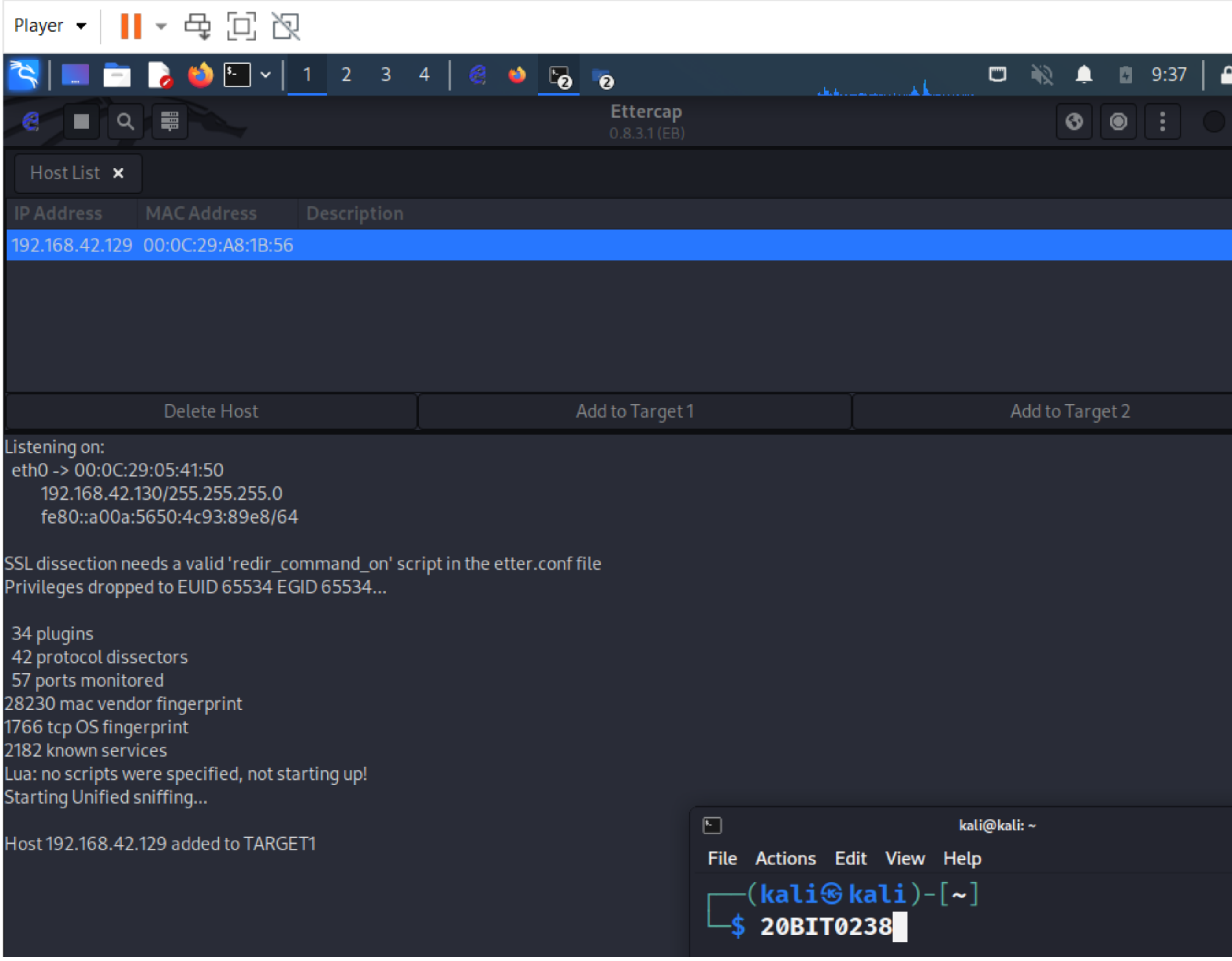
lbd www.iplt20.com



```
┌──(root㉿kali)-[~]
└─# lbd www.iplt20.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 EdgePrism/5.0.8.0
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 13:19:06, 13:19:06, 13:19:06, 13:19:06, 13:19:06, 13:19:06, 13
7, 13:19:07, 13:19:07, 13:19:07, 13:19:07, 13:19:08, 13:19:09, 13:19:09, 13:19:09, 13:19:09, 13:19:10,
9:10, 13:19:11, 13:19:11, 13:19:11, 13:19:13, 13:19:13, 13:19:13, 13:19:13, 13:19:13, 13:19:14, 13:19:
3:19:14, 13:19:14, 13:19:14, 13:19:14, 13:19:14, 13:19:14, 13:19:15, 13:19:15, 13:19:15, 13:19:15, 13:
