Reconnaissance Plan for Artemis, Inc.

Objective: To build a comprehensive profile on Artemis, Inc. by gathering publicly available data on the company's digital and organizational footprint, including its technology stack, contact information, employee details, and network resources. This will allow us to proceed with a well-informed approach in subsequent penetration testing phases.

Reconnaissance Tools and Methods

1. Google Dorking

- **Purpose**: Leveraging advanced search queries, Google Dorking can reveal unsecured files, directories, and sensitive information on public websites.
- **Usage**: Customized queries like `site:artemis.com filetype:pdf` can identify documents or specific directories related to Artemis.

2. Shodan

- **Purpose**: An internet-connected device search engine that indexes devices, services, and open ports accessible on the public internet.
- **Usage**: Shodan queries for Artemis's IP range can uncover exposed services, open ports, and device details.

3. Whois Lookup

- **Purpose**: Reveals domain registration details such as registrant contact info, IP ranges, and DNS servers.
- **Usage**: Use Whois to uncover Artemis's network information, potentially providing IP addresses for further targeting.

4. theHarvester

- **Purpose**: Aggregates email addresses, subdomains, IP addresses, and URLs associated with a target domain.
- **Usage**: `theHarvester -d artemis.com -b all` helps identify external points for further investigation and possible email addresses.

5. LinkedIn and Social Media Profiling

- **Purpose**: Social media platforms offer insights into employee roles, company structure, and technology stacks used.

- **Usage**: LinkedIn profiles reveal job descriptions that often list the technologies employees use, providing indirect hints about Artemis's infrastructure.

6. Maltego

- **Purpose**: A visualization tool that maps relationships between people, companies, and infrastructure elements like domains and IP addresses.
- **Usage**: Maltego's transforms can help uncover hidden connections and visualize data gathered across multiple sources.

7. DNS Dumpster

- **Purpose**: Maps DNS records and subdomains, providing a topological view of Artemis's domain space.
- **Usage**: Useful for identifying subdomains and public-facing records that might serve as entry points or contain misconfigurations.

8. Hunter.io

- **Purpose**: Locates and validates corporate email addresses associated with a target domain.
- **Usage**: Hunter.io can identify standard email formats used at Artemis, which could be valuable for social engineering strategies.

9. FOCA (Fingerprinting Organizations with Collected Archives)

- **Purpose**: Extracts metadata from public documents like PDFs and Word files to gather information on software versions, internal IPs, and usernames.
- **Usage**: FOCA can analyze files on Artemis's site, providing data on internal systems and potentially vulnerable applications.

10. SpiderFoot

- **Purpose**: An automated OSINT tool that collects data on IP addresses, subdomains, employee information, and more.
- **Usage**: SpiderFoot aggregates data from sources like DNS records, social media, and financial reports, giving a comprehensive view of Artemis's digital presence.

11. Recon-ng

- **Purpose**: A modular OSINT framework used for gathering data on domains, IPs, and people.
- **Usage**: Recon-ng's modules automate data gathering and simplify the aggregation of OSINT from sources such as social media and data dumps.

12. Censys

- **Purpose**: Searches internet-connected devices, much like Shodan, but with enhanced visibility into certificates and service details.
- **Usage**: Useful for identifying SSL certificates associated with Artemis and validating host information.

13. Wayback Machine (Internet Archive)

- **Purpose**: Allows viewing of past versions of Artemis's website to analyze historical configurations and potentially deprecated systems.
- **Usage**: Reviewing old web pages may reveal previously used email addresses, links, and systems that are still accessible.

14. Pastebin Monitoring

- **Purpose**: Pastebin and similar sites often contain data dumps or sensitive information mistakenly shared.
- **Usage**: Search for any pastes mentioning Artemis or containing sensitive information like credentials.

15. Company Press Releases and News Articles

- **Purpose**: Public announcements often reveal new technology deployments, partnerships, and organizational changes.
- **Usage**: Reviewing press releases can help identify key personnel, technological investments, and changes in infrastructure or security posture.

Methodology

Using these tools, we will conduct the reconnaissance in a systematic approach, starting with **domain and network enumeration** to locate subdomains, IPs, and exposed services. This will be followed by **social and employee profiling** via LinkedIn and similar sites to identify potential social engineering vectors and gather indirect technology insights. Finally, we will perform **data and metadata analysis** through tools like FOCA and the Wayback Machine to extract potentially sensitive information and map the historical evolution of Artemis's technology and infrastructure.

Expected Outcomes

By applying these tools, we aim to:

- **Identify Exposed Network Resources**: Detect internet-facing assets for further analysis.
- **Map Technology Stack**: Infer technologies used internally at Artemis based on metadata and employee profiles.

- **Uncover Potential Vulnerabilities**: Identify public-facing assets and configurations that may have vulnerabilities.
- **Prepare for Targeted Scans**: Ensure efficient focus in later penetration testing phases by establishing a list of high-priority targets.

Summary

This structured OSINT-driven approach leverages a diverse set of tools and techniques to build a robust profile on Artemis, Inc. The findings from this phase will guide subsequent testing and analysis, laying a comprehensive foundation for penetration testing efforts.