

Full Red Team Engagement Kill Chain

Attack Flow-Chain

OSINT → Phish → Exploit → Privilege Escalation → Lateral Move → Persistence → Exfiltration → Cleanup

MITRE Phase	Technique	Tool Used	Result	Business Impact
Recon	T1595	Shodan	Attack surface mapped	Entry planning
Initial Access	T1566	Evilginx2	Credentials stolen	Unauthorized access
Exploitation	T1190	Metasploit	Server takeover	Data control
Priv Esc	T1068	Mimikatz	Admin access	Full authority
Lateral	T1021	Psexec	Spread inside network	System hopping
Persistence	T1053	schtasks	Stealth access	Long-term breach
Exfiltration	T1041	DNS tunneling	Data theft	Data loss
Defense Evasion	T1036	LOLBins	Undetected presence	Prolonged intrusion