StealthCup 2025: Reconnaissance Cheatsheet

This cheatsheet focuses on reconnaissance techniques optimized for stealth, minimizing the risk of triggering alerts from IDS, SIEM, and EDR solutions within the StealthCup environment.

Primary Goal: Gather information about the target network (`10.0.x.0/24`) without being detected.

1. Initial Kali Box Enumeration

Before conducting external reconnaissance, thoroughly examine your initial foothold (the Kali box implant deployed by "Danilo").

- **System Configuration**: Understand your starting position and available resources.
    - **Commands**:

```
# Network configuration
ip a
ip route
cat /etc/resolv.conf

# Running services
ss -tuln
netstat -antup

# System information
uname -a
cat /etc/os-release
```

    - **Evasion Tip**: These commands are standard system checks and unlikely to trigger alerts.
- **Analyze Existing Data**: Check the Kali box for any pre-existing data, logs, or configuration files left by "Danilo".
    - **Commands**:

```
# Check command history
history
cat ~/.bash_history

# Look for interesting files
ls -la /home /tmp /var/log
find / -type f -mtime -7 2>/dev/null

# Check for stored credentials
find / -name "id_rsa*" -o -name "*.pem" -o -name "*.key" 2>/dev/null
grep -r "password" --include="*.txt" --include="*.conf" /home/ /etc/
2>/dev/null
```

- **Evasion Tip**: File system operations on your own Kali box are unlikely to trigger network alerts.

- **Existing Connections**: Identify established connections that might reveal targets.
  - **Commands**:

```
# Check current connections
ss -antup
netstat -antup

# Check routing table for network segments
ip route
route -n
```

  - **Evasion Tip**: Analyzing existing connections provides valuable information without generating new traffic.

2. Passive Reconnaissance (Zero Noise)

These techniques involve listening only and generate no network traffic from your Kali box.

- **Network Sniffing**: Capture traffic on the local segment to identify hosts, services, and communication patterns.
  - **Tools**: `tcpdump`, `wireshark` (tshark CLI)
  - **Example (`tcpdump`)**:

```
# Capture traffic on eth0, don't resolve names (-n), don't use
promiscuous mode initially
sudo tcpdump -i eth0 -n -p not arp and not icmp
# Filter for specific protocols (e.g., LDAP, SMB)
sudo tcpdump -i eth0 -n -p 'port 389 or port 139 or port 445'
```

  - **Evasion Tip**: Avoid promiscuous mode (`-p`) initially if possible, as it can sometimes be detected. Analyze captured PCAPs offline.

- **Protocol-Specific Monitoring**: Target industrial and enterprise protocols.
  - **Example (OT Protocol Monitoring)**:

```
# Monitor for Modbus TCP traffic
sudo tcpdump -i eth0 -n 'port 502' -w modbus.pcap

# Monitor for common ICS protocols
sudo tcpdump -i eth0 -n 'port 502 or port 102 or port 44818 or port
20000 or port 47808' -w ics_traffic.pcap
```

- **Evasion Tip**: Passive monitoring doesn't generate traffic. Analyze captured PCAPs offline to identify control systems, protocols, and communication patterns.

- **ARP Table Analysis**: Examine local ARP cache to identify hosts.
  - **Commands**:

```
# View ARP table
arp -a
ip neigh

# Look for specific device types
arp -a | grep -i "phoenix"  # May identify PLC devices
```

  - **Evasion Tip**: Reading local ARP tables generates no network traffic.

3. Targeted Reconnaissance for Specific Objectives

AD Environment Discovery

- **Domain Controller Identification**: Locate DCs without active scanning.
  - **Passive Methods**:

```
# Parse from DNS or DHCP configuration
grep -i "domain" /etc/resolv.conf

# Listen for broadcast domain announcements
sudo tcpdump -i eth0 -n 'udp port 389 or port 88'

# Monitor for Kerberos traffic
sudo tcpdump -i eth0 -n 'port 88'
```

  - **Evasion Tip**: Listening for broadcast traffic is completely passive and generates no alerts.

