Phase 1. Perform Reconnaissance

Goal: Build as robust a profile on the target (Artemis) as possible. The profile should include the target's technology stack, email addresses, phone numbers, resumes, and so on.

Procedure: Detail the activities you plan to use to obtain as much publicly available information as you can.

Deliverable: Provide a minimum two-page description of all the tools and methods you will use to accomplish this task. Deliverables should cover at least 15 tools/resources.

- **Active Recon :** It means interacting directly with a target to gather information. This is not recommended because it violates the rule of "hiding traces" in pen testing.
- **Passive Recon :** It means gathering information about a target using vast information present on the internet. In it, we aren't interacting directly with the target so there is no fear of recording or logging of our activity by target.

1. **Internet Search Engine**
    a. **Internet Search Engines** (Google, Yahoo, Duckduckgo, Bing, etc) - Internet searches provide a wealth of information about a target. There is a way to use internet searches to gain and gather information about the target including: contact information (phone number / email address), social media profiles, links for partners and affiliates, product information, articles, linkedin profile, press releases, etc. Google has a feature called Google Dorking (Google Hacking) is a form of passive reconnaissance allowing you to be a tester to use search strings, operators, Boolean, regular expression to search files, websites to find information that is not readily available with a generic Google search. By using specialized Google queries (Google Dorking), it's also possible to search for files that were not intentionally exposed to the internet but still publicly available as well.
    b. **Google Directives** - Google provides an enhanced method for search using directives. First write the name of the directive you want to use, then a colon(:) and then the term you want to use in the directive. You can combine two or more directives as well.
        i.
```
for e.g- site:geeksforgeeks.org  dhcp snooping
filetype:pdf "some text"
site:geeksforgeeks.org filetype:png "your text"
```
    c. **Google Dorking** - Google has a feature called Google Dorking (Google Hacking) is a form of passive reconnaissance allowing you to be a tester to use search strings, operators, Boolean, regular expression to search files, websites to find information that is not readily available with a generic Google search. By using specialized Google queries (Google Dorking), it's also possible to search for files

that were not intentionally exposed to the internet but still publicly available as well.

2. **WHOIS**
    a. A WHOIS query is a passive reconnaissance tactic where the website shows a company's website and displays pertinent information that is considered public record. A person performing reconnaissance research can lookup registrant information, registrant company, tech contact, years in existence, ip address information, ASN (autonomous system number - administrative domain), and domain information about the company.
3. **Nmap Network Mapper (Nmap)**
    a. is a free and open-source platform that is used to perform initial device or network scanning. This tool is often used in the initial step of penetration testing. The most valuable Nmap tools are for gaining insight into a targeted network, including discovering accessible hosts, operating systems and port discovery. It scans individual IP addresses and ranges and returns valuable information such as the operating system, protocols, utilities, and available ports .
4. **Job Sites**
    a. There are various online job sites that companies utilize to find talent. Scouting the job sites can allow the user to find the company profile or job listings. In the Job Description, the employers list job duties and roles/responsibilities. A person could utilize this information to learn how the system works, the technologies, training required, tools being used, and the interconnectivity of the departments.
5. **HTTrack – Website Copier**
    a. This is a passive reconnaissance tactic that allows the user to download the offline copy of any website. Offline copy includes all images, pages, links and code from the original website. Using this tool, you do not have to spend much time on the target website. Spending too much time on any website may cause monitoring tools to log your activity.
6. **Social Media**
    a. Typically, companies have several social media profiles including (Twitter, Facebook, Instagram, etc). Many companies use social media to increase their visibility. From a reconnaissance perspective, information contained from a company profile includes employee information (titles, roles, responsibilities), networking events, community events, promotions, projects, etc.
7. **Dumpster Diving**
    a. This is another technique used for getting information from a target. Dumpster diving involves the monitoring of the waste bin or dust bin of an organization by an attacker and collecting information such as an important document that may have been disposed of carelessly by staff or workers in the organization.
8. **The Harvester**
    a. This application is designed to assist penetration testers in understanding the client's footprint on the Internet during the early phases of a penetration test.This program's goal is to collect emails, subdomains, hosts, employee names, open ports and banners from a variety of public sources, such as search engines, PGP key servers and the SHODAN computer database.
9. **Shodan**
    a. is a search engine that can be used to locate individual devices and types of devices. Webcams and cisco are the most used searches. The Shodan search

engine scans the entire Internet before parsing the banners returned by the scanned machines. When the search is over, the information returned by the Shodan search will most likely be about web servers and their models, as well as anonymous FTP servers if they operate in a specific area and system model information.

