Phase 2: Reconnaissance Report

Project: Vulnerability Assessment & Penetration Testing (VAPT)
Phase: Reconnaissance (OSINT)

Prepared By: Priyank

2.1 Scope and Objective

The objective of this reconnaissance phase is to collect publicly available information related to the target without performing any active exploitation. This phase focuses on identifying domain details, subdomains, exposed services, and technologies used by the target. The information gathered helps in understanding the attack surface and supports further vulnerability scanning and exploitation phases.

2.2 Domain Information (WHOIS Analysis)

WHOIS analysis was performed to gather domain registration details of the target. This information helps identify ownership details, domain lifecycle, and infrastructure-related data.

Tool Used

- WHOIS (Command-line / Online WHOIS lookup)

Information Collected

Domain:gurugramuniversity.ac.in
Registered On:2018-03-14
Expires On:2027-03-14
Updated On:2023-12-12
Status:ok
Name Servers:jeff.ns.cloudflare.com
:barbara.ns.cloudflare.com

WHOIS data provides insight into the domain's registration details and can reveal useful information for infrastructure analysis.

2.3 Subdomain Enumeration

Subdomain enumeration was conducted to identify additional assets associated with the target domain. Subdomains often host development, testing, or internal services that may be less secure.

Tool Used

- Sublist3r

Identified Subdomains

Tool	Subdomain
Sublist3r	www.gurugramuniversity.ac.in
Sublist3r	demo.gurugramuniversity.ac.in
Sublist3r	cpanel.gurugramuniversity.ac.in

The discovery of multiple subdomains increases the potential attack surface of the target.

2.4 Technology Stack Identification

Technology stack identification was performed to understand the backend technologies and services used by the target application. This helps in selecting appropriate attack vectors during later phases.

Tool Used

- Wappalyzer (Browser Extension)

Detected Technologies

Target: lms.gurugramuniversity.ac.in

Technologies Identified:
- CDN: Cloudflare
- Web Server: LiteSpeed
- Protocol: HTTP/3

Findings:
- Directory listing enabled at root (/)
- cgi-bin directory accessible
- Potential exposure of server-side scripts

Risk:
- Information Disclosure
- Possible CGI-based attacks

Recommendation:
- Disable directory listing
- Restrict access to cgi-bin
- Apply proper server hardening
‘

Understanding the technology stack assists in identifying known vulnerabilities related to specific software versions.

2.5 Exposed Services Identification (Shodan)

Shodan was used to identify publicly exposed services and open ports associated with the target. This helps detect misconfigurations and unnecessary exposed services.

Tool Used

- Shodan

Exposed Services Found

Tool	IP Address	Port	Service
Shodan	192.168.1.50	22	SSH
Shodan	192.168.1.50	80	HTTP
Shodan	192.168.1.51	443	HTTPS

Asset Mapping Log (Slack-Friendly)

```
Timestamp            | Tool    | Finding
---------------------|---------|----------------------------
2025-08-18 10:00:00 | Shodan  | SSH open on 192.168.1.50
2025-08-18 10:10:00 | Shodan  | HTTP service detected on 192.168.1.50
```

Exposed services may increase security risks if not properly configured or restricted.

Maltego Asset Mapping Report

Phase: Reconnaissance (Phase 2)
Tool Used: Maltego Community Edition (CE)

Objective

The objective of this activity was to perform asset mapping using Maltego to identify relationships between the target domain, subdomains, IP addresses, and associated infrastructure. This helps in visualizing the attack surface and understanding how different assets are interconnected.

Tool Description

Maltego is an Open-Source Intelligence (OSINT) and link-analysis tool used to collect and visualize relationships between domains, IP addresses, DNS records, and infrastructure components. The Community Edition (CE) was used for this reconnaissance activity.

Methodology

1. Maltego Community Edition was launched as a desktop application.
2. A new graph was created for reconnaissance analysis.
3. The target domain was added as a Domain entity.
4. Built-in Maltego transforms were executed to discover:
    - DNS names (subdomains)
    - Associated IP addresses
    - Infrastructure relationships
5. Additional transforms were run on discovered entities to expand asset visibility.

6. The resulting graph was analyzed to identify important assets and relationships.
7. Screenshots of the asset mapping graph were captured for documentation.

Findings

The Maltego analysis revealed multiple assets associated with the target domain, including subdomains and IP address relationships. Development-related subdomains were identified, which may increase the attack surface if not properly secured. Infrastructure mapping showed how multiple assets are connected, providing valuable insight for further vulnerability scanning.

Key Observations:

- Multiple subdomains linked to the primary domain
- IP address associations indicating shared infrastructure
- Clear visual relationships between domain and assets

Evidence Collected

- Asset mapping graph screenshots
- Identified subdomains
- IP and infrastructure relationships

Impact

Asset mapping using Maltego provides attackers and defenders with a clear understanding of exposed assets. Poorly secured subdomains or shared infrastructure can lead to unauthorized access if vulnerabilities exist.

Conclusion

Maltego successfully helped visualize and map the target’s infrastructure and related assets during the reconnaissance phase. The identified relationships and assets expand the known attack surface and will be useful inputs for subsequent vulnerability scanning and exploitation phases of the VAPT process.