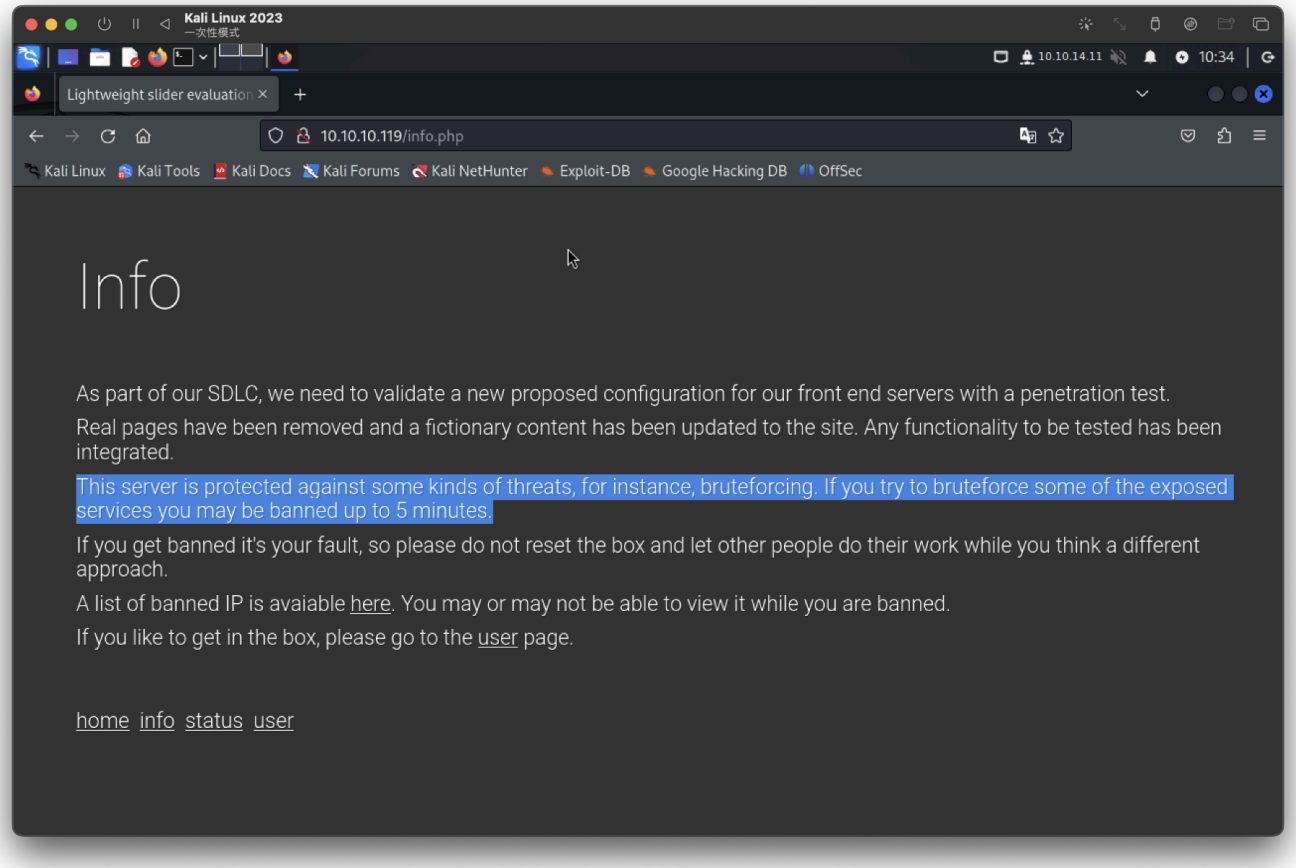
Lightweight,ldap

```
└─# nmap -sCV -p22,80,389 -A 10.10.10.119
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-20 10:19 PDT
Nmap scan report for 10.10.10.119
Host is up (0.30s latency).

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-date: TLS randomness does not represent time
| 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
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X (90%), Crestron 2-Series (86%),
HP embedded (85%), Oracle VM Server 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5.1 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
cpe:/o:oracle:vm_server:3.4.2 cpe:/o:linux:linux_kernel:4.1
Aggressive OS guesses: Linux 3.10 - 4.11 (90%), Linux 3.18 (90%), Linux 3.2
- 4.9 (90%), Linux 5.1 (90%), Crestron XPanel control system (86%), Linux
3.16 (86%), Linux 5.0 (85%), HP P2000 G3 NAS device (85%), Oracle VM Server
3.4.2 (Linux 4.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   300.73 ms 10.10.14.1
```

