**VulnHub – DC4**

1. Discover host on the network. Command: sudo netdiscover -I eth1 -r 192.168.56.0/24.

A screenshot of a computer

Description automatically generated

1. Perform a nmap scan to show which ports are open. I will use the flags to prevent pings and a scan of all ports using the SYN stealth scan.

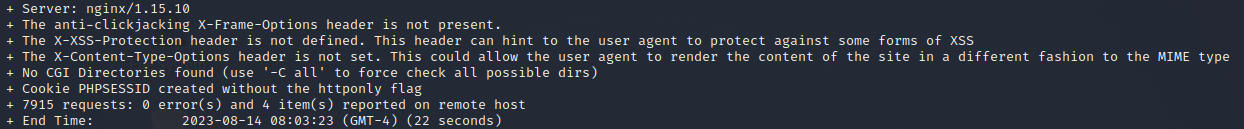


* Next, I will try and find out what services are running on these ports.





1. Time to scan for vulnerabilities. This first scan will look for any information that can be used to help with exploitation.

* There was one thing found, however nothing else was discovered. I will look into this vulnerability after a few more tools/searches.

1. Viewing the actual webpage reveals an admin login page.

A screenshot of a computer

Description automatically generated

* The page source code doesn’t reveal anything of importance.
* Attempting to enter incorrect information or sql shows no change or error on the webpage.
* A close up of a sign

  Description automatically generatedtrying to modify the url to get into a linux directory gives you a 404 error. Example: 192.168.56.113/../etc/passwd

1. I will attempt to use dir-search tool to find any webpages that could be of interest.



* However, the results lead to nothing.

1. Next use burp suite to brute force the logins. I am using the rockyou.txt to achieve this.

A screenshot of a computer

Description automatically generated

1. The password was found **username**:admin, **password**:happy.
2. Looking around the login page I can see a command link and a log out link.

A screenshot of a computer

Description automatically generated

1. A black background with text

   Description automatically generatedA screenshot of a computer program

   Description automatically generatedIt appears that I can run specific commands here. I will look at the source code to determine how they may work.

* This is very interesting because the value directly resembles a linux command. This might mean that the value in the values tag may actually execute all strings.
* A screenshot of a computer

  Description automatically generatedExactly what I mentioned earlier. I can now set up a reverse shell to get into the system.

1. A screenshot of a computer

   Description automatically generatedI modified the list command to set up net cat. This will allow me to get inside the system.



1. A computer screen shot of a computer code

   Description automatically generatedWith the attacking machine waiting and listening, run the command.

A screenshot of a computer program

Description automatically generated

* Now I am in the server.

1. Upgrade the shell.

A black background with white text

Description automatically generated

1. Going to the home directory I see 3 users.



1. Jim’s home directory a few interesting files.

A screenshot of a computer screen

Description automatically generated

* I just tried using sudo, I don’t have permissions to do so.
* Navigating into backups folder, I see a file called “old-passwords.bak”. Take this file and download it onto your machine.
* For attacker.



* For victim.
* This could mean that we have access to Jim, Charles, or Sams account for ssh.



* The password was found. Username: ‘jim’, and password: ‘jibril04’.

1. Now ssh into the machine.



A black background with white text

Description automatically generated

1. Looking at the home directory of jim I notice when I called strings on mbox there was some information about the admin to jim. I don’t know if it is significant yet.

A computer screen shot of a program

Description automatically generated

* This references a mail box. There is a mailbox located on linux in ‘/var/mail’.

1. A screenshot of a computer program

   Description automatically generatedOnce in the mailbox you can see a jim file.

* We now have Charles password.

A close up of words

Description automatically generated

1. Running ‘sudo -l’ shows that we can run ‘/usr/bin/teehee’ without sudo password. This can be used for exploitation.

* A screen shot of a computer screen

  Description automatically generatedThis can be used to append items to a file. I know this because when you call strings on this file you get a glimse of a help message.

1. Since we created a user named ‘michael’ and set the password to nothing, now we can just call ‘su michael’ and we are root.



1. Done

A screenshot of a computer

Description automatically generated