CyberGuard Toolkit

CyberGuard Toolkit is a Bash-based security scanning suite designed for Linux systems. It provides a command-line interface with a Metasploit-inspired aesthetic, using colorful output to perform network scans, local PC vulnerability checks, and security log analysis. Developed by **Wilson Goal BUGIRI**, this tool is intended for security researchers and system administrators to identify potential vulnerabilities and take action.

Operating System: Linux (tested on Ubuntu/Debian-based systems)
Privileges: Must be run as root (using sudo)

Dependencies

The following tools must be installed on your system:

nmap: For network scanning and vulnerability detection
thc-hydra: For SSH brute-force attempts
metasploit-framework: For HTTP exploitation
ss: For listing open ports
iptables: For blocking ports
grep, awk, sed: Standard Linux text-processing utilities

Install these on a Debian-based system with:

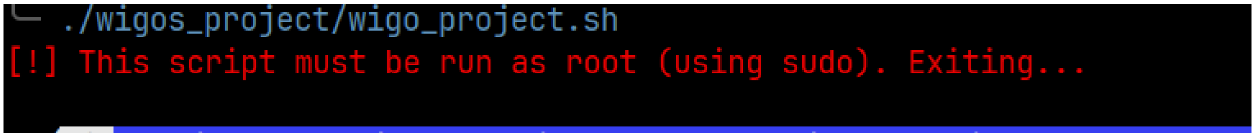
```
sudo apt update
```

sudo apt install nmap thc-hydra metasploit-framework iproute2 iptables
Optional

A wordlist like /usr/share/wordlists/rockyou.txt for Hydra (often included with Kali Linux or downloadable separately).

How to Run the Toolkit

Save the Script:
Copy the script into a file named cyberguard.sh.
Make it Executable:
chmod +x cyberguard.sh
Run with Sudo:

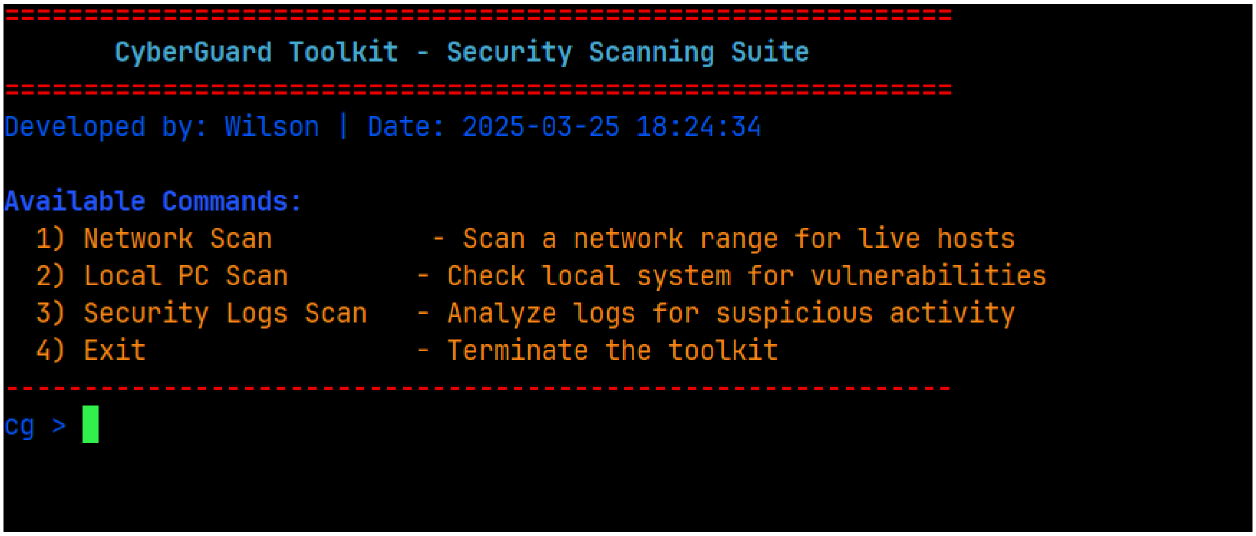


```
└─ ./wigos_project/wigo_project.sh
[!] This script must be run as root (using sudo). Exiting...
```

The script requires root privileges to access system files and execute commands like iptables.

sudo ./cyberguard.sh
How to Access: Run the script, and the main menu appears automatically.

