NETSPI

NETSPI.COM • 612.465.8880

Red Team Toolkit

Better defend against sophisticated attacks with sophisticated adversary simulation

Red Team Toolkit (RTT) is an offensive security platform and tooling suite for red teamers and penetration testers. The toolkit enables teams to perform advanced network operations, collaborate on target exploitation, and better simulate sophisticated adversaries. The RTT Platform provides a unified, easy-to-use web interface that provides multi-user support with tiered permissions, providing a single interface for managing and interacting with targets, as well as recommendations for remediation and improving your organization's network security program.

More than just a tool

The RTT Platform is a suite of offensive security tools that drive stealthy cyber-operations through all phases of an attack, including initial access, privilege escalation, persistence, and impact. RTT includes several tools, including Slingshot and Throwback. Each tool has a specific purpose to facilitate stealthy operations and adversary emulation.

Identify weaknesses in your defense in depth

Use sophisticated attack techniques through all phases of an attack chain to identify gaps in your defense in depth. Work with defensive teams to improve detection capabilities.

OpSec at every layer

The RTT platform features over 15 defensive countermeasures. Evasion techniques include leveraging syscalls for stealthy code injection, in-memory obfuscation of modules, as well as AMSI, ETW, and PowerShell logging bypasses. OpSec has been built into every layer of every tool within the RTT Platform.

Slingshot

Slingshot is a powerful post-exploitation agent for red team operations. Built with OpSec first, Slingshot empowers teams to emulate sophisticated adversaries through stealthy injection techniques, memory obfuscation, malleable network profiles, and loads of defensive evasion capabilities. It empowers operations with a limited detection surface, powerful modularity, and ephemeral concepts.

15+ defensive evasion techniques

5+ automated pivoting techniques

Trusted by the world's largest companies

Used to perform stealthy operations for 10+ years

Used by 3 out of 4 DoD departments

TOOLKIT FEATURES

Agent automation via API

In-memory PowerShell and .NET

Native syscall API broker

AMSI, ETW, and PS logging bypass

Full filesystem integration

25+ integrated commands

HTTP/S beaconing

Full Mimikatz functionality

SOCKS proxying

5+ SMB pivoting techniques

Malleable C2 profiles

10+ defensive countermeasures

For more information, contact sales at sales@netspi.com or connect with us here.