**Profile of the organization's security posture**

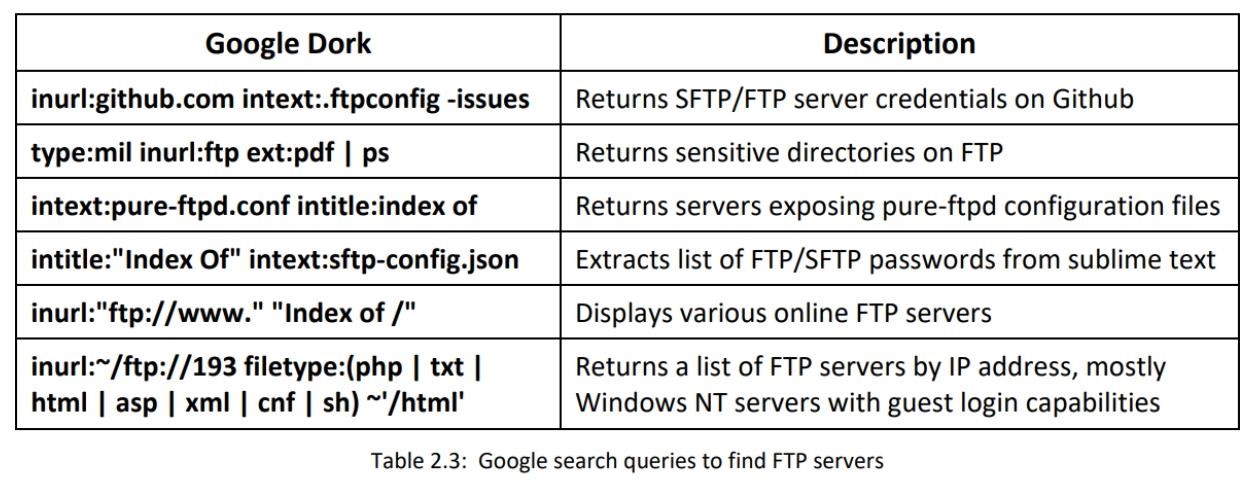
|  |  |
| --- | --- |
| **Organization Information** | Nextcloud.com |
| **Network Information** | 2a01:4f9:2b:29dc::155] |
| **System Information** |  |
|  |  |

|  |  |
| --- | --- |
| **Organization Information** |  |
| Employee details (employee names, contact addresses, designations, and work experience) |  |
| Addresses and mobile/telephone numbers |  |
| Branch and location details |  |
| Partners of the organization |  |
| Web links to other company-related sites |  |
| Background of the organization |  |
| Web technologies |  |
| News articles, press releases, and related tech documents |  |
| Legal documents related to the organization |  |
| Patents and trademarks related to the organization |  |

|  |  |
| --- | --- |
| **Organization Information** |  |
| Domain and sub-domains |  |
| Network blocks |  |
| Network topology, trusted routers, and firewalls |  |
| IP addresses of the reachable systems |  |
| Whois records |  |
| DNS records and related information |  |

|  |  |  |
| --- | --- | --- |
| **System Information:** | |  |
| Web server OS | |  |
| Location of web servers | |  |
| Publicly available email addresses | |  |
| Usernames, passwords, and so on. | |  |
| software versions, | |  |
| server names, | |  |
| database schema | |  |
| **Footprinting Using Advanced Google Hacking Techniques** | |  |
| • Files containing passwords | |  |
| • Sensitive directories | |  |
| • Pages containing logon portals | |  |
| • Error messages that contain sensitive information | |  |
| • Pages containing network or vulnerability data, such as  IDS, firewall logs, and configurations | |  |
| • Advisories and server vulnerabilities | |  |
| • Software version information | |  |
| • Web application source code | |  |
|  |  |  |
| • | Connected IoT devices and their control panels, if unprotected |  |
| • | Hidden web pages such as intranet and VPN services |  |

Examples



**Gathering Information from IoT Search Engines**

Internet of Things (IoT) search engines crawl the Internet for IoT devices that are publicly accessible. Through a basic search on these search engines, an attacker can gain control of Supervisory Control and Data Acquisition (SCADA) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc. Many of these IoT devices are unsecured, i.e., they are without passwords or they use the default credentials, which can be exploited easily by attackers. With the help of IoT search engines such as Shodan, Censys, and Thingful, attackers can obtain information such as the manufacturer details, geographical location, IP address, hostname, and open ports of the target IoT device. Using this information, the attacker can establish a back door to the IoT devices and gain access to them to launch further attacks.

**Footprinting through Web Services**

This section aims to familiarize you with finding the target company’s top-level domains, sub-domains, and geographical location.

* **Netcraft**

Source: https://www.netcraft.com

Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning.

* **Pentest-Tools Find Subdomains**

Source: https://pentest-tools.com

Pentest-Tools Find Subdomains is an online tool used for discovering subdomains and their IP addresses, including network information and their HTTP servers.

