FORTRA | bakotech

Cobalt Strike

is a threat emulation tool that is ideal for Red Team post-exploitation tasks based on a hidden agent and an updatable base of attack scripts.

KEY FEATURES

POST EXPLOITATION

Beacon is Cobalt Strike's payload to model an advanced actor. Beacon executes PowerShell scripts, logs keystrokes, takes screenshots, downloads files, and spawns other payloads.

BROWSER PIVOTING

Use a Browser Pivot to go around two-factor authentication and access sites as your target.

SHARED SESSIONS

Multiple Red Teamers can log on to the team server for collaborative engagements, communicating in real time. In addition to shared sessions, team members can also share hosts, captured data and download files.

COVERT COMMUNICATION

Using asynchronous "low and slow" communication to remain undetected, Beacon can simulate an embedded attacker. Beacon's flexible Command and Control language, Malleable C2, can be used to alter network indicators to blend in with normal traffic or cloak its activities by emulating different types of malware.

RECONNAISSANCE

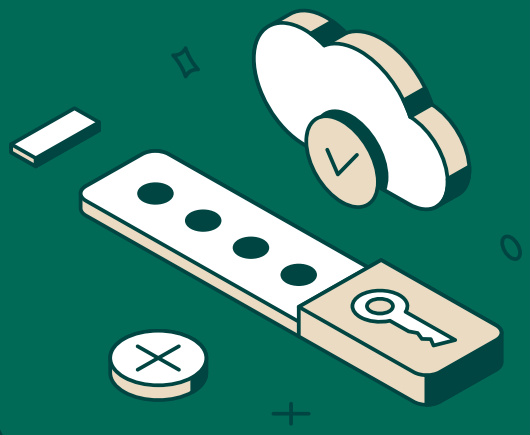
Cobalt Strike's System Profiler is ideal for client-side reconnaissance activities. It can discover the internal IP address, applications, plugins, and version information of the visitor.

REPORTING AND LOGGING

Cobalt Strike's reports provide a timeline and a list of indicators from red team activity. These reports are made to benefit our peers in security operations. Cobalt Strike exports reports as both PDF and MS Word documents.

CHECK YOUR COMPANY'S SECURITY

against targeted attacks with one of the most powerful kits available to pentesters.



ADVANCED ADVERSARY SIMULATIONS

Use Beacon, Cobalt Strike's post-exploitation payload, to control your target's network, all while remaining undetected.

DYNAMIC RED TEAM ENGAGEMENT

Red Teams can use a shared team server to collaborate on realistic attacks and generate thorough reports to document all post-exploitation activities.

FLEXIBLE FRAMEWORK AND BIG COMMUNITY

Modify the built-in scripts and write your own, as well as create and share your extensions in the Community Kit.

TAILORED SCRIPTS.
Create scripts using Cobalt Strike's scripting language, Aggressor Script. New scripts are easily loaded and managed in the console, where you can perform further interaction.

ADJUSTABLE ATTACK KITS.
Modify the kits loaded from the Cobalt Strike arsenal to suit the needs of each attack. For example, you can redefine script templates from the resource set used in your workflows, as well as create your own Beacon Object File (BOF).

INTEROPERABILITY WITH CORE IMPACT.
Organizations with both Core Impact and Cobalt Strike can take advantage of session passing and tunneling capabilities between these two tools.

COMMUNITY KIT.
The Community Kit serves as a central repository for projects from the user community so fellow security professionals may also benefit from these extensions.

FORTRA | bakotech®

fortra@bakotech.com