## Lab 6: Cracking Hashes with John the Ripper

**Scenario**

A software house employs you. A hacker cracked most of the PC’s passwords. Using a password cracking tool, the hacker gained control of the employee’s PC, created directories, and did other things. The company wants cybersecurity specialists to conduct a forensic investigation into the cyber attack to prevent such attacks in the future. The company also decided to provide awareness to employees of this type of attack; hence, they would not be fooled by the hacker in the future.

**Solution**

The company hires you as a certified cybersecurity practitioner because they want you to hack and find their vulnerabilities ethically. One of the crucial phases of system hacking is password cracking. Cracking passwords is frequently the first step in a hack. A password is a crucial piece of data required to enter a system. As a result, most attackers employ password-cracking strategies to obtain unauthorized access. An attacker can attempt to guess a password manually or use automated tools and methods, like a dictionary or brute-force approach. Password cracking methods are generally successful because most passwords are weak or simple to guess. In this lab, we employ the **Responder** tool to retrieve data such as the OS version, client version, NTLM client IP address, and hashes of the NTLM username and password from the target system.

The two primary components of Windows OS used to resolve names for hosts connected to the same link are LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service). There is a good chance of obtaining user credentials in an internal network penetration test because there is little knowledge of this attack. An attacker can spoof the server by watching for LLMNR/NBT-NS broadcast requests and sending a response posing as the real server.

|  |
| --- |
| 1. Open the **MATE** terminal on the ParrotOS machine. Execute the command **apt** **install responder** to install the responder utility.    2. Execute the command **Responder -I enp0s3**. The -I specify the interface.    3. Responder starts listening to the network interface for events.    4. Switch to the Windows 10 machine. Open the **File Explorer**. Then type **//192.168.10.15** and press **Enter**.    5. The Windows security pop-up appears. Type **username:** **Administrator** and **password: @dmin123**.    6. Switch back to the ParrotOS machine. The responder starts capturing the access logs of the Windows 10 machine. It collects the hash of the logged-in users of the target machine. Press **Ctrl+C** to terminate the session.    7. By default, Responder stores the logs in **/usr/share/Responder/logs**. Execute the command **cd** **/usr/share/Responder/logs** to go to the Responder logs directory. Then type **ls** and press **Enter**. The **HTTP** logs text file is displayed.    8. Now, attempt to crack the hashes to learn the logged-in user’s password. The **John the Ripper** tool must be installed on the system to crack the password hash. To install the tool, open a new **Terminal** window and execute the command **sudo apt install john**.    9. After installing John the Ripper, execute the command **john [Log File Name.txt]**. John the Ripper starts cracking the password hashes and displays the password in plain text. It concludes the demonstration of performing an active online attack to crack a password using Responder. |