

Network Scannning using sparta

Name-> Vijay Bhushan Singh

E-mail-> vijay8303blw@gmail.com

College-> Indian Institute of Information Technology, Manipur

Phone_no-> 8303420912

INSTALLATION OF SPARTA

```
172.31.102.13 - Remote Desktop Connection
Applications Places Terminal Jun 6 00:41
cdac@kali: ~
—(cdac@kali)-[~]
-$ sudo apt-get update 66 apt-get install Sparta python-requests
[sudo] password for cdac:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/non-free Sources [121 kB]
Get:3 http://kali.download/kali kali-rolling/contrib Sources [75.6 kB]
Get:4 http://kali.download/kali kali-rolling/main Sources [16.3 MB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.0 MB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [257 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [864 kB]
Fetched 84.8 MB in 15s (5,728 kB/s)
Reading package lists... Done
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?
—(cdac@kali)-[~]
```

SCANNING NETWORKS WITH SPARTA

a) ipconfig

```
(cdac@kali)-[~]
└─$ ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.31.102.13 netmask 255.255.240.0 broadcast 172.31.111.255
    inet6 fe80::526b:8dff:fe4c:53 prefixlen 64 scopeid 0x20<link>
    ether 50:9b:8d:fe:4c:53 txqueuelen 1000 (Ethernet)
    RX packets 142755 bytes 96386345 (91.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24592 bytes 113802279 (108.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

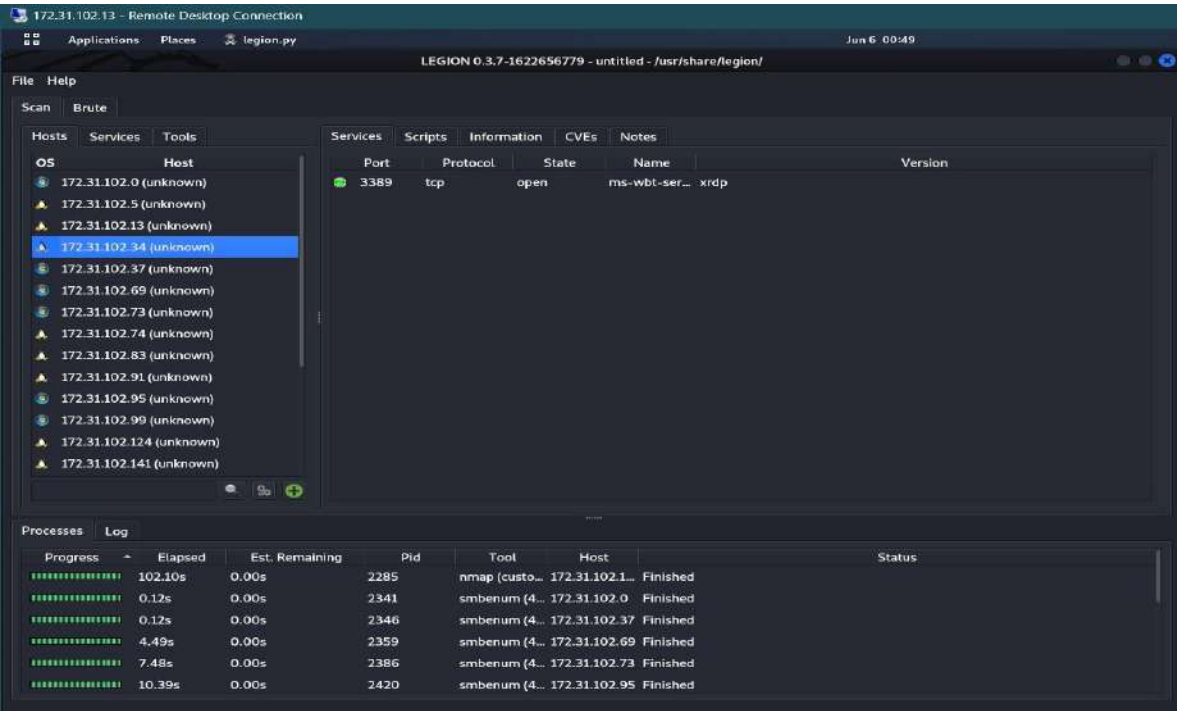
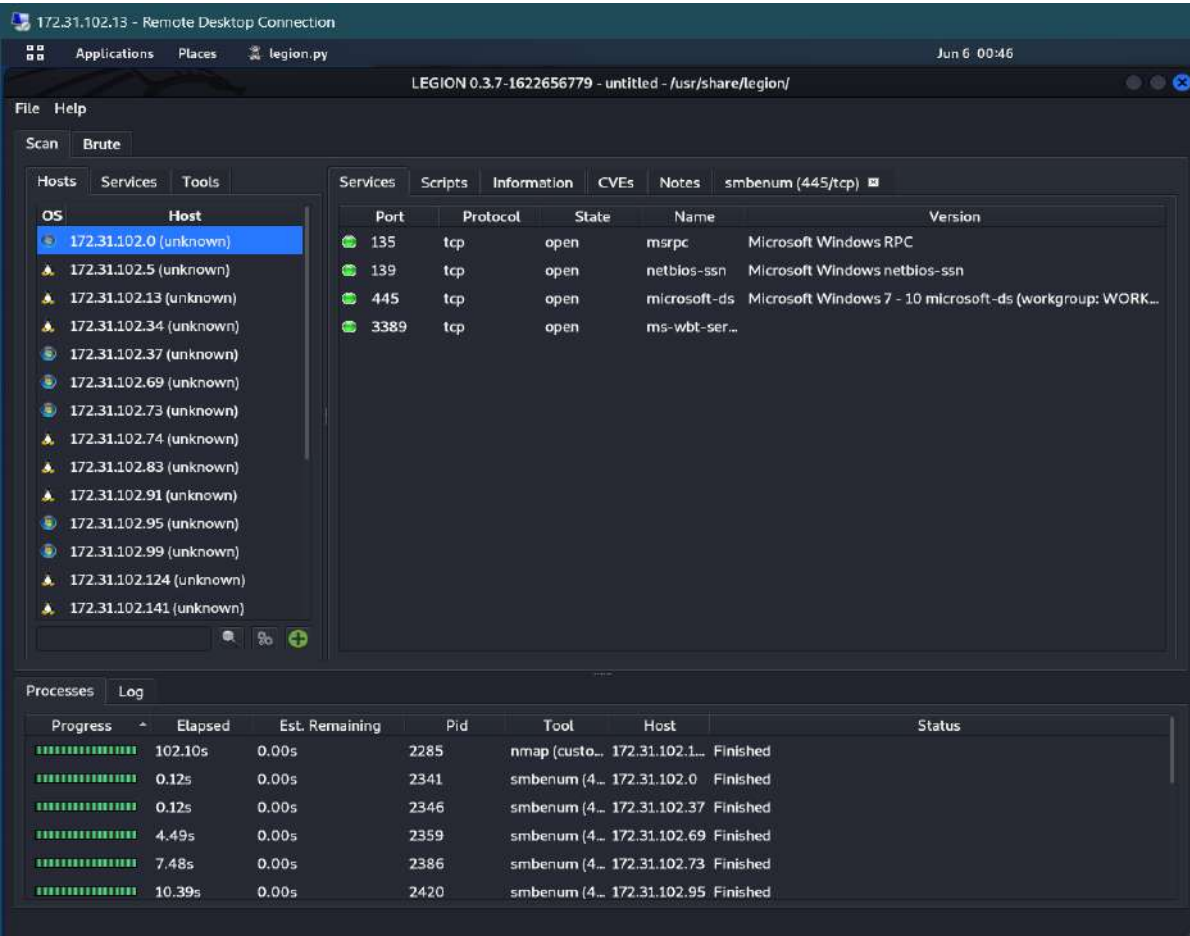
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4322 bytes 10107370 (9.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4322 bytes 10107370 (9.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

