Contents

Задание 1.2 Анализ доменных имен

Анализ доменных имен

Большинство организаций управляют своей ИТ-инфраструктурой, как публичной, так и внутренней, именуя ее логически и на основе мнемонических (легко запоминаемых) имен. Каждый узел сети охарактеризован адресом, по которому к узлу можно обратиться. Для того, чтобы удобно, по памяти, даже при смене адреса, обращаться к определенному узлу сети, таким узлам дают доменные имена.

Из-за такой распространенной практики злоумышленники могут обнаружить все связанные с организацией ИТ-активы и впоследствии атаковать их. В свою очередь, белые хакеры могут имитировать эту деятельность: для того, чтобы показать организации, как много о ней могут узнать злоумышленники.

С высокой вероятностью все имена узлов, принадлежащих компании ООО ”Компания” с сайтом company.corp, будут располагаться в доменах 3-го уровня домена company.corp.

Домен 3-го уровня – это часть доменного имени, расположенная перед доменным именем второго уровня. Например, часть ”blog” в ”blog.example.com” является доменом 3-го уровня, а ”example.com” является доменом 2-го уровня. Они могут использоваться для разных целей, но выбор доменного имени зависит от намерений и потребностей владельца.

Например:

- web.company.corp

- mail.company.corp
- support.company.corp
- portal.company.corp
- moscow.company.corp

Таким образом, зная доменное имя 2-го уровня, мы можем попытаться найти массу имен 3-го уровня, которые будут ссылать нас на неизвестные нам ранее узлы инфраструктуры организации.

Поиск доменных имен, принадлежащих организации

Вначале мы можем не знать, какие вообще доменные имена 2-го уровня принадлежат организации. Самый простой способ в этом случае: воспользоваться поисковыми сервисами и попытаться найти сайты организации, которые она сама о себе публикует.

> Примечание: Единственной проблемой на этом этапе может стать ситуация, когда вы можете неправильно определить сайт организации. Это зависит только от вашей насмотренности и умения выявить контактные данные или идентификаторы организации, которые относятся именно к вашей цели.

Дополнительно, существуют системы закрытые и открытые, которые собирают информацию о зарегистрированных организацией доменных именах и могут вам сообщить о них.

Это могут быть следующие организации и сервисы:

Whois – это протокол поиска информации о зарегистрированных доменных именах, IP-адресах и автономных системах. Утилита whois является встроенной утилитой терминальной оболочки многих дистрибутивов операционных систем, таких как MacOS и Ubuntu Linux.

СПАРК (https://spark-interfax.ru/) – это система, собирающая всю доступную информацию о компаниях и извлекая из нее знания, помогает получать подробную информацию о бизнесе организаций и о привязанных к нему информационных активах, сайтах и доменных именах.

RIPE (Réseaux IP Européens) – это некоммерческая организация, которая занимается управлением и распределением ресурсов IP-адресации и автономных систем в странах Европы, Ближнего Востока и Центральной Азии. На ее сайте https://apps.db.ripe.net/db-web-ui/fulltextsearch можно найти различные данные (включая доменные имена), связанные с владельцем выделенных ему сегментов IP-адресов.

Поиск доменных имен и поддоменов

Поиск доменных имен заключается в способах подбора, предугадывания а также сбора из открытых источников доменных имен организации и делится на активный и пассивный методы.

Методы активного поиска доменных имен и поддоменов

Данный метод подразумевает активное взаимодействие с DNS-сервисом организации, т.е. выполнение запросов непосредственно к инфраструктуре, принадлежащей, арендуемой или управляемой целевой организацией.

Получение информации о доменных именах и поддоменах от DNS-сервиса организации возможно следующими способами (не ограничиваясь ими):

1. Опрашивание DNS сервиса на известные ему записи раскрывающие доменные имена, связанные с доменом 2-го уровня. Т.е. выполнение запросов к таким DNS записям, как: CNAME, MX, NS, SRV и т.д. Подробнее

- A – используется для указания доменного имени, например, testdomain.com, на IP-адрес его хост-сервера;
- MX – записи, отвечающие за обмен электронной почтой;
- NS – предназначены для идентификации DNS-серверов, ответственных за домен;
- SRV – записи для выделения службы, размещенной на определенных серверах;
- PTR – обратный поиск DNS: с помощью IP вы можете получить связанный с ним домен;
- SOA – начало записи: это информация о зоне DNS и других записях DNS;
- CNAME – сопоставляет целевое доменное имя с другим доменным именем.

Чтобы получить записи всех типов можно использовать тип запроса ANY.

Пример выполнения запроса: `nslookup -q=ANY example.com ns.example.com`

2. Перебор доменных имен на DNS сервисе компании при помощи использования словарей или правил мутации. В данном случае мы заранее подготавливаем большой список слов и возможных поддоменов и опрашиваем DNS сервис в формате слово.example.com, чтобы выявить все имена, которые существуют в инфраструктуре организации.

Пример использования утилиты subfinder со стандартным словарем для перебора доменных имен:

```
subfinder -d ya.ru
```

3. Выполнение запроса AXFR. AXFR запрос, или Zone transfer — это процесс передачи копии базы данных с DNS-зоной от главного сервера к вторичному. В идеале трансфер зоны ограничен только для определенных доверенных серверов, но неправильно сконфигурированные серверы разрешают трансферы любому, кто их попросит.