, 13:19:16, 13:19:16, 13:19:16, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< X-LLID: dc1cd80e1582407429ba90b78b0c42f5
> X-LLID: 8ad4163e4f084079f2a5fbdb9882739d

www.iplt20.com does Load-balancing. Found via Methods: HTTP[Diff]

┌──(root㉿kali)-[~]
└─# 
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

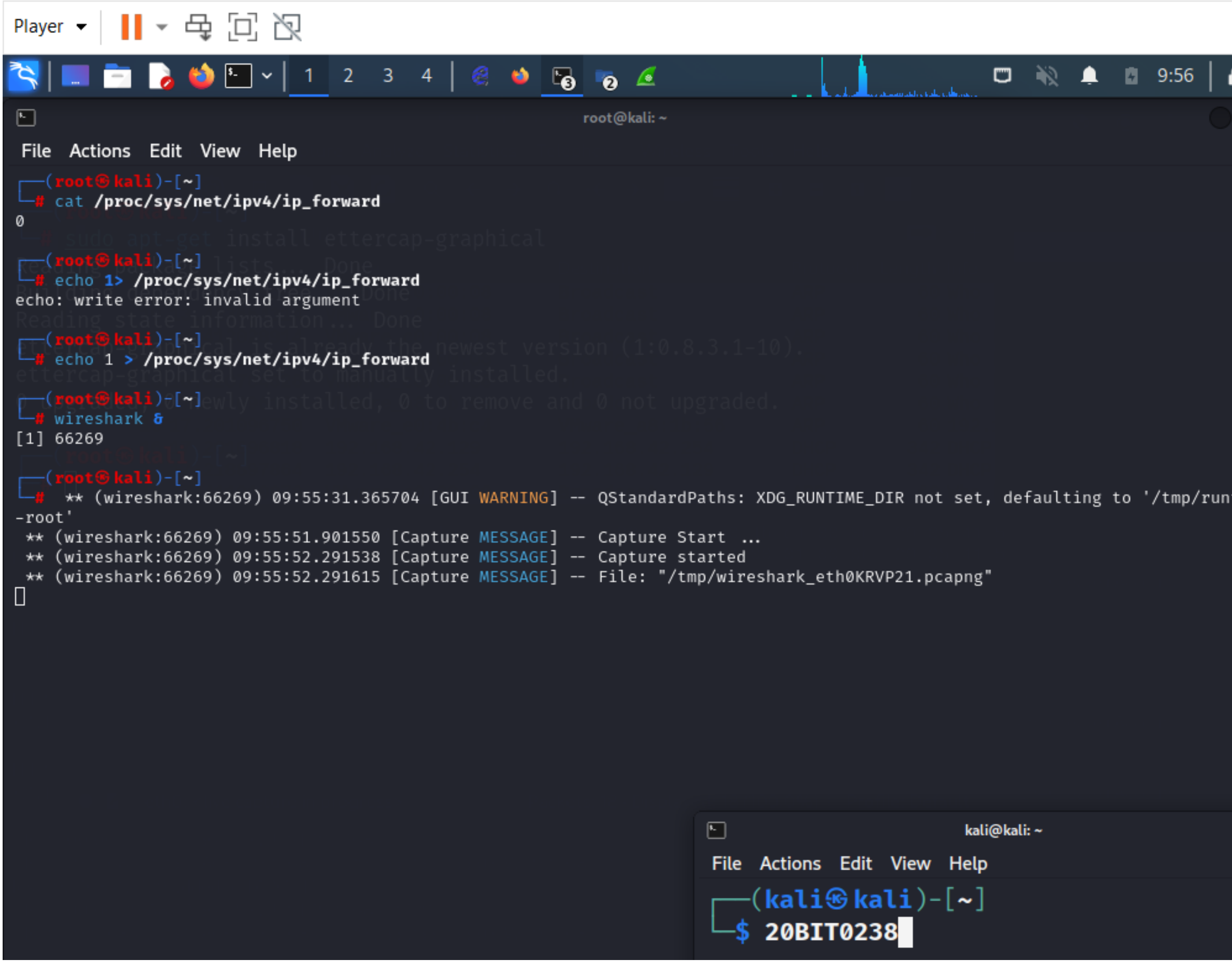
3. Perform an ARP poisoning using ettercap GUI in Kali targeting the mutilidae website of your Metasploitable VM to obtain username (Registration Number) and passwords (First Name) in the ettercap window pane. Provide all intermediate snapshots of setting up target ip etc and the final capturing of username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



