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 establishing a permanent `sliver` beacon 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 11 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 isn't doing this using the method most people do. Hank wants you to check this out.

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

3. The new plan for persistent access is in place. There is is a `sliver` beacon currently active on `costumes.artstailor.com` that periodically attempts to connect to an mtls listener on your kali host. You can catch that beacon by starting `sliver` on kali and issuing the `mtls` command to start the listener.

   Once you have captured a beacon, initiate an interactive session. You can start a socks5 proxy through that session by issuing the `sliver` command

```
socks5 add
```

and you can create a port forward on `kali` by issuing:

```
portfwd add --remote target-IP:target-port
      [ --bind host-interface:host-port ]
```

The default host port binding is `127.0.0.1:8000`

4. Use one of these methods amd RDP into `books.artstailor.com`. Use credentials you have already captured to log in there as either a domain or local user. (Note, the same local user may exist on a number of machines.)

5. Once you've established that you can log in to book via RDP, find a way to get `NT AUTHORITY/SYSTEM` privilege on the host. If you have been paying attention, you'll have some idea what to do, however, Windows11 has a slightly different interface from previous versions of Windows, so don't expect everything to be identical to what you've seen before. Don't waste too much time if you get stuck–ask for help.

   To exfiltrate interesting files, you may need to know how to

   (a) Change ownership of a file with `takeown`.

   (b) Change permissions on a file with `icacls`.

6. Identify any directories on this machine associated with users you have not encountered in past exercises. See if they have any interesting files.

7. 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 shouldn't be shared with you, that is a finding.