Reconnaissance Practice Report

1. Objective

The objective of this task was to carry out reconnaissance using passive Open-Source Intelligence (OSINT) techniques. The focus was on collecting information that is already available on the internet about a target domain. No direct interaction with the target system was performed. This activity helped in understanding how much information about an organization is publicly exposed and how it can be used during the initial phase of a security assessment.

2. Scope of Assessment

- Target Domain: amazon.com
- Type of Reconnaissance: Passive (OSINT)
- Environment: Academic / Educational
- Level of Interaction: No active scanning or exploitation

The assessment was limited strictly to publicly accessible sources and tools.

3. Tools Used

The following tools were used to gather and analyze open-source information:

- WHOIS – Used to obtain domain registration and ownership details
- Sublist3r – Used to identify subdomains related to the target
- Wappalyzer – Used to detect technologies used by the website
- Shodan – Used to view publicly indexed infrastructure information
- Maltego – Used for visual mapping of assets and relationships
-

4. Methodology

The reconnaissance process was carried out in a step-by-step manner:

1. A WHOIS lookup was performed to understand domain ownership, registrar details, and name server configuration.
2. Sublist3r was executed to enumerate subdomains associated with the target domain.

3. Wappalyzer was used to identify the technology stack and security mechanisms used by the website.
4. Shodan was checked to review any infrastructure or services indexed publicly.
5. Maltego was used to visually map the relationship between the domain, subdomains, and related assets.

All observations were noted and verified using tool outputs and screenshots.

5. Key Findings

5.1 WHOIS Information

The WHOIS lookup showed that the domain amazon.com is registered with MarkMonitor Inc. and owned by Amazon Technologies, Inc..
The domain has been active since 1994 and uses multiple name servers, which indicates a globally distributed and well-managed infrastructure.

5.2 Subdomain Enumeration

Sublist3r identified approximately 220 subdomains related to the target. These included domains associated with services, merchants, and partner programs. This reflects the large digital footprint of the organization and highlights how multiple assets are exposed publicly.

5.3 Technology Stack

According to Wappalyzer, the website makes use of modern technologies such as:

- Amazon Web Services (AWS)
- Amazon CloudFront CDN
- HTTP/3 protocol
- HSTS security headers

These technologies are commonly used to improve performance, scalability, and security.

5.4 Asset Mapping

Maltego was used to create a visual representation of the relationships between the main domain, subdomains, and infrastructure components. This helped in understanding how different assets are interconnected and publicly visible.

6. Importance of Reconnaissance

Reconnaissance is an important phase of any security assessment. It helps security professionals understand what information is available to attackers without performing any direct attack. By identifying exposed assets and technologies, organizations can take preventive steps to reduce unnecessary information disclosure.

7. Conclusion

This task successfully demonstrated the use of passive OSINT techniques to gather meaningful information about a target domain. The findings show that a significant amount of infrastructure and asset information can be collected without active scanning. Regular monitoring of publicly available data can help organizations reduce security risks and improve their overall security posture.