Network Scanning using sparta

SPARTA is a Python GUI application that simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase. It automates scanning, information gathering, and vulnerability assessment with tools like Nikto, WhatWeb, Nmap, Telnet, Dirbuster, and Netcat. It was designed with a simple point-and-click user interface and displays discovered services in an easy-to-navigate.

Installation of Sparta

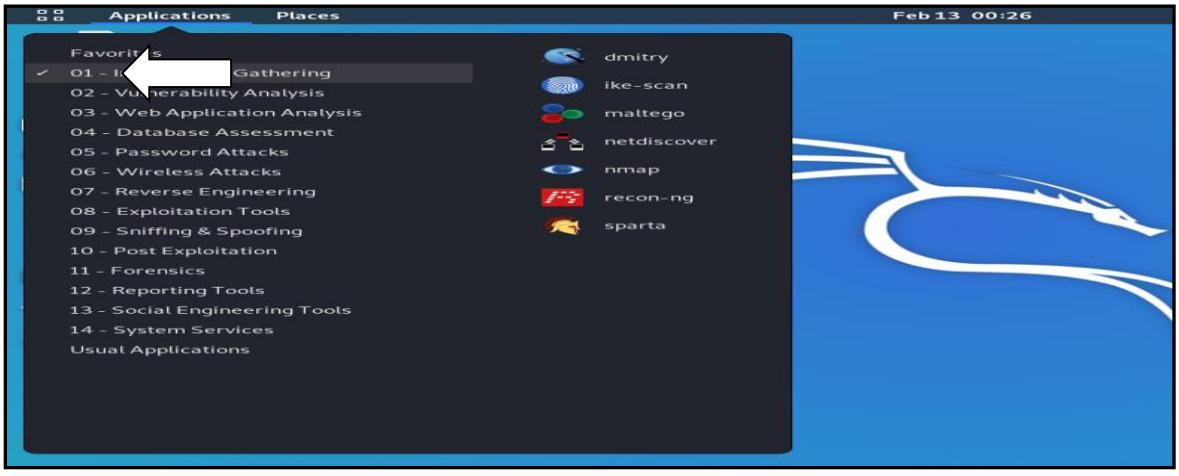
Sparta is pre-installed in most versions of Kali Linux, but lightweight Kali users need to install it following the procedure for installation.

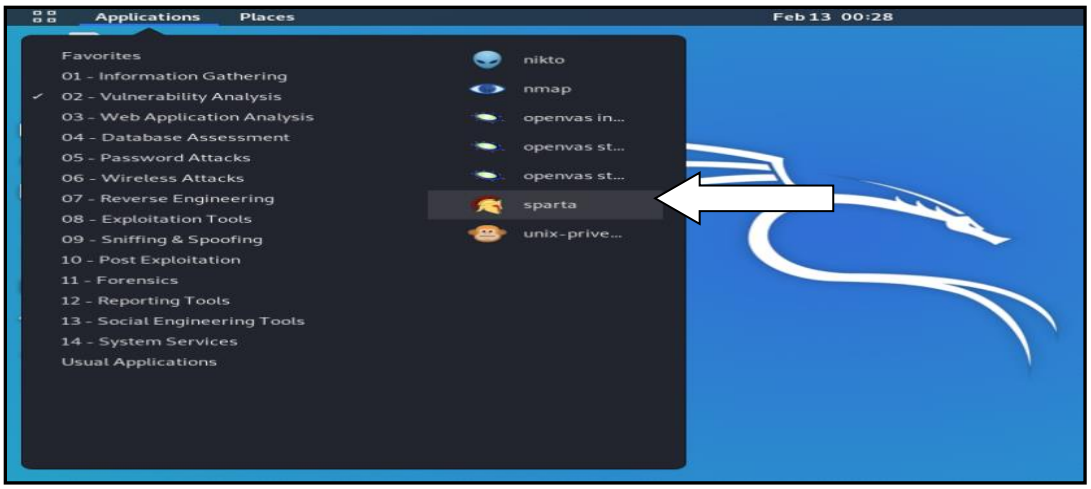
1. Open the terminal and run the command

apt-get update && apt-get install Sparta python-requests

2. 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.