Intended Output:



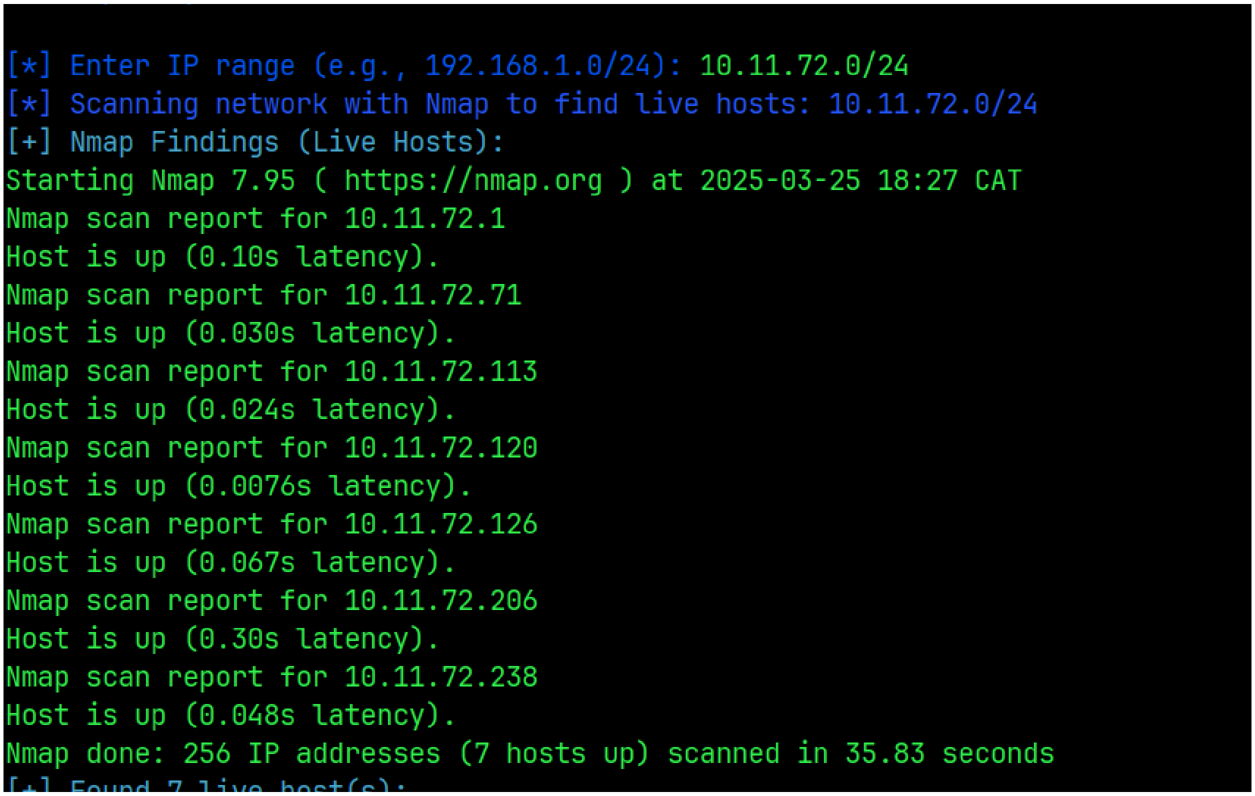
```
============================================================
       CyberGuard Toolkit - Security Scanning Suite
============================================================
Developed by: Wilson | Date: 2025-03-25 18:24:34

Available Commands:
  1) Network Scan           - Scan a network range for live hosts
  2) Local PC Scan         - Check local system for vulnerabilities
  3) Security Logs Scan    - Analyze logs for suspicious activity
  4) Exit                  - Terminate the toolkit
------------------------------------------------------------
cg > 
```

1) Network Scan

Purpose: Scans a specified IP range for live hosts and optionally checks for vulnerabilities.

How to Run:

Select 1 at the main menu.
Enter an IP range (e.g., 192.168.1.0/24) when prompted.
Choose whether to scan for vulnerabilities (y/n).