```
192.168.42.129  00:0C:29:A8:1B:56
```

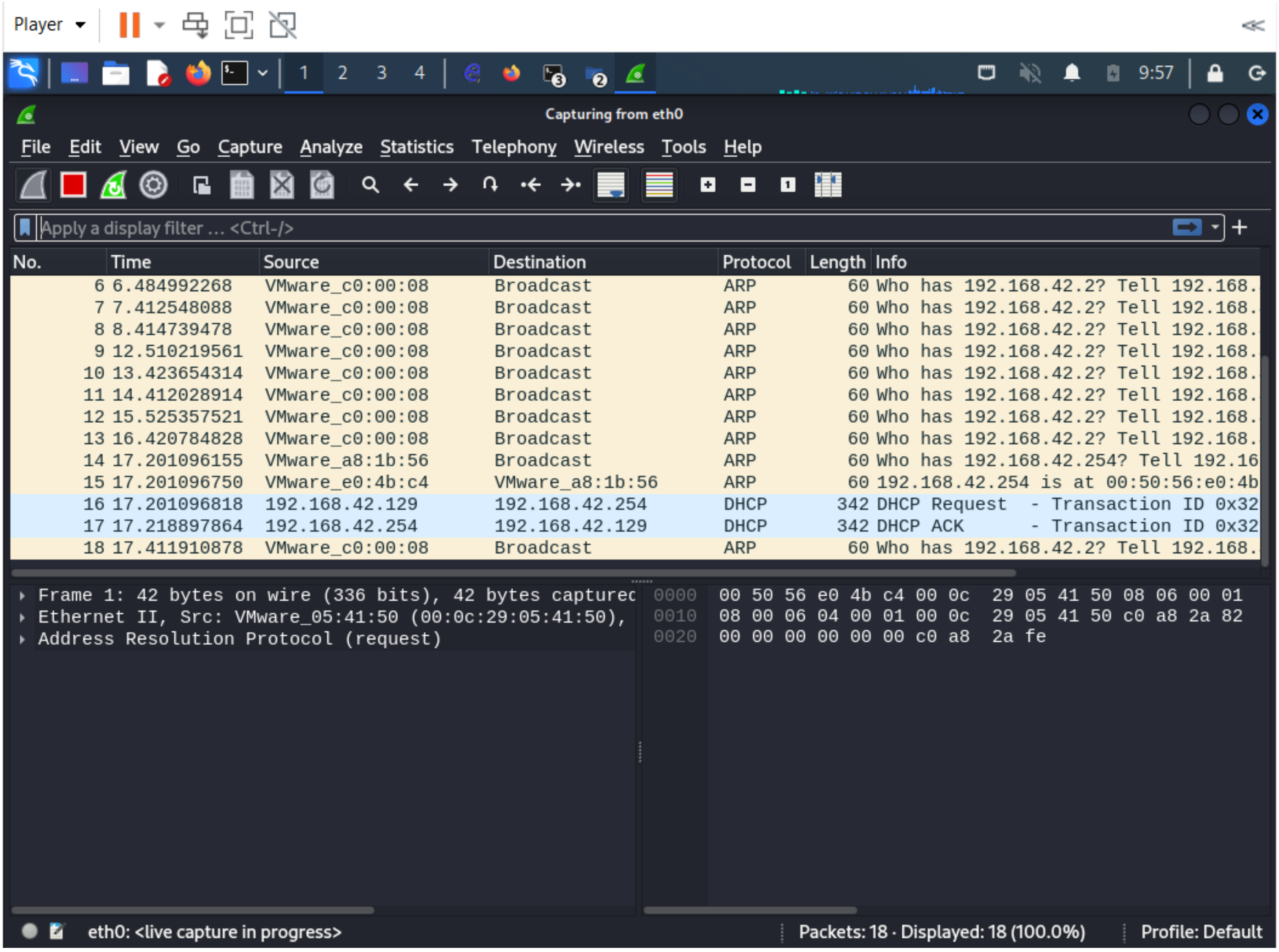
```
Listening on:
 eth0 -> 00:0C:29:05:41:50
      192.168.42.130/255.255.255.0
      fe80::a00a:5650:4c93:89e8/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.42.129 added to TARGET1
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



