**Walkthrough - DC4**

1. Perform netdiscover scan.
2. A screen shot of a computer

   Description automatically generatedA black background with white text

   Description automatically generatedPerform nmap scan.

* I performed a ‘-sV’ to obtain the services running on those ports.

1. A screen shot of a computer code

   Description automatically generatedPerform Nikto scan.

* Nikto states that it found a file that contains the credentials, however I believe this is a mistake due to the fact you can append anything to the urls.

1. The webpage contains 5 different visible URLS and 2 invisible ones that must be found crawling. One of the files thankyou.php has a piece of text that changes on re-fresh (like the hint suggested). To access this you go to contact > submit.

A screenshot of a computer

Description automatically generated

* Notice the bottom says 2019, but with the thankyou.php is now was 2017. Maybe this page is vulnerable.

A close up of a computer screen

Description automatically generated

1. Notice this url. The url shows that we can use Local file Inclusion to obtain sensitive information.
   1. https://tcm-sec.com/local-file-inclusion-a-practical-guide/ (good resource)





1. Now we can use the following:

* A black background with white text

  Description automatically generatedWhich now shows you sensitive data.

A computer screen shot of a program

Description automatically generated

* I reorganised the passwd file to show it more clearly.
* <https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/> (good article)

1. A screenshot of a computer

   Description automatically generatedNext we want to use Burp Suite to capture the request for the accessing of logs.
2. A screenshot of a computer code

   Description automatically generatedNext insert the following.

* I only changed the GET request.
* Send it.

1. Now go into the web-browser and change ‘access.log’ to ‘error.’log’. At the end of log include this ‘&cmd=id’.



* If you see this, then you are successful.

1. Since the previous command worked, we can now use it to create a netcat connection.

A screenshot of a computer program

Description automatically generated

1. Upgrade to get into shell.
2. Now it was time to search for possible exploits for privilege escalation. I used the command ‘find -perm -u=s -type -f 2>/dev/null’ to find any binaries that could be useful. I found a binary called ‘screen’ which turns out to be exploitable.

A screenshot of a computer program

Description automatically generated

1. Following an searchsploit exploit.

* I couldn’t do it on the victims machine, so I had to create the files on my kali machine and set up a python simple server.
* Then I used the ‘wget’ command to download all of the necessary files.

A close-up of a computer code

Description automatically generated

1. I followed the walkthrough and I am not able to get through this stage. I realised why I am unable and I think it is because gcc on victims machine is different from mine. Since version are different the compilation is not working.

**Error**: */lib/x86\_64-linux-gnu/libc.so.6: version `GLIBC\_2.34' not found.*