Phase 1: Reconnaissance

Perform Reconnaissance Goal: Build as robust a profile on the target (Artemis) as possible. Should cover at least 15 tools/resources.

1. Maltego
    a. This tool focuses on finding particular relationships between assets, people, companies, and website domains for investigative tasks.
    b. Over 58 data sources are used to gather the information leading to these relationships.
    c. Use transforms within Maltego to draw power (perform searches, and utilize tools) from other tools/resources such as Shoden and Farsight DNSDB.
    d. Build off of domains or IP addresses to find relating subdomains, IP addresses, and more
2. UserSearch.org
    a. Use this tool to find people by usernames and emails.
    b. This is a great tool when reviewing sites such as those relating to social media, the company's website, etc. where you can find the emails and usernames of the employees working for the company and then use them through the tool.
    c. The tool searches through dating sites, forums, crypto chat sites, and loads of other communities.
3. DorkSearch
    a. A tool with plenty of semi-secret search terms that can be used in Google. Using them can show results not really intended to be in Google aka Google Hacking.
    b. This tool not only can help sharpen the tester's Google Hacking skills but also helps with prebuilt screens.
        i. For example, when searching google with:

1. intitle:index of /views/auth/passwords
    a. Helps find parts of vulnerable servers
2. intitle:index of *.pl
    a. Helps find vulnerable files being hosted

c. Primary features:
    i. PreBuilt : Access over 7,000 prebuilt Dorks.
    ii. Builder : Build your own, mix & match, discover new Dorks.
    iii. Submit : Create your own dork and have them credit it to your handle/name.

4. Mitaka
    a. This is available as a Chrome Extension and also for Firefox.
    b. It allows you to search over a dozen major search engines for domains, URLs, IP addresses, MD5 hashes, ASNs, and Bitcoin addresses.
    c. Helps to fill in gaps other tools may have missed by searching / scanning on various engines that are not being used already.
        i. -- e.g. VirusTotal, urlscan.io, Censys, Shodan, etc.
5. SpiderFoot
    a. A collection of OSINT resources similar to Maltego
    b. It searches for IP addresses, CIDR ranges, domains, subdomains, ASNs, email addresses, and phone numbers.
    c. This tool also offers a CLI version that could be very helpful with automation and connections to current scripts used for reconnaissance.
6. Spyse
    a. This tool is described online as ‘the most complete internet asset registry‘ online.
    b. The tool is known to provide the back-end data for many major OSINT tools.

    c. It collects publicly available data on websites, and their WHOIS information (such as owners, associated servers, and IoT-linked devices).
    d. Identify potential security risks and connections between various entities.
7. BuiltWith
    a. Use to find out what sites being hosted by the company are built with.
    b. Detects whether a website is built using WordPress, Joomla, or any other CMS-like platform.
    c. Generate a list of the plug-ins that the website is currently using, its frameworks, and even its server information that's publicly available.
8. Intelligence X
    a. Search through the archive of historic versions of websites online and leaked data.
    b. This information is generally taken off line and hidden from the public.
    c. This tool keeps the information online forever and is great for looking for vulnerabilities that may have not been fully corrected with current versions.
9. Grep.app
    a. A tool used to search through a half a million git repos at a time.
    b. This could greatly help when searching for vulnerabilities and other reconnaissance assistance such as looking for vulnerabilities of a particular version of a server/service/etc..
10. Recon-ng
    a. Written in python and easily implemented into python scripts as needed.
    b. Search public information about the company.
    c. It works in modules, with a lot of inbuilt functionality designed for easy use.
    d. Normalize the data outputs
    e. Linking into databases

f. URL requests to websites
g. Using/managing API keys to gather data directly from API interfaces
h. All of this helps the tester to focus more on the reconnaissance instead of on the repetitive OSINT gathering tasks.

11. theHarvester
    a. Find public information on an organization's computer network passively.
    b. The tool uses Netcraft for data mining and the Alien vault threat exchange. In doing so, it can quickly identify known vulnerabilities.
    c. The tool can gather emails, names, subdomains, IPs, and URLs on the organization.
12. Shodan
    a. A tool used to find intelligence on IoT devices.
    b. It can detect open ports, vulnerabilities on targeted systems, and scan devices that are not typically supported by standard port scanners.
    c. Devices such as cameras, building sensors, security devices, Xboxes, security cameras, household fridges, and so on could be found linked to the company's networks all of which could contain vulnerabilities.
13. Metagoofil
    a. A free tool on GitHub
    b. It is used to pull out information and metadata on public documents, such as PDF, Doc, Docx, Xls, and other common document formats making it an excellent choice for a document investigation tool.
    c. Find usernames of those who created documents, as well as their real names and sometimes even their addresses.

d. Also artifacts such as server name, network share resources, and directory information of the network shares can be found as well for more possible vulnerabilities and important reconnaissance information.

14. Searchcode
    a. This tool allows you to search through software code.
    b. Sensitive information is sometimes left within the source code of computer programs either on purpose thinking no one would care to look or on accident.
    c. Emails, usernames, and even passwords could be found inside the source code. In addition, other information involving vulnerabilities could be found as well.
15. Babel X
    a. This tool helps with language barriers.
    b. While it is easy to spot what information you need when sifting through information that is in your own language, it is very difficult to sift through information of another language that you don’t know.
    c. This tool helps to remedy this problem and finds information relating to over 200 different languages.
16. OSINT Framework Resource
    a. This resource is one of the primary go-tos to find more tools and resources for all OSINT needs.

References

Top 17 open source intelligence tools (OSINT) to find anyone online - 2022. News & Article. (2022, April 10). Retrieved May 9, 2022, from https://usersearch.org/updates/2022/04/10/top-16-open-source-intelligence-tools-ever-made-osint/

Mine, merge, map data with Maltego. Maltego. (n.d.). Retrieved May 9, 2022, from https://www.maltego.com/product-features/

YouTube. (2018, November 21). *Maltego - automated information gathering*. YouTube. Retrieved May 9, 2022, from https://www.youtube.com/watch?v=zemNLx0-LRw