Asset Mapping Using Maltego

1. Introduction

Asset mapping is a critical phase of reconnaissance in cybersecurity assessments. It involves identifying and analyzing digital assets associated with a target, such as domain names, IP addresses, servers, and network infrastructure. This step helps in understanding the target's attack surface and identifying potential entry points for further security testing.

In this task, **Maltego Community Edition** was used as an Open Source Intelligence (OSINT) tool to perform asset mapping of a target domain in a Kali Linux virtual machine environment.

2. Tool Used

- **Tool Name:** Maltego Community Edition
- **Version:** Maltego Graph (Desktop) 4.11.1
- **Platform:** Kali Linux (Virtual Machine)
- **Purpose:** Visual OSINT-based asset mapping and infrastructure analysis

Maltego provides a graphical interface to discover relationships between domains, DNS records, IP addresses, and network infrastructure.

3. Objective

The objectives of this asset mapping exercise were:

- To identify DNS records associated with the target domain
- To discover IP addresses linked to the target
- To analyze hosting and network infrastructure
- To visually map relationships between identified assets

4. Target Information

- **Target DNS Name:**
  `lms.gurugramuniversity.ac.in`

This DNS name was selected as the starting point for asset mapping.

5. Methodology

The following methodology was used during the asset mapping process:

1. A new Maltego graph was created for the target domain.
2. A **DNS Name entity** was added to the graph.
3. Maltego transforms were executed to gather related infrastructure data.
4. Discovered entities were expanded to identify additional relationships.
5. The resulting graph was analyzed and documented.

6. Asset Mapping Process

6.1 DNS Enumeration

The DNS Name entity `lms.gurugramuniversity.ac.in` was analyzed using Maltego transforms to identify related DNS properties. The transform execution confirmed the existence of valid DNS records associated with the target.

6.2 IP Address Identification

Transforms were executed to resolve the DNS name to its corresponding IP address(es). This step helped identify the server hosting the target application.

6.3 Infrastructure Mapping

Additional transforms were used on the identified IP address to obtain:

- Network information
- Hosting provider details
- Netblock associations

This revealed the underlying infrastructure supporting the target domain.

6.4 Relationship Analysis

Maltego visually displayed relationships between:

- DNS Name
- IP Address
- Network infrastructure

These relationships provided a clear graphical representation of how the target is hosted and connected within the network.

7. Results and Findings

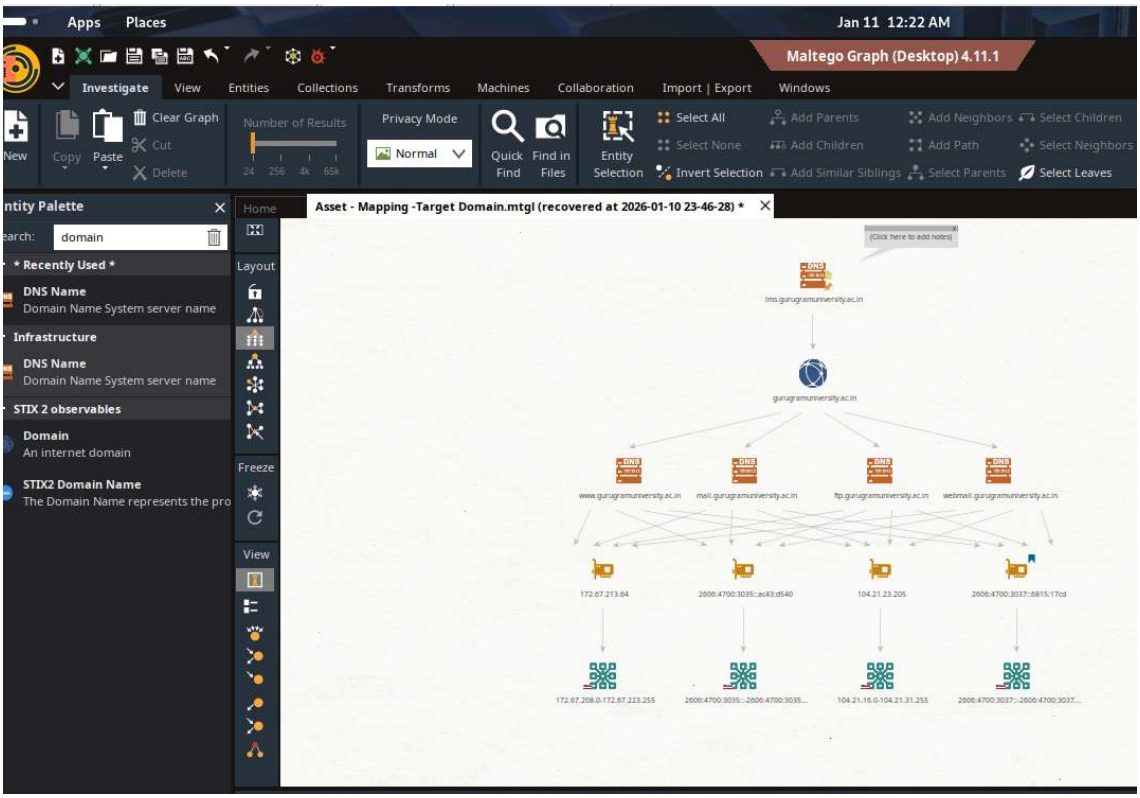
The asset mapping process produced the following key findings:

- The target DNS name successfully resolved to its hosting IP address.
- Infrastructure details such as network range and hosting information were identified.
- The visual graph highlighted the direct relationship between the DNS name and its underlying infrastructure.
- The mapped assets represent potential attack surfaces for further reconnaissance and security assessment.

8. Screenshots

The following screenshots were captured during the process:

- **Maltego Asset Map:** Showing DNS name and related infrastructure
- **IP Mapping View:** Highlighting IP address and network relationships



9. Limitations

- Maltego Community Edition has limitations on the number of transforms and data sources.
- Some advanced infrastructure and relationship data are restricted to paid versions.
- Results are dependent on publicly available OSINT sources.

10. Conclusion

Maltego was successfully used to perform asset mapping of the target DNS name `lms.gurugramuniversity.ac.in`. The tool provided a visual and structured representation of the target's DNS and infrastructure assets. This asset mapping exercise

helped identify key components of the target's digital footprint and established a foundation for subsequent reconnaissance and vulnerability assessment activities.