Project Proposal
Intuitive Web Interface for Blocklist Maintenance

Sponsor
Dr. Phil Romig, Department of Computer Science

BACKGROUND

An increasingly critical component of any Information Security program is the ability to quickly detect and respond to ongoing cyber-threats. Just a few years ago it was considered sufficient to identify and remediate malicious activity within hours or days. Today minutes can make the difference between a minor inconvenience and a costly information security incident. To address this emerging threat Mines began developing a Security Operations Center (SOC) in the fall of 2019. The SOC is staffed primarily by students who monitor the school's infrastructure for Indicators of Compromise (IOC). When a computer exhibits suspicious behavior the SOC operator on duty will attempt to contact the owner or a system administrator who can further investigate and address any issues. The department of Information Technology and Solutions (ITS) would like to reduce the time between detection and response by providing the SOC operator the ability to directly remediate a compromise rather than waiting for a system owner to respond.

One common IOC encountered by the SOC is communication between an infected computer and the entity controlling the compromised system. Interrupting this "command-and-control" traffic can significantly reduce the impact of a cyber-attack. Mines' boarder firewall supports two features specifically designed to facilitate blocking malicious traffic (1) the ability to query a list of banned IP addresses: either external addresses known to be used to coordinate attacks or internal addresses suspected of being infected and (2) the ability to query a list of banned domain names, redirecting any request to those domain names to a site controlled by the school.

The firewall is designed so that both of these lists can be downloaded from a webserver every few minutes allowing us to separate firewall administration from maintenance of the lists.

WORK TO BE PERFORMED

A team taking on this project will be asked to develop the infrastructure needed to maintain and host these blocklists. The team will have the freedom to design a solution based on the functional requirements provided by the sponsor. Requirements will include:

1. The HTTP server queried by the firewall for the current list of blocked addresses and domain names. The details of the firewall query and the response format will be provided at the project kickoff.

2. A database that will store the blocked objects. A complete schema for the database will be developed during the project but at a minimum the data elements will include IP address or domain name, date to remove the entry from list sent to the firewall, name of the person who added the entry and the reason the entry was created.

3. Tools used for database maintenance including a web-based application that can be used to view and edit each list. The application will need to authenticate users via Shibboleth and use LDAP to identify authenticated users authorized to view or update the database.

4. A website hosting the page(s) to which users visiting blocked domain will be redirected.

5. Documentation, including end-user documents with information about how to use the system and technical documentation about the architecture, technology and security controls used.

DESIRED SKILLS

A team interested in taking on this project should have a basic knowledge of the Linux operating system and at least one common scripting language (Perl or Python are preferred). Team members will need to develop an understanding of the API used by the firewall to pull the lists, web programing, database management, HTTP, Transport Layer Security, and the Simple Authentication Markup Language. While teams are expected to be able to work independently the sponsor is familiar with all the information needed and will be available to provide guidance at any time.

WORK ENVIORMENT

This project is ideal for a team of three students. Team members may work on campus or at home, whichever they prefer. Most work can be done independently, with minimal coordination with the sponsor, there will be one or more sprints at the end of the project that involve integrating the final product with the school's production network. This work will need to be done in coordination with ITS staff during off-peak hours. The sponsor will provide all the needed hardware and software.