PenTest Lab Exercise Ex0d0 – Books is Breached

Goal

Contact a host using RDP through a pivot, elevate to `NT AUTHORITY/SYSTEM`, and exfiltrate sensitive data.

Tasks

1. When Hank was talking to Art and Otto (at the tailor shop) about your suggestion for persistent access to the `costumes` host, he happened to overhear a conversation at the watercooler as he was leaving. Debbie Nolan was telling Brian Oppenheimer that she's doing the books for Art and just brought her home computer in a week ago as a work computer, but she had a problem. Art made a domain account for her but she wasn't using it yet, and someone named Oliver (who is apparently quite precocious) keeps finding out and changing her password, so she can't log in. Brian said he knew just the thing to do to fix it so she'd be able to fix up her password, that Windows 10 was supposed to make this particular feat impossible, but he was smarter than all those Microsoft guys and had figured out a workaround. Not only that, Windows is supposed to make it so that if you do this once, you can't do it again, but he can fix that too. All Debbie has to do is run `\reset` before exiting. He told her that even though lots of people have heard about this for earlier versions of windows, even if they had, it wouldn't be a problem because he was doing it a different way. Hank wants you to check this out.

2. Log in to Netlab and schedule an Ex0d0 lab.

3. Figure out which machine is vulnerable, what the vulnerability is, and how you can exploit it. Find some way of getting `NT AUTHORITY/SYSTEM` privilege on the host. Don't waste too much time if you get stuck–ask for help.

4. Identify any directories on this machine associated with users you haven't encountered in past exercises. See if they have any interesting files.

5. Write a partial penetration test report with any incremental findings you have made and turn it in via Canvas. Remember–if you are able to get access to information that you shouldn't find, that is a finding.