Nebula : flag00

Hey, guys i just decided to solve the Nebula machine from exploit education.

nebula is a vulnurable VM that teaches a variety of common (and less than common) weaknesses and vulnerabilities in Linux. Below listed are some of the things that we would be able to learn.

1. SUID files
2. Permissions
3. Race conditions
4. Shell meta-variables
5. $PATH weaknesses
6. Scripting language weaknesses
7. Binary compilation failures

At the end of Nebula, the user will have a reasonably thorough understanding of local attacks against Linux systems, and a cursory look at some of the remote attacks that are possible.

So lets get started, Download the image from here the above give url and mount it on your VM. The username and passwords are as given below for the VM.

Username: nebula

Password: nebula

Navigate to level00, the task for the level00 is to run a executable file thats located somewhere on the filesystem. Inorder to do that we will use the find command.

As always manual pages would help, “man find”.

Login to the VM using the uname and password : nebula

once logged in, lets try using the find command to locate to the file.

LEVEL 00

This level requires you to *find* a Set User ID program that will run as the "flag00" account. You could also find this by carefully looking in top level directories in / for suspicious looking directories.

Alternatively, look at the find man page.

To access this level, log in as level00 with the password of level00.

Source code

There is no source code available for this level.

Since this file a Set UID program, it would have a executable permission. Lets try finding all executable files in the system.

$ find / -perm 4000

```
nebula@nebula:~$ find / -perm 4000_
```

You can see this would return in a lot of errors since, we do not have permission to access the entire file system.

```
/rofs/usr/bin/at
/rofs/usr/bin/chfn
/rofs/usr/bin/chsh
/rofs/usr/bin/gpasswd
/rofs/usr/bin/mtr
/rofs/usr/bin/newgrp
/rofs/usr/bin/passwd
/rofs/usr/bin/sudo
/rofs/usr/bin/sudoedit
/rofs/usr/bin/traceroute6.iputils
/rofs/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/rofs/usr/lib/eject/dmcrypt-get-device
/rofs/usr/lib/openssh/ssh-keysign
/rofs/usr/lib/pt_chown
/rofs/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/rofs/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/rofs/usr/sbin/pppd
/rofs/usr/sbin/uuidd
find: `/rofs/var/cache/ldconfig': Permission denied
find: `/rofs/var/lib/php5': Permission denied
find: `/rofs/var/lib/sudo': Permission denied
find: `/rofs/var/spool/cron/atjobs': Permission denied
find: `/rofs/var/spool/cron/atspool': Permission denied
find: `/rofs/var/spool/cron/crontabs': Permission denied
nebula@nebula:~$
```

Now lets try to redirect all of the errors to a different place in the filesystem which we have access to, in most cases temperory storage spaces like “/dev/null”, “/dev/shm”, “/tmp/” would be a good choice to redirect errors. Inorder to redirect errors you should be familiar with standin, standout and errors in the file system.

Stanin – is represented by 0

standout – is represented by 1

Errors – are represented by 2

Thus running the below command will redirect all errors to a different place, allowing us only to view the results.

$ find / -perm 4000 2>/dev/null

```
nebula@nebula:~$ find / -perm 4000 2>/dev/null
nebula@nebula:~$
```

This leaves us with nothing, since we do not have an exact match. We could find partial matches for the file permissions in the system.

$ find / -perm -4000 2>/dev/null

```
nebula@nebula:~$ find / -perm -4000 2>/dev/null_
```

```
/rofs/bin/ping
/rofs/bin/ping6
/rofs/bin/su
/rofs/bin/umount
/rofs/sbin/mount.ecryptfs_private
/rofs/usr/bin/at
/rofs/usr/bin/chfn
/rofs/usr/bin/chsh
/rofs/usr/bin/gpasswd
/rofs/usr/bin/mtr
/rofs/usr/bin/newgrp
/rofs/usr/bin/passwd
/rofs/usr/bin/sudo
/rofs/usr/bin/sudoedit
/rofs/usr/bin/traceroute6.iputils
/rofs/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/rofs/usr/lib/eject/dmcrypt-get-device
/rofs/usr/lib/openssh/ssh-keysign
/rofs/usr/lib/pt_chown
/rofs/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/rofs/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/rofs/usr/sbin/pppd
/rofs/usr/sbin/uuidd
nebula@nebula:~$
```

We do have a lot of results, what we can do is to pipe the output to more and look at all the results or something similar, but we do know that its named “flag00” so i could grep for all results that contain the name “flag00”

$ find / -perm -4000 2>/dev/null | grep flag00

```
nebula@nebula:~$ find / -perm -4000 2>/dev/null | grep flag00
/bin/.../flag00
/rofs/bin/.../flag00
nebula@nebula:~$
```

We have a couple of results, lets take a look into the “/bin/.../flag00”

“...” - here is a directory.

