Pen testing lab

Goals:

1. Apply the phases of pen testing in a virtual environment
2. Understand network scanning and nmap
3. Use metasploit
4. Analyze network logs with wireshark
5. Synthesize all your current knowledge with pen testing:
    a. Computer Networks
    b. Web app security
    c. Cryptography
    d. CIANA

Prerequisites:

1. Virtualization environment as in HW0
2. **Connect your Kali VM to the Metasploitable VM** – this will help you understand some concepts of networking, IPs, and subnet masks
3. Basic understanding of computer networking
4. Good internet connection

Instructions

1. Connect Kali VM to Metasploitable: Explain what you had to do for the network settings of the VMs, the IPs, and how you proved that the two VMs can talk to each other. Include screenshots that prove your claims. You may use the following guide: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
2. Perform nmap scan from the Kali VM to the Metasploitable VM: Perform at least three different scans from the scans listed in the website https://nmap.org/bennieston-tutorial/. Q1: Explain why you chose these scans and what information they provided to you.
    a. WHILE you are running nmap, take a tcpdump file on the kali linux machine.
    b. You should create three files: nmap1.pcap, nmap2.pcap, nmap3.pcap
    c. Analyze the packets in these files. Q2: What packets does your nmap send? What is the metasploitable's response?
3. Analyze what you found:
    a. Look up the ports and what they do.
    b. Follow the following tutorial: https://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-vulnerability-assessment/.
4. Use Metasploit:
    a. Pick one exploit from the ones that you have found in 3.
    b. Execute the exploit using Metasploit.
    c. Take a tcpdump while the exploit is executed. Q3: Can you find the packets that correspond to the exploit? Do they have a discrete signature?

d. Q4: Explain the exploit that you have implemented. Include all screenshots that describe the story of your exploit.

5. Cover your tracks:
    a. Use any of the following techniques to cover your tracks: https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/
    b. Q4: How will you verify that your tracks have been covered?
6. Report: Answer all the questions that are included in parts 1 – 5.
7. Optional, no extra credit
   Install Nessus: https://uwnthesis.wordpress.com/2013/07/31/kali-how-to-install-nessus-on-kali/
    c. Perform another scan on metasploitable with nessus
    d. Did you discover anything that nmap may not have shown?
    e. Fun exercise: use Nessus to scan your home devices.