Hello Everyone! In this exercise, you will learn about Sparta, a network reconnaissance tool. SPARTA automates the scanning, enumeration, and vulnerability assessment processes. Apart from its scanning capabilities, SPARTA also has a built-in brute-force tool for cracking passwords.

Sparta automates scanning, information gathering, and vulnerability assessment with tools like Nikto, What Web, Nmap, Telnet, Dirbuster, and Netcat. Sparta can identify the live hosts in a network, find the services running on each host, and perform bruteforce attacks to find out default credentials for the common services such as RDP, SSH etc. It is recommended that Kali Linux is used as it already has Sparta installed, however SPARTA would most likely also work in other Linux based systems. Sparta GUI can be opened in Kali Linux directly by visiting the "Information Gathering" section in Applications or via a quick search for the app.

A brute force attack uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. an Attacker targets a specific list of usernames by making a lot of password guesses. They do this over and over again until they find a combination that matches.

Sparta is capable of password cracking through the Brute Force technique using an open-source tool Hydra. In this exercise, you will observe this. The attacker selects a username as cdac and a wordlist rockyou.txt to be used in

the attack. Wordlists in Kali Linux can be found in the /usr/share/wordlists/directory. Above Screenshot shows that the Brute force attack is successfully completed on the target IP and the valid password is Found! Here it is 123456.

Such types of password-cracking brute force attacks can be prevented by using the passwords which are found in lists of leaked and easily guessed passwords. A strong password is a combination of uppercase letters, lowercase letters, numbers, and symbols. A word that can be found in a dictionary or the name of a person, character, product, or organization should never be used as a password.

Brute force RDP attacks require hundreds, thousands or even millions of login attempts. You can slow the attacks by setting up a simple policy that locks users out after a certain number of attempts for a specified amount of time. Here's are the steps to set up an account lockout policy on Windows. Open the Start Menu Type Administrative Tools and open the program listed under 'Best Match' In the opened dialog box, double-click on Local Security Policy to open On the left-hand side, Browse to Account Policies > Account Lockout Policy Double click the policy you wish to edit Set a new value and Click OK

When scanning the Internet, hackers often look for connections that use the default RDP port (TCP 3389). It means you can essentially 'hide' your RDP connection by

changing the listening port to something else. To do so, use the Windows Registry Editor to change the registry subkey, as shown. For executing the exercise, go through the step-by-step lab manual of this exercise.

Thank You.