$ cd /bin/.../

$ ls -la

$ ./flag00

```
nebula@nebula:~$ cd /bin/...
nebula@nebula:/bin/...$ ls -la
total 8
drwxr-xr-x 2 root   root      29 2011-11-20 21:22 .
drwxr-xr-x 3 root   root    2728 2012-08-18 02:50 ..
-rwsr-x--- 1 flag00 level00 7358 2011-11-20 21:22 flag00
nebula@nebula:/bin/...$ ./flag00
-bash: ./flag00: Permission denied
nebula@nebula:/bin/...$ _
```

so we get an error, looking at the challenge, we do know that we have to login as “level00” with a password “level00” to execute the file. Lets try doing that.

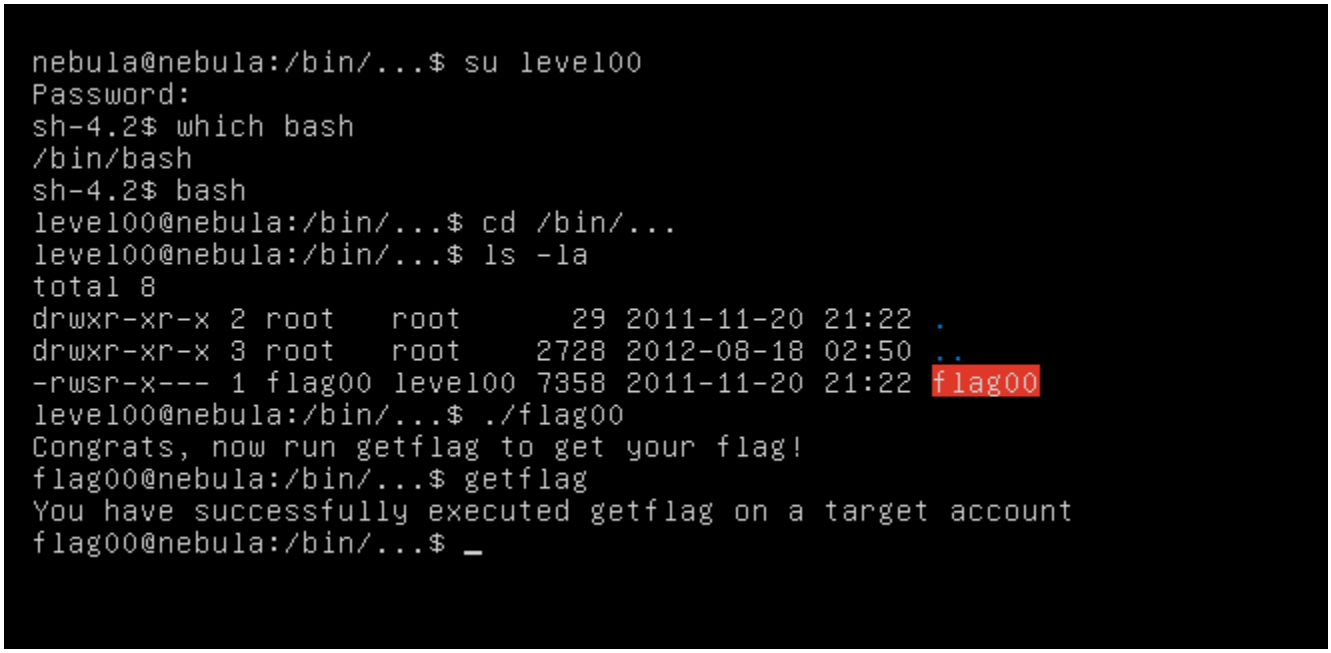
$ su level00

$ cd /bin/.../

$ ./flag00

we might have to run “getflag” to complete the challenge

$ getflag



Thats it for level00, hope you have learnt something. Ill come up with another post for the next level.

Later.

-blankdash