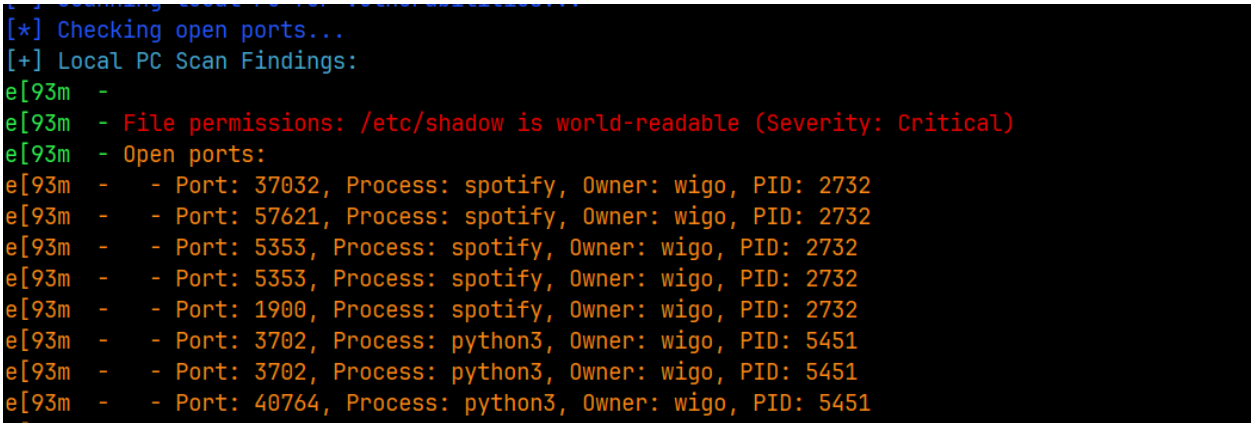
```
[*] Enter IP range (e.g., 192.168.1.0/24): 10.11.72.0/24
[*] Scanning network with Nmap to find live hosts: 10.11.72.0/24
[+] Nmap Findings (Live Hosts):
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 18:27 CAT
Nmap scan report for 10.11.72.1
Host is up (0.10s latency).
Nmap scan report for 10.11.72.71
Host is up (0.030s latency).
Nmap scan report for 10.11.72.113
Host is up (0.024s latency).
Nmap scan report for 10.11.72.120
Host is up (0.0076s latency).
Nmap scan report for 10.11.72.126
Host is up (0.067s latency).
Nmap scan report for 10.11.72.206
Host is up (0.30s latency).
Nmap scan report for 10.11.72.238
Host is up (0.048s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 35.83 seconds
[+] Found 7 live host(s):
```

2) Local PC Scan

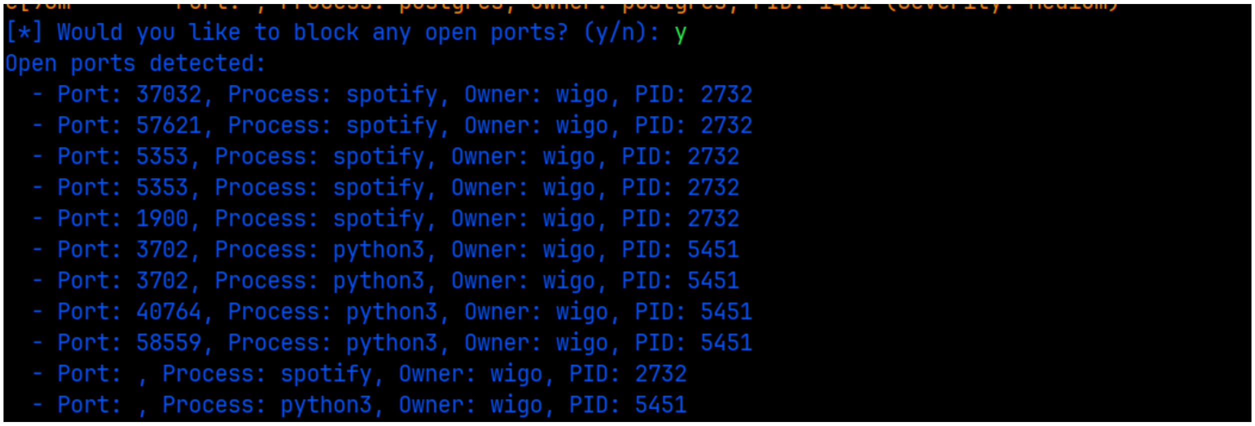
Purpose: Checks the local system for vulnerabilities like readable sensitive files and open ports.

How to Run: Select 2 at the main menu.

