IP Infiltration Screenshots:

Pinging 172.17.4.54 to test connectivity:

A screenshot of a computer

Description automatically generated with medium confidence

Nmap 172.17.4.54 to check open ports (vulnerability scanning):

A screenshot of a computer

Description automatically generated

^We can see there are multiple ports still open, meaning we can infiltrate these ports to gain access to the IP.

^FTP & SSH means that we can gain remote access to the IP. We can also deduce that since it’s open, the ftp server was never configured and secured, so the default login could work.

^Domain & HTTP is open, meaning that we can use software’s and tools to infiltrate the domain.

Sudo nmap -O 172.17.4.54 & nmap -A 172.17.4.54 to scan for more information regarding the IP:

Text

Description automatically generated

^The MAC address is expressed.

^The operating system is expressed.

Text

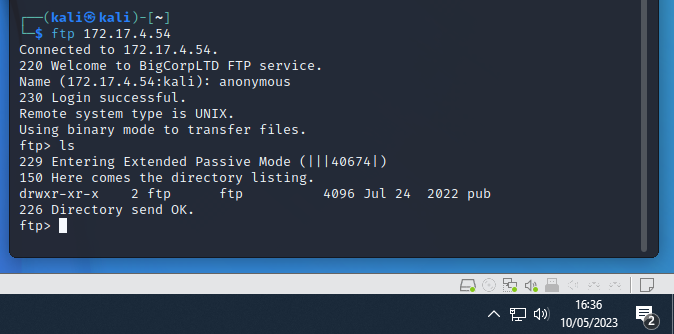
Description automatically generated

Text

Description automatically generated

^Expresses more information regarding every open ports – showing us the different mediums in which we can infiltrate.

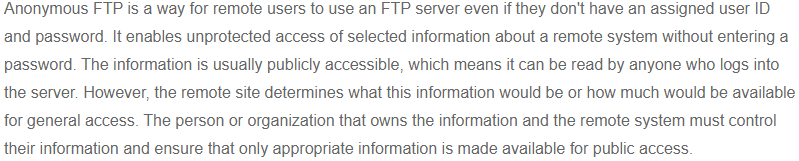
ftp 172.17.4.54 to show connectivity to the ftp server:



^We’ve managed to interact with the IP’s ftp server (remote access)

^We’ve managed to login into the ftp server with the username ‘anonymous’. This means that the ftp server is in default settings, which makes it vulnerable to attackers.

^We exercised our control within the server by using ‘ls’ command to express brief information about the IP ftp server.



^information will be limited, depending on if the IP’s user configured their information properly. It could be a case of nothing being public, or everything being public.

Graphical user interface

Description automatically generated

^ ‘ls -la’ will express all the directories

^We then change into the directory listed – ‘cd pub’ and use ‘ls -la’ to see everything within this directory.

^We use the ‘get’ command in order to download the files from the IP ftp server to our personal PC’s.

^The downloaded files contain another Flag ID and some information on the next steps to take – this being to discover the users on the IP and to check the user ‘Jerry’ specifically.

Exploit the NFS/port 2049 to steal information from the victim’s files:

A screenshot of a computer

Description automatically generated

^We must create our own directory, in order to copy and paste the relevant files.

^We then use the NFS protocol to access the victim’s files and connect them to our directory, so we can copy and steal files.

^We then change our directory to our created directory to see our files, which will actually express the victim’s files, since we have copied and stolen everything.

^We ‘cat FLAG.txt’ to see what’s in the specific files, in this case, it’s a ‘Flag ID’.

Graphical user interface, text

Description automatically generated

^After changing directories, deeper into the IP’s files, we have discovered the users.

Text

Description automatically generated

^After going deeper, we have discovered another Flag ID.

^We have discovered the new username and password for the shared machine – but we have to run the password through a de-crypter since it’s hash’d.

Graphical user interface, application, website

Description automatically generated

^After using Md5 decryption tool, we discover that the hash is ‘toortoor1’.

^this is the root password to login to the ssh server.

Text

Description automatically generated

^We are being prompted to investigate the ftp server.

Text

Description automatically generated

^Another Flag ID is obtained.

Text

Description automatically generated

SSH exploitation:

A picture containing text, electronics, screenshot, software

Description automatically generated

^SSH has been successfully exploited with the password that was decrypted and obtained from Jerry’s deleted files.

A picture containing text, electronics, screenshot, software

Description automatically generated

^Another Flag ID has been obtained.

A picture containing text, electronics, screenshot, computer

Description automatically generated

^Another Flag ID has been obtained.

Using OpenVAS on the ParrotOS ‘attacker’ VM to scan for vulnerabilities on the server:

A screenshot of a computer

Description automatically generated

^in order to open OpenVas, we need to enter the following command into the terminal: ‘sudo gvm-start’.

A screen shot of a computer

Description automatically generated with low confidence

^we enter this command in order to create a new login for the website that can be entered by opening the IP link.

A screenshot of a computer

Description automatically generated

^We go on the task wizard and insert the victim IP address and start the scan in order for OpenVas to scan for any vulnerabilities on the IP server.

A screenshot of a computer

Description automatically generated with medium confidence

^Once the task is complete, its convert to a report with a severity level reading.

A picture containing text, number, font, screenshot

Description automatically generated

^The scanned vulnerabilities are then expressed in the order of severity.

Typing in the IP into the browser:

Graphical user interface, text, application, website

Description automatically generated

^Another Flag ID has been obtained.

A screenshot of a computer

Description automatically generated with medium confidenceBurpSuite & SQLMap Injection to exploit port 80:

^ We use Burp to open the victim’s web server and inserting our own malicious code into the ‘get request’ of the server’s database.

A screenshot of a computer

Description automatically generated^Then we save this code into our own file.

^We create and insert the code into our own text file and let SQLMap scan for exploits within the username parameter ‘-p username’.

^Once it’s complete SQLMap will create a log file in which it will express all the different mediums of ‘bypassing’ the login page.

A screenshot of a computer

Description automatically generated with medium confidence

^We copy and paste any of the payloads into the username parameter and type anything for the password and proceed to bypass the login page.

A screenshot of a computer

Description automatically generated

^We discover sensitive information as well as another Flag ID.

Custom Personal Script to scan for open ports:

A screenshot of a computer program

Description automatically generated with medium confidence

^python code

A screenshot of a computer program

Description automatically generated with medium confidence

^ The port scanner in effect, identifying all the open ports available for us to exploit.