Cybersecurity

Activity File

Activity File: C2 Research

- In this activity, you will continue to play the role of a pentester conducting an engagement on MegaCorpOne.
- You are tasked with researching various C2 frameworks using the C2 Matrix website and suggesting the best C2 framework for your current assessment on MegaCorpOne.
- You will then answer several questions about the frameworks you select.

Activity Instructions

Using the C2 Matrix site and Google, find two C2 frameworks that fit the following requirements.

Requirements

Throughout your initial scans on MegaCorpOne's domain, you've discovered several facts:

- Their network includes mostly Windows machines, with some Linux machines scattered throughout.
- Their firewall rules only allow ports 80, 443 TCP, and port 53 UDP outbound.

The service contract includes a few additional requirements:

- The C2 framework must support logging.
- The framework must have a full version released—i.e., the version must be 1.0 or higher. No "beta" or "PoC" versions are allowed.
- Your coworkers will help with this assessment, so the framework must support multiple users.

Note: It's okay if your primary C2 framework does not support all operating systems, as long as the secondary or tertiary framework supports the systems that the primary framework does not.

Questions

For each framework that you've identified as a good candidate, answer the following questions:

1. What is the name of the C2 framework? Cobalt Strike
2. What operating systems do its agents support? Windows
3. What channels can the agents communicate over? HTTP/S, DNS, TCP, SMB
4. What language is it written in? Java

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.

5. Is it open- or closed-source? Closed
6. Does the developer have a Slack or X link for potential support questions? No

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.