**Lab Report**

**Lab Completed: Exploitation with IPv6**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

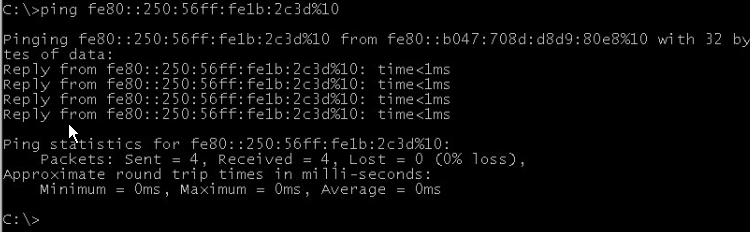
**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

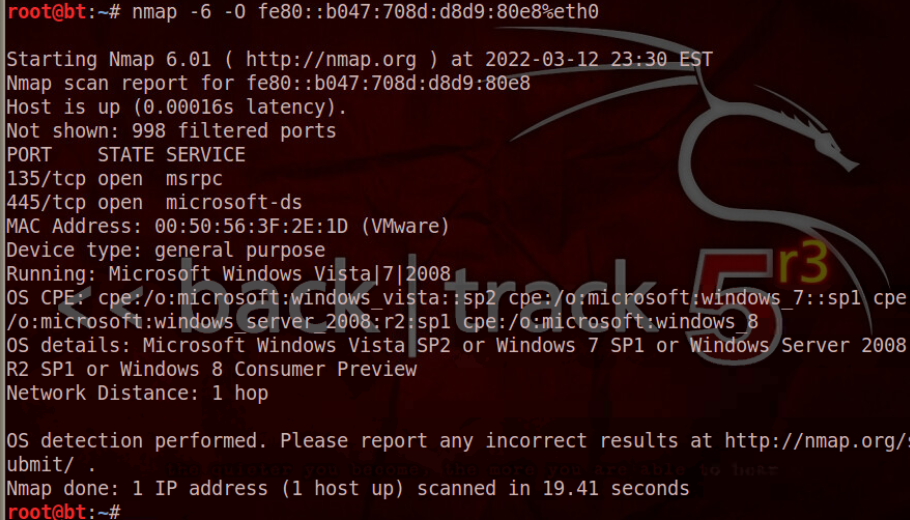
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we used msfconsole to exploit an smb vulnerability and once the exploit was successful we created a reverse shell. We used this reverse shell to upload nmap to the windows machine and then used ncat to create another reverse shell from target host back to the internal backtrack 5 machine.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



Here I was pinging the internal BT5 machine from Windows Server 2008



Here I had just completed an OS scan of the target host so that I knew which OS vulnerabilities to target in MSF.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

There was a very clear vulnerability in this version of SMB on Windows Server 2008 that allowed us to initiate a reverse shell from msfconsole

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

You could use this shell to copy files to/from the machine, search for other networked devices, install malware, etc.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

This would fall under the infiltration and escalation phase. We were infiltrating the system with a vulnerability.

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

This could be mitigated with a Windows Server 2008 security update.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

Really just whether or not this exploit in particular would be considered acceptable per the rules of engagement.