DATASHEET (CYBERSECURITY)

Advanced Bundle – Core Impact and Cobalt Strike

Core Impact and Cobalt Strike represent two distinct, yet complementary approaches to security assessment. Core Impact is an automated pen testing tool that focuses on initial access and security validation, while Cobalt Strike specializes in advanced post-exploitation techniques for red team operations. In additional to functioning independently, security teams can benefit from both platform during a single engagement, using specific capabilities from each tool during different phases. .

Interoperability: Unifying Pen Testing and Red Teaming

Interoperability between Core Impact and Cobalt Strike provides a combined strategy that enables teams to extend their capabilities throughout different phases of an engagement.

- **Session Passing:** Direct session passing and tunneling between Core Impact and Cobalt Strike allows teams to easily transition from initial access to advanced post-exploitation phases.
- **Interoperability through SOCKs proxy:** SOCKS Tunneling allows operators to run Core Impact modules like NTLMrelayx and exploits through the Cobalt Strike Beacon chain without having to deploy an agent in the compromised network.
- **Resource Sharing:** Both platforms can utilize shared .NET assemblies, modules, and execute-assembly commands across testing environments.

Shared Focus on Risk Assessment

While Core Impact and Cobalt Strike operate at different phases of security testing (automated exploitation and post-exploitation), utilizing both their technical architectures facilitates an advanced testing strategy. This combined approach offers several key strengths:

Ransomware and Phishing Simulations:

- **Core Impact:** Combines social engineering capabilities with the ransomware simulator to emulate multiple ransomware families, enabling credential harvesting, data encryption, and exfiltration for security awareness testing.
- **Cobalt Strike:** Imports phishing templates, then handles attachment stripping, encoding issues, and template customization while tracking clicks.

Reporting:

- **Core Impact:** Maintains detailed logs of all testing activities, including remote host operations and system interactions, which can then auto-populate standardized reporting templates for technical analysis.
- **Cobalt Strike:** Logs capture all operational activities, generating timeline-based reports and IOC (Indicators of Compromise) data derived from red team activities.

Real Time Collaboration:

- **Core Impact:** Enables interaction in the same session so users can securely share data, delegate testing tasks and get a common view of discovered and compromised network targets.

- **Cobalt Strike:** Connects to a team server to allow users share data, communicate in real-time, and control systems compromised during the engagement.

Additional Product Features

Penetration Testing with Core Impact

Core Impact determines the risk of security weaknesses through automated exploitation and assessment across multiple attack vectors, allowing teams to evaluate security controls and prioritize critical infrastructure vulnerabilities.

- **Automated Testing:** Uses Rapid Penetration Tests (RPTs) to automate key testing phases including reconnaissance, initial access, privilege escalation, and vulnerability validation.
- **Core Certified Exploits:** Maintains an expertly developed exploit database that covers multiple platforms, operating systems, and applications, with regular updates expanding coverage of new attack vectors.
- **Multi-Vector Testing:** Supports testing across diverse environments, exploiting security weaknesses associated with networks, people, web applications, endpoints, Wi-Fi, and SCADA environments.
- **Remediation Validation:** Maintains session data for automated retesting, allowing teams to verify the effectiveness of compensatory security controls and patches implemented after initial assessment.

Red Teaming with Cobalt Strike

Cobalt Strike enables advanced adversary simulation through customizable post-exploitation operations, allowing red teams to evaluate defensive measures against sophisticated persistent threats.

- **Flexible Framework:** C2 framework is built to adapt and is easily extendable to incorporate personalized tools and techniques.
- **Post-Exploitation:** Signature payload, Beacon, gathers information, executes arbitrary commands, deploy additional payloads, and performs other tasks that models the behavior of an advanced actor.
- **Malleable C2 Profiles:** Program used to set various default values, including how often Beacon checks in, tailoring the memory footprint, and controlling Beacon's network traffic indicators.
- **Arsenal Kit:** Tools for tailoring advanced threat simulation, including:
  - **The Sleep Mask Kit** – Hides Beacon in memory while it sleeps
  - **The Mutator Kit** – Uses an LLVM mutator to break in-memory YARA scanning of sleep masks
  - **User-Defined Reflective Loaders** – Custom reflective loaders that can bear individualized tradecraft

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.