- **Domain User Enumeration**: Identify domain users without aggressive querying.
  - **Low-Noise Methods**:

```
# If SMB access is available
rpcclient -U "" -N <dc_ip>
rpcclient $> enumdomusers

# Using LDAP with valid credentials (if available)
ldapsearch -x -h <dc_ip> -D '<username>@<domain>' -w '<password>' -b
'DC=<domain>,DC=<tld>' '(objectClass=user)'
```

- **Evasion Tip**: Use valid credentials when possible. Limit queries to specific information needed.

OT Environment Discovery

- **PLC and SCADA Component Identification**: Identify OT components passively.
  - **Passive Methods**:

```
# Listen for industrial protocols
sudo tcpdump -i eth0 -n 'port 502 or port 102 or port 44818 or port
20000 or port 47808'

# Analyze ARP tables for potential OT devices
arp -a | grep -i "phoenix"
```

  - **Evasion Tip**: Phoenix Contact PLCs often have identifiable MAC address prefixes or hostnames.
- **Historian and HMI Discovery**: Locate historian databases and HMI interfaces.
  - **Passive Methods**:

```
# Monitor for database traffic
sudo tcpdump -i eth0 -n 'port 1433 or port 3306 or port 5432'

# Look for web interfaces (HMI often uses web)
sudo tcpdump -i eth0 -n 'port 80 or port 443 or port 8080'
```

  - **Evasion Tip**: Many modern SCADA/HMI systems use web interfaces on standard or custom ports.

4. Low-Noise Active Reconnaissance

These techniques involve sending traffic but are designed to be less intrusive than standard scans.

- **Targeted Port Scanning (Known Services)**: Instead of scanning all ports, focus on common enterprise/OT ports.
  - **Tools**: `nmap`
  - **Example (`nmap` - Slow, specific ports)**:

```
# Scan specific common ports with slow timing, no ping, no DNS
resolution
nmap -sS -T2 --max-retries 1 --scan-delay 1s -p
21,22,23,25,53,80,110,135,139,443,445,1433,1521,3306,3389,5900,5985,598
6,47808 -Pn -n <target_IP>
# Use decoy scanning (-D) if necessary, but can be noisy if overused
# nmap -sS -T2 -D RND:5 <target_IP>
```

    - **Evasion Tip**: Use `-sS` (SYN scan) as it's often less logged than connect scans (`-sT`). Avoid OS detection (`-O`) and version scanning (`-sV`) initially as they are noisy. Use `-Pn` to skip host discovery if you already know the host is up.

- **OT-Specific Port Scanning**: Target industrial control system ports.
    - **Example (ICS Port Scan)**:

```
# Scan for common ICS/SCADA ports with extreme caution
nmap -sS -Pn -n --max-retries 1 --scan-delay 5s -p
102,502,20000,44818,47808,1911,9600,1962,20547,4840,41100 <target_IP>
```

    - **Evasion Tip**: Use extremely slow scanning (`--scan-delay`). Consider scanning one port at a time. Avoid version detection initially.

- **Service Banner Grabbing (Manual)**: Connect manually to identified open ports to grab banners.
    - **Tools**: `nc` (netcat), `telnet`
    - **Example (`nc`)**:

```
nc -nv <target_IP> <port>
# Example for HTTP
echo -e "HEAD / HTTP/1.0\r\n\r\n" | nc -nv <target_IP> 80
```

    - **Evasion Tip**: Mimic legitimate client behavior. Don't probe too many ports rapidly from the same source IP.

- **DNS Enumeration (Internal)**: Query internal DNS servers if identified.
    - **Tools**: `dig`, `nslookup`
    - **Example (`dig` - Zone Transfer Attempt)**:

```
dig axfr @<dns_server_ip> <domain_name>
```

    - **Evasion Tip**: Zone transfers are often logged/alerted. Prefer targeted queries for specific hostnames if possible.

