Outflank Security Tooling (OST)

OUTFLANK

SOLUTION OVERVIEW

OST is a curated set of offensive security tools created by well-recognized, expert red teamers to cover every significant step in the attacker kill chain, from difficult stages such as initial access to final exfiltration. It is Outflank's private tool set.

COMMON PAIN POINTS

- Need to stay undetected during engagements; current tools flagged by AV and EDR
- Current red team tools don't provide coverage for the entire kill chain
- Current tools were not developed by professional, dedicated teams
- Reliant on open source/public tools that are poorly documented, infrequently maintained, or no longer effective
- Red team is advanced but may have gaps in certain skill sets
- Having dedicated R&D resources in a red team is costly and hard to find the right people
- Using manual techniques and need to increase efficiency

DIFFERENTIATORS

- Includes techniques that are not publicly available
- Continuously updated with new tools that use the latest offensive techniques
- Great integration with Cobalt Strike
- Created by professional red teamers focused on research and development
- Developed, managed, and used by Outflank, one of the leading red teams world-wide
- Backing and resources from global enterprise software company
- Competitive pricing with bundling opportunities
- Cost savings of buying a license of OST instead of increasing headcount

KEY FEATURES

- Broad set of tools for red teams, a toolset that allows red teamers to simulate similar techniques as advanced attackers and safely perform deep-technical and difficult tasks.
- Focus on antivirus and EDR evasion OST tools that specialise in staying under the radar and are explicitly developed to assist in bypassing defensive measures and detection tools.
- Integrates with other red teaming solutions OST, developed to work in tandem work with **Fortra's** advanced adversary simulation tool, **Cobalt Strike**, extending the reach of these two tools to further enhance testing efforts.
- Tools for every phase of the attack chain, OST provides red teams with shortcuts for hard stages, like initial access or OPSEC-safe lateral movement.
- Full documentation within the application portal, with regular updates and extensive documentation, security teams can stay up-to-date and one step ahead of attackers.
- Access to developers and other users for support and knowledge sharing .

SOLUTION USE CASES

- **Evasion:** Create advanced payloads that enhance antivirus evasion and detection strategies using anti-forensic features
- **Initial access**: Gain a foothold with a phishing generator with MS Office documents or conceal payloads in images
- **Lateral movements:** Pivot throughout the environment while staying under the radar with a remote code execution toolkit
- **Post-exploitation:** Covertly interact with a target's desktop without impacting their user experience

S4Applications

Resources: https://s4applications.uk/fortra/outflank-security-tooling-ost/