Reconnaissance: All tools and Methods used to Perform Reconnaissance.

Vincent Kiweesi

Capstone

May 15th, 2023

The current goal is building a thorough profile on Artemis. The target is technological stack, contact information, phone numbers, and other details will all be included in this profile. Employ a number of tools and techniques to gather information that is readily accessible in order to complete this work. The tools and techniques that will be used will be described in general terms in this deliverable, and they will be mostly in passive reconnaissance. For methods use passive reconnaissance, tools that don't require the target to be interacted with are called passive tools. These technologies primarily rely on data that is made accessible to the public. Check for public records, business records, phone numbers, domain names, IP addresses, social networks, people searches, and email addresses in depth using the Osint framework.  
A platform for developing software GitHub is useful to learn more about Artemis's technology stack, it can be useful to search for any publicly accessible repositories that are connected to it.  
Also an employment board called Glassdoor offers data about businesses, such as ratings of the employer, wages, and interview questions. Glassdoor will be used to collect data about Artemis, including wages and employee reviews. Tools like nmap, telnet and netcat(nc) would be utilized in gathering information through scanning for open ports. Social engineering refers to all methods used to convince a target to give away certain information or carry out a particular action for improper motives.

Then Proceed to the following steps:

- using google.com to look up the company URL or on Osint Framework

-Using linux terminal to determine which ports are open to perform a banner grab.

-Utilize nmap command to view the open ports nmap www.artemis.com

- Use netcat(nc) and TELNET command to perform the banner grab nc www.artemis.com 21 and for telnet www.artemis.com press Control + C to terminate the connection. telnet www.artemis.com 25

-To target a specify port include the port number at the end of the command like nc www.artemis.com 21 or telnet www.artemis.com 25

-To get additional service information on a port number use nc www.artemis.com 443 and on the next line type HEAD / HTTP/1.0

Additionally, use OSINT described as data collected from publicly available sources to be used in an intelligence context. OSINT is a practice that anyone with Internet access can do. Available huge amounts of information about Artemis could be found utilizing the Osint tools starting from a passive reconnaissance phase.

The first step is to get to know Artemis by gathering enough information without actively engaging with them.

Find out the type of public facing assets through postings on social media to know about the insides of the organization or even gather information from satellite and street-view images to know more about the premises.

OSINT tools can help identify that open-source information of your Artemis is publicly available on the Internet. With this, the search for information about the company’s assets like internet-facing infrastructure information, from cloud-assets, hosting services, domain names, and more is made easier. The OSINT tools can help discover internal/external asset information and give a detailed report. These tools passively explore the Internet to find information publicly available about the assets of the company.

Employees of the company could post private information on social media. An IT manager might post something after spending a long day updating the server in full description. A search for sensitive material on websites or social media posts that are outside the boundaries of the network can be performed using OSINT technologies.

Aggregation of information. The OSINT program may aggregate all data after collecting and discovering information from public sources and can offer useful insights.

The who, what, when, where, and why thanks to this can now be discovered.

Best OSINT tools and applications

There are numerous resources available to use in gathering information.

What characteristics ought open-source intelligence systems have?

**Analysis and systems for OSINT:**

* Automated tools that can quickly scan the entire world.
* Flexible tools that use search criteria to weed out results that aren't relevant.
* Systems that allow both PCs and IoT devices to query data.
* Research tools that uncover relevant intelligence connected to a main search topic.
* Platforms that allow computers and IoT devices to access data simultaneously.
* Apparatuses that hackers are known to employ.
* A no-cost evaluation period or a free tool
* Useful tools, both free and paid, that are affordable.

With this choice in mind, a variety of tools can be employed in a variety of ways to acquire intelligence.

### Recon-ng

Python-based Recon-ng is an OSINT and web reconnaissance framework. By quickly properly examining the open-source information on the web, it can automate the process of acquiring information. Once it locates useful information, it will gather it and present it in an organized and understandable manner. An interactive command-line interface built on modules is included with the utility. The independent modules are discovery, exploitation, reporting, import, and recon. The user interface is quite similar to the well-known Metasploit Framework, which is used to break into systems. Contextual help, command completion, database interaction, API key management, and standardized outputs are other helpful features of the interface. Python 2.0 is needed to install Recon-ng, which is only compatible with Linux (Wilson, 2022).

### Shodan

The first search engine for Internet of Things (IoT) devices is called Shodan. Shodan scans every other website on the Internet in addition to Google's web index. Anything that is connected to the Internet, including webcams, servers, routers, surveillance, traffic lights, smart TVs, refrigerators, and vehicles, can be located. Shodan came up with a method to locate information on these IoT devices and included their open ports and vulnerabilities. These IoT devices are frequently not searchable. One of the few search engines that can find operational technologies present in industrial control systems is this one. Because of this, Shodan is a vital tool for cybersecurity in the sector. Shodan may be used to identify IoT devices as well as databases to check for data leaks on public websites. It can even find IoT devices hidden in video game servers within corporate networks (Wilson, 2022).

