E080–Through the Gate

Welcome to Penetration Testing and Ethical Hacking at the University of Florida. This is pentest exercise Ex080-Through the Gate. You're going to exploit some infrastructure misconfigurations and other things to gain access.

To prepare for this exercise, you really need to check out Beau Bullock's Tradecraft Security Weekly video that's an introduction to password spraying. This is called Attacking exchange OWA to gain access to AD accounts. The MailSniper powershell module that he uses is pretty well-known but it's really designed for use on Windows. Instead of using Mailsniper, you'll be using a password sprayer known as the SprayingToolkit.

Hank Hacker has some information for you to use. He sent the new kid Kory on a dumpster-diving expedition to get some intelligence on Arts Taylor Shoppe. Kory found part of a printed email that was sent to `w.clockwell@artstilor.com` and, in the email, Art says someone named Eve may have gotten the message about Reginald Vel Johnson High School homecoming, or may not have, and can William help him out with finding out if Eve got that message. There was also a handwritten note to "William Clockwell" saying that William will no longer be able to access remote desktop on the Costumes machine because of a change that Otto made to the router. Otto told him that letting remote desktop connections come in from outside is really insecure. It's a security hole. Hank says that this information, together with some earlier reconnaissance, tells them that a password spraying attack, might pay off. He wants you to try that.

Log into Netlab, schedule an exercise to your Ex080 lab. Do all those things that you're used to doing. The spraying toolkit is installed in kali's **git/SprayingToolkit** subdirectory. There's an `atomizer.py` program in there–a python program that does spraying. You can mount a spraying attack to attempt to get credentials and the `artstailor.com` network domain with the atomizer. To do that, you'll need to get a list of potential users, and you should use open source intelligence with Google and people who might be associated with Art's Taylor Shoppe. You can identify a number of such names, and you need a list of potential passwords. The typical passwords are the ones you should try. You should verify that `mail.artstailor.com` delivers mail via an https link. That is, you can get to `mail.artstailor.com` from outside with an https link, and you should use the appropriate Url as the target for atomizer.py. So whatever url you use to get to OWA on the artstailor network, that's what you should use for the atomizer as the target. Make sure you're using possible usernames that are in the artstailor domain that's `artstailor` *username*, and use passwords that are reasonable ones. And provide all the necessary parameters for spraying–all the necessary parameters for spraying–if you're using a password file and a username file. This is different from the set of parameters you would use if you're just trying one username and one password, or one password with a large number of usernames.

You should check out all the open ports on Arts Taylor com's router, `innerrouter`, to see if there is any possible way into that system. If you find any possibilities look for common misconfigurations that might be present in a tool of that sort. After you find the misconfiguration, exploit it to get access to the remote desktop service to a machine in the `artstailor.com` domain. You can do it. To do that, you'll need to find a way to forward a connection from `innerouter` to the rdp port of a machine in the `10.70.184.0/24` network–that is the 10 network that's behind that router. There will be some useful information available to you, and if you are tenacious you will find a key.

You should write and submit a partial penetration test report This will probably be the most complex penetration test report you've written so far, because there are several tactics you're using. Make sure that you have a finding for each of the vulnerabilities that you identify.

In your report, aside from the TTPs and findings, you should include a suggestion for a temporary change for the duration of this pentest that could be made to the configuration of the router (`innerouter`) to help you gain access to the `artstailor.com` internal network to help you avoid spending a lot of time doing some work. And justify why that change should be allowed and how it can be made secure. So, essentially, you're explaining to Hank in your pentest report what change you would like Otto to make to the artstailor network, to that router in particular, to make things easier for you to conduct the rest of the pentest.

There's plenty to do here. Get started, and good luck.