Applications>Information Gathering>sparta





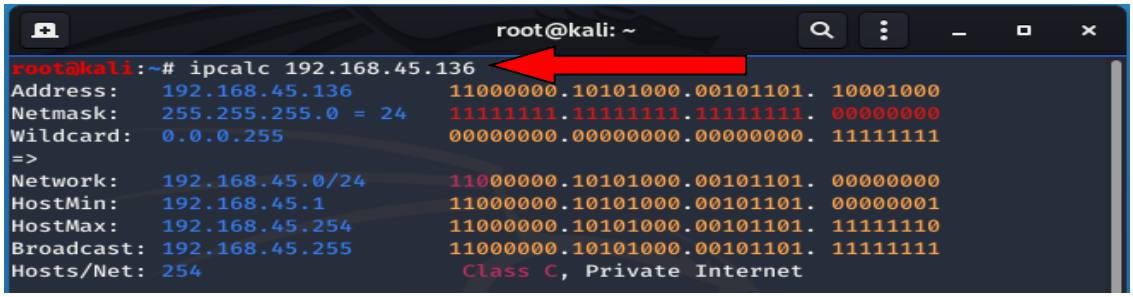
Scanning Networks with Sparta

Sparta can scan a range of IP addresses on a network, but it can also scan website domain names.

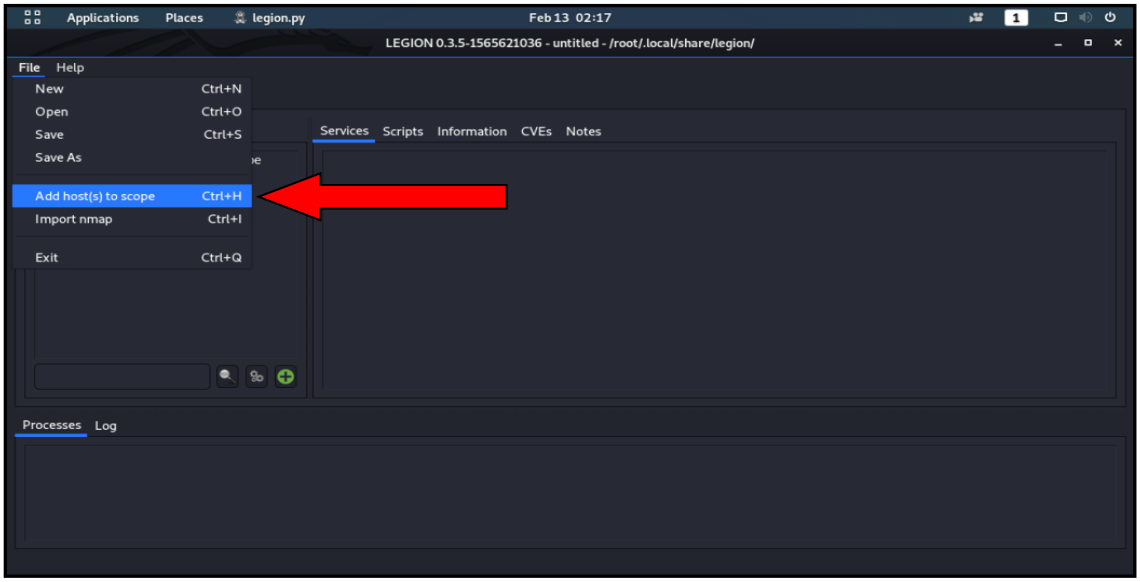
- Sparta needs a network id or a range of IPs for starting the scan. The range of IPs can be found using the following commands:

a) Ifconfig - to get the machine's IP address.

