CYBERSECURITY Associates

Nmap Scan

Introduction

Nmap is an incredibly powerful tool for an ethical hacker, where it's host discovery and service scanner can be used for an extensive range of applications. Put more simply nmap provides the ethical hacker the ability to understand vital information on the target device. A good example would be a device that is operating with Apache2 software would indicate that this is a web server and a potential exploit would be different to that used against a laptop or another device. Clearly, if you don't understand the fundamentals of the target, then any exploitation would be difficult to achieve. Nmap provides some clarity and is the foundation of any hacker to understand their target and what is running on it.

When using nmap there are many different "flags" that enhance the scan and enable the discovery of large amounts of information. These flags can also be used as a defensive layer as a default nmap scan will generate a significant amount of network traffic would indicate a potential compromise.

There are 2 versions of nmap: the Command Line Interface (CLI) and Graphical User Interface (GUI) called Zenmap.

Flags used

Flag	Explanation
-sS	Syn scan, this prevents a full 3-way TCP handshake from completing reducing the network traffic and identification of your device when you are scanning
-Pn	A ping scan can be compared to shouting in a small room to find out who else is also there. This helps with network discovery but also reveals your position when you are trying to be as invisible as possible
-A	This is an aggressive scan, it performs an Operating System (OS) detection and service version detection
-sC	This is a script scan, there are 100's of scripts built into nmap, this runs the most popular scripts against the target to see if there are any obvious vulnerabilities ready for us to exploit

Walkthrough

Step 1: Power on your Kali Linux machine;

Step 2: Log in using the username:root and password:toor;

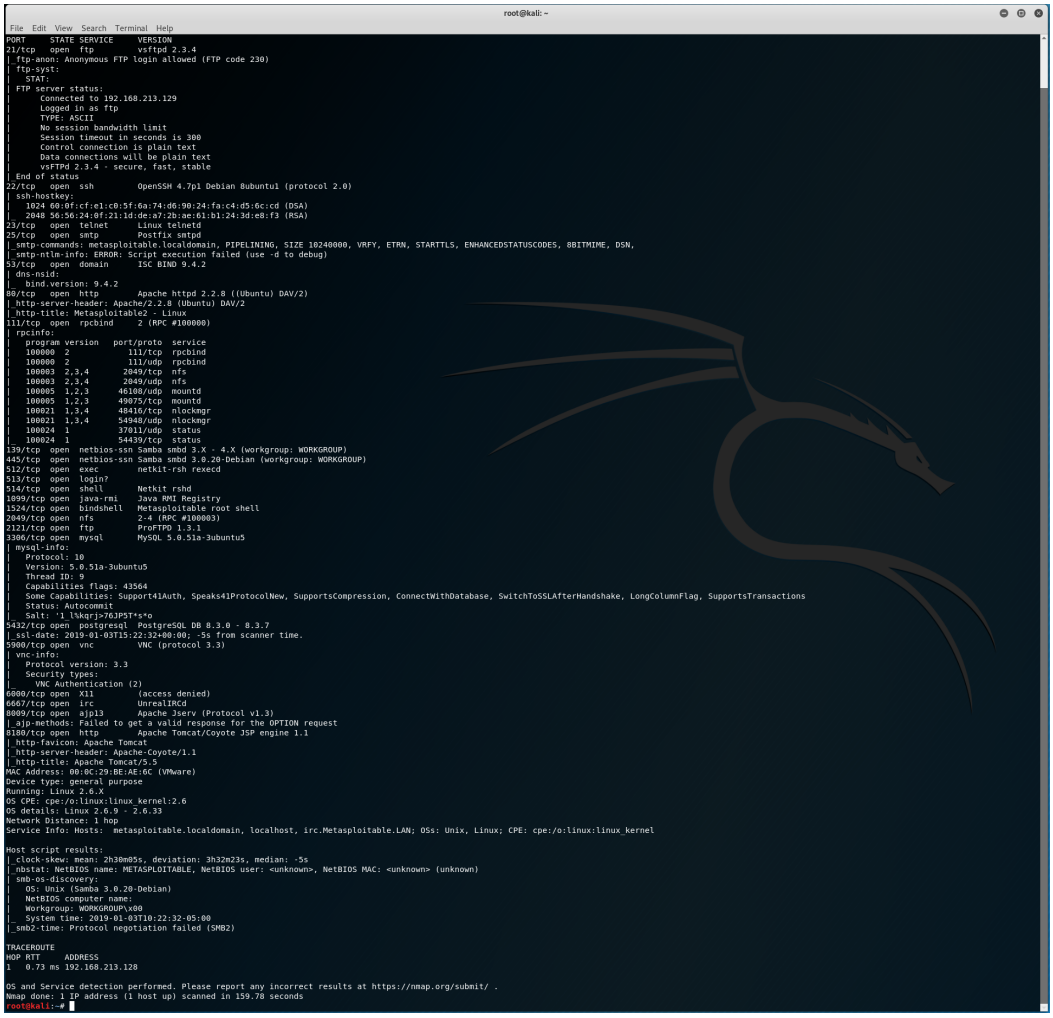
Step 4: Click on the  icon, this opens the terminal;

Step 5: Make sure you know what your target IP address is, have it written down somewhere;

Step 6: In the terminal, type nmap -sS -Pn -A -sC <target IP> and hit Enter;

Step 7: You will have to wait a little while, please be patient;

Step 8: You will have a result very similar to this;



Step 9: Make sure you study this report carefully, this information will be the foundation of all the next steps and attacks that we are able to perform.

Conclusion

Nmap is one of the fundamental capabilities of the ethical hackers toolkit. It provides a plethora of information that can mean the difference between a successful attack and one that ends in frustration. Nmap can show you what services a machine is running and provide detailed information surrounding the software versions, OS, and even surrounding network architecture. In any attack the reconnaissance and information gathering should be extensive and detailed. There are many flags that nmap can be modified to use, the flags used here are just some of the basic flags that need to be understood and used. There are even ways for nmap to get around firewalls and be used through a proxy, protecting your IP address and making you stealthy on the network.

Disclaimer

Any actions and or activities related to the material contained within this Website is solely your responsibility. The misuse of the information in this website can result in criminal charges brought against the persons in question. Cyber Security Associates Limited will not be held responsible for any criminal charges brought against any individuals misusing the information in these projects to break the law.