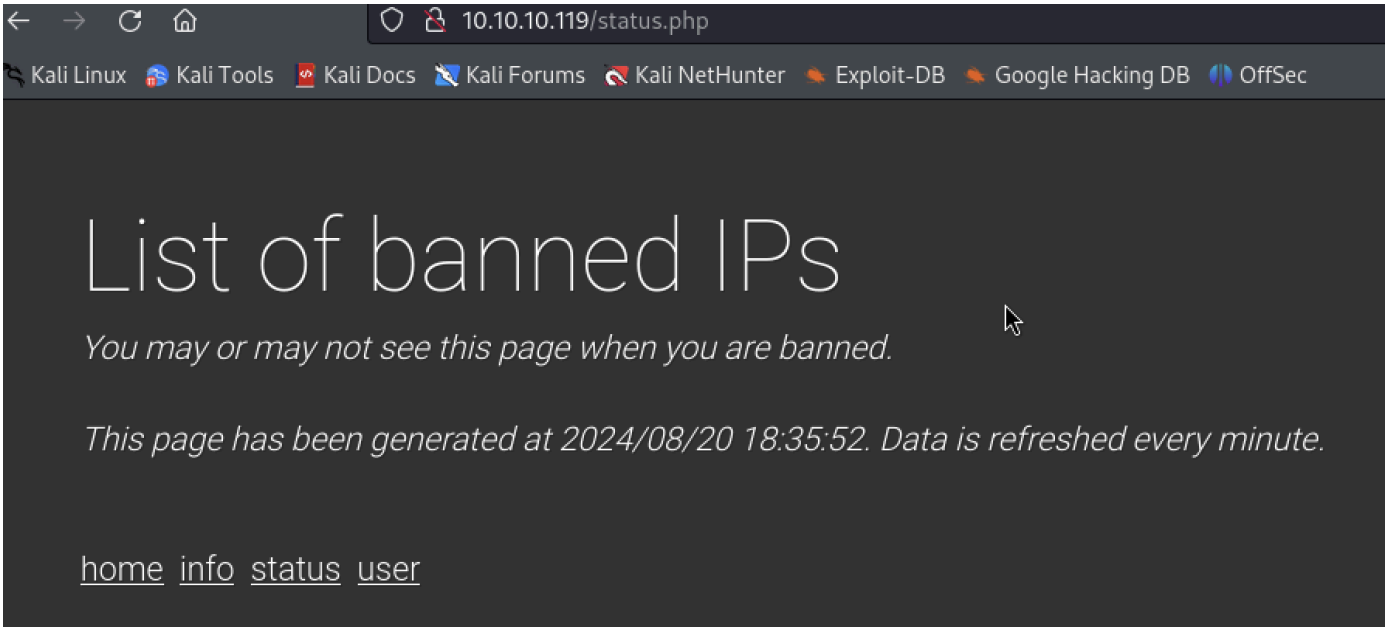
```
2   300.83 ms 10.10.10.119

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.12 seconds
```