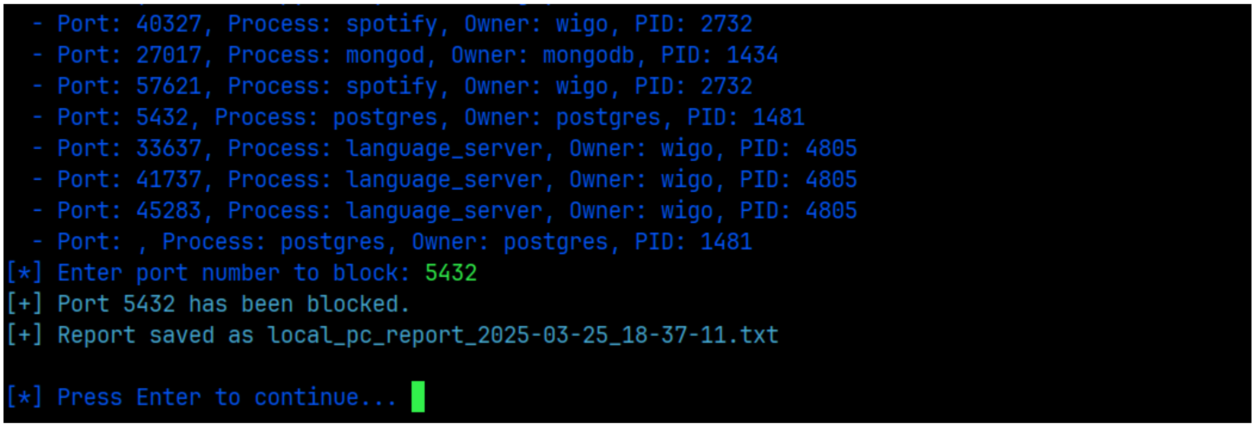
Intended Output:



```
[*] Scanning local PC for vulnerabilities...
[*] Checking open ports...
[+] Local PC Scan Findings:
e[93m  -
e[93m  - File permissions: /etc/shadow is world-readable (Severity: Critical)
e[93m  - Open ports:
e[93m  -   - Port: 37032, Process: spotify, Owner: wigo, PID: 2732
e[93m  -   - Port: 57621, Process: spotify, Owner: wigo, PID: 2732
e[93m  -   - Port: 5353, Process: spotify, Owner: wigo, PID: 2732
e[93m  -   - Port: 5353, Process: spotify, Owner: wigo, PID: 2732
e[93m  -   - Port: 1900, Process: spotify, Owner: wigo, PID: 2732
e[93m  -   - Port: 3702, Process: python3, Owner: wigo, PID: 5451
e[93m  -   - Port: 3702, Process: python3, Owner: wigo, PID: 5451
e[93m  -   - Port: 40764, Process: python3, Owner: wigo, PID: 5451
```



```
e[93m        Port: , Process: postgres, Owner: postgres, PID: 1481 (Severity: Medium)
[*] Would you like to block any open ports? (y/n): y
Open ports detected:
  - Port: 37032, Process: spotify, Owner: wigo, PID: 2732
  - Port: 57621, Process: spotify, Owner: wigo, PID: 2732
  - Port: 5353, Process: spotify, Owner: wigo, PID: 2732
  - Port: 5353, Process: spotify, Owner: wigo, PID: 2732
  - Port: 1900, Process: spotify, Owner: wigo, PID: 2732
  - Port: 3702, Process: python3, Owner: wigo, PID: 5451
  - Port: 3702, Process: python3, Owner: wigo, PID: 5451
  - Port: 40764, Process: python3, Owner: wigo, PID: 5451
  - Port: 58559, Process: python3, Owner: wigo, PID: 5451
  - Port: , Process: spotify, Owner: wigo, PID: 2732
  - Port: , Process: python3, Owner: wigo, PID: 5451
```