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

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

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

┌──(root㉿kali)-[~]
└─# wireshark &
[1] 66269

┌──(root㉿kali)-[~]
└─#  ** (wireshark:66269) 09:55:31.365704 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/run
-root'
 ** (wireshark:66269) 09:55:51.901550 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:66269) 09:55:52.291538 [Capture MESSAGE] -- Capture started
 ** (wireshark:66269) 09:55:52.291615 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0KRVP21.pcapng"
```

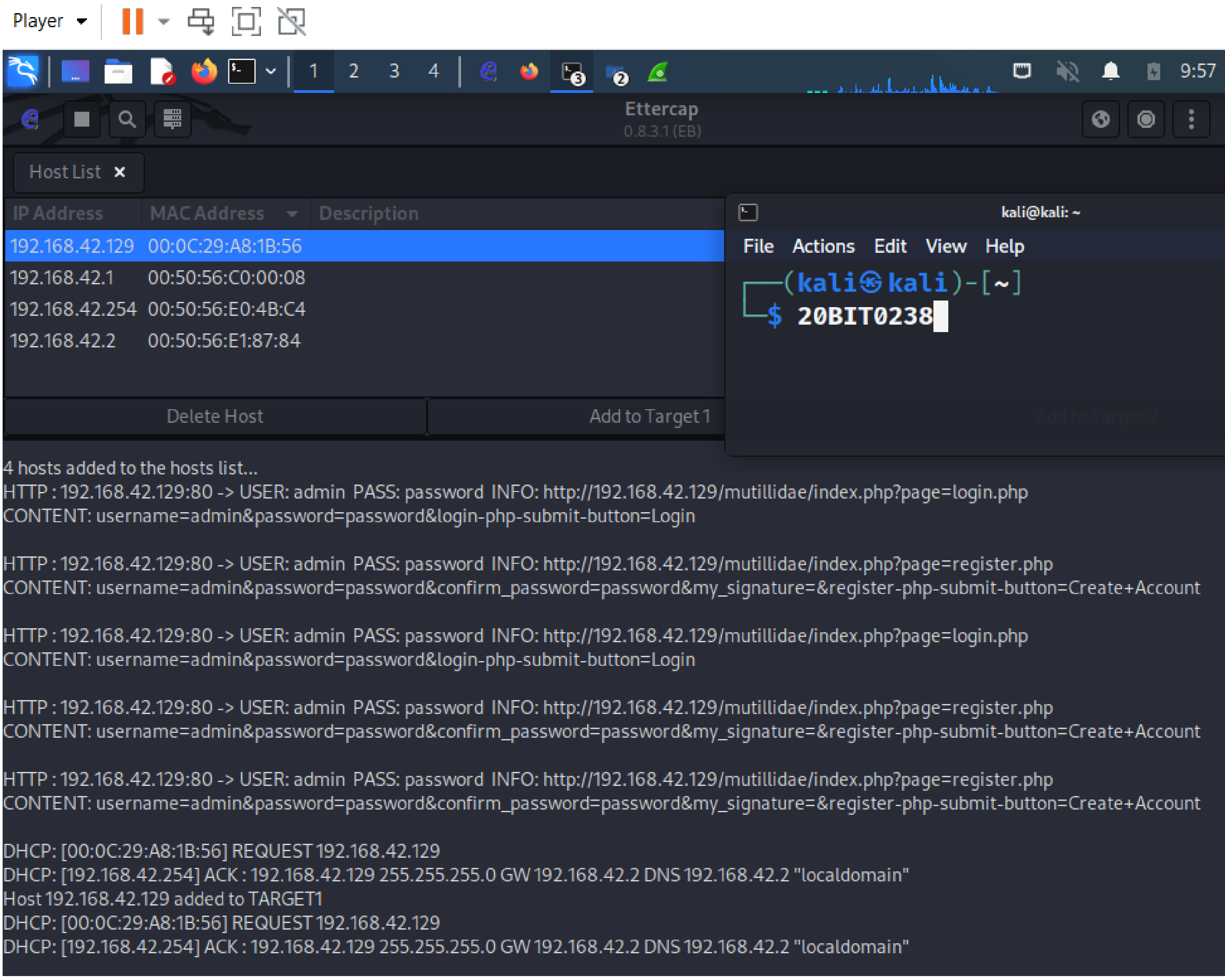
```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



```
No.   Time          Source              Destination         Protocol Length Info
    6 6.484992268   VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
    7 7.412548088   VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
    8 8.414739478   VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
    9 12.510219561  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
   10 13.423654314  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
   11 14.412028914  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
   12 15.525357521  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
   13 16.420784828  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
   14 17.201096155  VMware_a8:1b:56     Broadcast           ARP        60 Who has 192.168.42.254? Tell 192.16
   15 17.201096750  VMware_e0:4b:c4     VMware_a8:1b:56     ARP        60 192.168.42.254 is at 00:50:56:e0:4b
   16 17.201096818  192.168.42.129      192.168.42.254      DHCP      342 DHCP Request  - Transaction ID 0x32
   17 17.218897864  192.168.42.254      192.168.42.129      DHCP      342 DHCP ACK      - Transaction ID 0x32
   18 17.411910878  VMware_c0:00:08     Broadcast           ARP        60 Who has 192.168.42.2? Tell 192.168.
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes capturec
› Ethernet II, Src: VMware_05:41:50 (00:0c:29:05:41:50),
› Address Resolution Protocol (request)
```

