**Walkthrough – DC7**

1. Performing a netdiscover to determine the devices on the network 192.168.56.0/24.



* We have found the ip address of the victim machine 192.168.56.118.

1. Since we have the ip-address we can now use nmap to discover open ports on this system.





* As we can see there are two ports open, one for ssh and the other for http. Lets try and see what service is running behind these ports.



* Port 22 is running apparently openssh and port 80 is running apache 2.4.25.

1. A screenshot of a computer

   Description automatically generatedSince we know port 80 is up, this must be a webserver of some sort. We can go visit the site to determine more information.

* The site has a search box and a brief statement and hit from the creator.
* You can also see this is a Drupal based website.
* Something interesting is that the url could be used for file inclusion, when you attempt to search for something (ex, ‘hello’).

1. Now that we have a basic idea of the website we can use nikto to find other information we couldn’t find.

A computer screen shot of text

Description automatically generated

1. A close-up of a page

   Description automatically generatedModify the url I noticed that most drupal websites have a ‘node’ directory. This is true for this site too. When I type ‘/node/1’ the site stays the same, however when I type any number greater than 1 it gives me an error.

* A white rectangle with black text

  Description automatically generatedIf you go into the ‘reset password’ tab, I tried entering the username admin and the password reset link was sent. So ‘admin’ is an identified username.

A screenshot of a computer screen

Description automatically generated

1. I will now use a tool known as droopescan. This tool should give me more information.



* Nothing really came of it, besides possible versions.

A screenshot of a computer program

Description automatically generated

1. In the search box I was able to find something interesting.

A close up of a card

Description automatically generated

A black and white text

Description automatically generated

* This is significant because there might be a database somewhere that I can access or manipulate to obtain unauthorised access.
* A screenshot of a search results page

  Description automatically generatedThere seems to be a pattern where ‘./’ followed by some input will reveal some information.
* The 403 you have been denied is ‘/node/2’, which now confirms that node/2 is the admin page.
* Next following the node/ trend I was able to get another interesting response.

A white background with black text

Description automatically generated

1. I took a look at the hint and realised something. The creator had put his username in the website.

* This I typed into the search box and google. The interesting thing is that a github page appeared named ‘staffdb’.

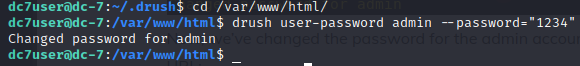
1. A screenshot of a computer

   Description automatically generatedSnooping around I found config.php which contained a username and password.
2. A screenshot of a computer program

   Description automatically generatedCredentials found for ssh.
3. SSH login.

A black background with white text

Description automatically generated

1. Drush command. I used an online resource to find out how to use drush to change passwords.

* Now we have reset admin username and password.

A screenshot of a computer

Description automatically generated

1. Now we are in the admin web-portal, go to extensions > install. Then search up php for drupal and download it. Once downloaded, upload the tar.gz file and wait for it to install.

* Then click on Enable newly added modules, to turn it on.

1. A screenshot of a computer program

   Description automatically generatedCreate a basic page. Since we now have PHP enabled, we can create a new page and write a netcat listener to it.

* Before you click save, make sure to have the listener set up to accept connections.

1. Update shell.
2. MFSVenom payload. Now it is time to create a pay to get into the system.



1. Since we have privileges on behalf of backup.sh, we can now append that payload to backups file.

* A screen shot of a computer

  Description automatically generatedremember we have permissions to do this.

1. A screenshot of a computer screen

   Description automatically generatedAfter waiting quite some time, finally got the flag.