CS4001: Offensive Security

Mark Anderson
Homework 3

February 13, 2020

1 Acquiring Infrastructure

Our base tools will be stored on a private VPS that the entire oeprational team shares. Access to this VPS will be controlled through SSH public key authentication for added security and convenience. File Sharing, Staging, and Networking will all be done on this VPS with any ongoing script development being version controlled and tracked through a private repository on Github.

2 Operational Security

All communication between members of the operational team will be conducted through the application 'Tox'. Tox is a p2p end-to-end encrypted messaging platform that allows for a high confidence of security. All team laptops will be encrypted using VeraCrypt with FIPS approved encryption algorithms (standard of AES-256). This will ensure that in the event of a hardware compromise there is a high level of confidence in data integrity.

3 Transferring Tools

Most of the tools needed to have on the target will be available from the tools developer's website. In the case that connections or downloads to these tools are denied we will be able to host these tools on our servers for transfer between the target. Infiltration methods will most likely be needed and we will have scripts with a variety of ways to stealthily upload tools to our target.

4 Connecting to Target

All target reconnaissance will be done with stealth and anonymity in mind. All port scans, connections, and enumeration will be done with a minimal footprint even if the operation will take longer in doing so. Connecting to the target will change on a case to case basis but virtually all connections will be allowed in the ROE. The team may need to connect through a web application, through ssh, telnet, or any means necessary to finish the operation.

5 On Target Actions

A fleshed out Rules of Engagement will be drafted up for each operation and will go over the details on what is allowed on the target system. The operator will only be permitted to engage in actions dictated in the ROE and will minimize footprint and persisting evidence on the target server. In the case of extenuating circumstances the operator will call in and refer up to determine which actions to be taken in the new uncovered circumstances.