Network Penetration Testing Methodology-Internal

6 Hr 39 Min Remaining

Instructions Resources Help  100%

Exercise 14: Auditing a Machine for Weak Passwords Using L0phtCrack

Scenario

Since security and compliance are high priorities for most organizations, attacks on a company or organization's computer systems take many different forms, such as spoofing, smurfing, and other types of **denial-of-service (DoS)** attacks. These attacks are designed to harm or interrupt the use of your operational systems.

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. In this lab, we will look at what password cracking is, why attackers do it, how they achieve their goals, and what you can do to do to protect yourself. Through an examination of several scenarios, in this lab, we describe some of the techniques they deploy and the tools that aid them in their assaults and how password crackers work both internally and externally to violate a company's infrastructure.

In order to be an **Expert Penetration Tester** or a **Security Administrator**, you must understand how to crack administrator passwords. In this lab, we crack the system user accounts using **L0phtCrack**.

In this lab, being a security auditor, you will be running the L0phtCrack tool by giving the remote machine’s administrator user credentials. User accounts' passwords that are cracked in a short amount of time are considered to be weak, and you need to take certain measures to make them stronger. The objective of this lab is to help students learn how to:

* Extract the Administrators password using L0phtCrack

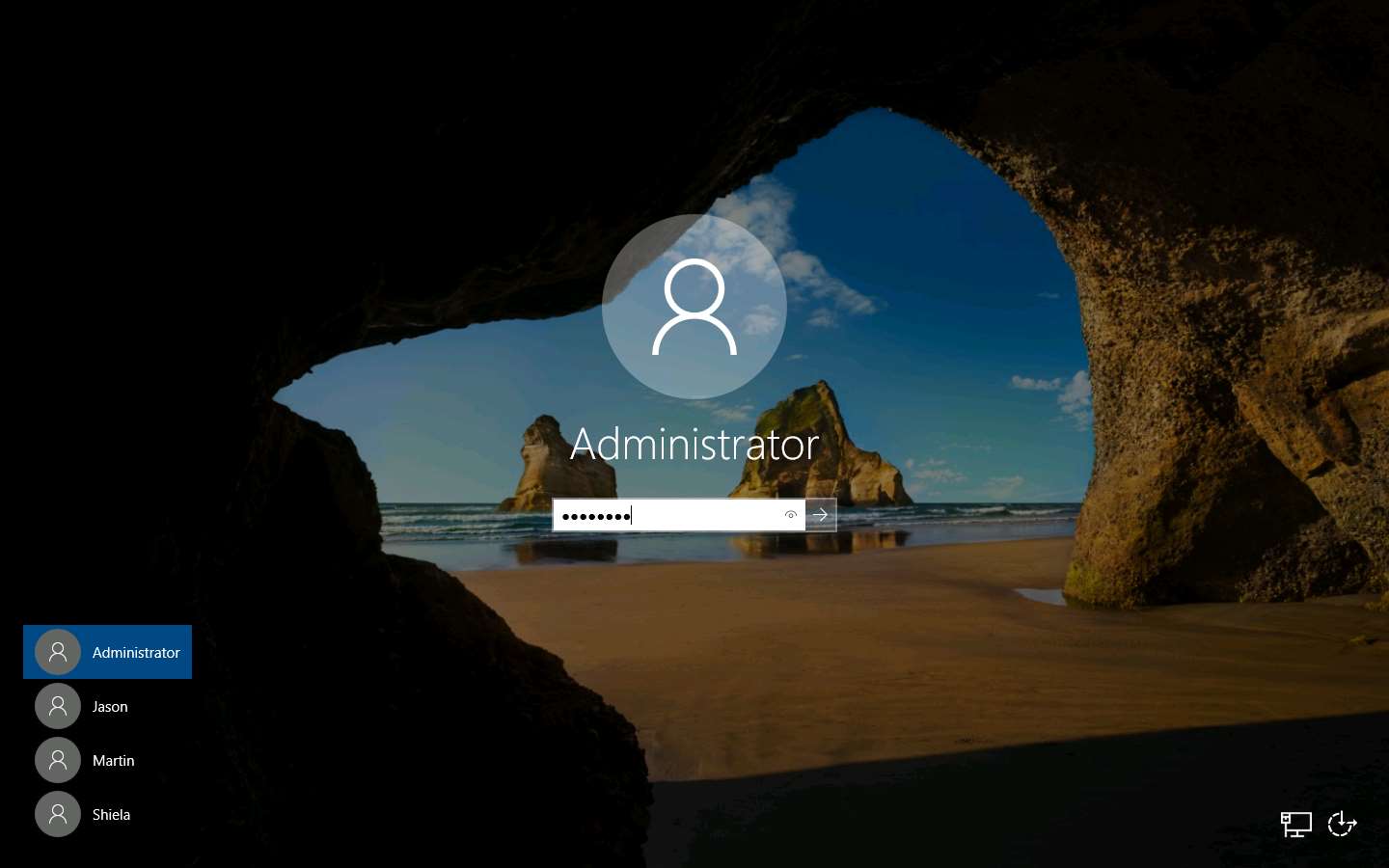
**Lab Duration**: **20** Minutes

1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10), click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10).



