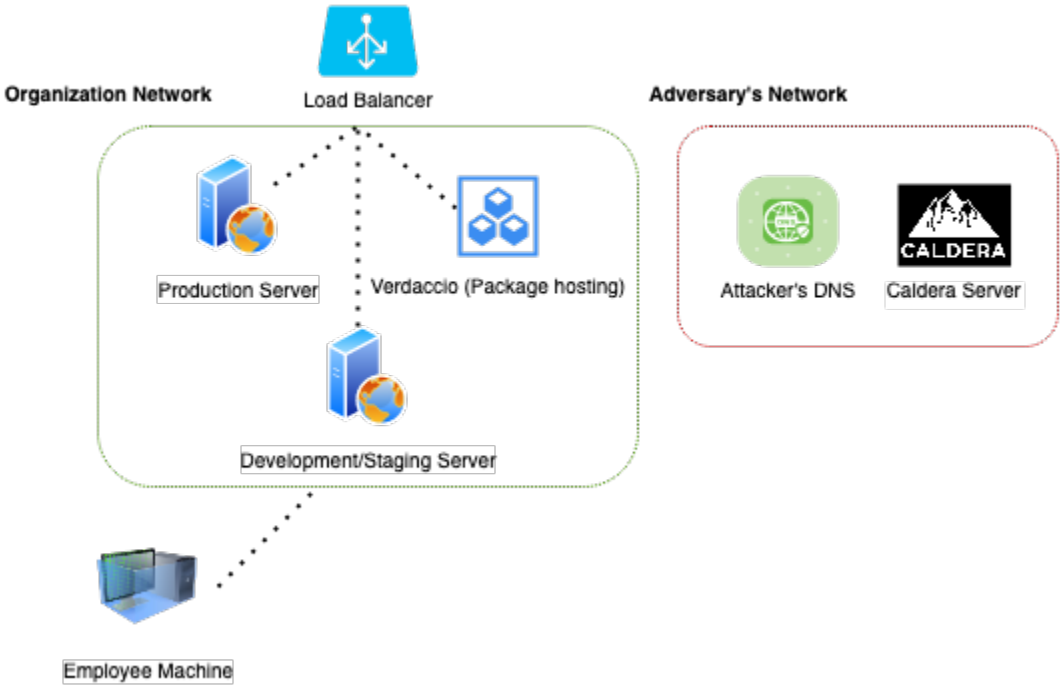
Project Proposal

CY Capstone Team-1



Vulnerability: Supply Chain Attack
Idea: Build an infrastructure for an organization that heavily relies on a JavaScript environment. This environment will be utilized for implementing the Dependency Confusion attack using custom scripts and the Caldera tool.

Implementation:

The implementation is divided into two halves.

1. Organization Network + Employee Machine
2. Adversary's Network

Organization Network

This segment is a virtual network deployed in GCP with three servers (Linux) with NodeJS and NPM installed. The servers, namely the Production, Deployment/Staging, and Repository, are the only components in the organization environment.

Production and Deployment servers will run the vulnerable web application we will be building. The web application will have vulnerabilities

1. **“None” algorithm attack:** This will allow us to do account takeovers and leak the private package that the admin has stored in their account.
2. **Dependency Confusion:** This is another supply chain attack that we will use to allow code injections and execute the malicious payload in the “development servers.”

The production server would be allowed to have DNS lookups, whereas the Development server will have outbound HTTP(s) and DNS lookup capabilities.

As shown in the diagram, we also have an **employee machine**, which can be outside or inside the organization's network. The idea is to compromise this machine, provided it tries to download the private package.

Adversary’s Network

This segment is a virtual network deployed in GCP with two servers (Linux). The servers, namely the Attacker’s DNS and Caldera servers, are the only components in the adversary’s environment.

The attacker’s DNS Server will run a Bind9 service with our custom domain name *0xparthhackerone.me.* This is where the callbacks will be made whenever the victim machine does a DNS lookup on our domain.

Caldera Server will be running on a Linux-based machine which will help us demonstrate the execution of the agent script.

Conclusion

Final report will include the executive summary of the attack and a presentation of the attack performed. The attack will also include mapping the whole attack to MITRE’s framework.