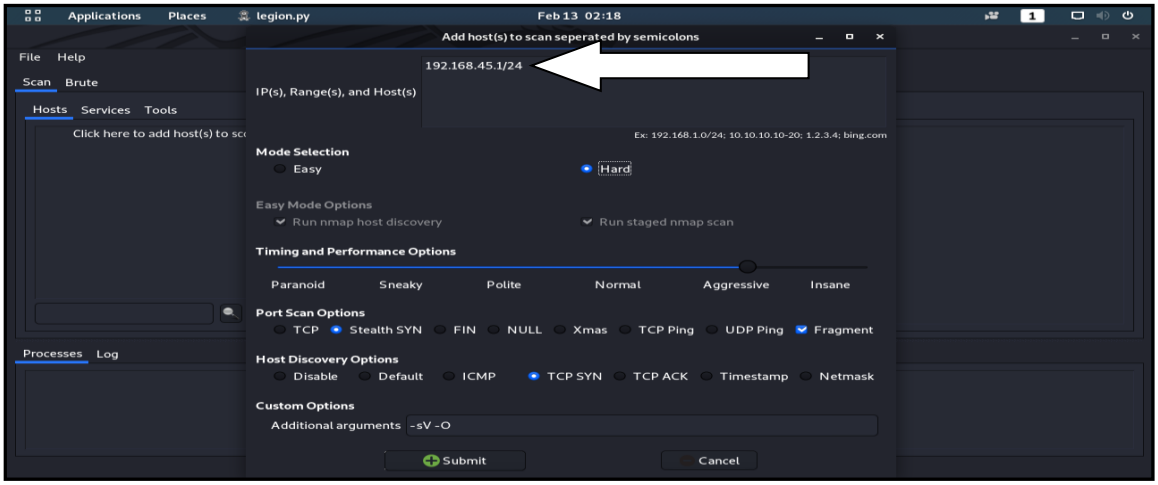
b) Ipcalc <userIPAddress>- to discover the range of IP addresses in the network.



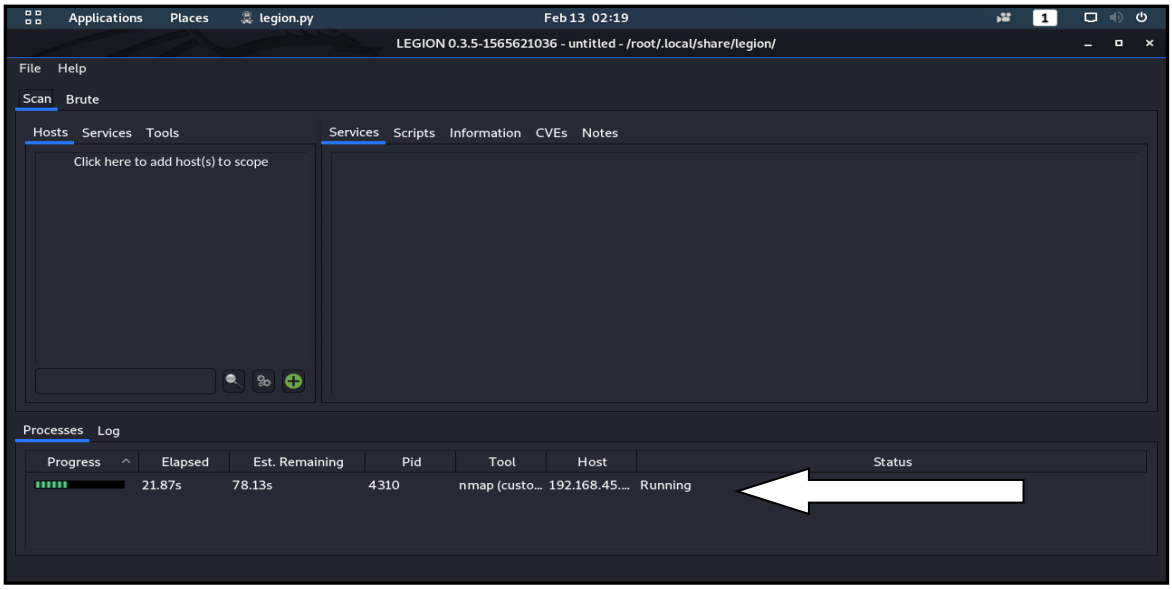
- Click on “File” and in file option click on "Add to Scope” to enter the IP range to scan.



