**Lab Report**

**Lab Completed: Using John the Ripper to Crack Linux Passwords**

**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.

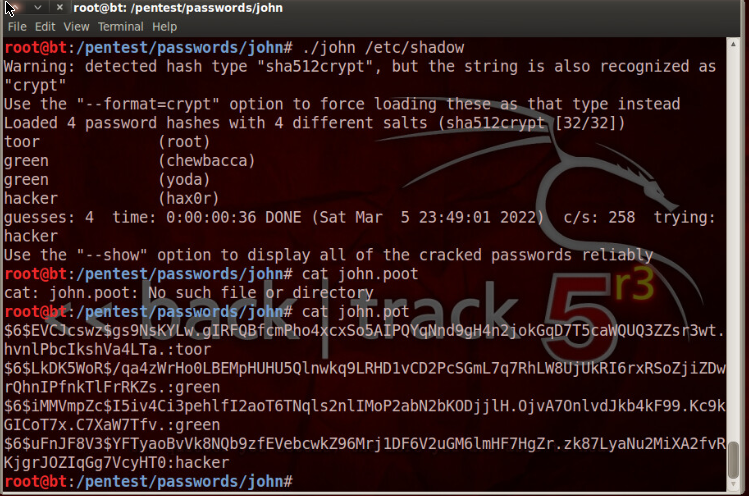
**Part 1: Lab Activity**

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

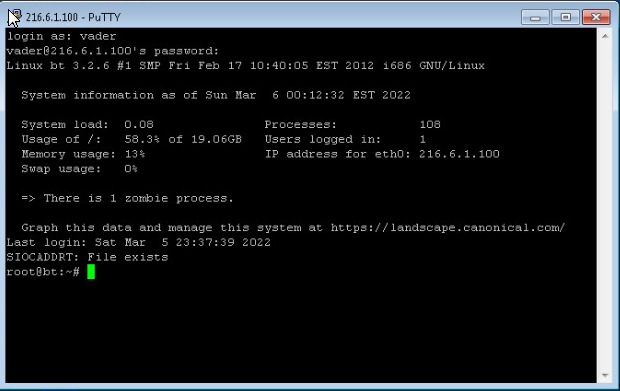
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we used John the Ripper to run a dictionary attack against the contents of /etc/shadow on a Kali Linux system. We then used a text editor to edit /etc/passwd creating a new account(vader) with root privileges and edit /etc/shadow to give this new account the same password as the existing root account. We generated a new ssh keypair for this machine and then logged in using ssh from the Windows 7 machine. We also generated an ssh keypair on the internal Kali Linux machine and used secure copy to copy the public key to the external Kali Linux authorized\_keys file.

**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 passwords and their corresponding hashes that were cracked using john the ripper



This is a screenshot from the Windows 7 system. I had just successfully ssh’d into the external Kali machine using the newly created vader account with root level permissions.

**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.

I don’t know if there were any vulnerabilities per-say in this lab. We were logged into a machine as root and used a password cracking tool as this user to crack passwords on the machine. Everything worked as it should have. If there was a vulnerability it would be that the user accounts all had weak passwords.

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

If you happened to have the root password of a remote system you could potentially use this in conjunction with secure copy to copy your public key to their authorized keys file and then from there use John the Ripper to take a whack at /etc/shadow.

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

I think this lab falls under both Access Extension and Assault. We are extending access by creating a new account with root level permissions and we are assaulting the machine by using John the Ripper to crack the hashes stored in /etc/shadow.

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

You could require more complex passwords for all users.

**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?

They may want to make sure they do not leave any additional root level accounts on the machines they are pentesting and ensure the authorized keys file is sanitized after the pentest is completed.