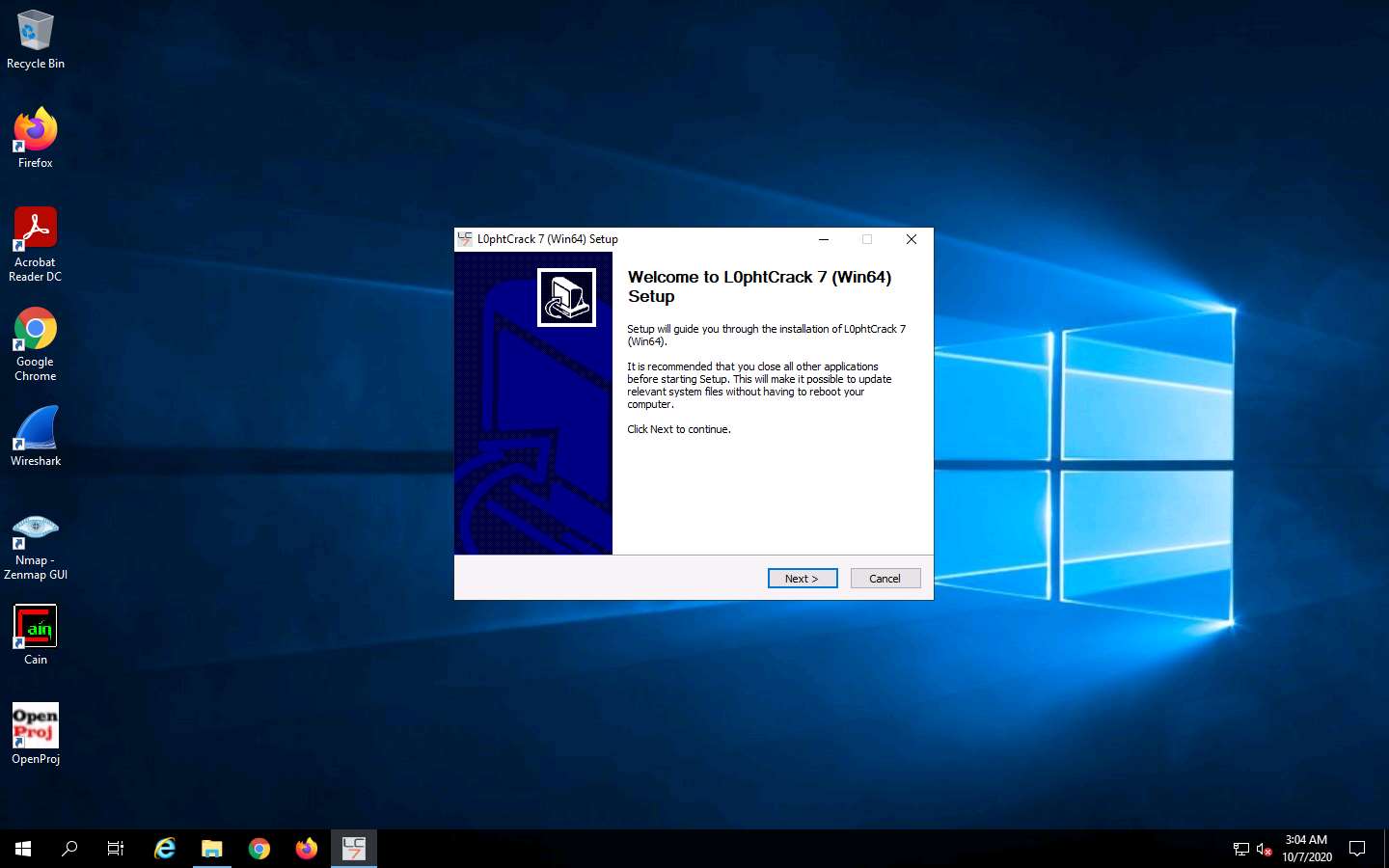
1. In the password field click Pa$$w0rd and press **Enter**.

You can use the **Type Password** option from the **Commands** menu to enter the password.

