**Lab Report**

**Lab Completed: Intrusion Detection**

**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.

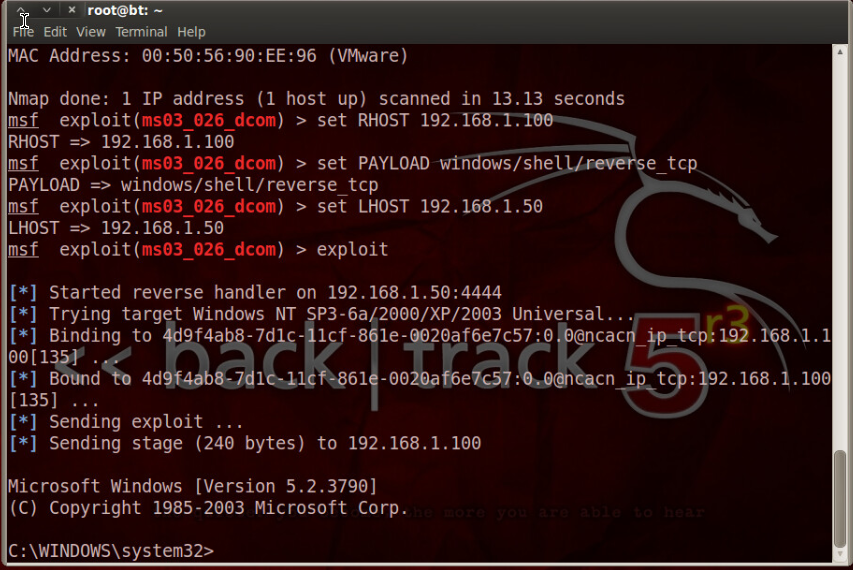
**Part 1: Lab Activity**

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

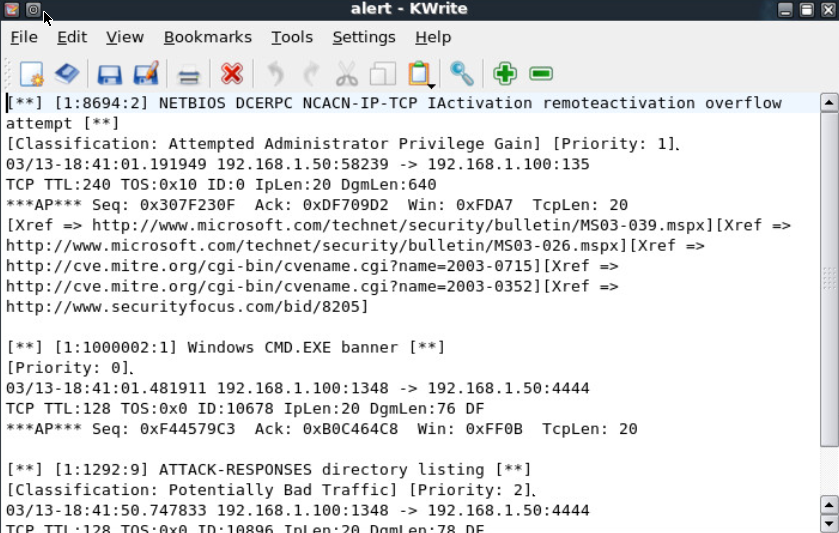
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we observed an intrusion detection framework (snort) in action. To do this we started snort on our sniffer machine and then simulated an internal attack using a remote dcom exploit via msfconsole. Snort picked up this attack and classified it in the generated snort alert file. We then simulated an external SQL injection attack, which snort also logged and correctly identified as an xp\_cmdshell exploit.

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



This is a screenshot of msfconsole after we had successfully executed the remote dcom exploit.



This is a screenshot of the alert generated by snort after analyzing the attack above.

**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.

In the case of the remote DCOM exploit, there was obviously an unpatched program interface with a vulnerability. In the case of the company website, they were not sanitizing their input fields.

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

Either of these attacks could be utilized to gain remote access to a machine or server, and from there any number of things can happen.

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

These exploits were in the infiltration and escalation phase. We were using unpatched vulnerabilities and poor implementation to infiltrate a target network.

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

The remote DCOM exploit could be prevented with a patch. The SQL injection could be prevented by properly sanitizing input server side.

**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?

In the case of the dcom exploit, a penetration tester may need to consider whether the machine is fair game and whether the exploit being used is allowed. In the case of the SQL injection you would also have to consider these things, but you also have to be very careful not to damage the database you are injecting commands into.