### Maltego

It offers interactive data mining with detailed visualizations that facilitate effective connection analysis. The software is used to conduct online investigations on the connections between data from various web sources. It can find publicly available information and relationships between people and businesses. Maltego, for instance, can discover connections between emails, users, businesses, websites, and other things. It uses this data to create a graph that displays all linkages and data points. Based on a library of transforms, Maltego enables discovery from a number of open sources. Maltego already has a comprehensive list of transforms, but you may add to it by using the API to access other publicly available data sources. The program is Java-based and can be installed on windows, macOS, and linux (Wilson, 2022).

**theHarvester**

Is a straightforward OSINT passive reconnaissance tool created in Python. The SHODAN database of internet-connected devices, PGP key servers, and search engines are only a few examples of the several public information sources from which it was intended to gather data. The tool is excellent for locating information that is located outside of an organization's boundaries, but it can also locate assets with a public facing inside the boundaries. It can find data on subdomains, URLs, IP addresses, email addresses, employee names, and more. Utilizing theHarvester is not that difficult. For passive reconnaissance, several of the most widely accessible sources, like Google, Hunter, and Baidu, aroused. Some modules, like bingapi, GitHub, and others, can be installed with an API key (Wilson, 2022).

### Recorded Future

Is an integrated threat intelligence tool. Large amounts of threat data may be gathered and analyzed instantly by the program. With the use of ML (Machine Learning), AI (Artificial Intelligence), and NLP (Natural Language Processing), it transforms any data into insightful information. With the use of the Threat Intelligence Platform (TIP), Recorded Future can execute passive reconnaissance, one of its numerous features. Recorded Future can gather and aggregate data from publicly accessible sources, including domain registrations, social network profiles, third-party websites, and more, by leveraging ML, AI, and NLP. When it discovers data leaks, including credentials, typosquat domains, code leaks, bank identification numbers, brand discussion on the dark web, and more, it operates automatically and gives real-time notifications (Wilson, 2022).

**Metagoofil**

Is a Python-based, open-source passive recon metadata collector. It is used to extract data from documents such as PDFs, Docs, XLS, PPTs, ODPs, and ODs that can be found on the target's website or any other open website. The program searches for the documents on Google, downloads them to the local disk, and then extracts all their metadata. These documents' metadata are analyzed by Metagoofil, which also gathers a lot of data. It can locate private data such as usernames, real identities, software versions, emails, pathways, and servers. Metagoofil is a tool that hackers can use to acquire username information and carry out brute-force assaults more quickly. Additionally, it can display to a hacker file paths that indicate OS, network, shared resources, and more (Wilson, 2022).

**Search code**

Is a special kind of search engine that searches the free source code for intelligence. Developers can utilize Search code to find issues with sensitive information being accessible in the code. Like Google, the search engine scans the code of active apps or apps that are still in development for information rather than indexing web servers. A hacker may be able to find usernames, weaknesses, or errors in the code by using the search results. Code repositories from GitHub, Bitbucket, Google Code, GitLab, CodePlex, and other sources are searched by Searchcode. Various language filters are available. For instance, by checking the box, Searchcode will restrict all the results so that you only see HTML, PHP, or JavaScript.

Key Features:

* Use a special character to search.
* Categorize by programming language.
* categories by repository
* Search through source code

**GHDB (Google Hacking Database)**

### A database of Google search queries that seeks to uncover publicly available information is known as. GHDB (Google Hacking Database) or Google Dorks or just the victims unknowingly disclose anything on the Internet that is vulnerable, including unprotected web consoles, open ports, login portals, sensitive folders, open webcams, username information files, and sensitive directories. Every day, the Google Dorks community publishes a number of sophisticated Google search phrases. Google dork queries include things like "intitle:index.of "users.db," which exposes files with users, and "intitle: "webcamXP 5," which displays any webcams with the brand XP5 that are now available for viewing.GHDB is designed for pen testers who are in the OSINT (operational security intelligence) phase.If a pen-tester is skilled at creating complex Google searches or can discover the ideal candidate in GHDB Almost anything can have security flaws in its configuration or coding (Wilson, 2022).