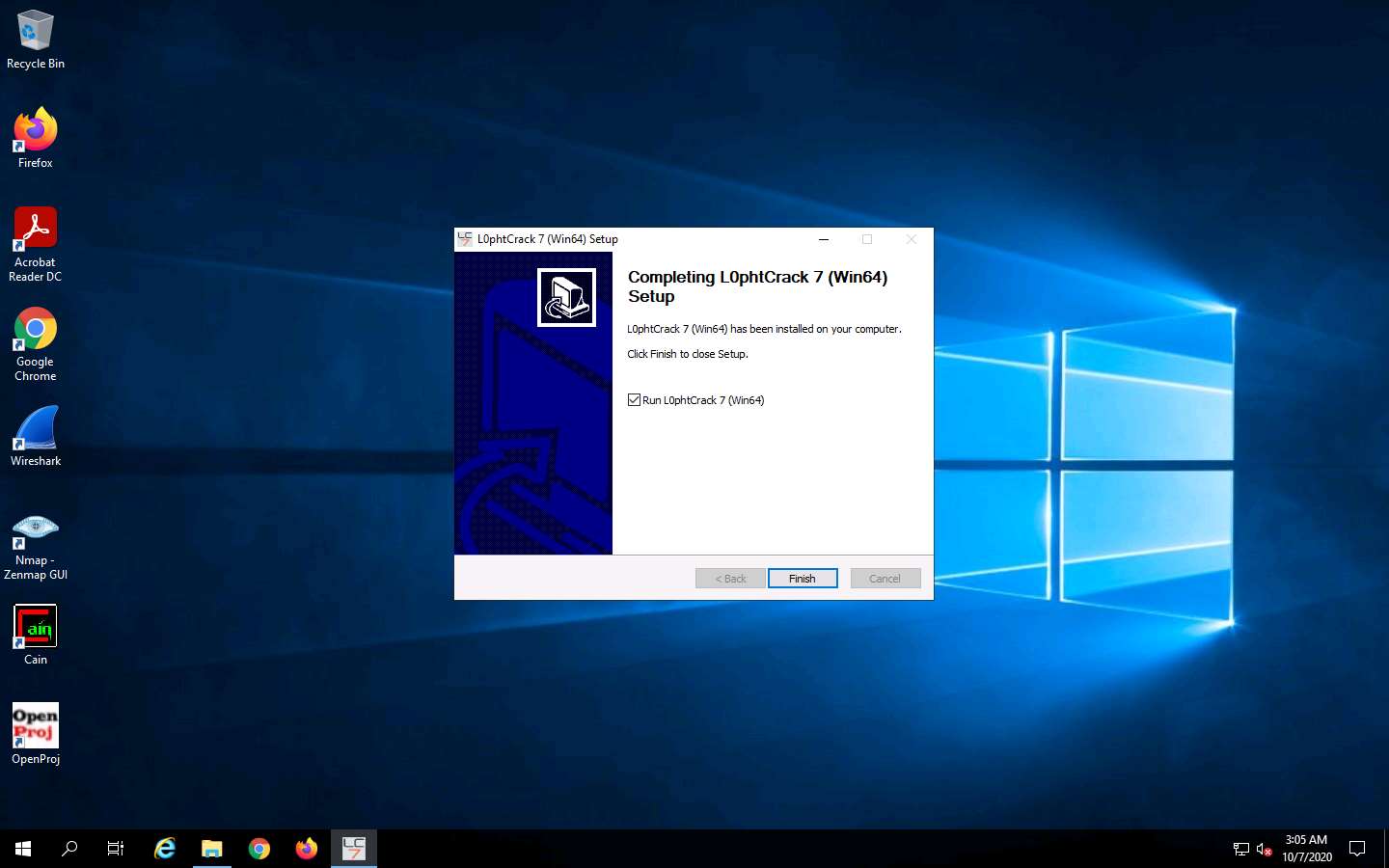


1. In this lab, we are going to audit user accounts on a machine to check for weak passwords using **L0phtCrack**. To install **L0phtCrack**, navigate to **E:\CPENT Module 06 Network Penetration Testing Methodology-Internal\L0phtCrack** and double-click **lc7setup\_v7.1.16\_Win64.exe**. If an **Open File -Security Warning** pop-up appears; click **Run**. Follow the wizard-driven installation steps to install **L0phtCrack**.