---

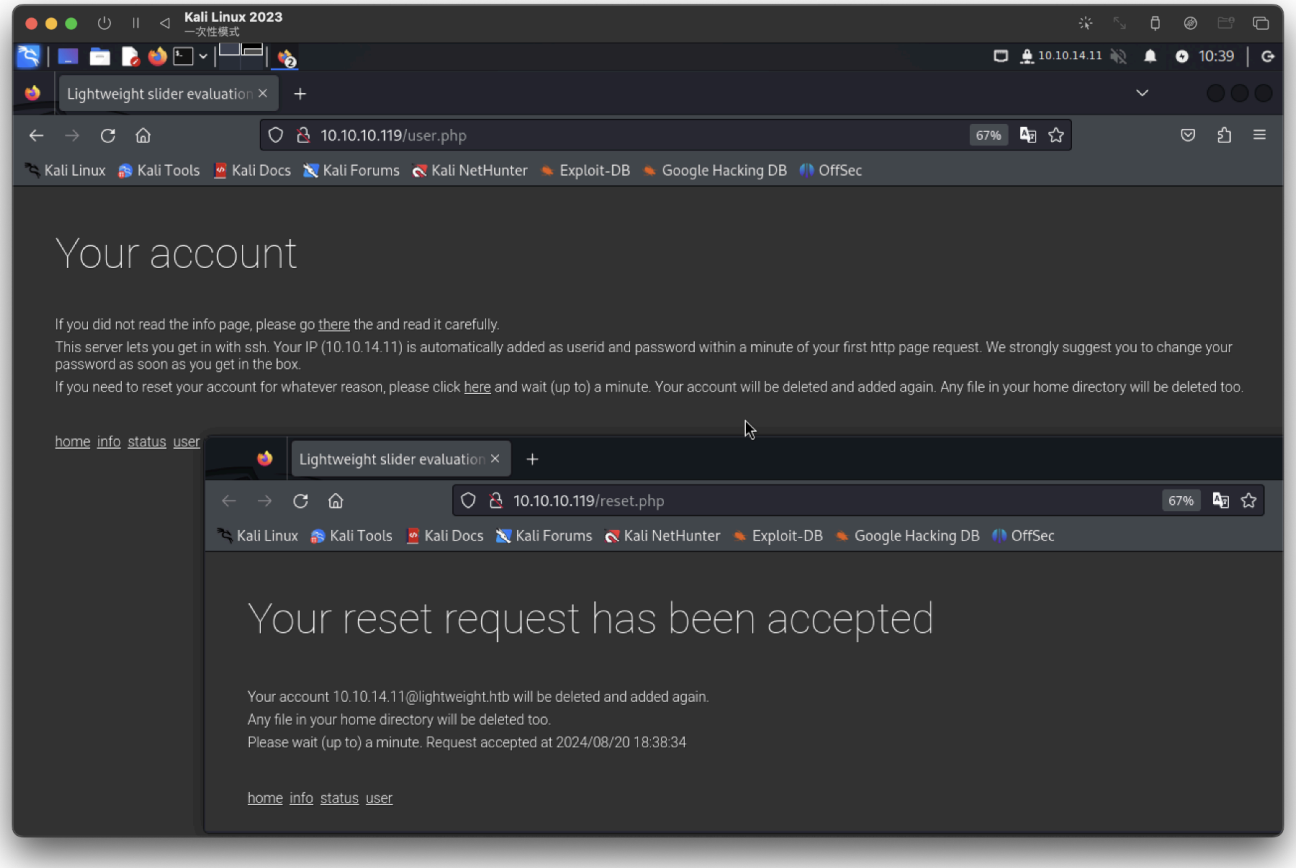
web頁面有3個PHP檔，
`/info.php` 。如果爆破會被禁5分鐘...



`/status.php` 提示而已..



`/user.php`疑似可以直連ssh，但因該也沒啥權限..



找到2組使用者

```
ldapuser1:x:1000:1000::/home/ldapuser1:/bin/bash
ldapuser2:x:1001:1001::/home/ldapuser2:/bin/bash
```

```
┌──(root㉿kali)-[~]
└─# ssh 10.10.14.11@lightweight.htb
The authenticity of host 'lightweight.htb (10.10.10.119)' can't be established.
ED25519 key fingerprint is SHA256:6X1×0lkFRaoWpmyPQUmUyw0+bJniDRfJ8bhyDelqxOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'lightweight.htb' (ED25519) to the list of known hosts.
10.10.14.11@lightweight.htb's password:
[10.10.14.11@lightweight ~]$ id
uid=1004(10.10.14.11) gid=1004(10.10.14.11) groups=1004(10.10.14.11) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[10.10.14.11@lightweight ~]$ whoami
10.10.14.11
[10.10.14.11@lightweight ~]$ ls
[10.10.14.11@lightweight ~]$ pwd
/home/10.10.14.11
[10.10.14.11@lightweight ~]$ cd ..
[10.10.14.11@lightweight home]$ ls
10.10.14.11  10.10.14.2  127.0.0.1  ldapuser1  ldapuser2
[10.10.14.11@lightweight home]$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ldapuser1:x:1000:1000::/home/ldapuser1:/bin/bash
ldapuser2:x:1001:1001::/home/ldapuser2:/bin/bash
10.10.14.2:x:1002:1002::/home/10.10.14.2:/bin/bash
127.0.0.1:x:1003:1003::/home/127.0.0.1:/bin/bash
10.10.14.11:x:1004:1004::/home/10.10.14.11:/bin/bash
[10.10.14.11@lightweight home]$
```

