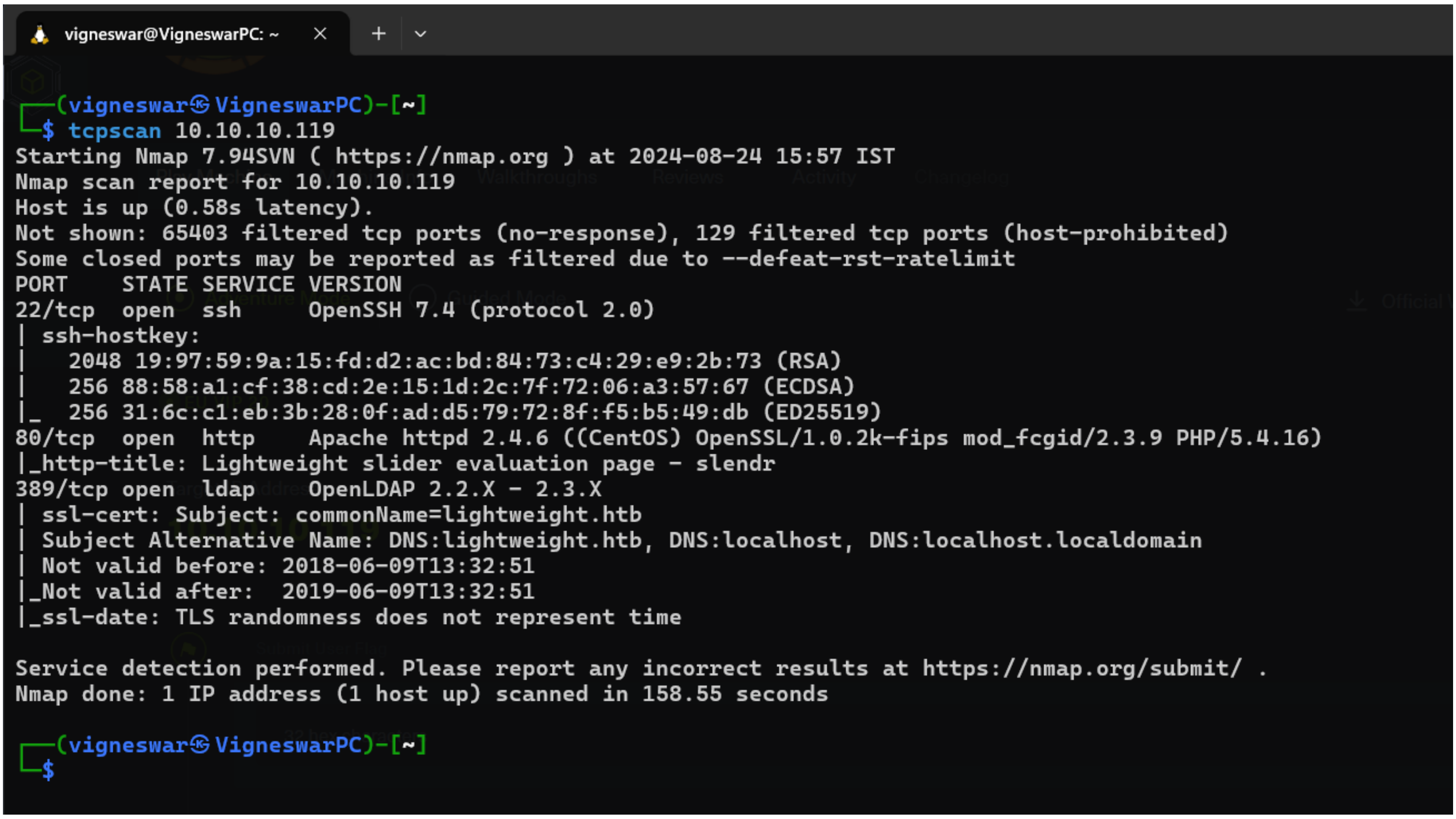
Information Gathering

1) Found open ports

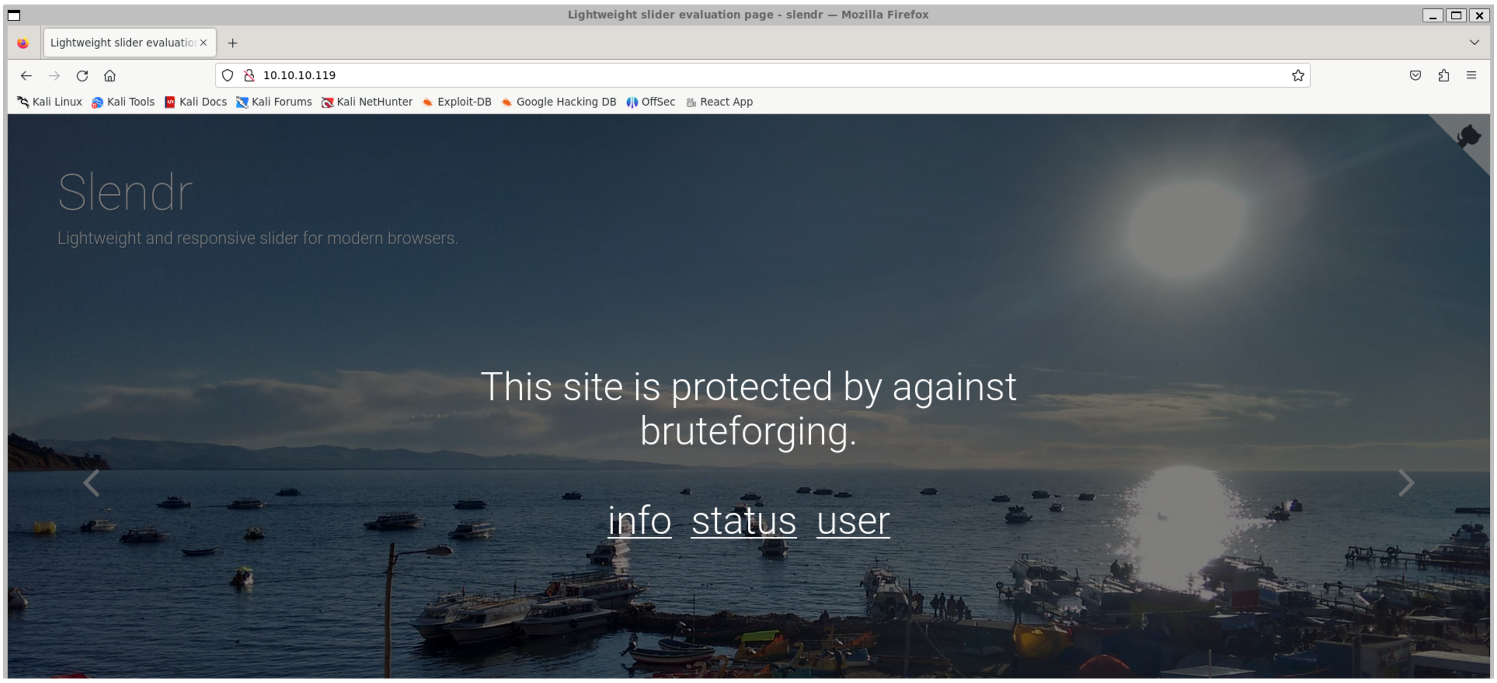


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.119
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 15:57 IST
Nmap scan report for 10.10.10.119
Host is up (0.58s latency).
Not shown: 65403 filtered tcp ports (no-response), 129 filtered tcp ports (host-prohibited)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 19:97:59:9a:15:fd:d2:ac:bd:84:73:c4:29:e9:2b:73 (RSA)
|   256 88:58:a1:cf:38:cd:2e:15:1d:2c:7f:72:06:a3:57:67 (ECDSA)
|_  256 31:6c:c1:eb:3b:28:0f:ad:d5:79:72:8f:f5:b5:49:db (ED25519)
80/tcp  open  http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16)
|_http-title: Lightweight slider evaluation page - slendr
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X
| ssl-cert: Subject: commonName=lightweight.htb
| Subject Alternative Name: DNS:lightweight.htb, DNS:localhost, DNS:localhost.localdomain
| Not valid before: 2018-06-09T13:32:51
|_Not valid after:  2019-06-09T13:32:51
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.55 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Checked the website



