PenTest Lab Exercise Ex030 – DNS Reconnaissance

Goal

Get experience with DNS reconnaissance, the fierce domain scanner, forward and reverse lookups, and possibly CeWL.

Tasks

1. Log in to your kali VM and use the `fierce` domain scanner to identify hosts in the `artstailor.com` domain.

2. Your goal is to find and note IP address blocks (i.e., groups of IP addresses) that are employed by hosts in the `artstailor.com` domain. (These address blocks need to be in your report.)

3. Inspect the source code for the `fierce` domain scanner to determine where its wordlist is stored.

   In your attack narrative, tell me where that is. Determine which names `fierce` finds in the `artstailor.com` domain that are identified because they are included in its default wordlist.

4. Use `CeWL` against the web server `http://www.artstailor.com` to create an alternate wordlist to use with `fierce` to see if it can find any extra hosts as compared to running with the default wordlist.

5. For each host found, identify the method `fierce` used to find that name in your attack narrative. Include this information in your report. Could you have gotten this same information using `fierce` in a different way?

6. Compare the results using `fierce` with results you achieve using the `dnsmap` domain scanner.

7. If you carried out all these steps carefully and correctly, you will have found `KEY005`.

8. Submit a partial penetration test report describing any security issues associated with the information you found and recounting your activities in your attack narrative. Identify at least one Mitre ATT&CK

Framework TTP that describes the activity you undertook. People can have honest disagreements about whether or not you identified a vulnerability. If you think you identified a vulnerability, make sure you include a finding with a CVSS severity score. If you determine that no vulnerability was identified, explain this in the attack narrative.

Make sure to respond to any demands I made in the tasks listed above. (I will expect you to do this without prompting in the future.)