Open Source Intelligence Gathering

OSINT

The start of the information gathering phase is going to start with basic open-source-intelligence. OSINT is the process of looking on social media sites, such as Instagram, Facebook, linked in, Twitter and any other platform where employees of companies reveal their personal details, anything from their dog's name (Dogs name could be used in a word list to attempt a brute force attack on their password) to their home addresses, phone number, hobbies and interests.

There are several techniques in which is used for open-source-intelligence gathering, these include checking if the employee's email has been compromised in a data breach (www.haveibeenpwned.com) and using applications such as h8mail to find their compromised password(new and old) and other applications such as hydra, these applications either find already leaked information or brute force/dictionary attack common passwords and reveal the user's current password. Looking for old employee information is a good idea as their login credentials might still be working and the system administrators might've forgotten to expire their credentials. So finding old employee information could serve useful.

Password lists for brute force attacks can be customised and personalised for individual companies. A good way to do this is to create a script, take all the text from the homepage of the website, have your script separate each word out and then create multiple variations of that same word. This will create a password list of fourteen thousand plus words in which can be used to brute force a password. You should also include common passwords in a separate list and perform multiple attacks until one list returns a positive result, be careful of false positives. Companies like Google and Facebook lock you out after three failed attempts to prevent password spraying, so finding an anime website, GTA website or movie torrent site that the target uses is a good way to perform brute force attacks as those sites might not have set their password fields to fail after three failed attempts. Good soft targets are those who are non-technical employees, so target employees who probably don't have many technical skills, knowledge and ability, this is because their passwords will be the weakest.

As the researcher, you're trying to collect meta-data in which can be used later in-order to bypass login fields, social engineering campaigns, and to try and make yourself look possibly like an employee.

Google Dorking is another open-source information gathering technique in which Google is being used to index websites, old versions and new versions for network log files, passwords, emails/usernames, penetration/bug reports, IoT devices such as cameras and more. A big advantage google Dorking is that it's good for finding vulnerable websites, just by searching "Index of admin" and "Inurl: Admin_Panel" you can find quite a few websites that have their admin panels exposed for public access. You can search anything from SQL injectable URLs to password/email lists, all can be used for OSI. In-short google dorks are great for finding out of date and vulnerable websites. Google works by crawling websites based on your search query, it doesn't say no when you are trying to find company information that shouldn't be publicly available.

A robots.txt file contains instructions for bots that tell them which webpages they can and cannot access. Robots.txt files are most relevant for web crawlers from search engines like Google. Check for robots.txt files. Robots.txt files are files that the web admin is hiding from public access and gaining access to such files without express permission is prohibited. Robots.txt files can reveal interesting directories such as /admin or /administration.

Shodan is a search engine for internet-connected-devices and any device that is exposed to the internet. Instead of indexing web pages, it indexes IoT devices and returns results based on queries, such as “port: 22” which will find SSH servers that are running on port 22. Shodan allows users to monitor network security, explore IoT devices and power plants. Shodan works by taking information from banners, which is metadata about a software that’s running on a device. Google works by crawling the web for information, Shodan works by indexing the web for IoT devices based on your query syntax.

Website third party vendors. As a researcher, you will need to find out what services a website is running and all their plug-ins, you can do this by using the wappalyzer extension in Firefox which returns results such as web hosting servers, analytics, programming languages, code libraries, frameworks and much more. Using Unix commands is another way to do more searching, such as nslookup which is used for querying internet domain name servers (DNS), other commands include ping to see if the target is online, dig which interrogates DNS servers, such as DNS lookups and displays the answers returned from the name servers that were queried.

Network utility tools:

- Dig
- nslookup
- ping
- host
- finger
- traceroute
- netstat
- tracepath
- hostname
- route
- whois

Enumerating subdomains. Enumeration of subdomains is a handy trick to finding sub-domains on a target, these aren’t supposed to be revealed, however, due to misconfiguration, and poor management of the website as the subdomains like /admin aren’t supposed to be easy to access however due to poor management and lack of competency attackers can enumerate the subdomains and find admin panels, blogs, forums, mails for routing mail traffic and much more if the configuration of the subdomains isn’t done properly then you could reveal sensitive company data to anyone who tries to find it. DNS enumeration is the process of locating all of the DNS servers and their corresponding records for an organisation.

Finding subdomains that are out of date and need to be renewed can be used against an organisation in a phishing campaign tricking employees for example to login to a portal that is trusted by the company (or was) and then employees logging in, basically handing their internal emails, usernames and passwords over to the attackers where they can dive deeper inside of the company. This is an easy attack as it’s easy to forget to renew domains annually and if it was set up to automatically to renew then something could’ve gone wrong and the system didn't renew. Once the attacker registers that domain they can use it in a phishing email to trick employees into handing their data over.

DNS enumeration can yield results such as the OS that is running on the target server, finding IP addresses of potential target systems, username and computer names. If DNS systems are not configured correctly then attackers can gather up sensitive information about your organisation's network which could result in a DNS zone transfer and DNS tunnelling.

Tools used for DNS enumeration:

- Maltego
- dnenum
- recon-ng
- dnsrecon
- theHarvester
- nslookup
- dig

Network vulnerabilities. Lastly scanning a target's network using software like Nmap is a great way to find out a lot of reconnaissance. It can yield results such as open ports, services running on those ports and operating systems that are being used. Nmap is a network mapping tool that creates a map of an organisations network for researchers and IT professionals to check what is running on their networks. Nmap is great for checking for what systems are running on the companies network, revealing security risks, port scanning, locating hosts and creating a road map of the network.

Not forgetting that the simplist way to find out information in your recon phase is to simply google. Google can yield a vass library in which you can use. Google emails, usernames, Google dork and search for employee information.

This document outlines only some of the techniques used in open-source-intelligence-gathering. OSINT is an efficient way and a completely legal way of taking seemingly harmless information that is freely available on the web and using it to get a foot hold into and organisations network.