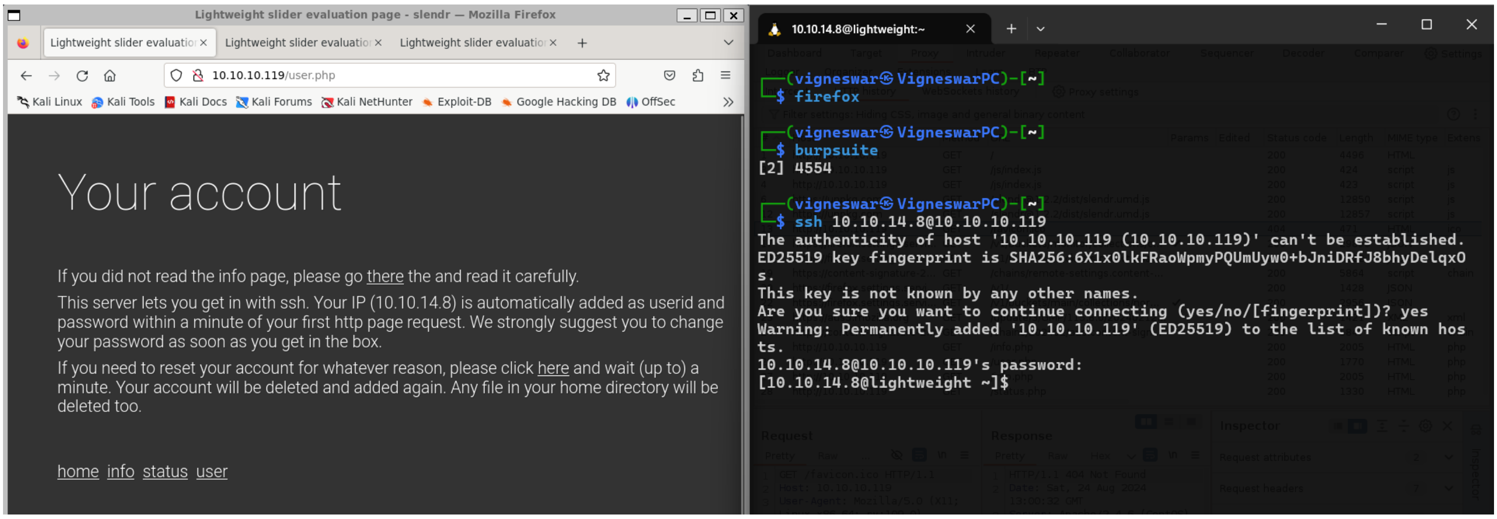
Slendr

Lightweight and responsive slider for modern browsers.

This site is protected by against bruteforging.

info status user

3) Logged in with ssh



Your account

If you did not read the info page, please go there the and read it carefully.

This server lets you get in with ssh. Your IP (10.10.14.8) is automatically added as userid and password within a minute of your first http page request. We strongly suggest you to change your password as soon as you get in the box.

