FOOTPRINTING

­­Lab-1

Summary

The FTP proxy server on host 10.129.45.17 is allowing unauthenticated access to the FTP service on port 2121. This vulnerability allows unauthorized access to the server's files and data, potentially exposing sensitive information to attackers.

Steps:

Host : 10.129.45.17

Let’s start dig which ports are open and what we got form it.

Sudo nmap -sCV -p- 10.129.45.17

-sCV is for default script and dig version information.

Graphical user interface, text, application, chat or text message

Description automatically generated -p- is for scan all port.

As we can see form scan results, here four ports are open. 21,22,53,2121

Two FTP ports are open in the system. One is proftpd and another one Is proxy ftp.

Let’s enumerate more for ftp port by using script FTP.

As we can see there is no more information, we got by using script.

Let enumerate manually.

I use wget to see what inside of proxy port.

Text

Description automatically generated wget ftp://10.129.45.17:2121/

Text

Description automatically generatedAs we can see it can connect with 2121 but login cred is wrong let use "ceil:qwer1234" which is given in hint.

As we can see that connection has been establish with cred.

Graphical user interface, text, application, chat or text message

Description automatically generatedAnd the file has been saved in INDEX.HTML, in that file there is list of other directory we can found on ftp server

Jump into ssh directory and see what we got.

Text

Description automatically generatedas we found in ssh directory, there are three file which can help to login into ssh port.

id\_rsa is a public key, which can help to get into ssh server.

For that we need to change permission of id\_rsa.

Chmod 600 id\_rsa

Let connect by using public key with username and host name.

ssh -i id\_rsa [ceil@10.129.45.17](mailto:ceil@10.129.45.17)

Text

Description automatically generated

Text

Description automatically generatedhola we are in ☺

Expected Results:

The FTP service on the target host should require authentication to access the server's files and data. The public key file id\_rsa should have restricted permissions to prevent unauthorized access.

Impact:

The vulnerability described above could potentially allow unauthorized users to access sensitive data and files on the target host, including personally identifiable information (PII) and confidential data. Attackers could leverage this vulnerability to escalate their privileges and gain unauthorized access to additional resources on the target network.