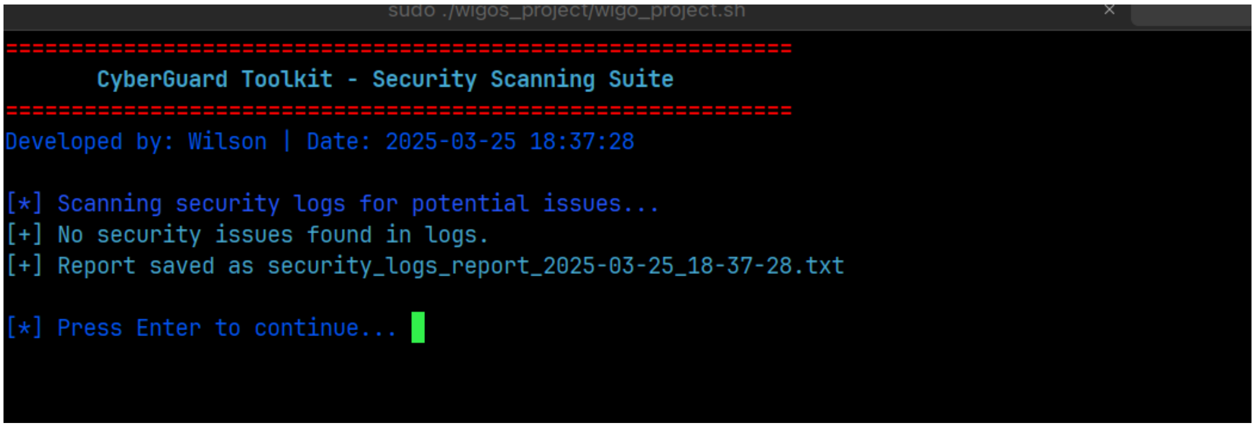
```
  - Port: 40327, Process: spotify, Owner: wigo, PID: 2732
  - Port: 27017, Process: mongod, Owner: mongodb, PID: 1434
  - Port: 57621, Process: spotify, Owner: wigo, PID: 2732
  - Port: 5432, Process: postgres, Owner: postgres, PID: 1481
  - Port: 33637, Process: language_server, Owner: wigo, PID: 4805
  - Port: 41737, Process: language_server, Owner: wigo, PID: 4805
  - Port: 45283, Process: language_server, Owner: wigo, PID: 4805
  - Port: , Process: postgres, Owner: postgres, PID: 1481
[*] Enter port number to block: 5432
[+] Port 5432 has been blocked.
[+] Report saved as local_pc_report_2025-03-25_18-37-11.txt

[*] Press Enter to continue...
```

3) Security Logs Scan

Purpose: Analyzes /var/log/auth.log and /var/log/syslog for suspicious activity (e.g., failed logins, risky commands).

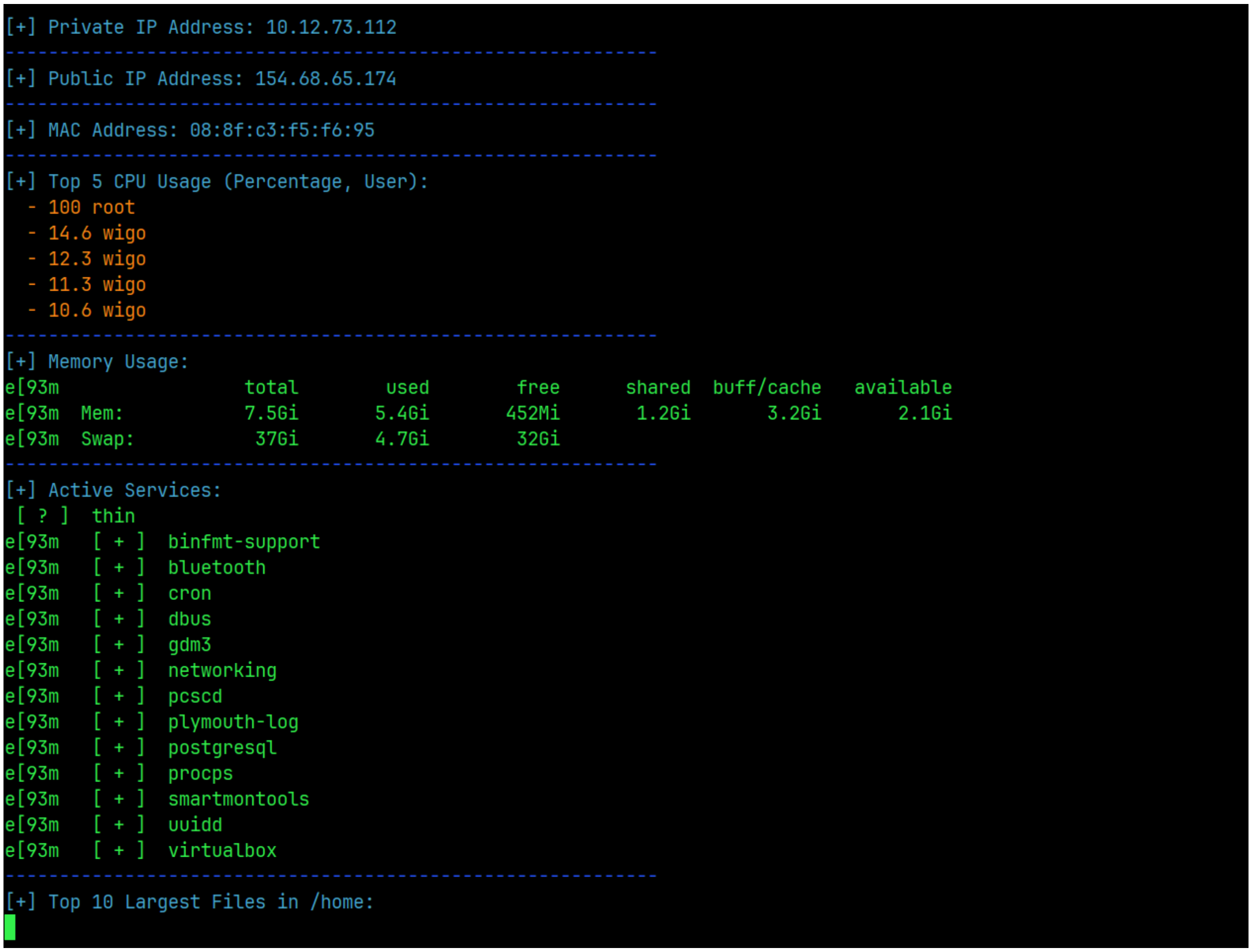
How to Run: Select 3 at the main menu.