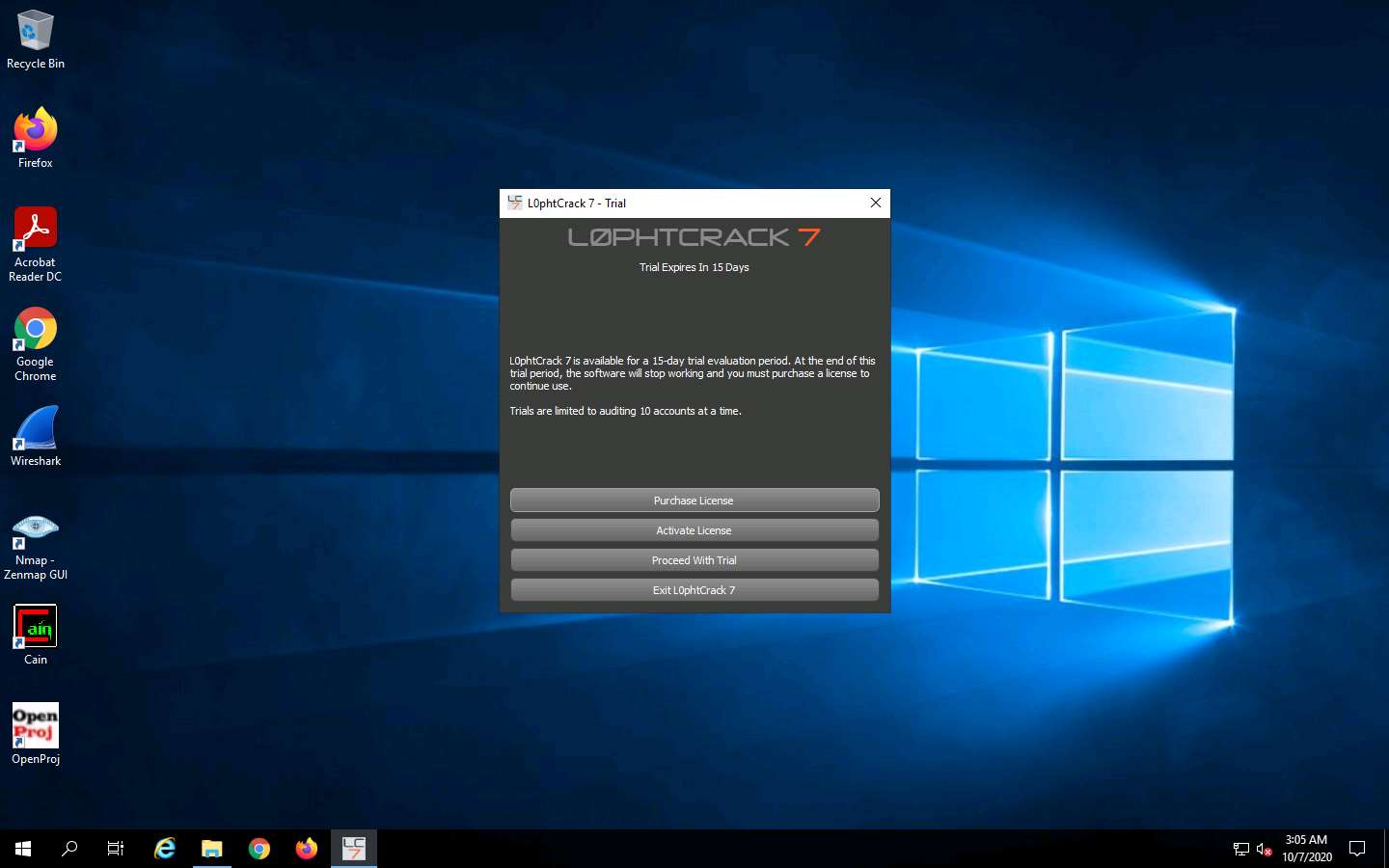
While installing the application, a **Program Compatibility Assistant** pop-up appears, click **Close**.



