Skillbox

Сбор информации

Специалист по кибербезопасности.
Модуль 1

Введение

Этот модуль посвящен разведке. Его цель — обучить вас пассивному и активному сбору информации об объектах сканирования.

1. Мы научимся работать с продвинутыми операторами поисковых систем для получения важной информации. Узнаем обо всех возможностях, чтобы правильно извлекать данные из поиска.

2. Освоим техники поиска уязвимости и ошибок.

3. Познакомимся со специализированными поисковыми системами, где есть вся информация о серверах, оборудовании, программном обеспечении, регистрационных данных и другой технической информации.

4. Поговорим о дополнительных источниках сбора данных об объектах исследования. Рассмотрим средства анализа информации.

Google Dorks: поиск документов

Google dorks (дорки) — это специальные операторы для извлечения критической информации. Они позволяют фильтровать запросы и искать проиндексированные данные. По ним часто можно найти и утечки данных.

Шпаргалка по продвинутым операторам Google находится ниже — она пригодится вам для сбора информации.

Операторы	Информация
intext: allintext:	Google ограничивает результаты теми, которые содержат все условия запроса, которые вы указали в тексте страницы.
cache:	Запрос покажет версию веб-страницы, которую Google имеет в своем кэше.
define:	Обращение к определениям словаря Google
filetype:	Запрос выводит все индексированные файлы указанного типа
inanchor: allinanchor:	Поиск страниц, на которые есть ссылки с определенным якорным текстом.
info:	Запрос представит некоторую информацию, которую Google имеет об этой веб-странице.
insubject:	Google соберет информацию о субъекте
intitle: allintitle:	Google выведет результаты содержащие это слово в заголовке.

Операторы	Информация
inurl: allinurl:	Google ограничит результаты материалами, содержащими это слово в URL.
link:	Запрос выведет список веб-страниц, на которых есть ссылки на указанную веб-страницу.
loc:	Фильтрует вывод по местоположению
location:	Находит новости в указанной геолокации
related:	Выводет список веб-страниц, которые «похожи» на указанную веб-страницу.
site:	Google ограничит результаты этими сайтами в данном домене.
after: before:	Устанавливает временные границы поиска after:2019-01-01 before:2020

Google Dorks

Поиск по типу данных

Для поиска файлов определенного типа используем запрос:

filetype:pdf

И конкретизируем его, указывая название:

documentation filetype:pdf

Поиск по сайту

Для поиска проиндексированных документов по конкретному сайту, которые не были скрыты настройками приватности, используем оператор site:

site:docs.google.com filetype:pdf

Поиск по url

Для поиска утечек данных или другой важной информации можно использовать элемент inurl:

inurl:passwords filetype:xls OR filetype:xlsx

inurl:emails filetype:xls OR ext:xlsx

Поиск по содержанию

Для уточнения запроса конкретизируем поиск по содержанию документа. Например, когда ищем логи, в которых указаны пароли.

allintext:password filetype:log

Можно найти и SQL-таблицы:

filetype:sql -github -gitlab backup

Оператор “-” исключает из выдачи ненужные страницы (теги) поиска.

Поиск файлов из общего доступа

Для поиска файлов и документов из общедоступного веб-сайта, например .env с базой паролей, используем такой запрос:

intext:DB_PASSWORD filetype:env
filetype:env intext:DB_USER

Google Dorks

Поиск по заголовкам

Закрытые ключи SSH используются для расшифровки информации, которой обмениваются в этом протоколе.

Можно найти ключи SSH, которые были проиндексированы Google, используя поиск по заголовкам:

intitle: "index.of" id_rsa-id_rsa.pub
filetype:pub "ssh-rsa"

Чтобы найти данные регистрации имен пользователей SSH-соединений, используем dork для извлечения этих имен из журналов PUTTY:

filetype:log username putty

Для поиска конфигурационных файлов:

inurl:ws_ftp.ini
"pwd=" "UID=" filetype:inc

В этих файлах также могут содержаться и личные данные.

Поиск уязвимостей

Используя фильтры заголовков, можно искать уязвимости по протоколам. В примере мы ищем открытые ftp-серверы и другие файловые системы:

intitle:"index of" inurl:ftp

intitle:index.of "parent directory"

inurl:/proc/self/cwd

intitle:"index of" share.passwd OR cloud.passwd OR ftp.passwd -public

Если результатов запросов слишком много, повторяем запрос и используем дополнительные фильтры:

intitle:"index of" inurl:ftp after:2019

Google Dorks

CMS

С помощью дорков можно находить страницы доступа к панели управления CMS и другим системам администрирования:

intitle:"WebSite X5 Manager" inurl:/admin/login.php

А также уязвимости и ошибки:

site:*/wp-admin/maint/repair.php
intext:define(WP_ALLOW_REPAIR,true);

К примеру, уязвимые к SQL-инъекциям сайты ищем так:

inurl:".php?id=" "You have an error in your SQL syntax"
intitle: "index of /" "db.sql"

Более полный список дорков доступен в Google Hacking Database:
https://www.exploit-db.com/google-hacking-database

Дополнительные возможности для поиска информации об объектах

Операторы info: и insubject: помогут больше узнать об объектах исследования. В случае, если страница недоступна, нам поможет оператор cache: - . Он показывает последнюю сохраненную копию объекта.

