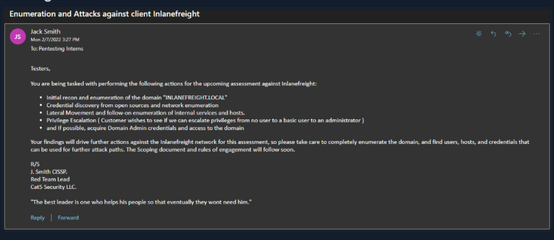
# Scenario

We are junior penetration testers working for `CAT-5 Security`. After a few successful engagements shadowing with the team, the senior members want to see how well we can do starting an assessment on our own. The team lead sent us the following email detailing what we need to accomplish.

### Tasking Email




This module will allow us to practice our skills (both prior and newly minted) with these tasks. The final assessment for this module is the execution of `two` internal penetration tests against the company Inlanefreight. During these assessments, we will work through an internal penetration test simulating starting from an external breach position and a second one beginning with an attack box inside the internal network as clients often request. Completing the skills assessments signifies the successful completion of the tasks mentioned in the scoping document and tasking email above. In doing so, we will demonstrate a firm grasp of many automated and manual AD attack and enumeration concepts, knowledge of and experience with a wide array of tools, and the ability to interpret data gathered from an AD environment to make critical decisions to advance the assessment. The content in this module is meant to cover core enumeration concepts necessary for anyone to be successful in performing internal penetration tests in Active Directory environments. We will also cover many of the most common attack techniques in great depth while working through some more advanced concepts as a primer for AD-focused material that will be covered in more advanced modules.

Below you will find a completed scoping document for the engagement containing all pertinent information provided by the customer.

## Assessment Scope

The following `IPs`, `hosts`, and `domains` defined below make up the scope of the assessment.

### In Scope For Assessment

| Range/Domain | Description |
|---|---|
| `INLANEFREIGHT.LOCAL` | Customer domain to include AD and web services. |
| `LOGISTICS.INLANEFREIGHT.LOCAL` | Customer subdomain |
| `FREIGHTLOGISTICS.LOCAL` | Subsidiary company owned by Inlanefreight. External forest trust with INLANEFREIGHT.LOCAL |
| `172.16.5.0/23` | In-scope internal subnet. |

### Out Of Scope

- `Any other subdomains of INLANEFREIGHT.LOCAL`
- `Any subdomains of FREIGHTLOGISTICS.LOCAL`
- `Any phishing or social engineering attacks`
- `Any other IPS/domains/subdomains not explicitly mentioned`
- `Any types of attacks against the real-world inlanefreight.com website outside of passive enumeration shown in this module`

## Methods Used

The following methods are authorized for assessing Inlanefreight and its systems :

### External Information Gathering (Passive Checks)

External information gathering is authorized to demonstrate the risks associated with information that can be gathered about the company from the internet. To simulate a real-world attack, CAT-5 and its assessors will conduct external information gathering from an anonymous perspective on the internet with no information provided in advance regarding Inlanefreight outside of what is provided within this document.

Cat-5 will perform passive enumeration to uncover information that may help with internal testing. Testing will employ various degrees of information gathering from open-source resources to identify publicly accessible data that may pose a risk to Inlanefreight and assist with the internal penetration test. No active enumeration, port scans, or attacks will be performed against internet-facing "real-world" IP addresses or the website located at `https://www.inlanefreight.com`.

### Internal Testing

The internal assessment portion is designed to demonstrate the risks associated with vulnerabilities on internal hosts and services ( `Active Directory specifically`) by attempting to emulate attack vectors from within Inlanefreight's area of operations. The result will allow Inlanefreight to assess the risks of internal vulnerabilities and the potential impact of a successfully exploited vulnerability.

To simulate a real-world attack, Cat-5 will conduct the assessment from an untrusted insider perspective with no advance information outside of what's provided in this documentation and discovered from external testing. Testing will start from an anonymous position on the internal network with the goal of obtaining domain user credentials, enumerating the internal domain, gaining a foothold, and moving laterally and vertically to achieve compromise of all in-scope internal domains. Computer systems and network operations will not be intentionally interrupted during the test.

### Password Testing

Password files captured from Inlanefreight devices, or provided by the organization, may be loaded onto offline workstations for decryption and utilized to gain further access and accomplish the assessment goals. At no time will a captured password file or the decrypted passwords be revealed to persons not officially participating in the assessment. All data will be stored securely on Cat-5 owned and approved systems and retained for a period of time defined in the official contract between Cat-5 and Inlanefreight.

> We provided the above scoping documentation so we become used to seeing this style of documentation. As we progress through our Infosec Careers, especially on the offensive side, it will be common to receive scoping documents and Rules of Engagement (RoE) documents that outline these types of information.

## The Stage Is Set

Now that we have our scope clearly defined for this module, we can dive into exploring Active Directory enumeration and attack vectors. Now, let's dive into performing passive external enumeration against Inlanefreight.

Previous Next Mark Complete & Next

Cheat Sheet
Resources

Table of Contents

Setting The Stage
Introduction to Active Directory Enumeration & Attacks
Tools Of The Trade
Scenario

Initial Enumeration
External Recon and Enumeration Principles
Initial Enumeration of the Domain

Sniffing out a Foothold
LLMNR/NBT-NS Poisoning - from Linux
LLMNR/NBT-NS Poisoning - from Windows

Sighting In, Hunting For A User
Password Spraying Overview
Enumerating & Retrieving Password Policies
Password Spraying - Making a Target User List

Spray Responsibly
Internal Password Spraying - from Linux
Internal Password Spraying - from Windows

Deeper Down the Rabbit Hole
Enumerating Security Controls
Credentialed Enumeration - from Linux
Credentialed Enumeration - from Windows
Living Off the Land

Cooking with Fire
Kerberoasting - from Linux
Kerberoasting - from Windows

An ACE in the Hole
Access Control List (ACL) Abuse Primer
ACL Enumeration
ACL Abuse Tactics
DCSync

Stacking The Deck
Privileged Access
Kerberos "Double Hop" Problem
Bleeding Edge Vulnerabilities
Miscellaneous Misconfigurations

Why So Trusting?
Domain Trusts Primer
Attacking Domain Trusts - Child -> Parent Trusts - from Windows
Attacking Domain Trusts - Child -> Parent Trusts - from Linux

Breaking Down Boundaries
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Windows
Attacking Domain Trusts - Cross-Forest Trust Abuse - from Linux

Defensive Considerations
Hardening Active Directory
Additional AD Auditing Techniques

Skill Assessment - Final Showdown
AD Enumeration & Attacks - Skills Assessment Part I
AD Enumeration & Attacks - Skills Assessment Part II
Beyond this Module

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left