Penetration Test Report: Antivirus Evasion in HOLO Network

Prepared for: Internal Security Team
Prepared by: [Your Name / Pen Tester Name]
Date: [Insert Date]
Target: HOLO Network – TryHackMe Environment
Report Classification: Confidential

---

1. Executive Summary

This penetration test focused on assessing the effectiveness of antivirus detection and evasion techniques within the HOLO network simulation on TryHackMe. The objective was to simulate a real-world attacker's ability to bypass endpoint defenses using common AV evasion techniques and gain command and control (C2) access.

The assessment revealed that traditional antivirus solutions may be susceptible to several well-known evasion strategies, including payload obfuscation, packing, and the use of staged PowerShell payloads. These methods successfully bypassed detection and enabled remote shell access on the target machine.

The findings highlight a critical gap in endpoint security that could potentially allow an attacker to execute remote code undetected.

---

2. Methodology

This engagement followed a structured methodology, aligned with the penetration testing execution standard (PTES), and included the following phases:

- **Reconnaissance:** Understanding the simulated network and the AV software in use.
- **Weaponization:** Creation of multiple payloads using tools like `msfvenom`, `Veil`, and `obfuscation` techniques.
- **Delivery:** Manual or automated delivery of the payload to the target host.
- **Exploitation:** Execution of the payload to verify AV evasion success and establish C2.
- **Post-Exploitation:** Limited interaction with the host to verify persistence and footprint.
- **Reporting:** Documenting findings and risk with remediation steps.

Tools Used:

- `msfvenom`
- `Veil`

- `PowerShell Empire`
- `Metasploit`
- `obfuscation/shellcode injection techniques`

---

3. Findings

ID	Finding	Severity	Status
F-001	AV Bypass via Encoded PowerShell Payload	High	Confirmed
F-002	Obfuscated `.exe` Delivery Success	High	Confirmed
F-003	Antivirus Failed to Detect Reverse Shell	Critical	Confirmed

F-001 – AV Bypass via Encoded PowerShell Payload

- **Description:** A base64-encoded PowerShell reverse shell payload was created and executed via command line on the target. AV software did not detect or block the execution.
- **Impact:** An attacker can gain remote shell access, bypassing security controls.
- **Recommendation:** Implement script execution monitoring, disable PowerShell v2, and enforce signed scripts policy via GPO.

F-002 – Obfuscated `.exe` Delivery

- **Description:** A custom `msfvenom` payload wrapped and encoded using Veil framework was delivered and executed on the host.
- **Impact:** Successful execution implies ineffective behavior-based detection or sandboxing.
- **Recommendation:** Leverage EDR with heuristic and behavior-based analysis rather than relying solely on signatures.

F-003 – Antivirus Failure to Detect Reverse Shell

- **Description:** The AV allowed a staged Metasploit reverse TCP shell to establish a connection to the attacker's listener.
- **Impact:** Full system compromise possible with administrative privileges.
- **Recommendation:** Block outbound reverse shell patterns and monitor suspicious network activity. Configure AV to inspect PowerShell and .NET executions.

---

4. Risk Ratings

Risk levels were determined using the CVSSv3 vector and internal criticality of the system. Each vulnerability was rated on:

- **Likelihood of Exploitation**
- **Impact on Confidentiality, Integrity, and Availability**
- **Existing Controls**

Finding ID	Likelihood	Impact	Risk Rating
F-001	High	High	High
F-002	High	Medium	High
F-003	Very High	Critical	Critical

5. Recommendations

- **Enhance Endpoint Security:** Upgrade to advanced EDR platforms with real-time behavioral detection.
- **Harden PowerShell:** Disable legacy versions, require script signing, and audit all PowerShell usage.
- **Regular AV Testing:** Implement routine red team testing to ensure AV solutions detect current attack vectors.
- **Network Segmentation:** Limit outbound communication capabilities of endpoints to prevent C2 channels.
- **User Training:** Educate users on safe file handling and the dangers of executing unknown files.

6. Conclusion

The antivirus solutions deployed in the HOLO network were insufficient in detecting and mitigating modern AV evasion techniques. The successful bypass and execution of obfuscated payloads demonstrate a need for stronger, behavior-based endpoint protection and robust security monitoring. Addressing these gaps will significantly enhance the organization’s defense posture.