Intended Output:

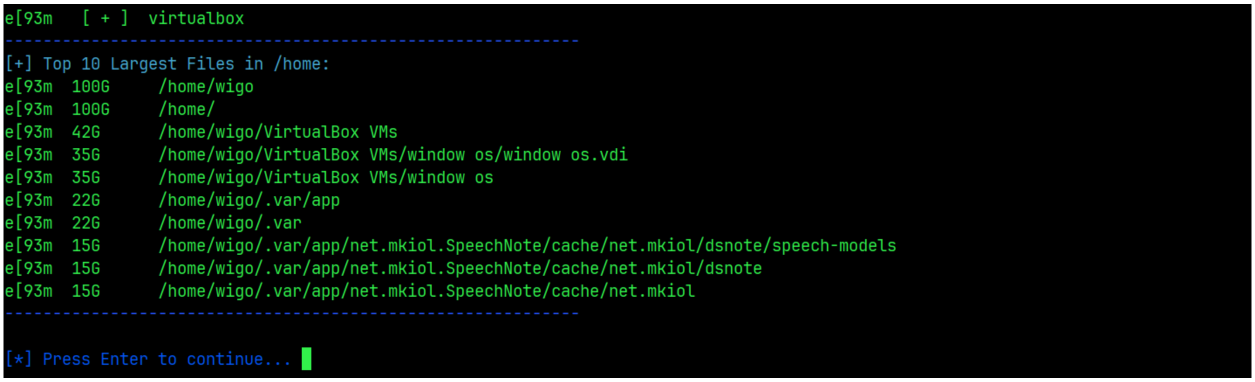


```
============================================================
       CyberGuard Toolkit - Security Scanning Suite
============================================================
Developed by: Wilson | Date: 2025-03-25 18:37:28

[*] Scanning security logs for potential issues...
[+] No security issues found in logs.
[+] Report saved as security_logs_report_2025-03-25_18-37-28.txt

[*] Press Enter to continue...
```