Для конкретизации времени поиска удобнее использовать операторы after: и before:
Логические операторы AND, OR помогут расширить или сузить результаты поиска.

У Яндекса схожий синтаксис запросов, что и у Google. Использовать их мы не будем, так как они менее эффективны, но познакомиться не помешает. Операторы Яндекса: https://yandex.ru/support/search/query-language/search-operators.html

Skillbox

Расширенные инструменты поиска

Расширенные инструменты поиска

Здесь мы рассматриваем системы поиска технической информации и оборудования, учимся использовать их для поиска уязвимого / плохо сконфигурированного оборудования.

Объект нашего исследования — поисковые системы, такие как Censys, Shodan, ZoomEye. Они ориентированы на оборудование, устройства и системы, подключенные к глобальной сети.

Shodan

Shodan.io — поисковая система, которая сканирует весь интернет на наличие подключенных к сети устройств. Если стандартные поисковые системы собирают данные об информации в сети, то shodan аккумулирует техническую информацию об устройствах, а именно:

- Данные о веб-технологиях и коды состояния серверов
- Информацию об используемых протоколах и портах
- Данные о сетевых сервисах и их версиях
- Данные о сертификатах, цифровых отпечатках и шифровании
- Другие метаданные (кодировки, time-зонах, куки)
- Геоданные

На основе полученной информации shodan формирует отчет о возможных уязвимостях.

Синтаксис Shodan

- city: поиск устройств по заданному городу
- country: поиск по странам
- geo: поиск по координатам
- hostname: поиск по названию хоста
- net: поиск по IP или /x CIDR
- os: поиск по операционным системам
- port: поиск по открытым портам
- before/after: поиск с указанием времени

Для поиска дорков для shodan используем операторы Google: site:github.com OR site:exploit-db.com shodan dork

Расширенные инструменты поиска

Censys

Censys.io — достойный аналог Shodan. Из очевидных плюсов у Censys улучшенная система поиска по сертификатам. Это позволяет находить хосты, защищенные WAF. Например, можно найти реальный IP домена, который спрятан за Cloudflare (по его параметрам и сертификату). Есть возможность находить сертификат, используя только хеш-суммы.

ZoomEye

ZoomEye.org больше специализируется на поиске устройств, используя их геоданные. Главной особенностью является карта, на которую нанесены нужные нам устройства. Также можно искать устройства по MAC-адресам.

Skillbox

Дополнительные средства поиска

Дополнительные средства поиска

Поисковые системы не всегда выдают достаточное количество данных. Чтобы получить больше, воспользуемся дополнительными средствами поиска.

Web.archive.org

Иногда данные могут быть удалены с сайта. Здесь нам на помощь приходит проект Web Archive, также известный как Wayback Machine. Он сохраняет историю всего интернета, слепки всех веб-сайтов (более 423 миллиардов страниц).

Мы можем проследить изменение сайтов с момента начала ведения архива, даже если этих страниц уже нет в интернете.

2ip.ru

Этот сервис представляет собой мультитул и нужен для сбора информации об интернет-ресурсах и пользователях. На нем вы можете получить сведения о доменных серверах, доступности сайта, системах управления контентом, владельцах домена, хостинге сайта, параметрах DNS, посещаемости и проверки на вирусы.

Здесь же вы найдете большое количество тестов и другой аналитической информации, сможете проверить анонимность своего соединения.

Viewdns.info

Для сбора подробной информации о DNS-серверах сервис подходит лучше всего. Его главная особенность — хранение истории DNS-серверов. Вы можете сопоставить доменное имя с IP-адресами, которые раньше ему принадлежали. Это крайне полезно для определения реального IP, если сайт был спрятан за системами защиты и перенес свое доменное имя на другие сервера.

Дополнительные средства поиска

iknowwhatyoudownload.com

Сервис помогает системным администраторам обнаружить большой поток трафика, чтобы проверить IP-адрес, например, для выявления запущенного торрент-трекера.

OSINTFramework.com

Это база данных различных утилит и сервисов, посвященных разведке открытых источников, поиску уязвимостей, утечек паролей и многому другому. К примеру, мы можем узнать, в каких социальных сетях зарегистрирован тот или иной аккаунт, используя почту или телефон, полученную на предыдущих этапах разведки.