### SpiderFoot

### Is an open-source intelligence reconnaissance tool. It is frequently referred to as the OSINT fingerprinting with the largest collection. The application may gather data on IP addresses, domain names, web servers, email addresses, and more by sending automated queries to more than 100 public sources. Python is used to create the program. Select the target and a fingerprinting module from the many hundreds available to begin using Spider Foot. Examples of SpiderFoot modules include "sfp\_arin.py" which searches the ARIN registry for contact information and "sfp\_crt.py" which extracts hostnames from old certificates in crt.sh. SpiderFoot will automatically gather data and provide a report after you select the modules (Wilson, 2022).

### OSINT Framework.

### The OSINT Framework will point you in the correct way if you haven't yet discovered your ideal OSINT tool (or if it isn't on our list). The OSINT framework is not a piece of software per se, but rather a group of tools that greatly simplify OSINT activities. The OSINT Framework delivers the data in an online interactive mind map that graphically arranges the data. The framework is well-liked by cyber-security researchers and pen-testers who are looking for tools for certain information-gathering and reconnaissance tasks. With the help of this framework, you may navigate through several OSINT tools that are categorized. The username, email address, location/maps, dark web, search engines, transit, public records, and many other categories are some examples (Wilson, 2022).

### Intelligence X

### Is a groundbreaking search engine and archive service that maintains not just previous iterations of web pages but also entire leaked data sets that would normally be taken down from the internet due to bad content or legal requirements. Although that might sound similar to what the Internet Archive's Wayback Machine does, there are several significant distinctions between Intelligence X and that service in terms of the kind of content it concentrates on preserving. Intelligence X lacks any differences when it comes to maintaining data sets, no matter how contentious they may be. The list of more than 49,000 Fortinet VPNs that were discovered to be vulnerable to a Path Traversal issue has already been saved by Intelligence X. Plaintext

passwords for these VPNs were also made public on hacker forums later in the week which, despite being deleted from these boards, Intelligence X kept them. The site has already indexed information gathered from the email servers of well-known politicians like Hillary Clinton and Donald Trump. The footage from the Capitol Hill riots in 2021 and the Facebook data dump of 533 million accounts are two more recent examples of media indexed by Intelligence X. Such information can be extremely important in a number of ways to intelligence gatherers, political analysts, news reporters, and security experts (Wilson, 2022).

### 

### DarkSearch.io

### DarkSearch.io can be a useful place for those who are new to the dark web to start their research activities, even though frequent users may already be aware of where to look for what. Like Ahmia, another free dark web search engine, DarkSearch also offers a free API for automated searches. Despite the fact that Ahmia and DarkSearch both have onion websites, neither search engine requires you to utilize Tor or even navigate to the onion versions. You may look up information on the dark web by simply going to darksearch.io from a standard web browser (Wilson, 2022).

### 

### Grep.app

### How do you conduct a search over 500,000 git repositories on the internet? Sure, you could use the unique search boxes provided by GitHub, GitLab, or BitBucket, but Grep.app works incredibly well. In reality, Grep.app has lately been utilized by journalists and Twitter users to estimate the proportion of repositories that use the Codecov Bash Uploader (Wilson, 2022).

Grep app can be helpful when looking for strings connected to IOCs, insecure code, or

malware that lurks in OSS repositories such as the Octopus Scanner,

### Git Paste-12, or malicious GitHub Action cryptomining PRs (Wilson, 2022).

### 

### BuiltWith

BuiltWith allows you to discover what popular websites are made using, as the name suggests. Different websites are powered by various tech stacks and platforms. For instance, BuiltWith can identify whether a website is powered by WordPress, Joomla, or Drupal and provide additional information.  
Additionally, BuiltWith creates a tidy list of popular JavaScript/CSS libraries (like jQuery

or Bootstrap) that a website makes use of. The service also offers a list of

the plugins that have been installed on the websites, as well as information.

about frameworks, servers, analytics, and tracking. It is possible to conduct reconnaissance with BuiltWith.  
What else? To identify common security flaws affecting a website, combine BuiltWith.

With website security scanners like WPScan, which, for instance, integrate with the WordPress Vulnerability Database API.  For those seeking to determine primarily the tech stack's composition, Wappalyzer might be more appropriate for a site because it offers a more targeted, brief result. Test out Wappalyzer and BuiltWith to find which better meets your requirements (Wilson, 2022).

In conclusion, the tools and techniques mentioned above will be used to create a thorough profile of Artemis. These tools have been divided into passive and active tools. While active tools need engagement with the target and rely on publicly accessible data, passive tools don't and rely on that information. We want to gather as much publicly available data on Artemis as we can using these tools and techniques.

Reference

Wilson, M. (2022, August 25). *BEST OSINT Tools & Software for Passive & Active Recon & Security!*. PC & Network Downloads - PCWDLD.com. https://www.pcwdld.com/osint-tools-and-software