PenTest Lab Exercise Ex150 – DC Has Fallen

Goal

Get Domain Admin.

Tasks

1. Hank Hacker, has asked you to scan the `artstailor.com` network for vulnerabilities associated with smb-related exploits released by the ShadowBrokers. Identify the CVE associated with this exploit as well as its common name(s). Identify an appropriate tool on Kali that can search for this particular vulnerability by scanning machines on a network. The primary domain controller, `pdc.artstailor.com` is not subject to this vulnerability, but Opp set up a backup domain controller just yesterday, so it may not be patched. (What's with this guy?) [Your best bet for saving time may be to read the whole assignment then determine any new host(s) that exist before doing any scanning. Then scan only the likely hosts.]

2. There are fewer than 10 metasploit exploits for the vulnerability you are looking for, but most of them will not successfully execute on Server 2016. Your goal is to be able to get access to a domain administrator account. In doing so, you may be able to exfiltrate sensitive data (yes, I'm talking about keys).

3. Things to consider:

    - You may notice that some of the machines that are normally powered up are off. The front-office group is on vacation this week and their machines are powered down.
    - If you are running an exploit that fails, you may want to execute it again before giving up on it entirely.

4. Show that your scan demonstrates the existence of a vulnerability in the smb service on a secondary domain controller in the `artstailor.com` domain.

5. Use some appropriate exploitation framework (hmmm, which one would we probably use?) to gain access to the vulnerable system.

6. Demonstrate that you have achieved domain admin status.

7. Write a partial penetration test report for Hank and submit your report the usual way.