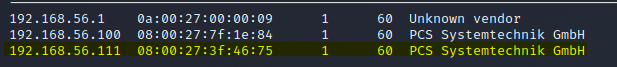
**VulnHub – DC2**

1. Use netdiscover to determine the hosts on the network.

* Victim is 192.168.56.111.

1. Perform an nmap scan to determine the available ports. This one is a no ping and SYN scan(stealthy).



* Results show that port 80 is open, which is most likely a webserver.
* Now I can perform a detailed scan on that port, so we will use the flags to prevent a ping and scan for os and version.







1. A screen shot of a computer screen

   Description automatically generatedNow its time to use nikto to scan for web vulnerabilities.

* Nikto states that this is a word press site, however my attempts to scan it with the ‘wpscan’ tool state that this website doesn’t work. I might need to go into burpe suite an change the head.

1. Visiting the actual website. The home page re-directs to dc-2 for some reason.

* A screenshot of a computer

  Description automatically generatedThere is a login page that nikto found.

A screenshot of a computer

Description automatically generated

* A screenshot of a computer

  Description automatically generatedThe lost your password link, takes you to a page where you get an error. This is because it redirects the ip-address to dc-2.com.

A screenshot of a computer

Description automatically generated

* The main webpage is under-construction.
* Checking all of the pages source code reveals nothing of interest.

1. A close up of a text

   Description automatically generatedTrying the login page. From trial and error there appears to be the user ‘admin’ available however I am unable to login due to password.

* A close-up of a logo

  Description automatically generatedAttempting SQL injection gives just an error for incorrect username and password.

1. Modifying the URL, I added an extra slash and I have found a hidden website.

A screenshot of a computer

Description automatically generated

1. This allows me to perform WP-Scan on this site.

A computer screen shot of a program

Description automatically generated

* I will checkout the readme.html, xmlrpc, and the wp-cron.php.

1. A screenshot of a computer

   Description automatically generatedGoing onto ‘xmlrpc’ I see a message that says post only requests.

* This means I can open up burp suite and send a malicious post request.

A screen shot of a computer

Description automatically generatedRequest Response.

A screen shot of a computer code

Description automatically generated

* A screenshot of a web page

  Description automatically generatedWhile navigating URLS I found author=1, to display admin posts.
* I ended up ditching this.

1. Found Flag one while looking at /index.php/flag

A text on a white background

Description automatically generated

1. Using cewl, I created a wordlist for a dictionary attack against usernames found in the wp-scan.

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. Now that we have usernames and passwords, we can use wp-scan to brute force.



* We have successfully found login credentials.

1. Now that we have logged in, I went to the pages tab and found flag 2.

A screenshot of a computer

Description automatically generated

* Since we found ssh port to be open, this must be what he is talking about.

1. SSH into tom or jerry’s account

* Tom’s was the one who worked, and I was about to ls his directory and discover flag3.
* I couldn’t cat, tails, or head the file, so I had to try vim and vi. Vi ended up working.

1. A screen shot of a computer

   Description automatically generatedFor flag 4, it was time consuming to escape the home directory of tom. Most commands were either not installed or restricted like ‘cd’. I later found out that ls and vi were the only commands I had access to so I just ls the directories above mine and went into jerrys home directory and found flag 4.

A screen shot of a computer

Description automatically generated

1. Privilege escalation.

A screenshot of a computer error

Description automatically generated

* I realised this didn’t really mean much, but it did help me obtain cd permissions.

1. Now I was trying to think what I had access to, then I remembered that the bin file contains all of the commands available to the system.

A black background with white text

Description automatically generated

* So I went into the file and ran it manually, now I switched users into jerry.

1. Calling ‘sudo -l’ I can see I am able to run git as privileged user without a password.

A screen shot of a computer code

Description automatically generated

1. A close up of a text

   Description automatically generatedGoing onto GTFOBins, I found the way to get into root directory.

A screen shot of a computer screen

Description automatically generated