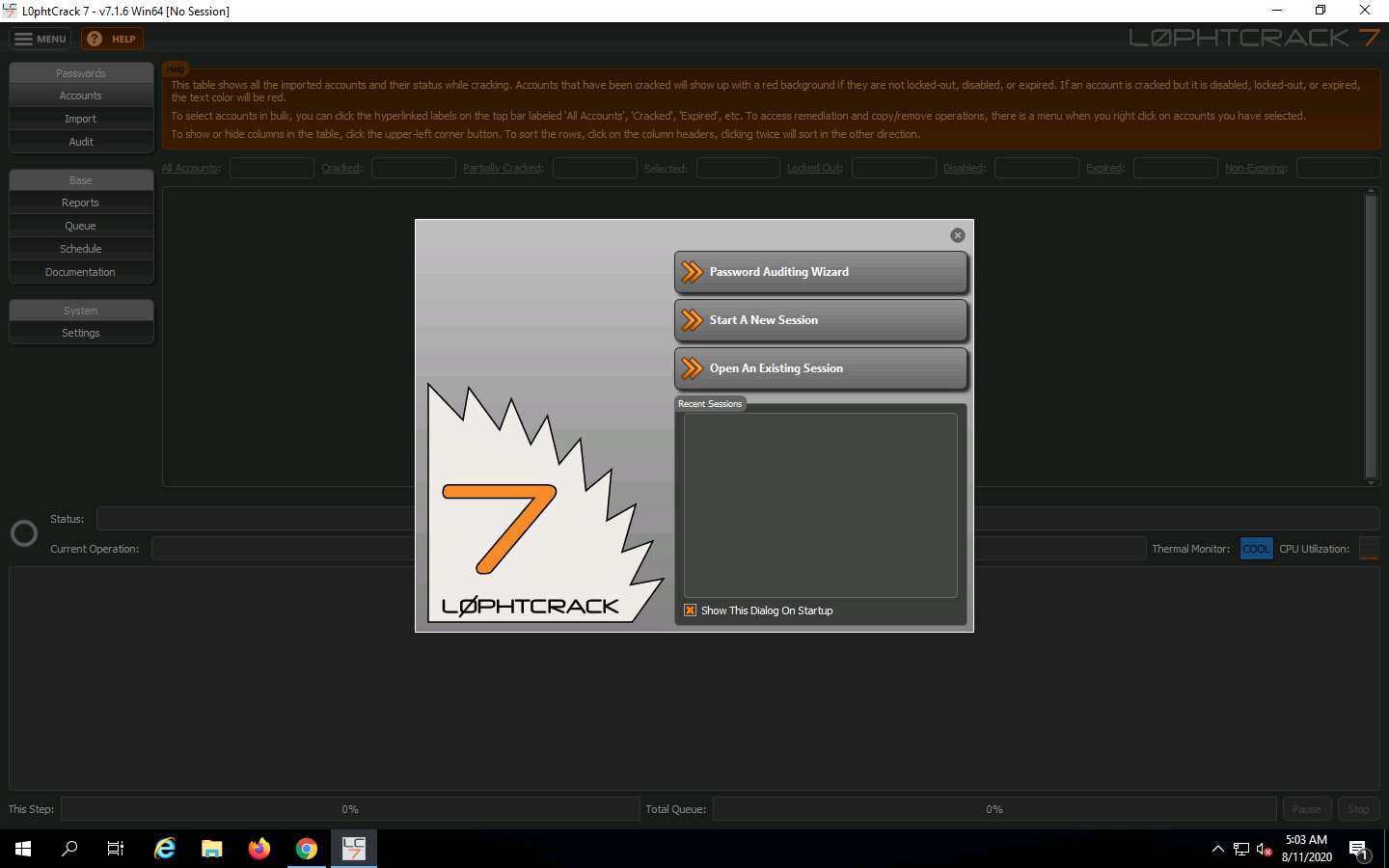
1. On the **Completing L0phtCrack 7 (Win64) Setup** page, ensure to check **Run L0phtCrack 7 (Win64)** and click **Finish** to launch the **L0phtCrack** tool.



