

Experimental Results - Fileless Malware Attack

Table 1: Attack Summary

Parameter	Value
Target System	Windows 10 Home (Build 19045)
Target IP	192.168.1.5
Attacker System	Ubuntu Linux
Attacker IP	192.168.1.4
Attack Method	PowerShell Reverse Shell
Connection Port	4444
Attack Success	Yes
Files Written	0 (Fileless)
Detection by AV	No (Defender Disabled)

Table 2: Vulnerable Ports Identified

Port	Service	State	Vulnerability	Exploitable
135	MS RPC	Open	Remote Code Execution	Yes
139	NetBIOS-SSN	Open	SMB Fileless Attacks	Yes
445	Microsoft-DS	Open	PowerShell Remoting	Yes
5040	Unknown	Open	Information Disclosure	No
7680	Pando-pub	Open	Unknown	No

Table 3: Attack Execution Results

Metric	Result	Notes
Payload Delivered	Success	PowerShell one-liner executed
Connection Established	Success	Reverse TCP on port 4444
Remote Commands	Success	whoami, systeminfo, ipconfig
File Artifacts	1 file (536 bytes)	shell.ps1 from previous test
Memory Execution	Verified	6 PowerShell processes detected
Detection Rate	0%	Windows Defender disabled
Persistence	Session-based	Lost on reboot/process kill