ASN КАК ИНСТРУМЕНТ ПОИСКА АВТОНОМНЫХ СИСТЕМ

Курбатов В.А., к.ф-м.н, доцент,
Катков Т.А., студент
Мылтыкбаев А.Р., студент
МТУСИ, г. Москва, Россия

Аннотация: ASN как инструмент командной строки, предоставляющий возможности сбора разведывательной информации об ASN, доменах, IP-адресах. В статье разобран функционал результативного поиска ASN по имени организации.

Ключевые слова: ASN, разведка, имитация атак, тестирование на проникновение, networking.

В современном мире, где информация играет основную роль в жизни общества, её защита и поиск становится приоритетным направлением развития информационных технологий[2]. Главным преимуществом в использовании технологий ASN является возможность собрать информацию об ASN (рис. 1):

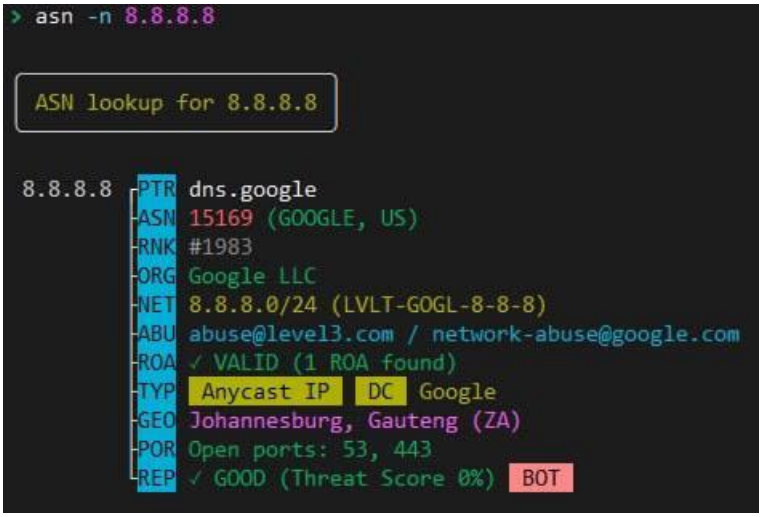

Рис. 1 – Пример использования ASN

Предоставляет интерфейс для поиска информации об ASN по IP/домену/подстроке организации и последующего извлечения информации о сетевой инфраструктуре, включая статистику BGP, а также связанные сетевые идентификаторы и организационные данные сети[3].

Утилита использует публичные API, такие как: Whois, Shodan, IFConfig, RIPEStat и др. для получения информации о цели.

Соседи: сбор BGB статистики об ASN может дать представление о соседствующих ASN. Благодаря этому складывается полная картина местонахождения организации в интернете, что может привести к обнаружению новых ASN, относящихся к цели [4].

Трассировка: позволяет получить трассировку до указанного ASN или IP, что потенциально может дать информацию о внешней структуре сети провайдера, центра хранения и обработки данных, хостинга и т.д.

Режим сервера:предоставляет HTTP-сервер для удобства использования в браузере и API, дублирующий функционал приложения. Браузерная интеграция позволяет сделать поиск информации по адресу, нажав на кнопку закладки.

Номер автономной системы – это уникальный идентификатор, который доступен в глобальном масштабе и позволяет автономной системе обмениваться информацией о маршрутизации с другими системами.

Автономная система (AS) – это группа IP-префиксов с четко определенной внешней политикой маршрутизации. Для того чтобы несколько автономных систем могли взаимодействовать, каждая из них должна иметь уникальный идентификатор. Номера автономных систем могут быть публичными или частными. Публичные ASN необходимы системам для обмена информацией через Интернет. Частный ASN можно использовать, если система взаимодействует только с одним провайдером через протокол Border Gateway Protocol (далее: BGP). Для получения номера автономной системы необходимо пройти через один из пяти региональных реестров Интернета [1].

Номера автономных систем напрямую связаны с точками обмена в Интернете, когда речь заходит о преимуществах вычислений на границе. Каждая сеть, использующая пиринг наInternet Exchange Point(IXP), является автономной системой, имеющей номер автономной системы. Пиринг через BGP возможен только потому, что каждая AS имеет уникальный идентификатор и вручную настраивается для прямого общения с другими

уникальными идентификаторами.

Существует четыре типа автономных систем, которым обычно требуется ASN. К ним относятся:

Multihomed–подключена более чем к одной автономной системе.

Stub-- Подключена только к одной другой автономной системе.

Транзитная– Обеспечивает соединения через себя. Например, сеть A может подключаться к сети C напрямую или через сеть B.

Точка обмена Интернета – автономная система, созданная физической инфраструктурой, расположенной в точках обмена Интернета.

Многие крупные организации имеют свои собственные ASN, вследствие чего чрезвычайно полезны для разведки, поскольку они позволяют нам перечислить IP-префиксы, принадлежащие данной организации.

Номер автономной системы необходим для любого соединения между двумя автономными системами, например для пиринговых сетей в точках обмена данными в Интернете.

Таким образом, ASN является удобной метрикой понимания сети определённой компании, помогая обнаружить больше конечных узлов компании при разведке. Полученная информация далее может быть использована для проведения работ по анализу защищённости и т.д.

Литература

1. Большаков А.С., Раковский Д.И., Программное обеспечение моделирования угроз безопасности информации в информационных системах - Правовая информатика, 2020г.

2. Информационное общество и безопасность личности / С.Е. Кузнецов, Й Бонсэйн, Б.Н. Сангаджиев, Д.А. Анищенко // Современные проблемы естественных наук и фармации: сборник статей Всероссийской научной конференции: Сборник статей Всероссийской научной конференции, Йошкар-Ола, 16–19 мая 2023 года. – Йошкар-Ола: Марийский государственный университет, 2023. – С. 211-214. – EDN BFTVXM.

3. Шелухин О.И., Симонян А.Г., Иванов Ю.А., Особенности DDoS атак в беспроводных сетях// журнал T-Comm - Телекоммуникации и Транспорт, 2012г.

4. Q. Vohra, E. Chen., BGP Support for Four-octet AS Number Space, May, 2007, URL: https://www.ietf.org/rfc/rfc4893.txt(датаобращения: 24.03.2024).