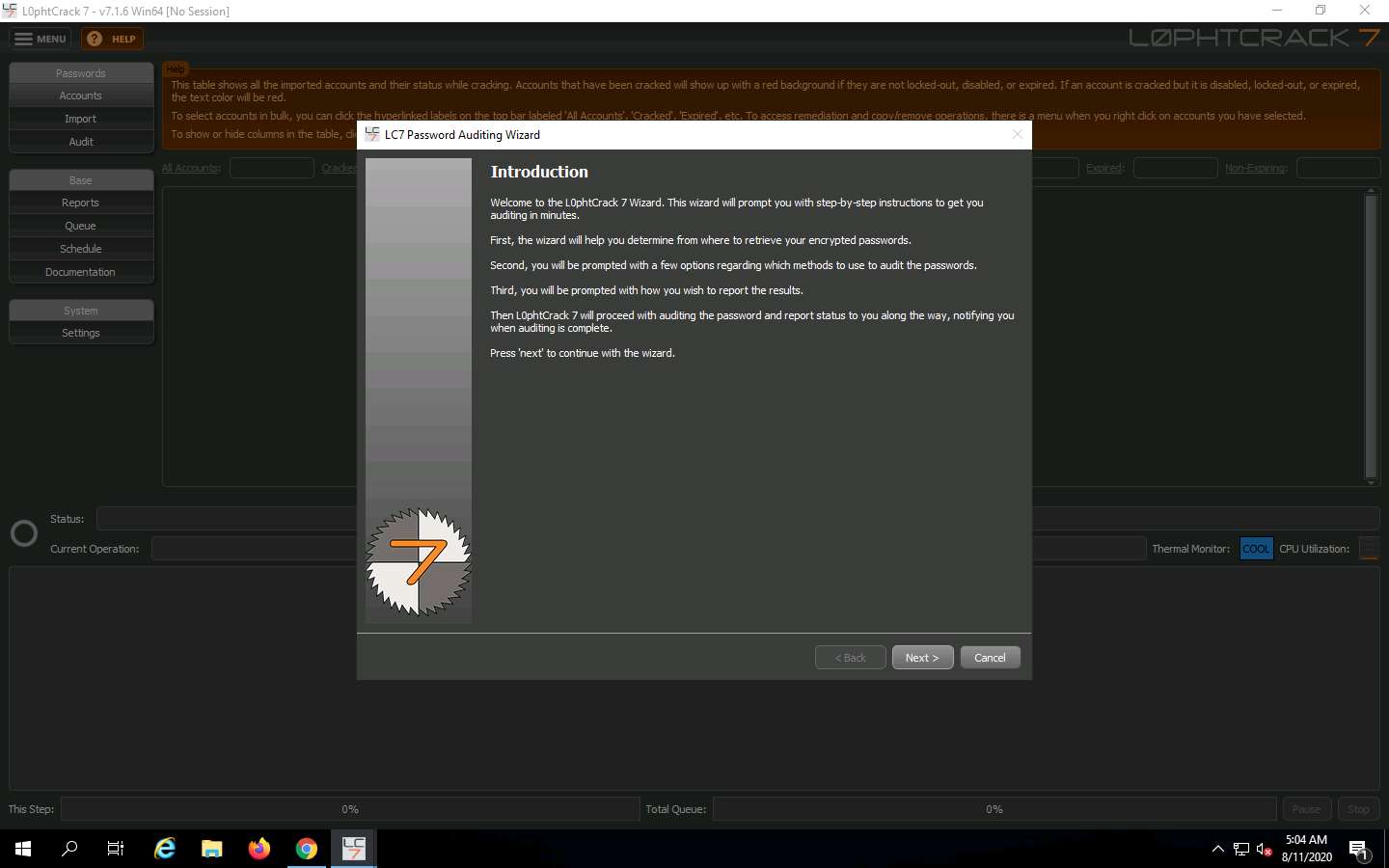
1. **L0phtCrack 7 - Trial** window appears. Click **Proceed With Trial** button.



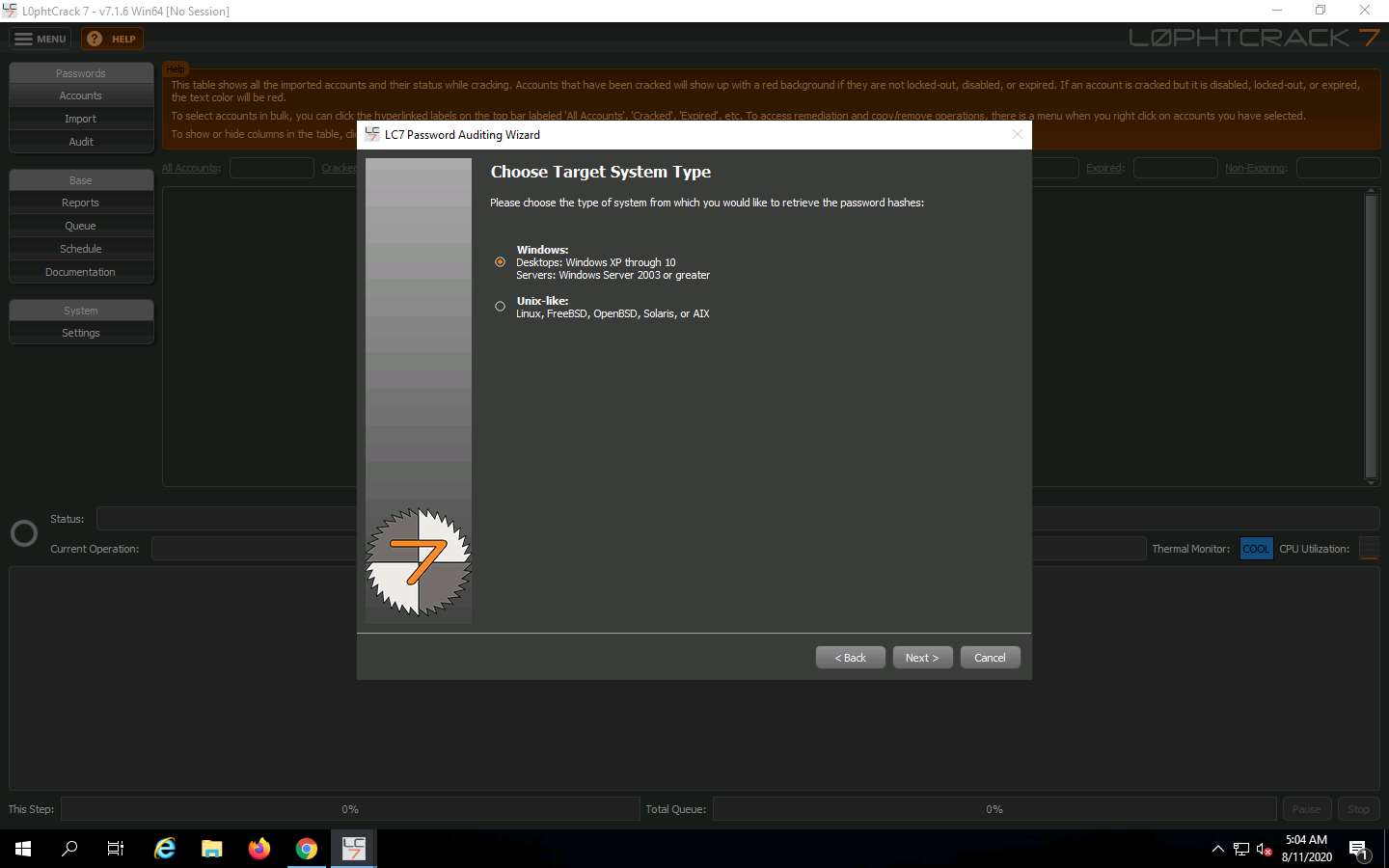
1. A L0phtCrack 7 pop up appears; select **Password Auditing Wizard** option.