**People Search on Social Networking Sites**

Searching for a particular person on a social networking website is fairly easy. Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites contain information that users provide in their profiles. They help to directly or indirectly relate people to each other through various fields such as common interests, work location, and education.

**People search service - Intelius**

Source: [https://www.intelius.com](https://www.intelius.com/)

**Footprinting through Job Sites**

Attackers can gather valuable information about the operating system, software versions, company’s infrastructure details, and database schema of an organization through footprinting job sites using different techniques

* **SHODAN Search Engine**

Source: https://www.shodan.io

Shodan is a computer search engine that searches the Internet for connected devices (routers, servers, and IoT.). You can use Shodan to discover which devices are connected to the Internet, where they are located, and who is using them.

Shodan is a search engine that enables attackers to perform footprinting at various levels. It is used to detect devices and networks with vulnerabilities. A search in Shodan for VoIP and VPN footprinting can deliver various results, which will help gather VPN-and VoIP-related information.

* **Censys**

Source: https://censys.io

Censys monitors the infrastructure and discovers unknown assets anywhere on the Internet. It provides a full view of every server and device exposed to the Internet.

* **EDGAR Database**

Source: https://www.sec.gov/edgar.shtml

The Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file with the U.S. Securities and Exchange Commission (SEC).

**D&B Hoovers**

Source: http://www.hoovers.com

D&B Hoovers leverages a commercial database of 120 million business records and analytics to deliver a sales intelligence solution that enables sales and marketing professionals to focus on the right prospects so that they can generate immediate growth for their business.

* **LexisNexis**

Source: https://www.lexisnexis.com

LexisNexis provides content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets. It maintains an electronic database of information related to legal and public records.

* **Business Wire**

Source: https://www.businesswire.com

Business Wire focuses on press release distribution and regulatory disclosure. This company distributes full-text news releases, photos, and other multimedia content from various organizations across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences.

* **Factiva**

Source: https://www.dowjones.com

Factiva is a global news database and licensed content provider. It is a business information and research tool that gets information from licensed and free sources and provides capabilities such as searching, alerting, dissemination, and business information management. Factiva products provide access to more than 33,000 sources such as licensed publications, influential websites, blogs, images, and videos. Its resources are made available from nearly every country worldwide in 28 languages, including more than 600 continuously updated newswires.

**BuzzSumo**

Source: https://buzzsumo.com

BuzzSumo’s advanced social search engine finds the most shared content for a topic, author, or domain.

* **Followerwonk**

Source: https://followerwonk.com

Followerwonk helps you explore and grow your social graph: Dig deeper into Twitter analytics: Who are your followers? Where are they located? When do they tweet? As shown in the screenshot, attackers use Followerwonk to track the geolocation of the target Twitter users.

* **Burp Suite Source:**

https://portswigger.net

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities

* **Website Mirroring Tool: HTTrack Web Site Copier**

Source: http://www.httrack.com

HTTrack is an offline browser utility. It downloads a website from the Internet to a local directory and recursively builds all the directories including HTML, images, and other files from the web server on another computer.

* **Extracting Website Information from https://archive.org**

Source: https://archive.org

Archive is an Internet Archive Wayback Machine that explores archived versions of websites. Such exploration allows an attacker to gather information on an organization’s web pages since its creation.

**Whois Lookup Result**

Whois services such as http://whois.domaintools.com or https://www.tamos.com can help to perform Whois lookups.

The screenshot shows the result analysis of a Whois lookup obtained with the two above-mentioned Whois services

**IP Geolocation Lookup Tools**

* **IP2Location**

Source: https://www.ip2location.com

As shown in the screenshot, attackers use IP2Location tool to identify a visitor's geographical location, i.e., country, region, city, latitude and longitude of city, ZIP code, time zone, connection speed, ISP, domain name, IDD country code, area code, weather station code and name, mobile carrier, elevation, and usage type information using a proprietary IP address lookup database and technology.

* **Extracting DNS Information**

DNS interrogation tools such as Professional Toolset (https://tools.dnsstuff.com) and DNS Records (https://networktools.com) enable the user to perform DNS footprinting.

* **Reverse DNS Lookup**

**Source: https://www.yougetsignal.com**

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

* **Traceroute**

Finding the route of the target host on the network is necessary to test against man-in-the-middle attacks and other related attacks. Most operating systems come with a Traceroute utility to perform this task. Example with the destination IP address or domain name as follows:

**tcptraceroute www.google.com**

You can create diagrammatic representations of the target organization’s network presence and also you can try to find

**1-Information Leakage:** If there is any sensitive information.

**2-Privacy Loss:** Through footprinting, hackers can access the systems and networks of the organization **3-Corporate Espionage**

**4-Reduce Focus Area recommendation**

1. **Identify Vulnerabilities**
2. **Draw Network Map:** Combining footprinting techniques with tools such as Tracert allows the attacker