Nebula
TECHNOLOGIES

Hello New Hire!

This week, we would like to have you perform a purple team tabletop exercise where you will learn to utilize network devices to protect our company resources. Attached is a network topology of the environment we have prepared for you. Due to an unforeseen bureaucratic speed bump, we are unable to provide you with more resources, so please stick to what we have prepared.

Exercise Instructions:

1. Conduct initial research on EternalBlue, which the Windows Server 2012 VM is vulnerable to. Give a brief explanation of this vulnerability.
2. With the Kali VM, conduct a baseline test by exploiting EternalBlue on the Windows Server 2012 VM using Metasploit. Briefly explain your methodology.
    a. Feel free to enlist the help of the internet if you are having trouble with this step.
3. Please configure a free IDS/IPS (Snort or Suricata) of your choice on pfSense, documenting your configuration process thoroughly.
4. With Snort/Suricata set up, apply configurations detect and prevent this exploit.
    a. Provide proof of your rules in use, along with an explanation of why it is effective.
5. Implement firewall rules that will block exploitation of EternalBlue. Corporate wants one inbound and one outbound rule. Each rule alone should be able to block the attacker (Kali VM) from obtaining a shell on the Windows Server 2012 VM.
    a. Provide proof of your rules in use, along with an explanation of why it is effective.
6. Please provide your responses in a professionally formatted report to be submitted on 07/29/2023 at 5:00am PST.

Thank you,
Betelgeuse Puppis
Lead Network Engineer

By the way, I will be away on some well-deserved PTO, so you are all alone for this one. Sucks. (Just don't take my name off the ticket so it looks like I did the work.)