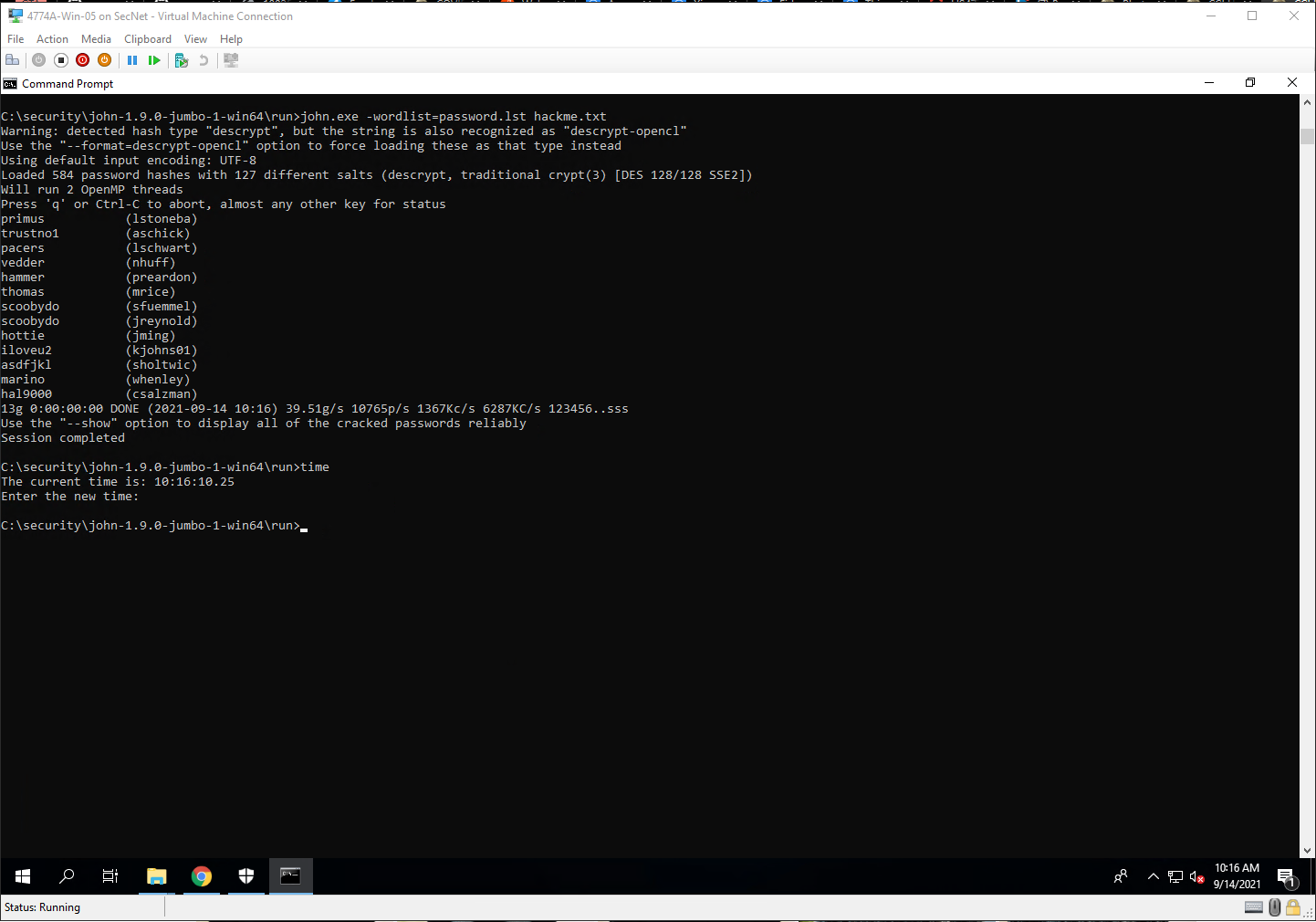
6.1 John The Ripper

Screenshots

Step 32

Step 38

A screenshot of a computer

Description automatically generated with medium confidence

Step 41A picture containing text, screenshot, computer

Description automatically generated

Project Questions

1. The dictionary force attack cracked 13 passwords.
2. The brute force attack cracked 26 passwords.
3. I let the brute force attack run for about 30 seconds.
4. JTR made approximately 0.432 guesses per second.

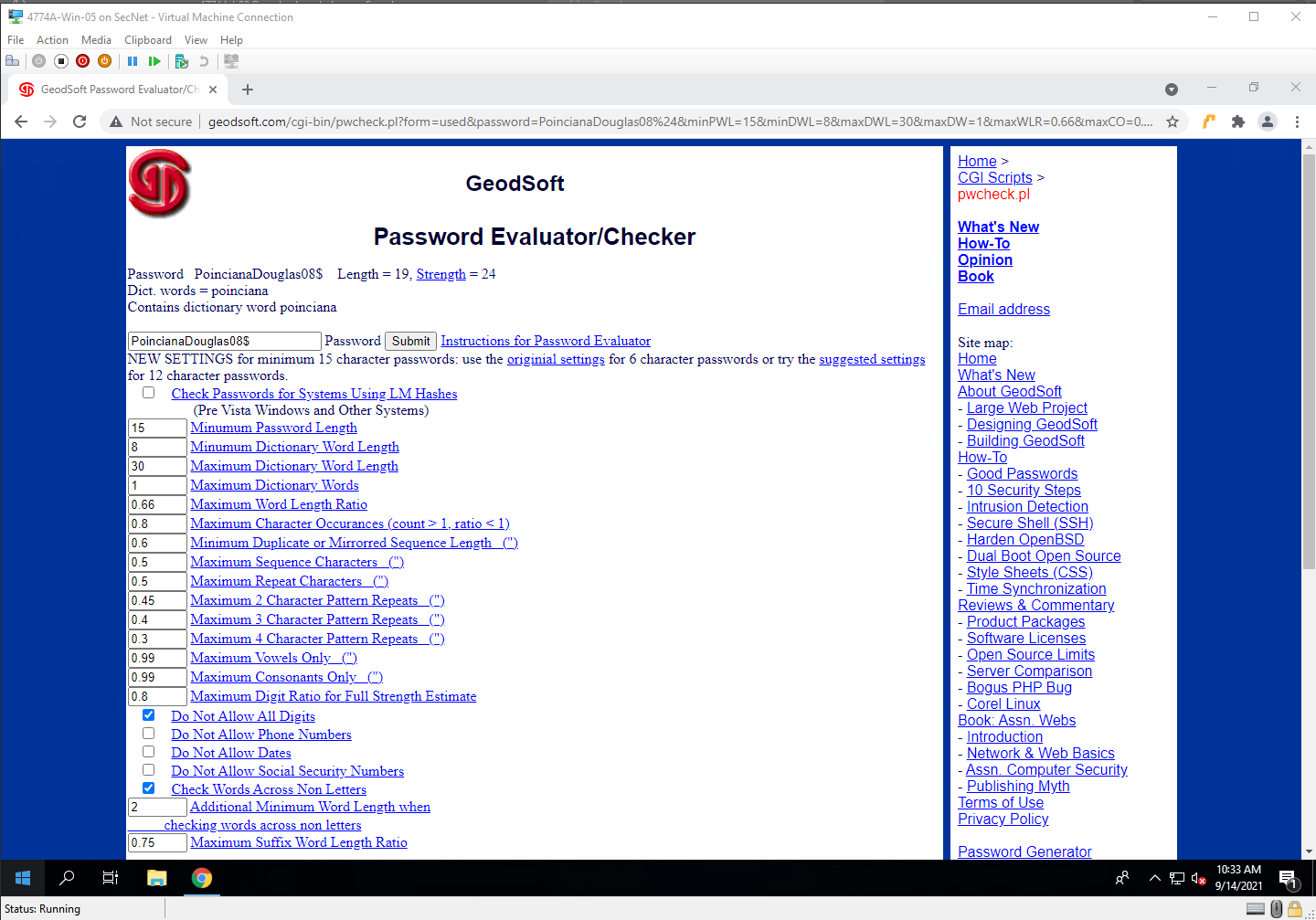
Thought Questions

1. The cracking program cracks passwords in one of two ways. A dictionary attack tries a predefined list of passwords. A brute force attack tries any combination of characters.
2. Password crackers can crack any password through a brute force attack, however stronger passwords will make that process take significantly longer.
3. I think that if you were to use a larger dictionary, it would take longer crack passwords because there is more to reference.
4. Yes, JTR does support using foreign language word lists.

