ZeroLogon Project

Team of 2 (max)

1. Project Introduction

The focus of this project is the ZeroLogon Windows Active Directory vulnerability. You will start by scanning a domain controller using nmap to gather information about it. Then, you will use that information to exploit a Domain Controller using the ZeroLogon vulnerability to find a flag in the administrator's account.

This project will require research before performing the exploitation. You must use the Kali machine assigned to you in the Pitt Cyber Range to complete this project.

Note: You can work on this project alone or with (ONLY) one other student in the same course.

2. Problem Statement

You are hired as a junior penetration tester and your first task is to find an important file in the Domain Controller Admin account of the company you are testing. Your supervisor left you the following note:

"We know that the DC at 15.15.0.108 is vulnerable to ZeroLogon. Use the following command `nmap 15.15.0.108 -A` to identify the NetBIOS_Domain_Name and NetBIOS_Computer_Name for the DC. There are plenty of resources online on how to exploit the ZeroLogon vulnerability (here's one example). Take your time to familiarize yourself with the exploit then **find the text file in the Documents folder for the DC Admin account and let us know what is typed in it**. Good luck!"

*** Section 6 below has useful hints and references. Search engines are useful too!*

3. Hints and References

- You may need to use `secretsdump.py` in this project. It is part of the Impacket collection. Before installing Impacket, make sure you have installed all what you need to install before attempting to install Impacket. Then, follow this YouTube video: https://youtu.be/3N82TddmEpg to install Impacket.
- If you break your machine (quite possible), post on Piazza to get it reverted to its original state
- In Windows, you use "`dir`" to list a folder content and "`type`" to display the content of a text file

7. Notes

Q) When does the DC machine revert back to its original state?

The DC machine is configured to automatically revert back to its original state at the following times:
12 AM/PM ET
3 AM/PM ET
6 AM/PM ET
9 AM/PM ET