b) ipcalc <user IP>

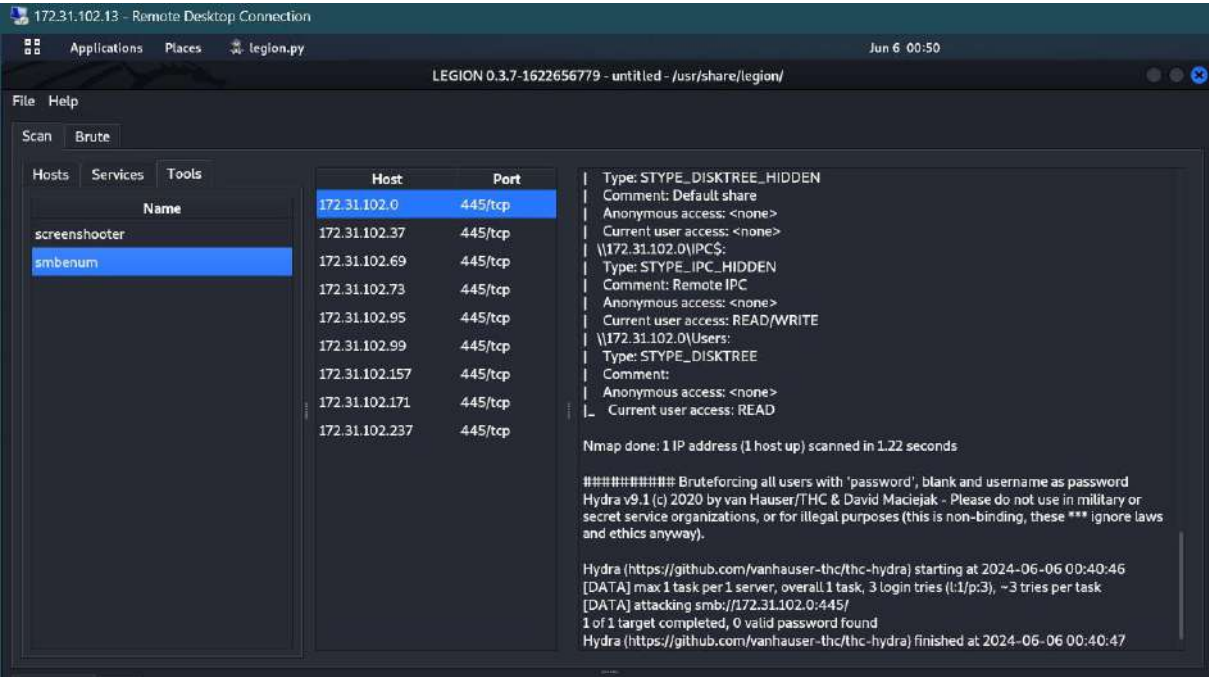
```
(cdac@kali)-[~]
└─$ ipcalc 172.31.102.13
Command 'ipcalc' not found, but can be installed with:
sudo apt install ipcalc
Do you want to install it? (N/y)y
sudo apt install ipcalc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ipcalc
0 upgraded, 1 newly installed, 0 to remove and 1950 not upgraded.
Need to get 26.3 kB of archives.
After this operation, 74.8 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ipcalc all 0.51-1 [26.3 kB]
Fetched 26.3 kB in 1s (25.9 kB/s)
Selecting previously unselected package ipcalc.
(Reading database ... 292125 files and directories currently installed.)
Preparing to unpack .../archives/ipcalc_0.51-1_all.deb ...
Unpacking ipcalc (0.51-1) ...
Setting up ipcalc (0.51-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.4.2) ...

