Search Skills

When doing ONSIT we can use a various amount of search skills to help us find all sorts of information

Within general search engines such as google we can use search operators to find specific things like file types containing specified terms E.g.

filetype:pdf cyber warfare report

will search google for pdf files containing the term cyber warfare report.

Specialised search engines

Shodan - is a search engine for devices connected to the internet and allows you to search for specific types and versions of servers, networking equipment, industrial control systems and IOT devices.

Shodan

Censys - focuses on internet connected hosts, websites, certificates, and other internet assets. Some of its use cases include enumerating domains in use, auditing open ports and services, and discovering rogue assets within a network.

Censys

VirusTotal - website that provides virus-scanning service for files using multiple antivirus engines. Allows users to upload files or provide URLs to scan them against numerous antivirus engines and website scanners in a single operation.

VirusTotal

Have I Been Pwned - can be used to check if an email address has been involved in a data breach.

Have I Been Pwned

Vulnerabilities and Exploits

CVE

Common Vulnerabilities and Exposures (CVE) program is essentially a dictionary of vulnerabilities. providing a standardised identifier for vulnerabilities and security issues in software and hardware products. Each assigned with a CVE ID like CVE-2024-29988.

CVE Program
National Vulnerability Database

Exploit Database

to exploit a vulnerable system we might need to find a working exploit code this is where we can use an exploit database. It lists exploit codes from various authors some of these codes are tested and marked as verified.

Exploit Database

Technical documentation

linux

Linux manual pages can check any commands manual by typing in:
Man [Command(IP)]

Microsoft Windows

Microsof provides an official docs website and can search things like commands such as ipconfig

Technical Documentation

Social Media

One of the best resources for ONSIT when trying to gather information for someone specific and making a targeted attack. Facebook and other platforms can giveaway details to things like security questions e.g. What school did you go to as a child and other information that could be useful for social engineering the target.