Finding Sensitive Information

When attacking a service, we usually play a detective role, and we need to collect as much information as possible and carefully observe the details. Therefore, every single piece of information is essential.

Let us imagine we are in an engagement with a client, we are targeting email, FTP, databases, and storage, and our goal is to obtain Remote Code Execution (RCE) on any of these services. We started the enumeration and tried anonymous access to all services, and only FTP has anonymous access. We found an empty file within the FTP service, but with the name `johnsmith`, we tried `johnsmith` as the FTP user and password, but it did not work. We try the same against the email service, and we successfully login. With email access, we start searching emails containing the word `password`, we find many, but one of them contains John's credentials for the MSSQL database. We access the database and use the built-in functionality to execute commands and successfully get RCE on the database server. We successfully met our goal.

A misconfigured service let us access a piece of information that initially may look insignificant, `johnsmith`, but that information opened the doors for us to discover more information and finally get remote code execution on the database server. This is the importance of paying attention to every piece of information, every detail, as we enumerate and attack common services.

Sensitive information may include, but is not limited to:

- Usernames.
- Email Addresses.
- Passwords.
- DNS records.
- IP Addresses.
- Source code.
- Configuration files.
- PII.

This module will cover some common services where we can find interesting information and discover different methods and tools we can use to automate our discovery process. These services include:

- File Shares.
- Email.
- Databases.

Understanding of What We Have to Look for

Every target is unique, and we need to familiarize ourselves with our target, its processes, procedures, business model, and purpose. Once we understand our target, we can think about what information is essential for them and what kind of information is helpful for our attack.

There are two key elements to finding sensitive information:

1. We need to understand the service and how it works.
2. We need to know what we are looking for.

Previous Next Mark Complete & Next