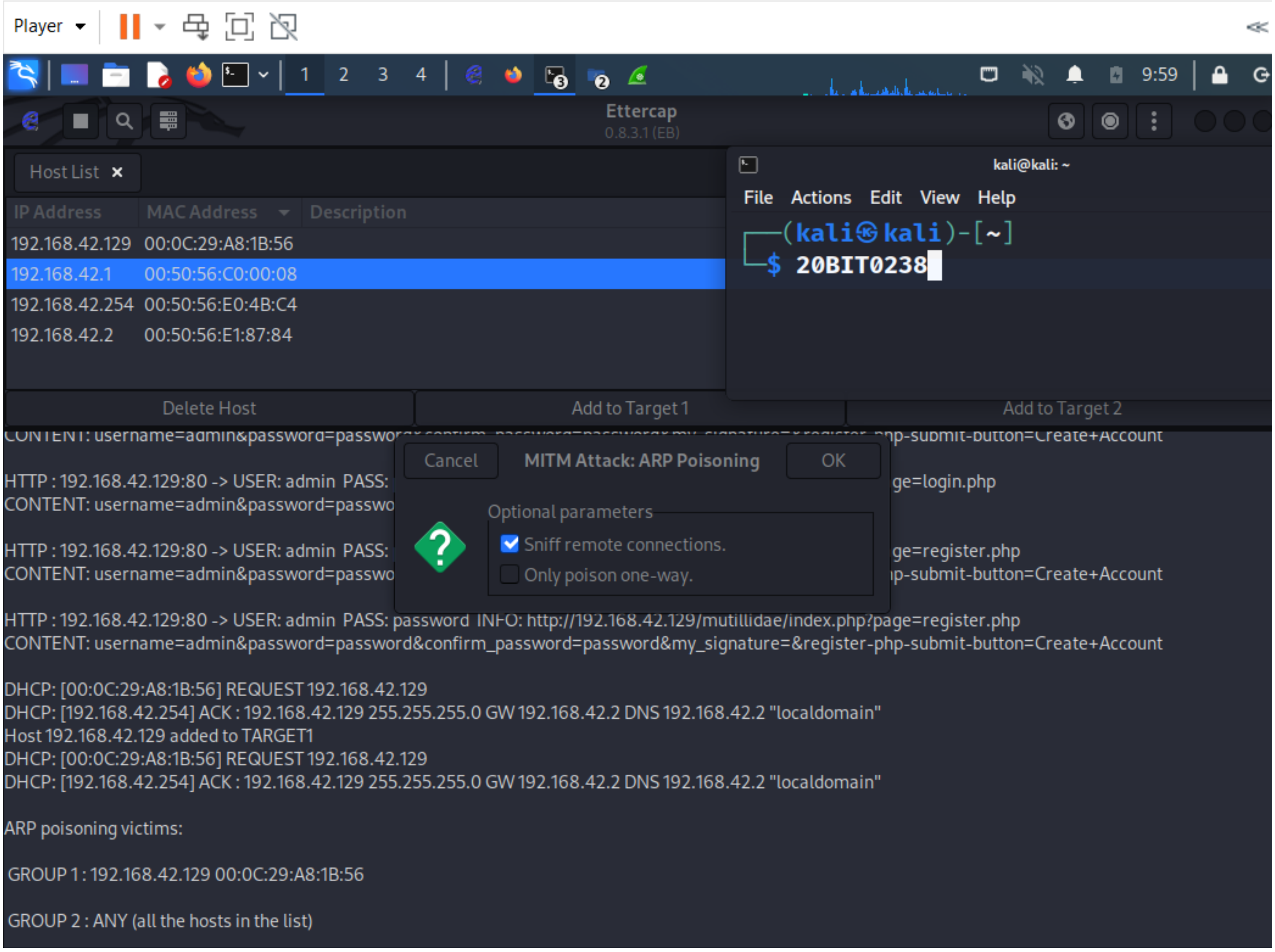
```
0000  00 50 56 e0 4b c4 00 0c  29 05 41 50 08 06 00 01
0010  08 00 06 04 00 01 00 0c  29 05 41 50 c0 a8 2a 82
0020  00 00 00 00 00 00 c0 a8  2a fe
```



IP Address	MAC Address	Description
192.168.42.129	00:0C:29:A8:1B:56	
192.168.42.1	00:50:56:C0:00:08	
192.168.42.254	00:50:56:E0:4B:C4	
192.168.42.2	00:50:56:E1:87:84	

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

```
4 hosts added to the hosts list...
HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=login.php
CONTENT: username=admin&password=password&login-php-submit-button=Login

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=login.php
CONTENT: username=admin&password=password&login-php-submit-button=Login

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

DHCP: [00:0C:29:A8:1B:56] REQUEST 192.168.42.129
DHCP: [192.168.42.254] ACK : 192.168.42.129 255.255.255.0 GW 192.168.42.2 DNS 192.168.42.2 "localdomain"
Host 192.168.42.129 added to TARGET1
DHCP: [00:0C:29:A8:1B:56] REQUEST 192.168.42.129
DHCP: [192.168.42.254] ACK : 192.168.42.129 255.255.255.0 GW 192.168.42.2 DNS 192.168.42.2 "localdomain"
```



IP Address	MAC Address	Description
192.168.42.129	00:0C:29:A8:1B:56	
192.168.42.1	00:50:56:C0:00:08	
192.168.42.254	00:50:56:E0:4B:C4	
192.168.42.2	00:50:56:E1:87:84	