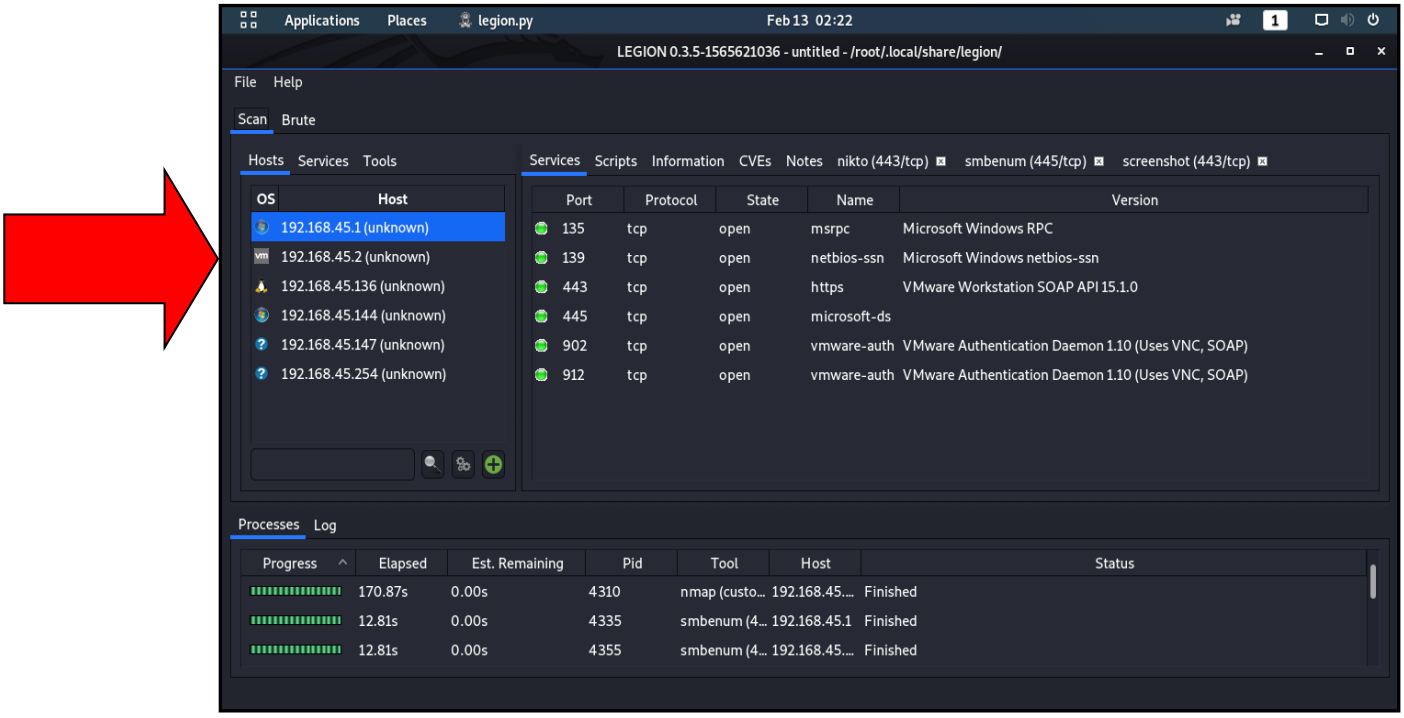
- Enter the IP address or range in the IP Range field in the Sparta prompt.