10. Maltego

a. With this tool, the user can pinpoint the location of an individual or business, map out the relationships between them, identify related IP addresses and phone numbers, or identify connections between different companies and individuals.

11. Have I Been Pwned?

a. This a web application that allows you to check whether the credentials of an email have been compromised. It utilizes known database leaks and checks whether your email address was part of those leaks. These leaks are from various sources including public leaks.

12. MX Toolbox

a. This is a valuable resource and includes features including, but limited to: a) Checking to see if your IP or host is on a blacklist, b) Test mail server for Simple Mail Transfer Protocol, otherwise known as SMTP, c) Run a DNS (domain name service) record IP address for host name, d) Check SPF (sender policy framework) and TXT records on a particular domain, e) DNS PTR record, sometimes called a reserve DNS record, for host name

13. NSlookup

a. You can use the nslookup tool to retrieve information about a domain. The information can include the domain name servers, the IP address, the mail servers, and various other records. It can tell you how the domain is configured, provide certain records, and may identify potential targets.

14. Open Source Intelligence - OSINT

a. http://osintframework.com/
b. The OSINT Framework is a web application that catalogs everything you could want to know about Open Source Intelligence Gathering. It has a horizontal hierarchical structure and clicking one category will provide other categories and eventually a link to a resource. The resource will usually provide instructions or a tool for you to perform that specific type of OSINT.

15. Business intelligence Resources

a. Sites like Crunchbase, newspapers Business Section, business magazines (Forbes, Entrepreneur, etc) that have articles in the Business Section have lot of information include profiles, mergers, funding, acquisitions, products, services, employees, departments, etc.

16. Wikipedia/Wikileaks

a. Wikipedia is a public website that details a company's profile including the history, the services/products offered, etc. These articles often accompany external references which can glean more information about the target. Wikileaks are documents that have been "allegedly" leaked from an insider of the company or a bad actor. The documents are posted and uploaded for the public to inspect.

17. Criminalip

a. Criminal IP is a comprehensive threat intelligence search engine that detects personal or corporate cyber asset vulnerabilities in real time and facilitates preemptive responses accordingly. It consists of two main features: SEARCH and INTELLIGENCE, which provide detailed threat-relevant information through banners and malicious behavior history. With Criminal IP, you can find all types of internet-facing information on malicious IPs, phishing sites, malicious links, certificates, industrial control systems, IoT devices, servers, CCTVs, and more.

18. **Certificate Transparency**

a. (https://transparencyreport.google.com/https/certificates) - This resource can be used to identify issued certificates of targets. This will help the attacker to widen the scope of penetration testing.

REFERENCES

https://thescipub.com/pdf/jcssp.2022.103.115.pdf

https://www.geeksforgeeks.org/reconnaissance-and-its-tools/

https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

https://beebom.com/criminal-ip-uses-ai-stop-phishing/

https://www.businessprocessincubator.com/content/what-is-reconnaissance-in-cyber-security/

https://haveibeenpwned.com/

https://systemweakness.com/hack-to-learn-osint-and-passive-reconnaissance-efb4cdc2419f

https://www.linkedin.com/pulse/what-maltego-how-employ-osint-michael-witzsche/

https://medium.com/@iFactoryDigital/we-review-mxtoolbox-2f8440549d2e

https://allabouttesting.org/passive-reconnaissance-techniques-for-penetration-testing/

https://osintframework.com/

https://blog.criminalip.io/2022/04/19/3926/

https://jaimelightfoot.com/blog/reconnaissance-information-gathering/

https://www.firecompass.com/blog/top-10-tools-for-reconnaissance/

https://raleigh.issa.org/google-dorking-google-hacking-a-form-of-passive-recon/