If you need to reset your account for whatever reason, please click here and wait (up to) a minute. Your account will be deleted and added again. Any file in your home directory will be deleted too.

home info status user

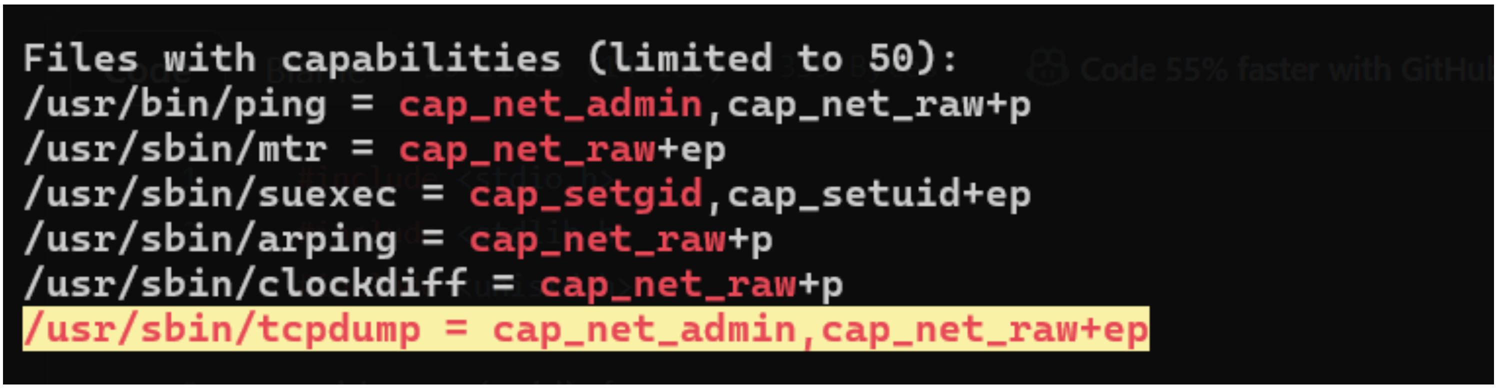
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ firefox

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ burpsuite
[2] 4554

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh 10.10.14.8@10.10.10.119
The authenticity of host '10.10.10.119 (10.10.10.119)' can't be established.
ED25519 key fingerprint is SHA256:6X1x0lkFRaoWpmyPQUmUyw0+bJniDRfJ8bhyDelqxO
s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.119' (ED25519) to the list of known hos
ts.
10.10.14.8@10.10.10.119's password:
[10.10.14.8@lightweight ~]$
```

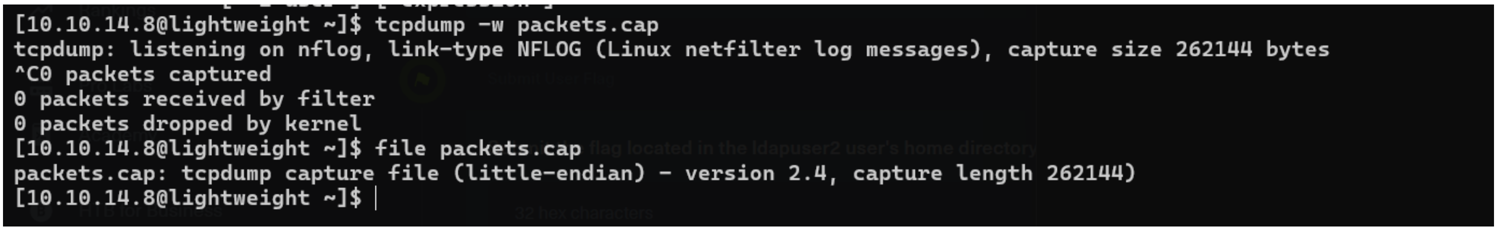
Vulnerability Assessment

1) Found linux capabilities



```
Files with capabilities (limited to 50):
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/sbin/mtr = cap_net_raw+ep
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+ep
```

2) Captured packets



```
[10.10.14.8@lightweight ~]$ tcpdump -w packets.cap
tcpdump: listening on nflog, link-type NFLOG (Linux netfilter log messages), capture size 262144 bytes
^C0 packets captured
0 packets received by filter
0 packets dropped by kernel
[10.10.14.8@lightweight ~]$ file packets.cap
packets.cap: tcpdump capture file (little-endian) - version 2.4, capture length 262144)
[10.10.14.8@lightweight ~]$
```