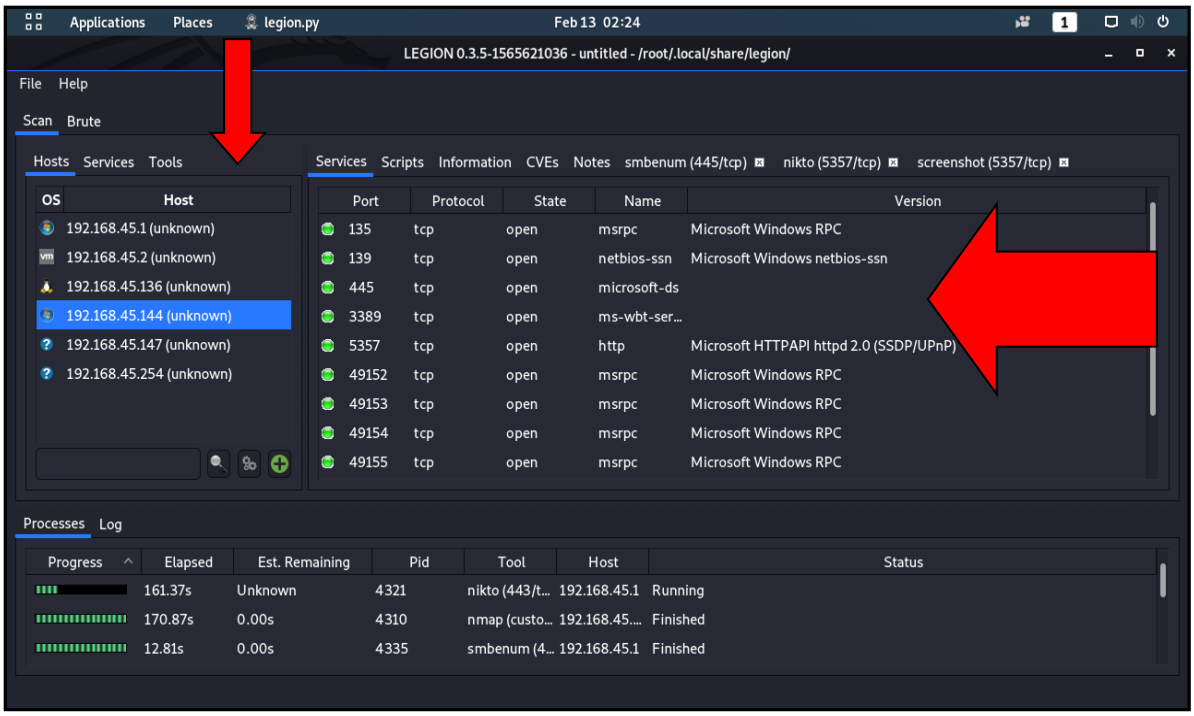
- After clicking on **Add to scope**, it automatically starts the basic process of running nmap, nikto and so on:

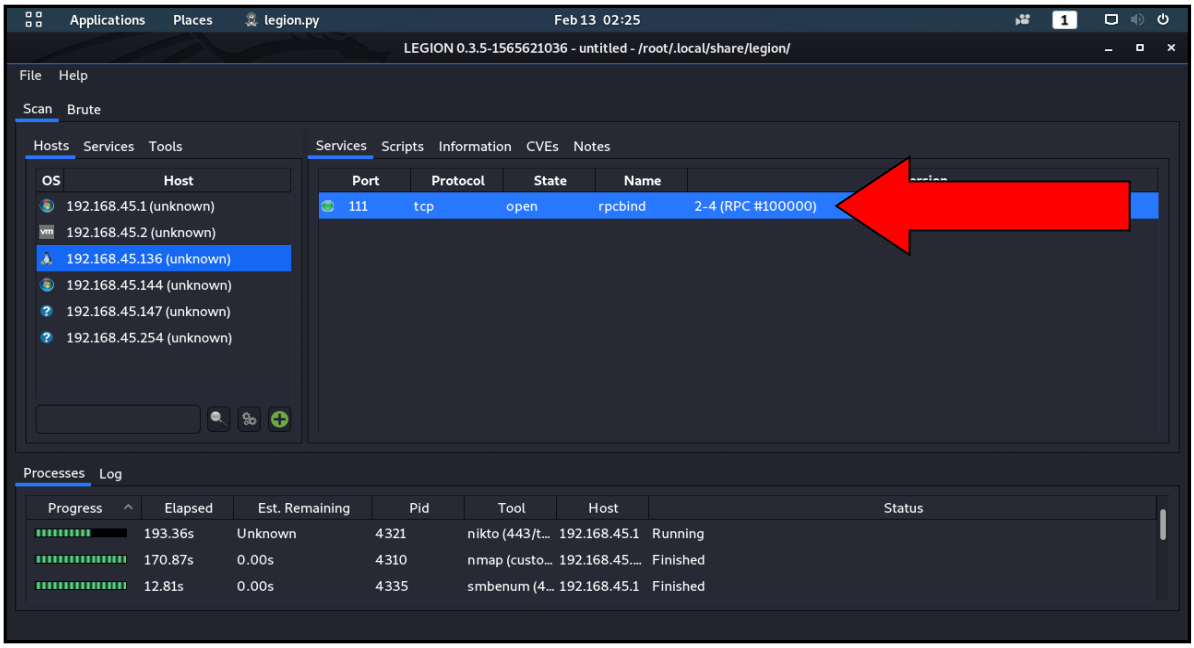


- The discovered hosts on the left-hand side pane can be seen.



- On the right-hand side, in the **Services** tab, user will see the open ports and the services they are running:





- Sparta is used for probing default ports to see if anything is open and available. After that, it runs Nmap, Nikto etc sequence of other scans looking at less common ports, and screenshots.

- By opening the “Services" tab, the services such as HTTP, HTTPS, and UDP etc can be seen; and in the "Tools" tab, the results on the target scans performed by Nikto and others can be seen specifically.

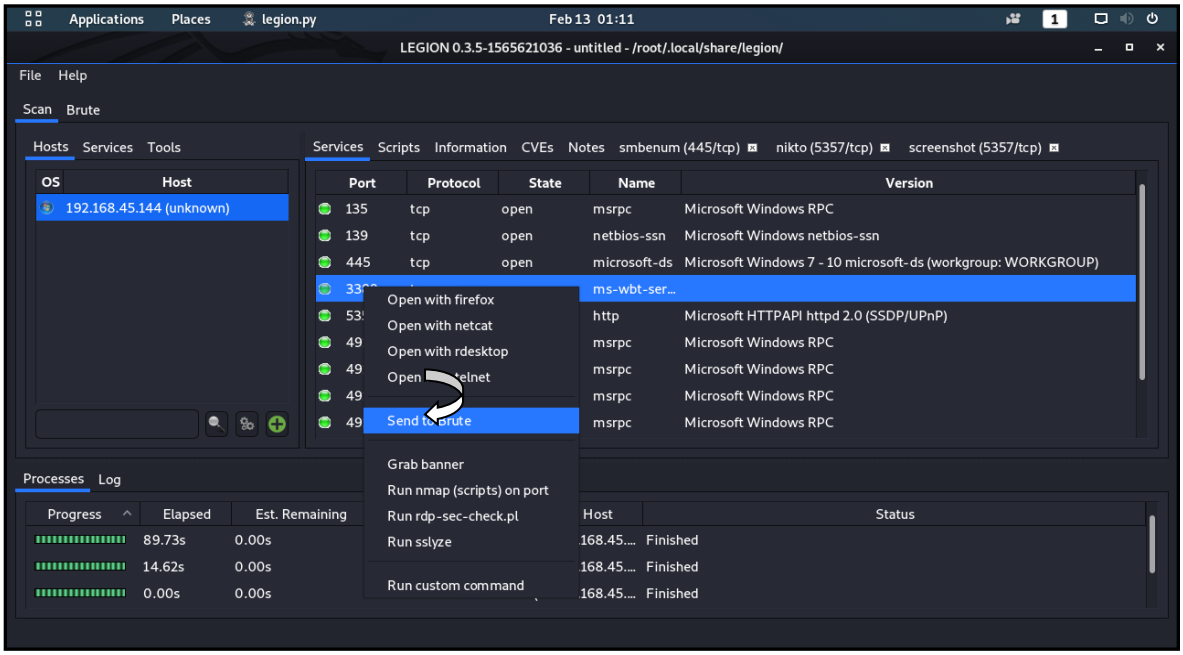
Brute force attack using Sparta

Sparta can be used to perform brute force attack on any particular service.