Пример выполнения такого запроса: `nslookup -q=AXFR example.com` (зачастую требует указания конкретного DNS-сервера, к которому будет отправлен запрос).

Другие примеры инструментов активного поиска:

- amass — многофункциональный инструмент для разведки
- Sublist3r — OSINT инструмент поиска поддоменов
- assetfinder — пассивный сканер поддоменов на Go

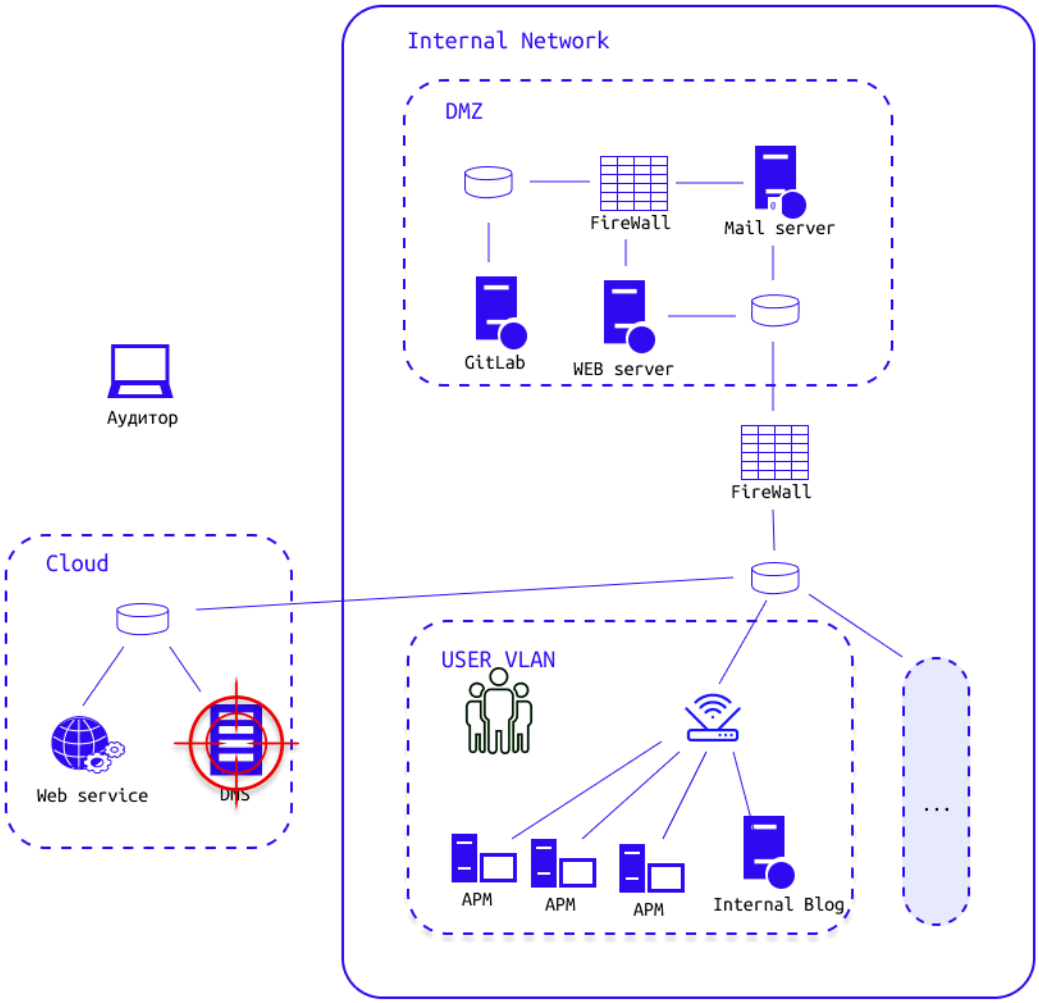
Методы пассивного поиска доменных имен и поддоменов

Методы пассивного поиска сводятся к использованию каких либо служб и сайтов, которые произвели активный поиск за нас или агрегировали известную информацию среди открытых источников. Есть множество веб-сайтов и служб, которые предлагают такие услуги в разной форме.

Примеры:

- dnsdumpster.com
- shodan.io
- censys.io
- crt.sh
- pentest-tools.com

Наша цель в типовой инфраструктуре:



Задание

> Story: Вы заключили договор на пентест с компанией ”Codovix” и можете приступать к работам. Для начала стоит провести разведку во внешней сети - доменного имени.

Необходимо:

1. Выполнить поиск подсказки в TXT записи доменного имени с помощью утилит dig, nslookup, host

2. Использовать подсказку для подготовки финального словаря паролей
3. Составить мини-отчет, где указать использованные подходы и затронутые угрозы безопасности. Отчет должен содержать название уязвимости, описание уязвимости, пример её эксплуатации, рекомендации к устранению

Теоретические вопросы

- Что такое доменное имя?
- Объясните разницу в уровнях доменных имен.
- Какие бывают типы записей?