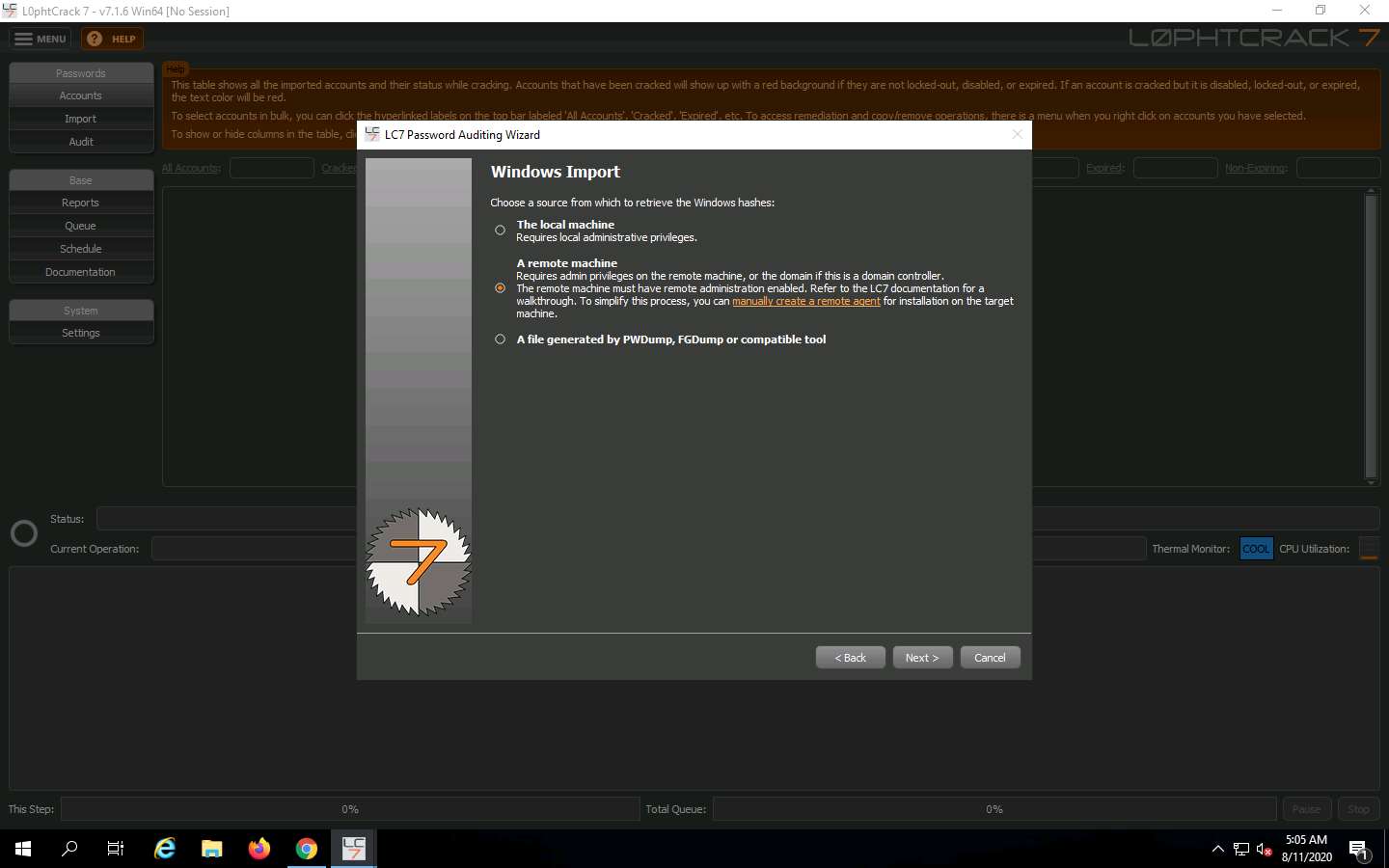
1. In the **Introduction** page of **LC7 Password Auditing Wizard**, click **Next**.



