Kalle Jalkanen
AB8822

With nmap i found that 192.168.1.100 has ports 22, 80, 139, 445 and 9200 open.

```
└─$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.858 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=2.15 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=1.84 ms
^C
── 192.168.1.100 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 0.858/1.613/2.145/0.548 ms
```

```
└─$ sudo nmap 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-27 09:54 EEST
Nmap scan report for 192.168.1.1
Host is up (0.00099s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:88:CC:DC (VMware)

Nmap scan report for 192.168.1.100
Host is up (0.0018s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
9200/tcp open  wap-wsp
MAC Address: 00:50:56:88:F4:EE (VMware)
```

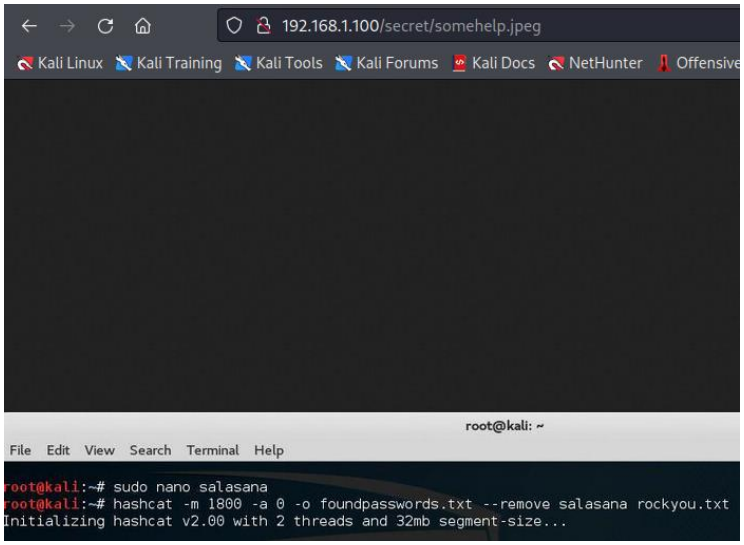
With dirbuster I found these folders from port 80

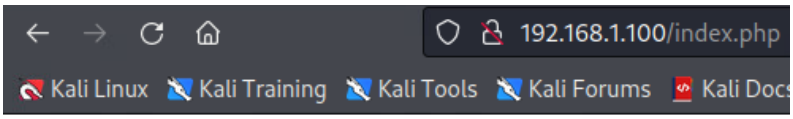
http://192.168.1.100:80/

Scan Information | Results - List View: Dirs: 3 Files: 1 | Results - Tree View | Errors: 0

Type	Found	Response	Size
Dir	/	200	11947
File	/index.php	200	196
Dir	/icons/	403	466
Dir	/icons/small/	403	472
Dir	/secret/	200	1135

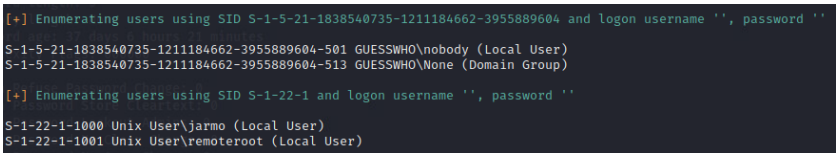
I found 2 readable things one was picture and one remainder text.



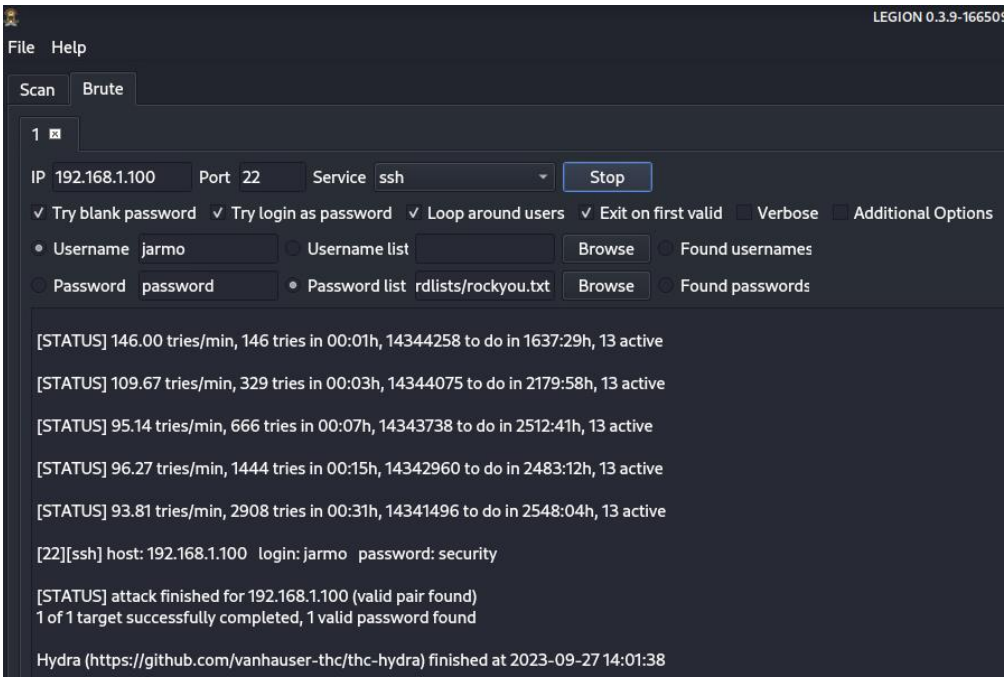


Remember this file, you want to check it later

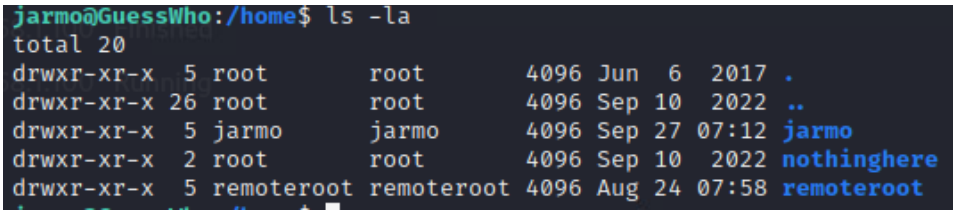
Googling ports 139 and 445 I found command ‘enum4linux 192.168.1.100’ and it gave me usernames ‘jarmo’ and ‘remoteroot’.

