Initial Access - Windows (Red Teaming Entry Point)

Objective: Train students on how real attackers gain a foothold in Windows based enterprise environments covering phishing, payload delivery, misconfigurations.

1 Initial Access Techniques (TTPs)

- Phishing with Weaponized Documents Crafting malicious WordPress, DDE, or embedded payloads.
- Abusing Free Services for Phishing Delivery Leveraging platforms like GitHub, Discord, CDNs, and other web services to host or deliver malicious content undetected.
- Delivering Malware Via LNK, HTA, ISO, BAT, PS1, OneNote files, and combining multiple file types for stealthy infection chains. (Not Well Known TTPs Included).
- Living Off the Land Binaries (LOLBins) Using trusted Windows binaries (e.g., mshta, certutil, rundll32) for payload execution and defense evasion.
- Setting Up Phishing Infrastructure On own server or locally, building your own phishing campaign servers with HTTPS, domain masking, tracking, and custom payload hosting.
- Securing Your Campaign Infrastructure Implementing non-fencing, real-time alerts, traffic filtering, and hardened server configurations to protect your infrastructure from detection or takedown.
- Bypassing MFA with Evilginx2 Setting up and using Evilginx2 to capture session tokens and bypass multi-factor authentication (MFA).
- Advanced Evasion Using HTML smuggling, SVG-based loaders, and chaining HTML + JavaScript + CSS for sandbox evasion and stealthy execution.
- Overview of C2 Frameworks (e.g., Cobalt Strike, Sliver, Mythic, Havoc), setup walkthrough, listener creation, and agent deployment.
- Implementing HTTPS, Domain Fronting Custom profiles, and redirectors (Apache/NGINX/CDN-based) to mask and protect C2 traffic from detection.

2 Execution Techniques

- User Interaction (click-based execution)
- Scheduled Tasks, Start-up Folder
- Exploiting Vulnerable Services For code execution

3 Real-World Case Studies

- How Attackers Got Initial Access In major breaches
- APT Tactics During initial access

4 NOTE

Everything you learn in this module is strictly from a Red Team perspective. Use these skills responsibly and never to harm, exploit, or attack anyone without proper authorization. Ethical conduct is the foundation of cybersecurity.

“Initial access is the breach point - where a simple click can collapse an empire.”