**VulnHub – DC3.2**

1. Discover the target on the network. Victim: 192.168.56.112



1. Determine which ports are open, on the webserver.

A screen shot of a computer

Description automatically generated

* Port 80 is the only port that is open. I later performed other scans to ensure that all of the ports were indeed closed and this is the only one.

1. A screenshot of a computer program

   Description automatically generatedNikto shows us the following information about the web-server. It highlights that there are some directories that might be interesting and it has found a text file and an administrator login page.

* The web framework appears to be Joomla.

1. Dirsearch tool ran and found some directories that I could check out.

A screen shot of a computer program

Description automatically generated

1. Searchsploit finding a Joomla 3.7 exploit.

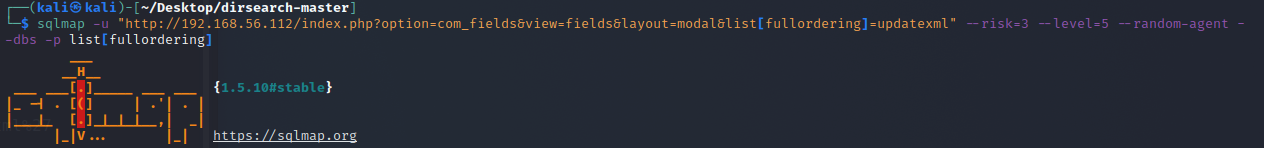
A screenshot of a computer program

Description automatically generated

A screen shot of a computer code

Description automatically generated

* I ended up modifying the file and inserting the recommended SQL map command into the sqlmap tool.

1. SQLMap of the database.

* A screen shot of a computer code

  Description automatically generatedThe result was the following databases being discovered.
* Running that same command but adding ‘--tables’ shows the databases with their associated atbles.

1. Using a modified version of the previous command, I was able to obtain the credentials of a user.

* A blurry image of a city

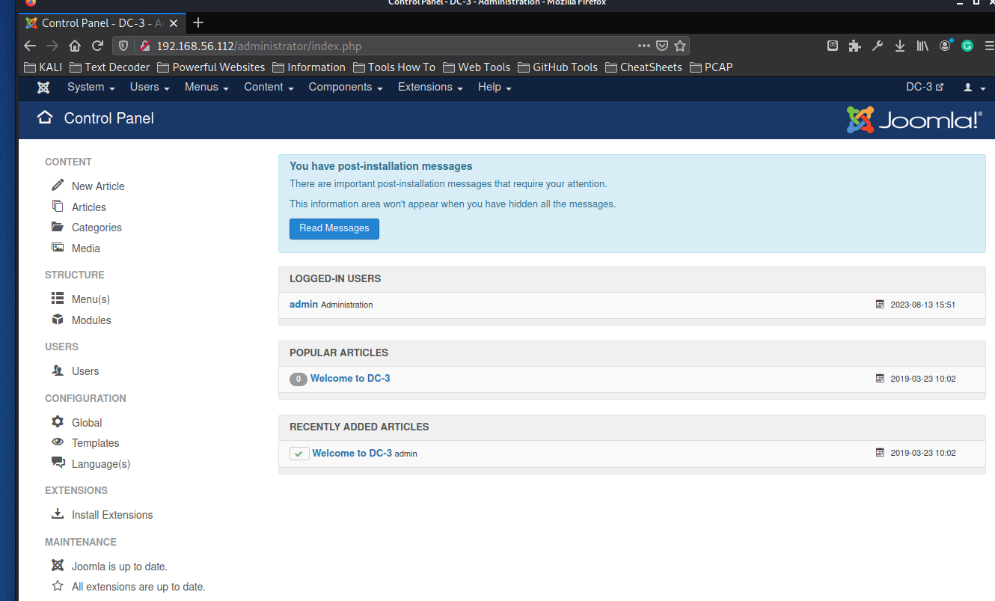
  Description automatically generatedThis took some time, however it eventually printed out the login data.

1. A screen shot of a computer

   Description automatically generatedNext, since we obtained the hash it is now time to crack it. The tool to use is john.

* The credentials are: username:admin, password:snoopy.

1. Login and the dashboard.



1. Now we need to establish a reverse shell. This is because there is no other way we can get into this server.

A screenshot of a computer

Description automatically generated

1. Once in there it was time to go into a directory to find php reverse shell.
2. A computer screen shot of a code

   Description automatically generatedOnce I had modified the file to have my ip and port, I then modified the template of the current web-server and save it.

* I then had to refresh the 192.168.56.112/index.php webpage. It was stuck on loading which meant that the reverse shell is working.

1. A computer screen shot of white text

   Description automatically generatedNow I am in the server. Ready to find the flags.
2. A screenshot of a computer

   Description automatically generatedLooking through the home directory for some flag or hints I found a hidden file.

* This is a hint that we need to get sudo privileges.

1. I looked around the system and experimented with some commands. However despite my efforts I was unable to look for any meaningful way to exploit and get sudo privs. I then decided to use ‘uname -a’ to view the kernel version and it happen to have an exploit available to obtain root privs.

* WEBSITE: <https://github.com/kkamagui/linux-kernel-exploits/tree/master>
* My first step was to transfer all of the required files onto the victims machine.

A screen shot of a computer code

Description automatically generatedA screenshot of a computer program

Description automatically generatedKali Victim

1. While attempting to run the program I realised that I didn’t give it permissions to actually run. I did a quick ‘chmod 777’ to hurry things up.

A screen shot of a computer code

Description automatically generated

* Once it executed, there were object files left. The one that required running was called ‘CVE-2016-4557’. This ran and had print statements to show you the progress of the exploit.
* A screen shot of a computer screen

  Description automatically generatedEventually the exploit worked, and I was given root privileges.

1. The flag was sitting in the root directory.

A screen shot of a computer

Description automatically generated