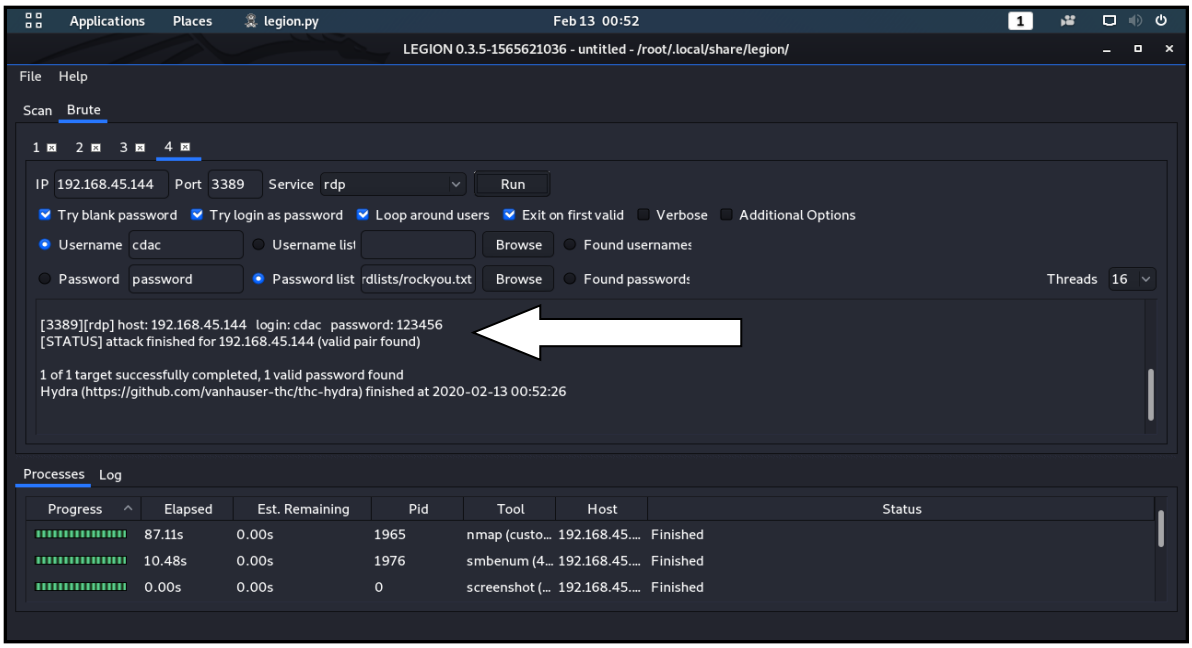
In the following image, brute force attack on rdp service has been shown.

For performing rdp brute force

a) Right-click on the rdp service
b) Select "Send to Brute" option.
c) Click on the "Brute" tab in the top left of the Sparta window.



