CCDC Week 5 Homework

Windows Week

Windows Fundamentals 2 TryHackMe - 40 points

Link: https://tryhackme.com/room/windowsfundamentals2x0x

Screenshot proof of completion **and documentation** of how you completed each question

Lab Time!! - 60 points

1. Connect to the VPN and clone the CCDC_Windows template on Kamino.
2. There are two Windows VMs
    a. Creds: Administrator:CCDC2025!
3. Which of the two servers is the Domain Controller? What is the domain name and NetBIOS domain name? How did you find this information? **(15 points)**
4. Using the Group Policy Editor, what settings would you change to enforce a secure password policy across all domain accounts? **(15 points)**
5. The domain controller's critical services include Active Directory Services, DNS, and SMB...
    a. Craft host firewall rules to:
        i. Allow inbound connections to Active Directory Services from the local network
        ii. Allow all inbound connections to DNS and SMB
        iii. Allow all outbound connections from the google chrome **executable** (don't use port #)
        iv. Block all other traffic by default
    b. Send screenshotted evidence of your applied ruleset, explaining how it meets the requirements **(20 points)**
6. Uh oh, on the other server (not the DC) it looks like there's a suspicious process! Where is it and what persistence method did the attacker use? **(10 points)**
7. There's something **really** wrong with the DNS service on the DC, and it looks like Active Directory isn't working correctly! How do you fix it? **(Up to +20 bonus points)**

Deliverables

1. A screenshot and documentation showing completion of **the TryHackMe room**.

2. Completion of the Lab with all specified questions answered, **with screenshot evidence**.