針對ldap進行nmap完整掃描看看

```
—# nmap -p389 10.10.10.119 --script *ldap*

PORT    STATE SERVICE
```

```
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       namingContexts: dc=lightweight,dc=htb
|       supportedControl: 2.16.840.1.113730.3.4.18
|       supportedControl: 2.16.840.1.113730.3.4.2
|       supportedControl: 1.3.6.1.4.1.4203.1.10.1
|       supportedControl: 1.3.6.1.1.22
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.826.0.1.3344810.2.3
|       supportedControl: 1.3.6.1.1.13.2
|       supportedControl: 1.3.6.1.1.13.1
|       supportedControl: 1.3.6.1.1.12
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|       supportedExtension: 1.3.6.1.1.8
|       supportedLDAPVersion: 3
|_      subschemaSubentry: cn=Subschema
| ldap-search:
|   Context: dc=lightweight,dc=htb
|     dn: dc=lightweight,dc=htb
|         objectClass: top
|         objectClass: dcObject
|         objectClass: organization
|         o: lightweight htb
|         dc: lightweight
|     dn: cn=Manager,dc=lightweight,dc=htb
|         objectClass: organizationalRole
|         cn: Manager
|         description: Directory Manager
|     dn: ou=People,dc=lightweight,dc=htb
|         objectClass: organizationalUnit
|         ou: People
|     dn: ou=Group,dc=lightweight,dc=htb
|         objectClass: organizationalUnit
|         ou: Group
|     dn: uid=ldapuser1,ou=People,dc=lightweight,dc=htb
|         uid: ldapuser1
|         cn: ldapuser1
|         sn: ldapuser1
|         mail: ldapuser1@lightweight.htb
```

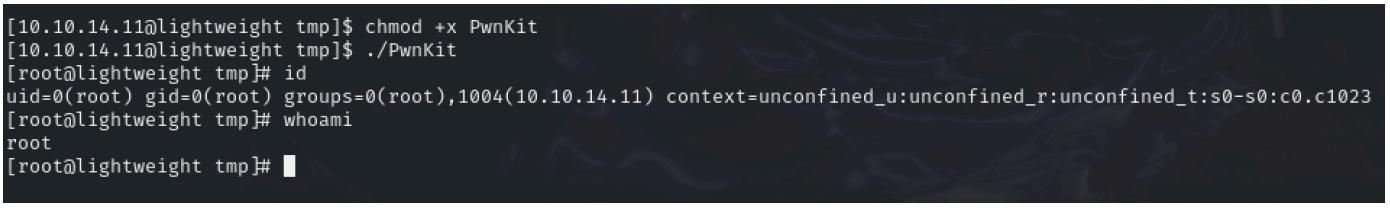
```
|         objectClass: person
|         objectClass: organizationalPerson
|         objectClass: inetOrgPerson
|         objectClass: posixAccount
|         objectClass: top
|         objectClass: shadowAccount
|         userPassword:
{crypt}$6$3qx0SD9x$Q9y1lyQaFKpxqkGqKAjLOWd33Nwdhj.l4MzV7vTnfkE/g/Z/7N5ZbdEQW
fup2lSdASImHtQFh6zMo41ZA./44/
|         shadowLastChange: 17691
|         shadowMin: 0
|         shadowMax: 99999
|         shadowWarning: 7
|         loginShell: /bin/bash
|         uidNumber: 1000
|         gidNumber: 1000
|         homeDirectory: /home/ldapuser1
|     dn: uid=ldapuser2,ou=People,dc=lightweight,dc=htb
|         uid: ldapuser2
|         cn: ldapuser2
|         sn: ldapuser2
|         mail: ldapuser2@lightweight.htb
|         objectClass: person
|         objectClass: organizationalPerson
|         objectClass: inetOrgPerson
|         objectClass: posixAccount
|         objectClass: top
|         objectClass: shadowAccount
|         userPassword:
{crypt}$6$xJxPjT0M$1m8kM00CJYCAgzT4qz8TQwyGFQvk3boaymuAmMZCOfm3OA7OKunLZZlqy
tUp2dun509OBE2xwX/QEfjdRQzgn1
|         shadowLastChange: 17691
|         shadowMin: 0
|         shadowMax: 99999
|         shadowWarning: 7
|         loginShell: /bin/bash
|         uidNumber: 1001
|         gidNumber: 1001
|         homeDirectory: /home/ldapuser2
|     dn: cn=ldapuser1,ou=Group,dc=lightweight,dc=htb
|         objectClass: posixGroup
|         objectClass: top
|         cn: ldapuser1
```

```
|         userPassword: {crypt}x
|         gidNumber: 1000
|     dn: cn=ldapuser2,ou=Group,dc=lightweight,dc=htb
|         objectClass: posixGroup
|         objectClass: top
|         cn: ldapuser2
|         userPassword: {crypt}x
|_        gidNumber: 1001
```