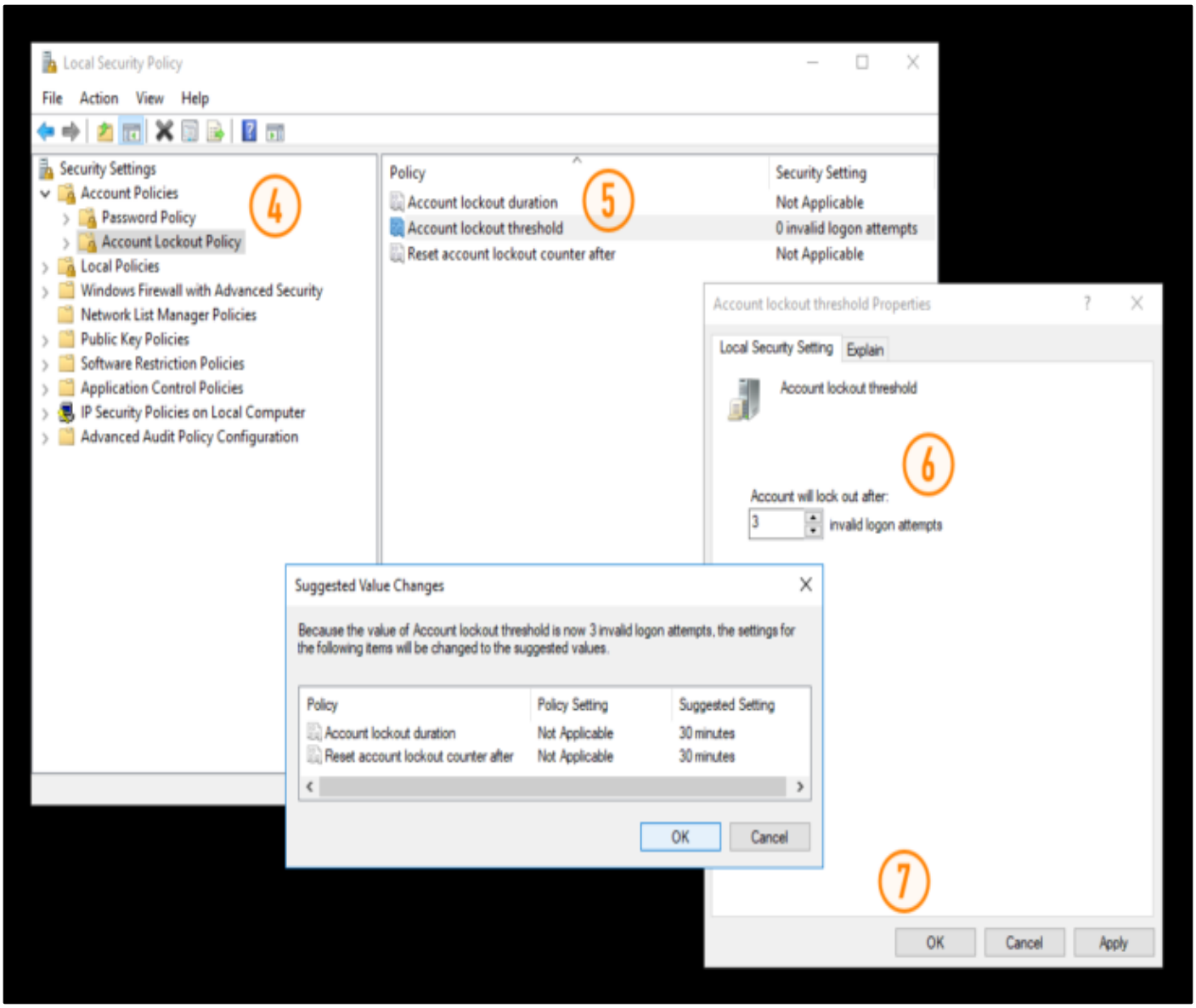
d) Select a username and wordlist to use in the attack. Wordlists in Kali Linux can be found in the /usr/share/wordlists/directory, here user use rockyou.txt which is a default text file for password. The SecLists repository and Hashes.org website also have great wordlists for penetration testers.
e) Password will be shown on the screen (if weak).



Protection against Scanning activities or Brute Force Attacks against a password

Follow the below-given steps to protect yourself from such types of activities:

1. Always use firewalls (at least host-based firewalls, such as windows defender).
2. Use Strong 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.
3. Set up policies that reject weak passwords. You can set up the policies in Windows, as given below.
    - 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



4. Hide the RDP services by changing it's default port. To do so, use the Windows Registry Editor to change the following registry subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber