Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Linux Forensics

DFIR-08-L3

Process Investigation

Lab Objective

Gain hands-on experience with forensic investigation methods learned during the lesson.

Lab Mission

Mimic bind shell behavior and investigate it using live analysis of the ***/proc/*** directory content.

Lab Duration

20–25 minutes

Requirements

- Working knowledge of the Linux environment

Resources

- VirtualBox that includes an NAT network of:
    - Ubuntu 20.04

Textbook References

- Chapter 8: Linux Forensics
    - Section 6: Process Investigation

Lab Task: Bind Shell Investigation

Mimic bind shell behavior and investigate it using live analysis of the ***/proc/*** directory content.

1. Start the Ubuntu 20.04 machine and copy ***nc*** from the ***/bin*** directory to the ***/tmp/bindshell*** directory.
2. In the ***tmp*** folder, use ***./bindshell -lvp 1339 >/dev/null &*** to create a running process in the background and then delete the ***bindshell*** executable with the ***rm*** command.

   Note: Using the ampersand (&) puts the process in the background and allows it to continue to execute even when changes are made to the executable. Also, if the DNS name server is not working, type **sudo nano /etc/resolv.conf** and change the name server to ***8.8.8.8***
3. Verify the process is running by using ***lsof -i -n -P -l*** and change directories to the ***/proc*** folder under the ***bindshell*** process ID. Your ID may be different from the image below.

4 Find evidence the process communicates over the network. There are two indicators that may prove network communication: network libraries and socket connections. Run ***cat maps*** to show the libraries and then run ***ls -la /fd*** to determine if sockets are being used.

```
john@john:/proc/2674$ cat maps
559c2eb75000-559c2eb77000 r--p 00000000 08:03 1572881                    /tmp/bindshell (deleted)
559c2eb77000-559c2eb7c000 r-xp 00002000 08:03 1572881                    /tmp/bindshell (deleted)
559c2eb7c000-559c2eb7e000 r--p 00007000 08:03 1572881                    /tmp/bindshell (deleted)
559c2eb7f000-559c2eb80000 r--p 00009000 08:03 1572881                    /tmp/bindshell (deleted)
559c2eb80000-559c2eb81000 rw-p 0000a000 08:03 1572881                    /tmp/bindshell (deleted)
559c2eb81000-559c2ec01000 rw-p 00000000 00:00 0
559c305d3000-559c305f4000 rw-p 00000000 00:00 0                          [heap]
7f3b3af9e000-7f3b3afa0000 r--p 00000000 08:03 1711509                    /usr/lib/x86_64-linux-gnu/libnss_dns-2.32.so
7f3b3afa0000-7f3b3afa4000 r-xp 00002000 08:03 1711509                    /usr/lib/x86_64-linux-gnu/libnss_dns-2.32.so
7f3b3afa4000-7f3b3afa5000 r--p 00006000 08:03 1711509                    /usr/lib/x86_64-linux-gnu/libnss_dns-2.32.so
7f3b3afa5000-7f3b3afa6000 r--p 00006000 08:03 1711509                    /usr/lib/x86_64-linux-gnu/libnss_dns-2.32.so
7f3b3afa6000-7f3b3afa7000 rw-p 00007000 08:03 1711509                    /usr/lib/x86_64-linux-gnu/libnss_dns-2.32.so
7f3b3afa7000-7f3b3afa8000 r--p 00000000 08:03 1711517                    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
7f3b3afa8000-7f3b3afaa000 r-xp 00001000 08:03 1711517                    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
7f3b3afaa000-7f3b3afab000 r--p 00003000 08:03 1711517                    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
7f3b3afab000-7f3b3afac000 r--p 00003000 08:03 1711517                    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
7f3b3afac000-7f3b3afad000 rw-p 00004000 08:03 1711517                    /usr/lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
7f3b3afad000-7f3b3afb0000 r--p 00000000 08:03 1711511                    /usr/lib/x86_64-linux-gnu/libnss_files-2.32.so
7f3b3afb0000-7f3b3afb8000 r-xp 00003000 08:03 1711511                    /usr/lib/x86_64-linux-gnu/libnss_files-2.32.so
7f3b3afb8000-7f3b3afba000 r--p 0000b000 08:03 1711511                    /usr/lib/x86_64-linux-gnu/libnss_files-2.32.so
7f3b3afba000-7f3b3afbb000 r--p 0000c000 08:03 1711511                    /usr/lib/x86_64-linux-gnu/libnss_files-2.32.so
7f3b3afbb000-7f3b3afbc000 rw-p 0000d000 08:03 1711511                    /usr/lib/x86_64-linux-gnu/libnss_files-2.32.so
7f3b3afbc000-7f3b3afc5000 rw-p 00000000 00:00 0
7f3b3afc5000-7f3b3afeb000 r--p 00000000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3afeb000-7f3b3b158000 r-xp 00026000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3b158000-7f3b3b1a4000 r--p 00193000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3b1a4000-7f3b3b1a5000 ---p 001df000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3b1a5000-7f3b3b1a8000 r--p 001df000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3b1a8000-7f3b3b1ab000 rw-p 001e2000 08:03 1710732                    /usr/lib/x86_64-linux-gnu/libc-2.32.so
7f3b3b1ab000-7f3b3b1af000 rw-p 00000000 00:00 0
7f3b3b1af000-7f3b3b1b3000 r--p 00000000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1b3000-7f3b3b1c2000 r-xp 00004000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1c2000-7f3b3b1c5000 r--p 00013000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1c5000-7f3b3b1c6000 ---p 00016000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1c6000-7f3b3b1c7000 r--p 00016000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1c7000-7f3b3b1c8000 rw-p 00017000 08:03 1711695                    /usr/lib/x86_64-linux-gnu/libresolv-2.32.so
7f3b3b1c8000-7f3b3b1ca000 rw-p 00000000 00:00 0
7f3b3b1ca000-7f3b3b1ce000 r--p 00000000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
7f3b3b1ce000-7f3b3b1dd000 r-xp 00004000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
7f3b3b1dd000-7f3b3b1e0000 r--p 00013000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
7f3b3b1e0000-7f3b3b1e1000 ---p 00016000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
7f3b3b1e1000-7f3b3b1e2000 r--p 00016000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
7f3b3b1e2000-7f3b3b1e3000 rw-p 00017000 08:03 1710728                    /usr/lib/x86_64-linux-gnu/libbsd.so.0.10.0
```

