CPTC Homework #5

Questions (25 pts)

1. Given the username "administrator" and the "password", provide the `crackmapexec` commands that
    a. Authenticate to MSSQL, SMB, and LDAP
    b. Use pass the hash to authenticate to the previous services
    c. Perform a kerberoast and an asreproast
    d. Perform a SAM dump
    e. Perform command execution

Lab (75 pts)

Assume Breach user: CPP-TESTER:AwesomeSauce123!
Neo4j credentials: neo4j:bruh
Target: 192.168.1.215

Perform Any 3

- Kerberoast
- ASReproast
- Pass the Hash
- SMB Command Execution (psexec/smbsexec/atexec/etc)
- Unquoted Service Path
- IIS Webshell
- MSSQL Command Execution
- Any Windows/AD CVE
- AD ACL Abuse
- Privilege Token Abuse
- DCSync OR LSASS/SAM dump
- Smb Share Enumeration

Explain the theory behind attack

- Include prerequisites
- Include why an attacker might consider this attack

Screenshot the results

Explain what each command does