НИЯУ «МИФИ»
Кафедра №42 «Криптология и Кибербезопасность»

Информационная безопасность АСУ ТП

Лабораторная работа №1. Поиск компонентов АСУ ТП в глобальной сети.

1. Теория

Целью данной лабораторной работы является анализ методов выявления и идентификации компонентов АСУ ТП. Основными методами выявления и идентификации компонентов АСУ ТП являются поиск с помощью прослушивания и анализа трафика в сети (пассивный поиск) и поиск с помощью сканирования сети (активный поиск).

Целями такого поиска являются:

– получение списка сетевых компонент (объектов сети);

– идентификация объектов сети;

– получение общей информации о сетевых компонентах и списка активных сервисов.

По результатам собранной информации становится возможным реализовывать различные сценарии атаки на идентифицированные объекты сети.

Методы активной и пассивной идентификации в сетях TCP/IP опираются на особенности реализации сетевых сервисов и ответов от них. Их можно разделить на два класса:

– особенности реализации сервисов, обеспечивающих взаимодействие по стандартным сетевым протоколам;

– нестандартные сетевые сервисы (реализующие взаимодействие по специальным промышленным протоколам, зачастую собственной разработки, так называемым «проприетарным» протоколам).

Shodan (https://www.shodan.io) — специальная поисковая система, которую можно использовать для нахождения подключенных к интернету устройств и точной информации о различных веб-сайтах. Shodan опрашивает порты устройств и на основе полученных ответных баннеров делает выводы об устройствах и сервисах. Для поиска устройств

возможно применять фильтры, например: country, city, os (операционная система), port, hostname. Кроме того, возможен поиск по ключевым словам либо кодам ответов. На рисунке приведен пример поиска оборудования Cisco, возвращающего код http-ответа «200».

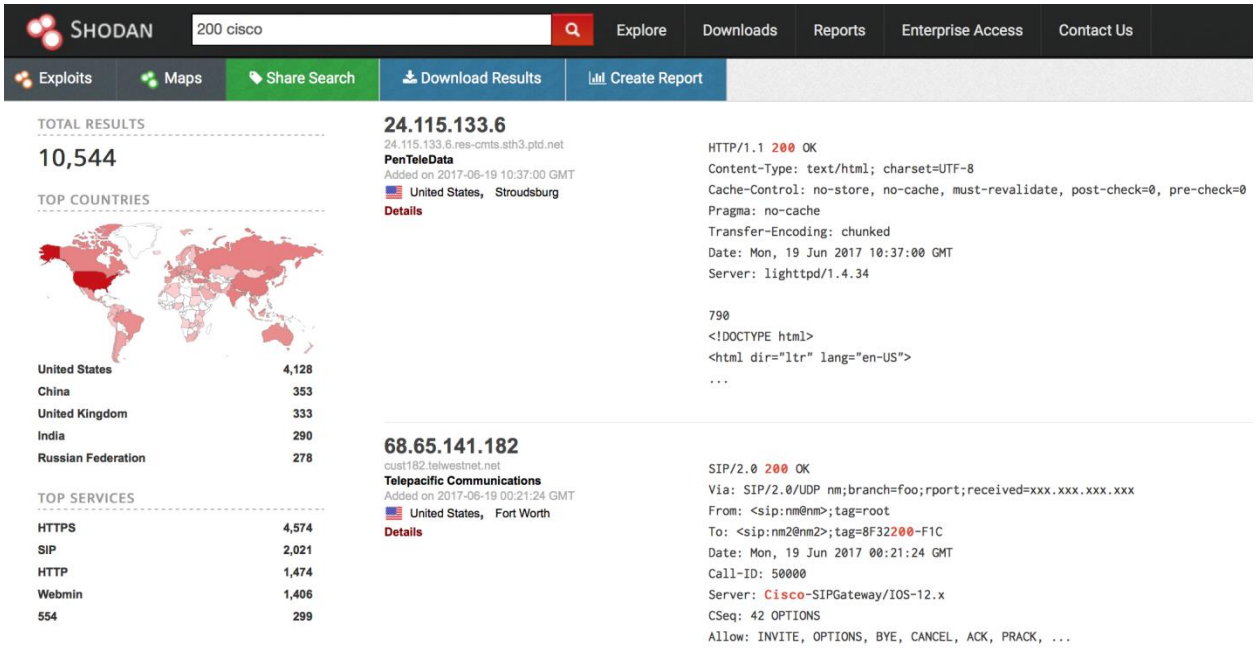

Рисунок 1. — Пример поиска через Shodan

2. Задание

1. Описать, какие компоненты АСУ ТП возможно найти в глобальной сети. Какие особенности позволят их идентифицировать?
2. Составить запросы для Shodan, которые позволят обнаружить компоненты АСУ ТП в глобальной сети. Объяснить, почему запросы составлялись таким образом. Число запросов — не менее 8 различных для разных компаний-производителей.
3. Привести результаты поиска и их краткий анализ.

Изучение Shodan API и CLI (https://developer.shodan.io/, https://cli.shodan.io/)

1. Реализовать программное средство на языке программирования `bash`, которое осуществляет поиск всех доступных IP адресов, являющихся узлами АСУ ТП сети
2. Идентифицировать, какие порты открыты на данных узлах
3. Идентифицировать, были взломаны данные узлы известными хакерскими группировками
4. *Получить доступ к одному из узлов

Для защиты лабораторной работы необходимо предоставить отчет, содержащий в себе описание хода выполнения и результатов всех указанных в задании пунктов.