Libresolv is a dedicated library that can prove network connectivity.

```
john@john:/proc/2674$ ls -la fd/
total 0
dr-x------ 2 john john  0 Mar 22 09:39 .
dr-xr-xr-x 9 john john  0 Mar 22 09:39 ..
lrwx------ 1 john john 64 Mar 22 09:39 0 -> /dev/pts/0
l-wx------ 1 john john 64 Mar 22 09:39 1 -> /dev/null
lrwx------ 1 john john 64 Mar 22 09:39 2 -> /dev/pts/0
lrwx------ 1 john john 64 Mar 22 09:39 3 -> 'socket:[49811]'
```

5 Obtain information about who or what started the process by using the ***strings environ*** command. If the string did not work, install with ***sudo apt install binutils***.

```
john@john:/proc/2674$ strings environ
SHELL=/bin/bash
SESSION_MANAGER=local/john:@/tmp/.ICE-unix/1613,unix/john:/tmp/.ICE-unix/1613
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1546
GTK_MODULES=gail:atk-bridge
PWD=/tmp
LOGNAME=john
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/john
USERNAME=john
```

Although environmental variables do not contain much information in this case, they can still be used to reveal who ran the executable and how the user was connected.

```
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=john
GNOME_TERMINAL_SERVICE=:1.107
DISPLAY=:0
SHLVL=0
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/john
_=./bindshell
```

6 Obtain the deleted binary's hash and compare it with the original binary's hash. Copy the executable with the ***cp exe /tmp/recovered*** command. Create an MD5 hash to the file with ***md5sum /tmp/recovered*** and then compare it to the NC with the ***md5sum /bin/nc*** command.

Hints

- The ***cp*** command can be used to copy folders and files (***cp*** was introduced in LNX-02).
- Execute the ***bindshell*** file to get information with the tag ***-lvp 1339*** and insert it in ***/dev/null***. **Note**: Make sure you are getting the nameserver.
- ***/dev/null*** is a special file in the Linux file system. Anything written to this file will disappear.
- The command ***lsof -i -n -P -l*** is used to list live processes.
- Change the directory to the process ID and list what is in the process.
- For Step 4, refer to ***maps*** and ***fd*** in Chapter 8 of the textbook.
- The ***strings*** tool can be used to inspect information.
  Note: It may be necessary to run ***sudo apt install binutils*** to your Ubuntu box if the ***strings*** tool does not run.
- The ***md5sum*** command uses the MD5 algorithm to print the checksum of a given file.
- Check the MD5 of the ***.exe*** file and ***/bin/nc***.