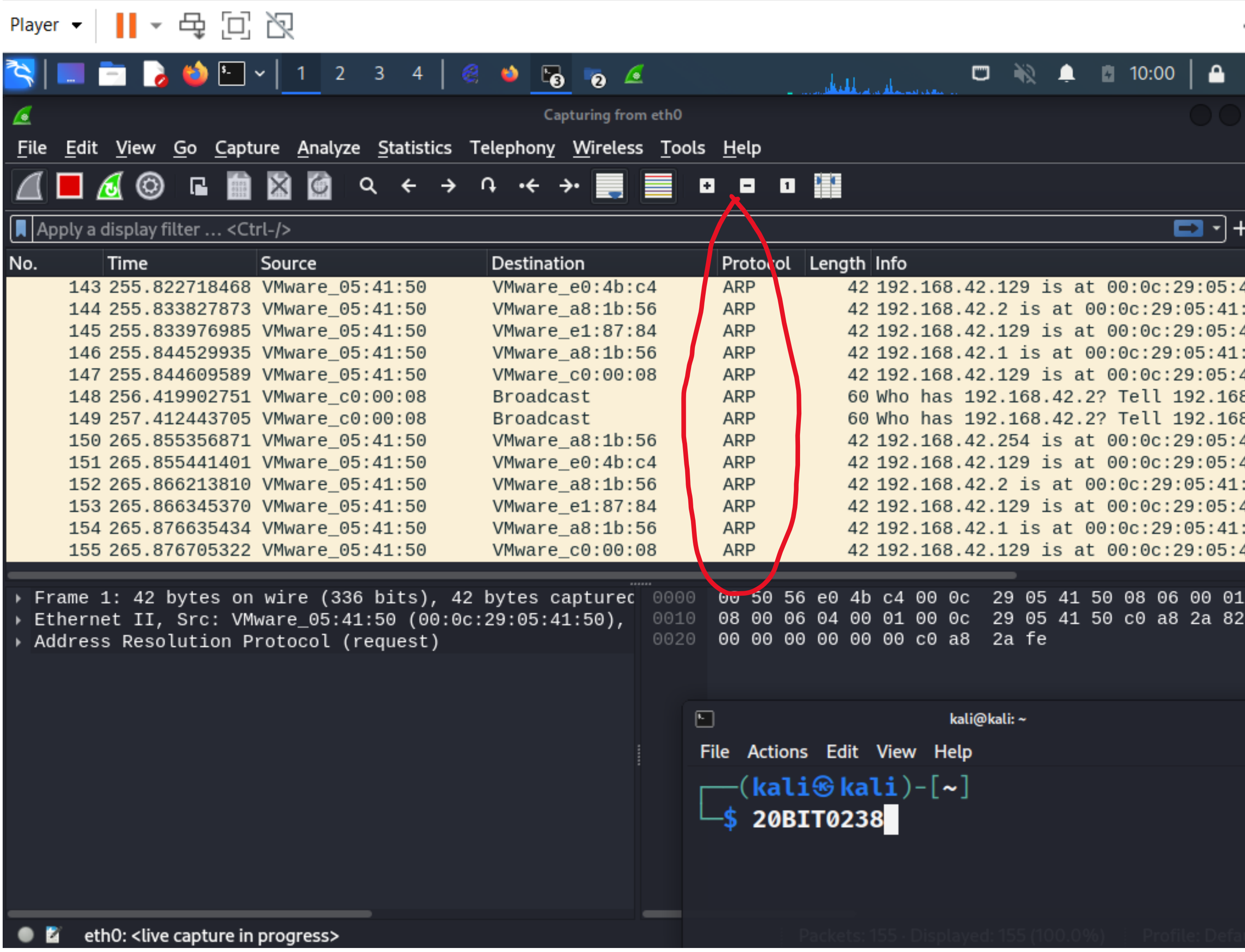
```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

```
CONTENT: username=admin&password=passwo                                                          php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS:                                                   ge=login.php
CONTENT: username=admin&password=passwo

HTTP : 192.168.42.129:80 -> USER: admin  PASS:                                                   ge=register.php
CONTENT: username=admin&password=passwo                                                          p-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

DHCP: [00:0C:29:A8:1B:56] REQUEST 192.168.42.129
DHCP: [192.168.42.254] ACK : 192.168.42.129 255.255.255.0 GW 192.168.42.2 DNS 192.168.42.2 "localdomain"
Host 192.168.42.129 added to TARGET1
DHCP: [00:0C:29:A8:1B:56] REQUEST 192.168.42.129
DHCP: [192.168.42.254] ACK : 192.168.42.129 255.255.255.0 GW 192.168.42.2 DNS 192.168.42.2 "localdomain"

ARP poisoning victims:

 GROUP 1 : 192.168.42.129 00:0C:29:A8:1B:56

 GROUP 2 : ANY (all the hosts in the list)
```

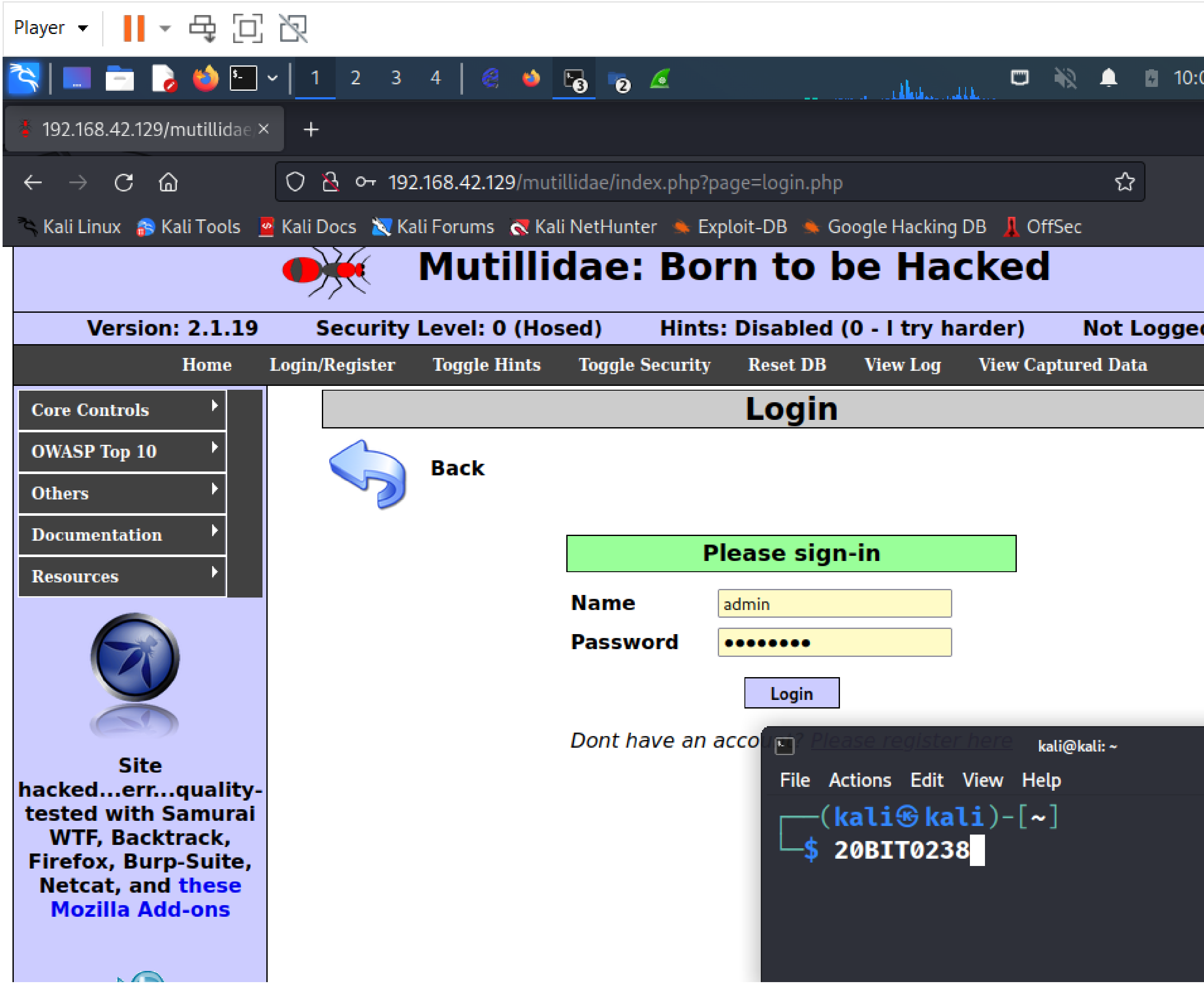

Player
1
2
3
4
10:00
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source              Destination         Protocol  Length Info
  143 255.822718468 VMware_05:41:50     VMware_e0:4b:c4     ARP         42 192.168.42.129 is at 00:0c:29:05:4
  144 255.833827873 VMware_05:41:50     VMware_a8:1b:56     ARP         42 192.168.42.2 is at 00:0c:29:05:41:
  145 255.833976985 VMware_05:41:50     VMware_e1:87:84     ARP         42 192.168.42.129 is at 00:0c:29:05:4
  146 255.844529935 VMware_05:41:50     VMware_a8:1b:56     ARP         42 192.168.42.1 is at 00:0c:29:05:41:
  147 255.844609589 VMware_05:41:50     VMware_c0:00:08     ARP         42 192.168.42.129 is at 00:0c:29:05:4
  148 256.419902751 VMware_c0:00:08     Broadcast           ARP         60 Who has 192.168.42.2? Tell 192.168
  149 257.412443705 VMware_c0:00:08     Broadcast           ARP         60 Who has 192.168.42.2? Tell 192.168
  150 265.855356871 VMware_05:41:50     VMware_a8:1b:56     ARP         42 192.168.42.254 is at 00:0c:29:05:4
  151 265.855441401 VMware_05:41:50     VMware_e0:4b:c4     ARP         42 192.168.42.129 is at 00:0c:29:05:4
  152 265.866213810 VMware_05:41:50     VMware_a8:1b:56     ARP         42 192.168.42.2 is at 00:0c:29:05:41:
  153 265.866345370 VMware_05:41:50     VMware_e1:87:84     ARP         42 192.168.42.129 is at 00:0c:29:05:4
  154 265.876635434 VMware_05:41:50     VMware_a8:1b:56     ARP         42 192.168.42.1 is at 00:0c:29:05:41:
  155 265.876705322 VMware_05:41:50     VMware_c0:00:08     ARP         42 192.168.42.129 is at 00:0c:29:05:4