(cdac@kali)-[~]
└─$ ipcalc 172.31.102.13
Address: 172.31.102.13      10101100.00011111.01100110. 00001101
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255        00000000.00000000.00000000. 11111111
=>
Network: 172.31.102.0/24    10101100.00011111.01100110. 00000000
HostMin: 172.31.102.1      10101100.00011111.01100110. 00000001
HostMax: 172.31.102.254    10101100.00011111.01100110. 11111110
Broadcast: 172.31.102.255  10101100.00011111.01100110. 11111111
Hosts/Net: 254              Class B, Private Internet
```

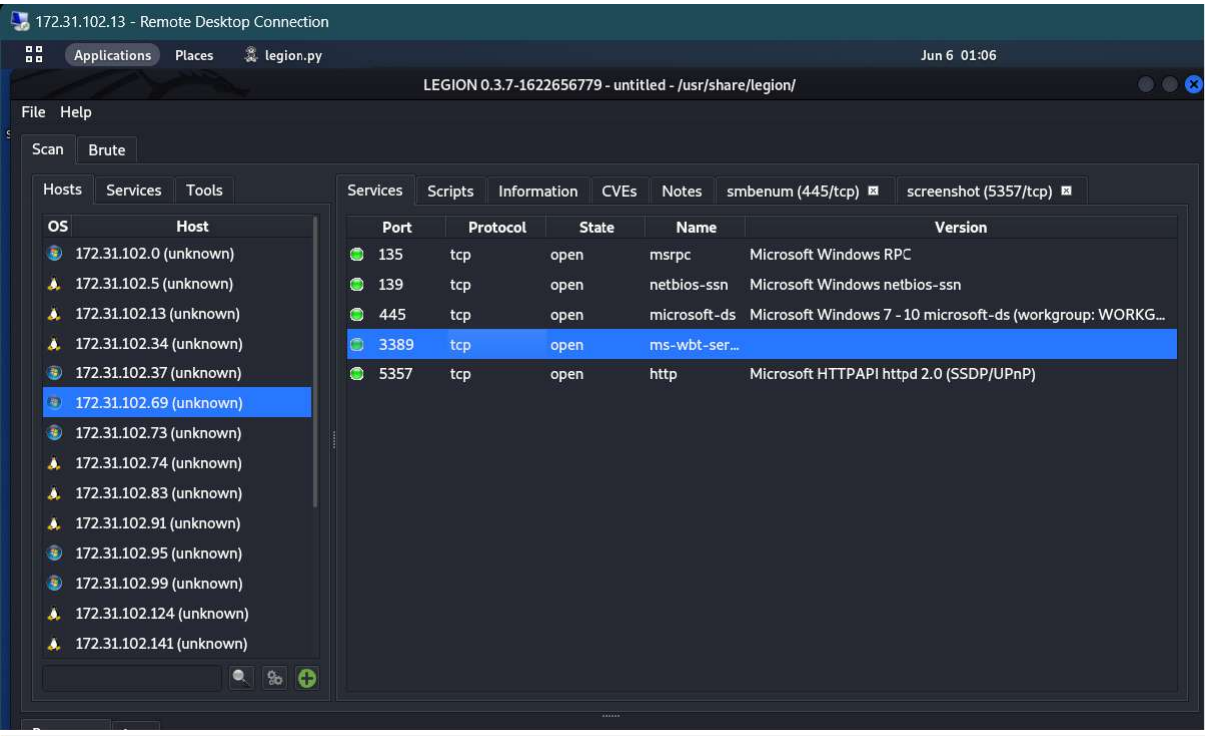
Using and configuring Sparta



In SCAN COLUMN, Tools Window

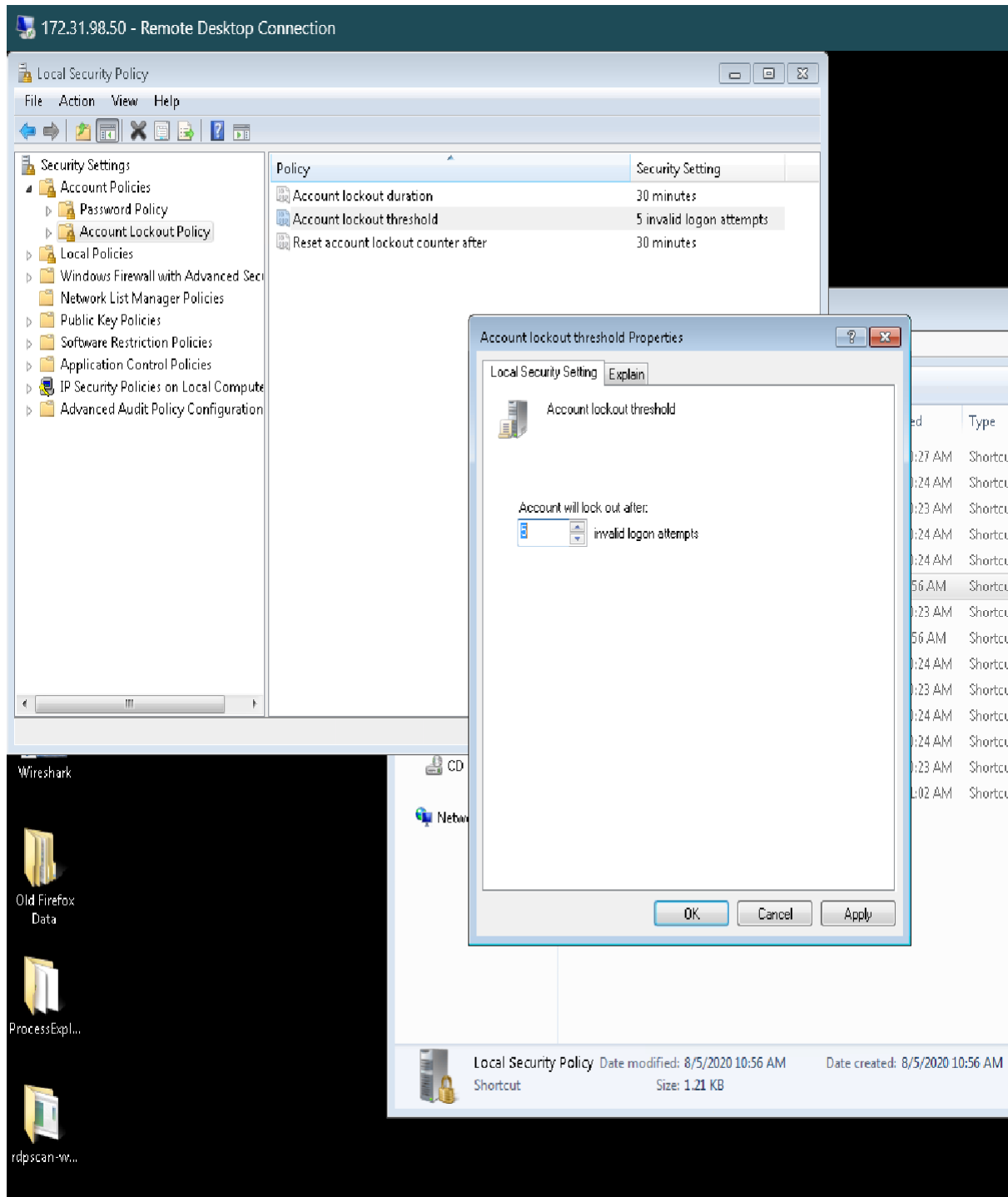


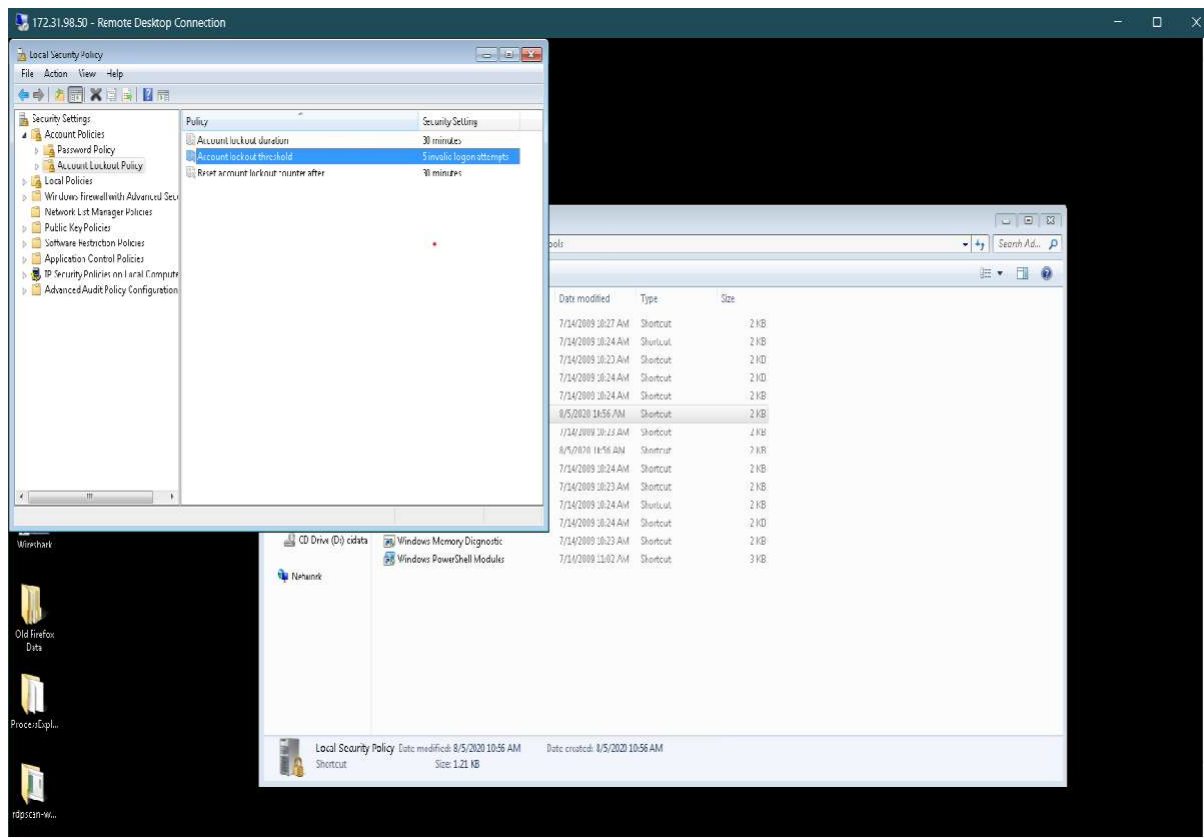
BRUTE FORCE ATTACK USING SPARTA



After clicking Send to brute, go to Brute menu & there itself attack will happen.

PROTECTION AGAINST SCANNING ACTIVITIES OR BRUTE FORCE ATTACKS AGAINST A PASSWORD





Setting up policy that rejects weak passwords.

=====