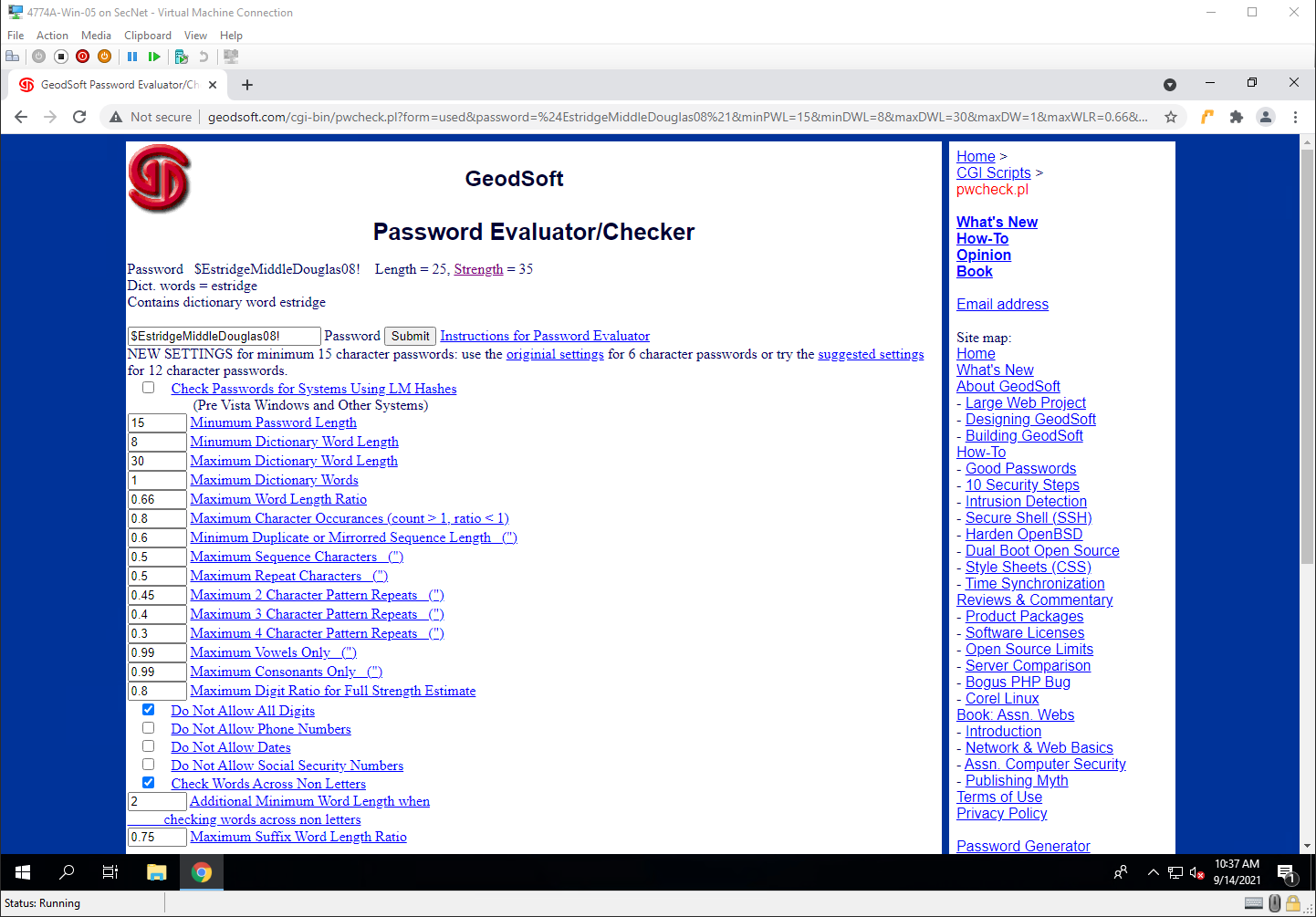
6.6 Password Evaluator

Screenshots

Step 4



Step 7



Project Questions

1. My normal password was 19 characters long.
2. My strong password was 25 characters long.
3. My normal password has a number at the end of it.
4. The password with a repeated word had issues because by default, the security option “Maximum Dictionary Words” is set to 1.

Thought Questions

1. It’s a phrase that, although makes no sense to most people, makes sense to me and is easy for me to remember.
2. I would hope so. That way others’ passwords would be more secure because its not a basic password. It is also better because it is harder to remember complex passwords.
3. Yes, hackers know what patterns users use to choose their passwords, and they use that knowledge to further their goals.
4. No, I don’t use the same password for every account. I have my main password that allows me to access my password vault where I have passwords stored