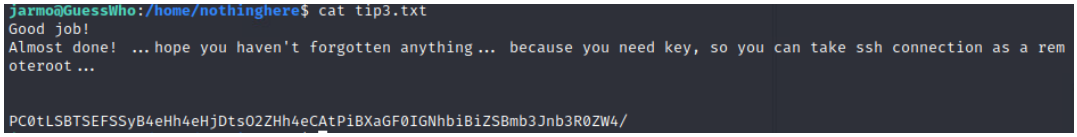


I used legion to brute force ssh password with user ‘jarmo’. Password found was ‘security’.



I connected with ssh and from /home/nothinghere I found tip3.





Bottom line text was base64 encoded and decrypting it.

<--- SHARK xxxxxxöödxxx -> What can be forgotten

In root folder was tip2. It looks like a script.

```
jarmo@GuessWho:/$ cat tip2.txt
#!/bin/bash

TEST=`/sbin/ifconfig eth0 | grep 'inet addr:' | cut -d: -f3 | awk '{ print $1}'`
echo "R29vZCBqb2IgZmluZGluZyB0aGlzISBIb3BlIHlvdSBkaWQgZ2V0IHRpcDEsIGJlY2F1c2UgdGhhdCBpbWFnZSB3aWxsIGhlbHAgeW91LCBtYX
liZSBldmVuIG1vcmUgdGhhbiB3aGF0IHlvdXIgZXllcyBjYW4gc2VlIG9uIHRoYXQuIEJ1dCBhbnl3YXlzLCBpZiB5b3UgaGF2ZW50IHlldCBmb3VuZC
B3YXkgaW4sIHRoZW4gbWF5YmUgaXQgaXMgdGltZSB0byByBjaGVjayBwb3J0IDkyMDAsIHRoZXJlIGlzIGtub3cgdnVsbmVyYWJpbGl0eSBvbiBzZXJ2aW
NlIHdoaWNoIGlzIG9uIHRoYXQgcG9ydC4gWW91IGNhbiB1c2UgaXQgdG8gZmluZCBzb21lIGhhc2hlcwoKPC0tLSBQaWN0dXJlIHh4eDcxanh4eHh4eC
AtPiBUaGVyZSBpcyBzb21ldGhpbmcgdGhlcmUh" | ncat -u $TEST 12345
```

Again, there was base64 encrypted text. Decoded text is…

```
Good job finding this! Hope you did get tip1, because that image will help you, maybe even more than what your eyes can see on that. But anyways, if you havent yet f
ound way in, then maybe it is time to check port 9200, there is know vulnerability on service which is on that port. You can use it to find some hashes

<--- Picture xxx71jxxxxxx -> There is something there!
```

I looked picture again with command ‘strings somehelp.jpg’ and it includes tip1.txt.

```
ob*U
tip1.txtUT
Jp9p
"aLR$
cU&JH
VH>vv
ob*U
tip1.txtUT
```

I unzipped file and it gave me tip1.txt

```
┌──(kali㉿kali-vle)-[~/jarmos]
└─$ unzip somehelp.jpeg
Archive:  somehelp.jpeg
warning [somehelp.jpeg]:  21432 extra bytes at beginning or within zipfile
  (attempting to process anyway)
  inflating: tip1.txt
```

And again, there was base64 text.

```
└─$ cat tip1.txt
R29vZCBqb2IgZmluZGluZyB0aGlzISBUaGlzIHBpY3R1cmUgd2lsbCBoZWxwIHlvdSBsYXRlciBvbiwgd2hlbiB5b3UgaG9wZWZ1bGx5IGZpbmQgZmlsZShz
KSB3aGVyZSBpcyBoYXNoZWQgcGFzc3dvcmRzLiBTbyB0aGF0J3Mgd2hhdCB5b3UgbmVlZCB0byBmaW5kLiBiNYXliZSB5b3Uga25vdyB3aGVyZSB0byBsb29r
LCBpZiBub3QsIGZlYXIgbm90ISBNYXliZSBtb3JlIHRpcHMgd2lyZXNoYXJrIGNhbiBzZWU/IAoKN3VueHh4eHh4eHh4IC0+IFNoYXJr
```

```
Good job finding this! This picture will help you later on, when you hopefully find file(s) where is hashed passwords. So that's what you need to find. Maybe you know
where to look, if not, fear not! Maybe more tips wireshark can see?

7unxxxxxxxxx -> Shark
```

That bottom line text looks like one tip is one part of whole text. These 3 tips combined is ‘7un71jöödxxx’. I used this string to make password list. I filled those last three x with all possibilities. Then I tried to brute force remoteroots ssh but I did not find password.

From /etc/passwd remoteroot’s full name says that for ssh connections it doesn’t need password but it won’t work so maybe it means something else.

```
jarmo:x:1000:1000:jarmo viinikanoja,,,:/home/jarmo:/bin/bash
remoteroot:x:1001:1001:used for ssh connections doesnt need password,404,,:/home/remoteroot:/bin/bash
```

This was dead end to me. I tried to find how I use port 9200 to find something but I didin’t find any attacks that sounds good for this one and if sounds good they did not work.