PenTest Lab Exercise Ex0a0 – HashTag

Goal

Crack passwords.

Tasks

1. Log in to the ndg box and schedule an Ex0a0 lab.
2. Crack as many of the hashes you captured from mimikatz on costumes.artstailor.com as you can using John the Ripper. The rockyou password file is helpful, however, some passwords may not be cracked using it.
3. Note that John the Ripper LM and NTLM hashes are formatted as `username:hash` in the hash file. You should be able to find the rock you file in `/usr/share/wordlists` in `Kali`.
4. Submit a partial penetration test report covering your activities for this exercise. It is important to note that when reporting cracked passwords, it is customary not to report the entire password to your client. Instead, I recommend that you provide the first two and the last two characters of the password. That's enough to let the user know that you, indeed, have cracked their password, but (unless the password is only 4 characters long) it usually does not reveal any other information (such as password selection strategies) to your client.
5. In your report, you should make recommendations about any password security best practices (from NIST Special Publication 800-63B) that this password choice indicates `artstailor.com` is not enforcing for memorialized secrets. Also report any good Windows-specific password security practices that aren't being followed.
6. Sorry key fans, no key is available as a direct result of carrying out this exercise.