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes capturec   0000  00 50 56 e0 4b c4 00 0c  29 05 41 50 08 06 00 01
› Ethernet II, Src: VMware_05:41:50 (00:0c:29:05:41:50),   0010  08 00 06 04 00 01 00 0c  29 05 41 50 c0 a8 2a 82
› Address Resolution Protocol (request)                     0020  00 00 00 00 00 00 c0 a8  2a fe
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

eth0: <live capture in progress>
Packets: 155 · Displayed: 155 (100.0%)
Profile: Defa



Mutillidae: Born to be Hacked

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

Login

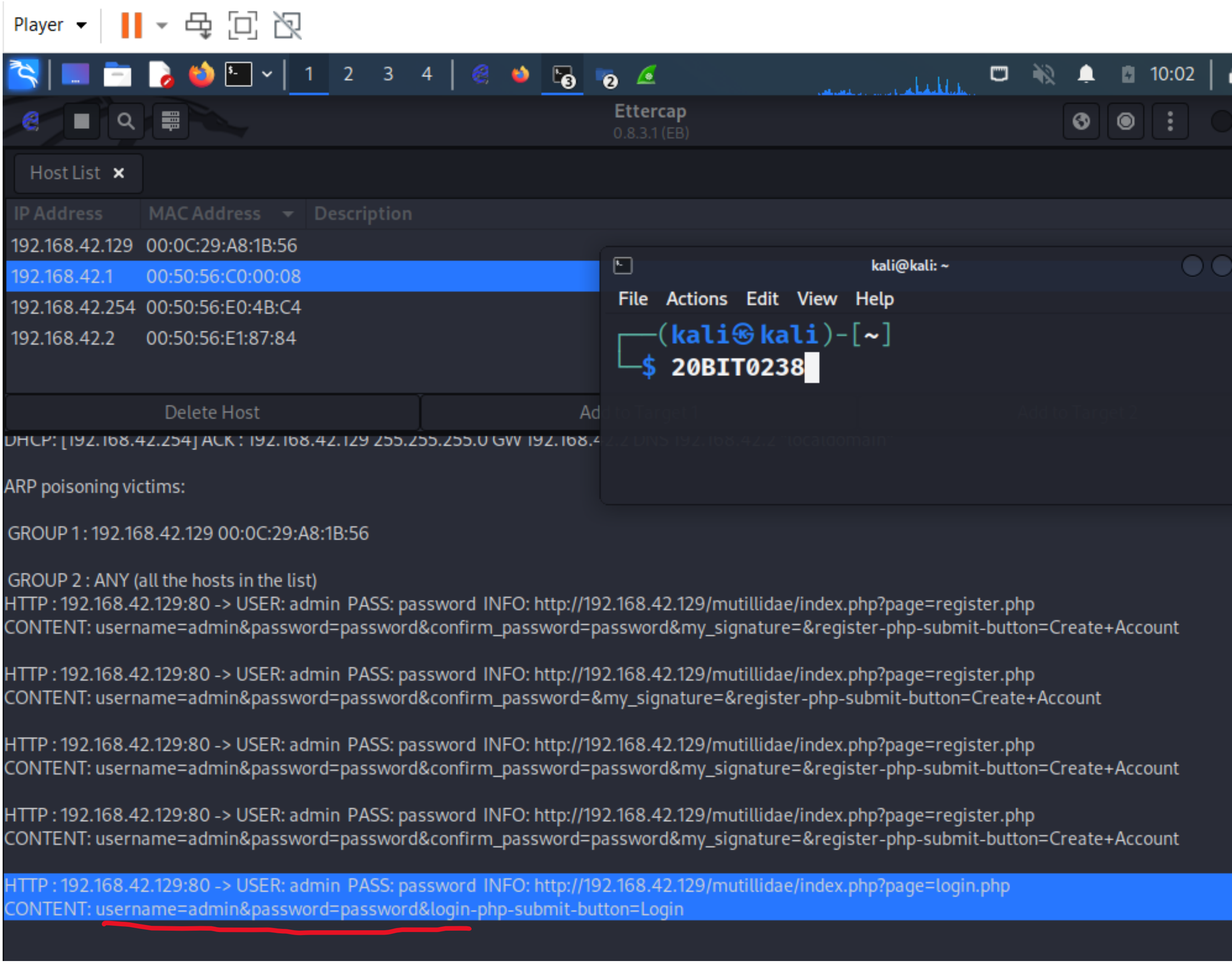
Please sign-in

Name	admin
Password	••••••••

Dont have an acco Please register here

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

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



IP Address	MAC Address	Description
192.168.42.129	00:0C:29:A8:1B:56	
192.168.42.1	00:50:56:C0:00:08	
192.168.42.254	00:50:56:E0:4B:C4	
192.168.42.2	00:50:56:E1:87:84	

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

```
DHCP: [192.168.42.254] ACK : 192.168.42.129 255.255.255.0 GW 192.168.42.2 DNS 192.168.42.2 "localdomain"

ARP poisoning victims:

 GROUP 1 : 192.168.42.129 00:0C:29:A8:1B:56

 GROUP 2 : ANY (all the hosts in the list)
HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=register.php
CONTENT: username=admin&password=password&confirm_password=password&my_signature=&register-php-submit-button=Create+Account

HTTP : 192.168.42.129:80 -> USER: admin  PASS: password  INFO: http://192.168.42.129/mutillidae/index.php?page=login.php
CONTENT: username=admin&password=password&login-php-submit-button=Login
```