**Lab Report**

**Lab Completed: Using Metasploit to Attack a Remote System**

**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:

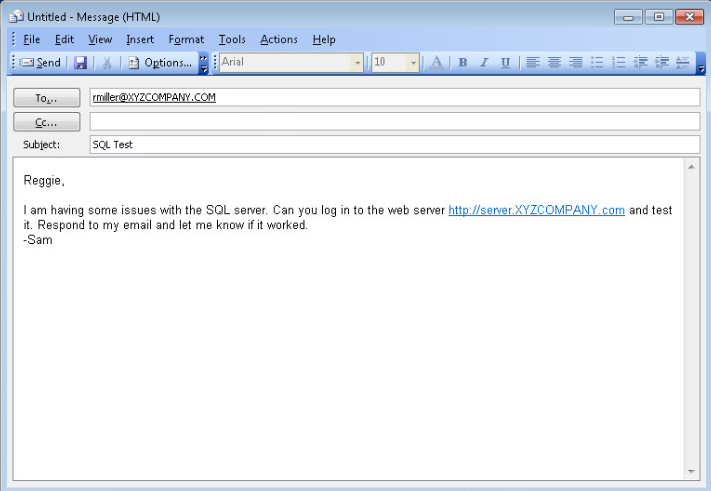
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we impersonated an employee of a company and sent a spear phishing email asking another employee to test a website in the domain under the guise that it wasn’t working. In reality this was a copy of the website running on our machine, and their authentication attempt (username and password) were captured in the apache log.

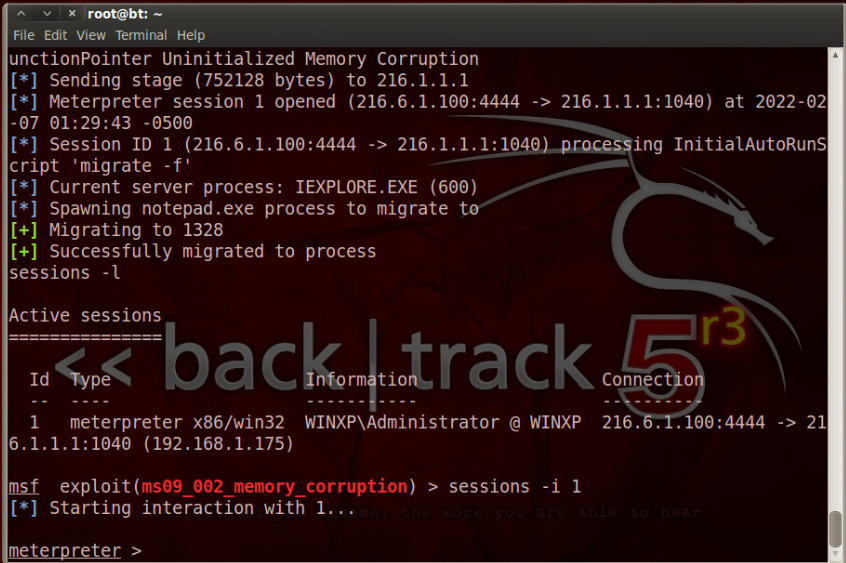
We then set up a listener using metasploit at this same address and asked the employee to retest. Upon opening the link to retest we exploited their browser and then quickly transferred to another process.

After gaining a foothold in their system, we added a new route, and then did an arp scan to identify additional machines on the same network. We then exploited a vulnerability in Windows Remote Procedure Call, effectively pivoting to another system on the internal network.

**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 the first spear phishing email I sent to rmiller with a bogus link to our locally hosted copy of their website.



In this part of the lab we had just sent the second spear phishing email, the bogus link was clicked again, and we established a reverse tcp shell.

**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.

The employee was definitely a weak point. They obviously open the link and then enter their username/password without checking out where it is actually taking them. Whatever email filtering program they use(if any) is subpar.

The first compromised machine is running a vulnerable version of Internet Explorer. The second compromised machine is running a vulnerable version of Windows 2003 without a service pack.

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

If you needed to gain a foothold inside of a network that is sitting behind a firewall, the first attack could be used to do this. The second attack can be used to compromise additional machines that may not have been breachable from an external host.

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

This is definitely in the system hacking phase. We are using hacking tools to compromise multiple machines on a private corporate network.

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

The employee here needs some a security refresher for sure. They should definitely patch both machines.

They could also institute some kind of IPS/IDS system that would help detect and stop outbound connections like this in the case that a machine or machines are breached.

**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?

I would hope the first point of entry is a machine that they are in the clear to target, but doing a cursory scan of other networked computers after compromising the first, it may not be as clear cut as to which available machines they are able to go after in their pentest. It could be that the secondary system we pivoted to was off limits.