**VulnHub – DC1**

1. A close up of a text

   Description automatically generatedFirst is to perform a scan of the network to determine the victims IP address.



1. Next, we must perform an nmap scan onto the victims ip address. This scan will just discover the ports. Once ports are discovered I will use the nmap command to check for services.

* A computer screen shot of a computer code

  Description automatically generatedThe scan revealed that there are 3 ports open. Ports 22, 80 and 111.
* Next I scanned each port for the service and ran this command to do it.



* A screen shot of a computer

  Description automatically generatedThere is an OpenSSH 6.0p1 service, an Apache 2.2.22 (quite a low version, may have vulnerabilities), and rcpbind 2-4.

A screenshot of a computer

Description automatically generated

**JUST FOR REFERENCE**: *This is what my notes look like.*

1. A screenshot of a login page

   Description automatically generatedUse the tool nikto to look for vulnerabilities in http, rpc or ssh. While nikto is running, I will quickly look at the website and look for anything out of the ordinary, which also includes reviewing the page source code for any hidden comments.

* A screen shot of a computer

  Description automatically generatedLooking at some of the directories and files nikto found (still running) was robots.txt, this showed some directories and files that are ‘forbidden’.

A screen shot of a computer

Description automatically generated

* With a quick google search, I found out that this is vulnerable. I would need to craft special requests in burpe suite for this to work.
* A screen shot of a computer screen

  Description automatically generatedThis was the results of the nikto scan. It found a few things.
* Looking at external resources I found: <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/drupal#get-number-of-users>
* A screenshot of a computer

  Description automatically generatedA screen shot of a computer

  Description automatically generatedThey recommend trying to figure out users, users 1 & 2 give access denied, while user 3 gives page not found.

1. A computer screen shot of a program

   Description automatically generatedTo get an exploit going we need to find a vulernability, however to find this we need the version of the Drupal website. I found a tool online called Droopescan which can list the possible versions of this site and plugins.

* These versions mean we can go into searchsploit and find some possible exploits.

1. Using Metasploit: “mfsconsole”, then use the exploit directory for drupal.

* Next, call the command ‘options’ to display the available options. Don’t forget that when setting the RHOST and LHOST to do the following “LHOST 192.x.x.x” or “RHOSTS 192.x.x.x” (don’t include equals sign!).
* Set LHOST 192.168.56.101 (attacker) and RHOST 192.168.56.110 (victim).
* Run the exploit.

A screen shot of a computer

Description automatically generated

* A screen shot of a computer

  Description automatically generatedNow we are in.

1. Once in, we ‘ls’ to view current directory contents. We see all of the web directory files.



* Flag 1 gives a hint to the next flag.

1. A screenshot of a computer

   Description automatically generatedTraversing out of that directory and into the home directory reveals a flag4 directory with a file that gives another hint.
2. A screenshot of a computer program

   Description automatically generatedFlag 1 stated that there was config file, which by default for Drubal (get it by google searching) is /sites/default/settings.php.

* Entering that directory reveals credentials for what appears to be mysql.

1. A close up of a number

   Description automatically generatedImproving the shell.

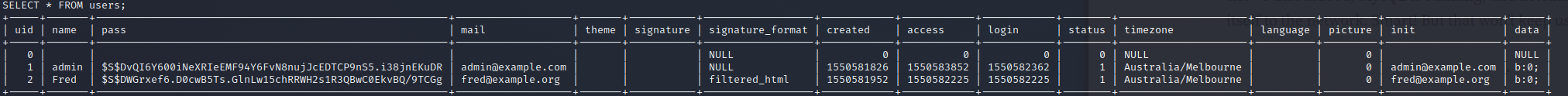
* Make sure while in the msfconsole, you type shell before you try and change the shell. If you don’t it won’t work.
* Then you can upgrade.

1. Finding mysql is quick using the following command.

* A screenshot of a computer program

  Description automatically generatedwe can then use the credentials from earlier to login to the mysql database.
* A screenshot of a computer program

  Description automatically generatedWe can then find the correct database to get into.
* Next, call “SHOW TABLES;” which reveals all of the tables in this database.



* What we can see now is the password hashes of the accounts admin and Fred.

1. A computer screen shot of a computer program

   Description automatically generatedOur next step is to try and get into the root file, using the command find to look for binaries with set UID we can see that find is used. This is significant because it can be used to look into another directory, like root.

* A screen shot of a computer

  Description automatically generatedLets use find to look into the root folder.
* There we can see the final flag.

1. A screen shot of a computer screen

   Description automatically generatedThe final flag is found.