PenTest Lab Exercise Ex080 – ThroughTheGate

Goal

Exploit infrastructure misconfigurations to gain access.

Tasks

1. In preparation for this exercise, watch Beau Bullock's *Tradecraft Security Weekly* video on password spraying, Attacking Exchange/OWA to Gain Access to AD Accounts. The `MailSniper` Powershell module he uses is a collection of tools for use on Windows. Instead of using `MailSniper`, you'll employ the `atomizer.py` password sprayer of the `SprayingToolkit`.

2. Hank Hacker tells you that he sent the new kid, Kory, on a dumpster-diving expedition to gather intelligence on Art's Tailor Shop. Kory found part of a printed email sent to `w.clockwell@artstailor.com`. In the email, Art asks him if someone named Eve got the message about the Reginald Vel Johnson High School Homecoming. There was another hand-written note to "William Clockwell" saying he will no longer be able to remote desktop to "costumes" because of a change Otto made on the router. Otto told him that allowing remote desktop into the network is definitely a security hole.

   Hank says this information, together with earlier reconnaissance, indicates that a password spraying attack might pay off as an initial foothold into the network. He wants you to mount such an attack.

3. Log in to Netlab and schedule an Ex080 lab.

4. The `SprayingToolkit` is installed in user kali's `git/SprayingToolkit` subdirectory. You can use `atomizer.py` to mount a password spraying attack to attempt to get credentials for users in the `artstailor.com` domain. To do that you'll need a list of potential users (OSInt using google and people who might be associated with Art's Tailor Shoppe can help you identify a number of such names) and a list of potential passwords. Verify that `mail.artstailor.com` delivers mail via an `https` link and use the appropriate URL as the *target* for `atomizer.py`. Make sure that if you are using files for possible usernames and passwords that you provide *all* the necessary parameters for spraying!

5. Check out all open ports on the `artstailor.com` router to see if there is any possible way into the system. If you find any possibilities, look for any common misconfigurations that might be present.

6. *After* you find the misconfiguration, exploit it to get access to the remote desktop service to a machine in the `artstailor.com` domain. To do this, 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.

7. There will be some useful information available to you. If you are tenacious, you will find a key.

8. Write and submit a partial penetration test report. Make sure you have a finding for each of the vulnerabilities you identify.

9. In your report, aside from TTPs and findings, include a suggestion for a temporary change (for the duration of the penetration test) to the configuration of the router to help you gain access to the `artstailor.com` internal net (`10.70.184.0/24`) in the future. Justify why that change should be allowed and how it can be made secure.