- **SMB Enumeration (Careful)**: Enumerate SMB shares and sessions cautiously.
    - **Tools**: `smbclient`, `smbmap`, `enum4linux-ng`
    - **Example (`smbclient` - List Shares Anonymously)**:

```
smbclient -L \\\\<target_IP> -N
```

- **Example (`smbmap` - Null Session)**:

```
smbmap -H <target_IP> -u '' -p ''
```

- **Evasion Tip**: Null sessions and anonymous share listing are frequently monitored. Perform these actions sparingly and during expected "business hours" if possible. Avoid tools that perform overly aggressive enumeration.

5. Host Discovery (Stealthy Alternatives)

Standard ICMP/ARP scans can be noisy.

- **ARP Scan (Local Subnet)**: Less likely to traverse firewalls but good for local discovery.
  - **Tools**: `arp-scan`, `nmap -PR`
  - **Example (`arp-scan`)**:

```
sudo arp-scan --localnet
```

  - **Evasion Tip**: ARP scans are generally less monitored than ICMP scans within the local subnet.
- **Targeted TCP/UDP Probes**: Send probes to common ports on potential hosts instead of ICMP.
  - **Tools**: `nmap -PS<portlist>`, `nmap -PA<portlist>`, `nmap -PU<portlist>`
  - **Example (`nmap` - SYN to port 80)**:

```
nmap -PS80 -T2 --scan-delay 1s -Pn -n <target_range>
```

  - **Evasion Tip**: Probing common ports like 80 (TCP) or 53 (UDP) might appear more legitimate than ICMP echo requests.

6. Network Topology Mapping

Understanding the network structure helps plan attack paths with minimal alerts.

- **Traceroute Alternatives**: Map network paths without traditional traceroute.
  - **Example (TCP Traceroute)**:

```
# TCP traceroute to port 80 (appears as normal web traffic)
tcptraceroute <target_IP> 80
```

  - **Evasion Tip**: TCP traceroute to common ports appears more like normal traffic than ICMP traceroute.

- **Passive Network Segmentation Analysis**: Identify network segments and firewalls.
    - **Method**:

```
# Analyze TTL values to identify network hops
sudo tcpdump -i eth0 -n 'tcp[13] == 2' | grep "ttl"
```

    - **Evasion Tip**: Analyzing existing traffic patterns can reveal network segmentation without active probing.

7. Reconnaissance Data Organization

Organizing gathered information helps minimize redundant (and potentially alerting) activities.

- **Target Inventory**: Maintain a structured inventory of discovered assets.
    - **Example Format**:

```
IP: 10.0.x.100
Hostname: srv01.plumetech.local
OS (if known): Windows Server 2022
Open Ports: 80, 443, 445
Services: HTTP, HTTPS, SMB
Role: Web Server
Notes: Part of DMZ segment
```

- **Network Map**: Build a logical map of the network.
    - **Components to Track**:
        - Domain controllers
        - Jump boxes/bastion hosts
        - OT/IT boundary devices
        - Engineering workstations
        - HMI/SCADA servers
        - Historian databases
        - PLCs and control systems

General Evasion Tips for Reconnaissance

- **Timing**: Use slow scanning profiles (`-T2`, `--scan-delay`) to avoid rate-based detection.
- **Targeting**: Scan specific IPs or small ranges rather than the entire subnet at once.
- **Source IP**: Your Kali box is the initial source. Be mindful of actions originating from it.
- **Protocols**: Prefer scans/probes using common protocols (TCP 80, 443, UDP 53) where possible.
- **Correlation**: Avoid performing multiple noisy actions in quick succession. Space out activities.
- **Analyze Traffic**: Before active scanning, passively listen to understand baseline traffic patterns and identify potential targets/services.

- **Business Hours**: Conduct reconnaissance during normal business hours when legitimate traffic is higher.
- **Incremental Approach**: Start with completely passive techniques, then gradually introduce low-noise active techniques only as needed.

Remember to cross-reference findings with the Alert Evasion Cheatsheet and the Scoring System Cheatsheet to estimate the potential alert cost of each action.