無法從這裡獲得太多資訊。密碼應該不會被破解。
但確認ssh跟ldap的使用者完全一致。

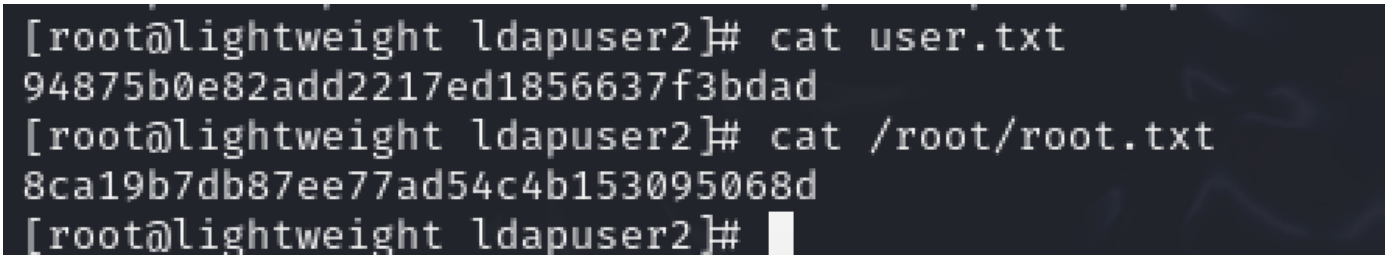
有版本漏洞（PwnKit）

提權了？

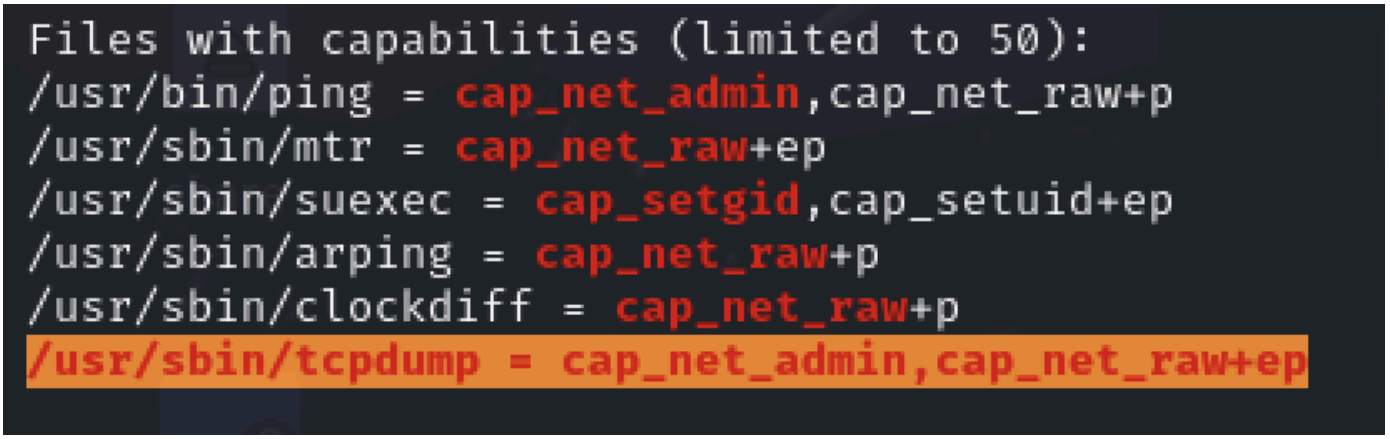


と...好快...

user、root flag



發現可以使用tcpdump，應該是針對ldap



```
tcpdump -i lo 'port 389' -w tso.pcap -v
```

針對本地389Port 並存檔且輸出詳細資訊

我猜監聽端口找到密碼還是什麼的？
懶得做