4)System info
Purpose : check system all info



```
[+] Private IP Address: 10.12.73.112
------------------------------------------------------------
[+] Public IP Address: 154.68.65.174
------------------------------------------------------------
[+] MAC Address: 08:8f:c3:f5:f6:95
------------------------------------------------------------
[+] Top 5 CPU Usage (Percentage, User):
  - 100 root
  - 14.6 wigo
  - 12.3 wigo
  - 11.3 wigo
  - 10.6 wigo
------------------------------------------------------------
[+] Memory Usage:
e[93m                 total        used        free      shared  buff/cache   available
e[93m  Mem:           7.5Gi       5.4Gi       452Mi       1.2Gi       3.2Gi       2.1Gi
e[93m  Swap:           37Gi       4.7Gi        32Gi
------------------------------------------------------------
[+] Active Services:
 [ ? ]  thin
e[93m   [ + ]  binfmt-support
e[93m   [ + ]  bluetooth
e[93m   [ + ]  cron
e[93m   [ + ]  dbus
e[93m   [ + ]  gdm3
e[93m   [ + ]  networking
e[93m   [ + ]  pcscd
e[93m   [ + ]  plymouth-log
e[93m   [ + ]  postgresql
e[93m   [ + ]  procps
e[93m   [ + ]  smartmontools
e[93m   [ + ]  uuidd
e[93m   [ + ]  virtualbox
------------------------------------------------------------
[+] Top 10 Largest Files in /home:
```



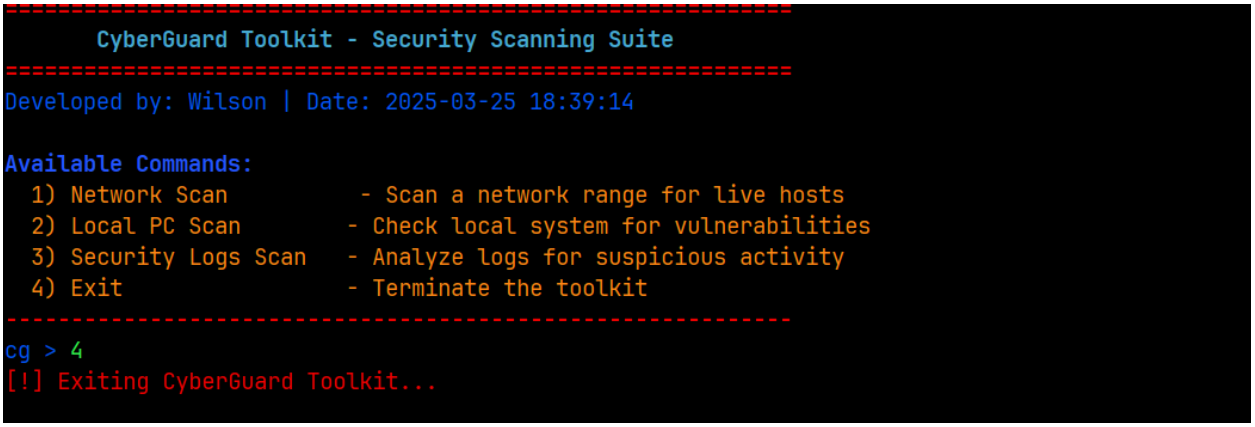
```
e[93m   [ + ]  virtualbox
------------------------------------------------------------
[+] Top 10 Largest Files in /home:
e[93m  100G     /home/wigo
e[93m  100G     /home/
e[93m  42G      /home/wigo/VirtualBox VMs
e[93m  35G      /home/wigo/VirtualBox VMs/window os/window os.vdi
e[93m  35G      /home/wigo/VirtualBox VMs/window os
e[93m  22G      /home/wigo/.var/app
e[93m  22G      /home/wigo/.var
e[93m  15G      /home/wigo/.var/app/net.mkiol.SpeechNote/cache/net.mkiol/dsnote/speech-models
e[93m  15G      /home/wigo/.var/app/net.mkiol.SpeechNote/cache/net.mkiol/dsnote
e[93m  15G      /home/wigo/.var/app/net.mkiol.SpeechNote/cache/net.mkiol
------------------------------------------------------------

[*] Press Enter to continue...
```

5) Exit

Purpose: Terminates the toolkit.

How to Run: Select 4 at the main menu.

Intended Output:



```
============================================================
       CyberGuard Toolkit - Security Scanning Suite
============================================================
Developed by: Wilson | Date: 2025-03-25 18:39:14

Available Commands:
  1) Network Scan          - Scan a network range for live hosts
  2) Local PC Scan        - Check local system for vulnerabilities
  3) Security Logs Scan   - Analyze logs for suspicious activity
  4) Exit                 - Terminate the toolkit
------------------------------------------------------------
cg > 4
[!] Exiting CyberGuard Toolkit...
```