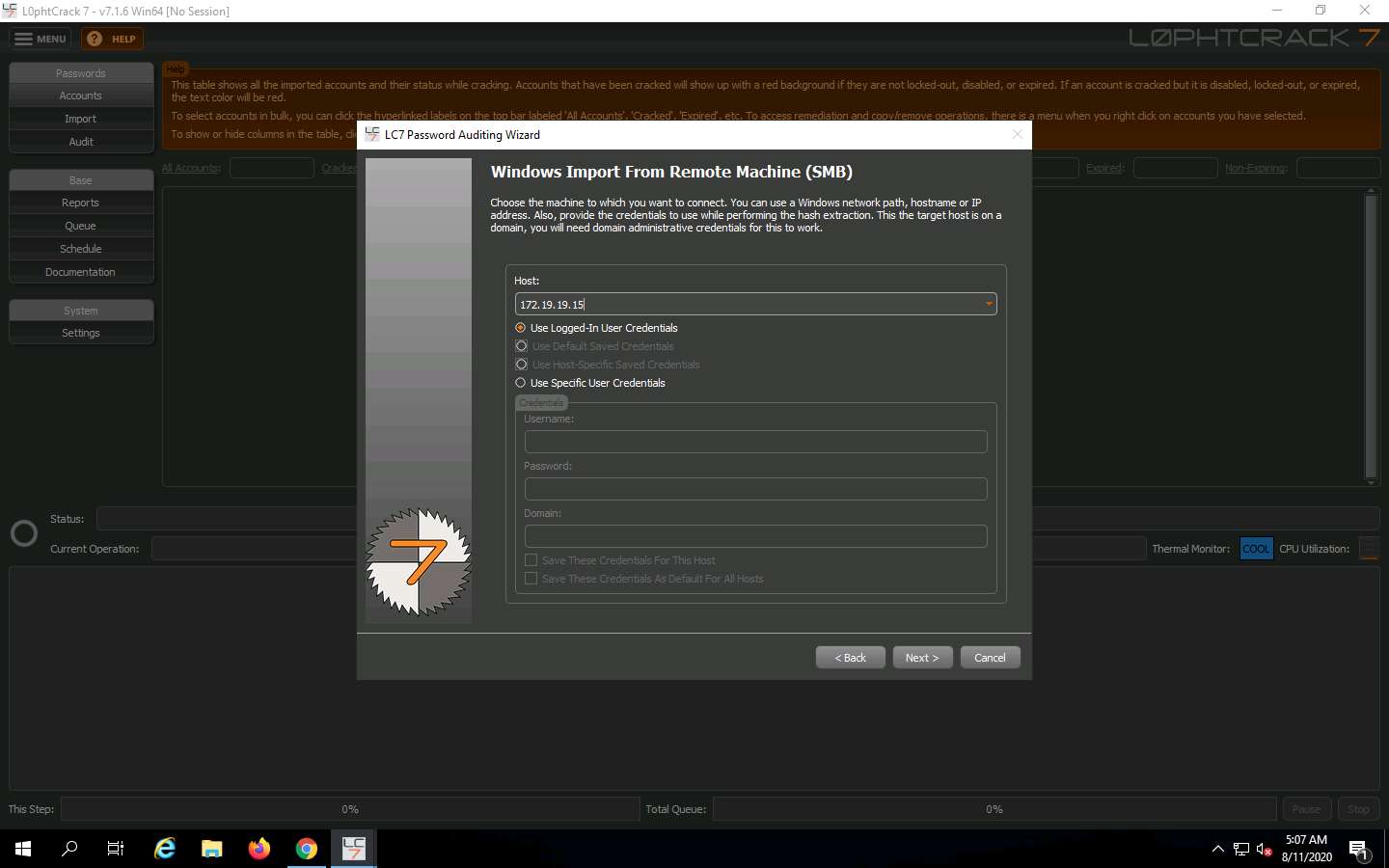
1. In the **Choose Target System Type** window select **Windows:** radio button and click **Next**.



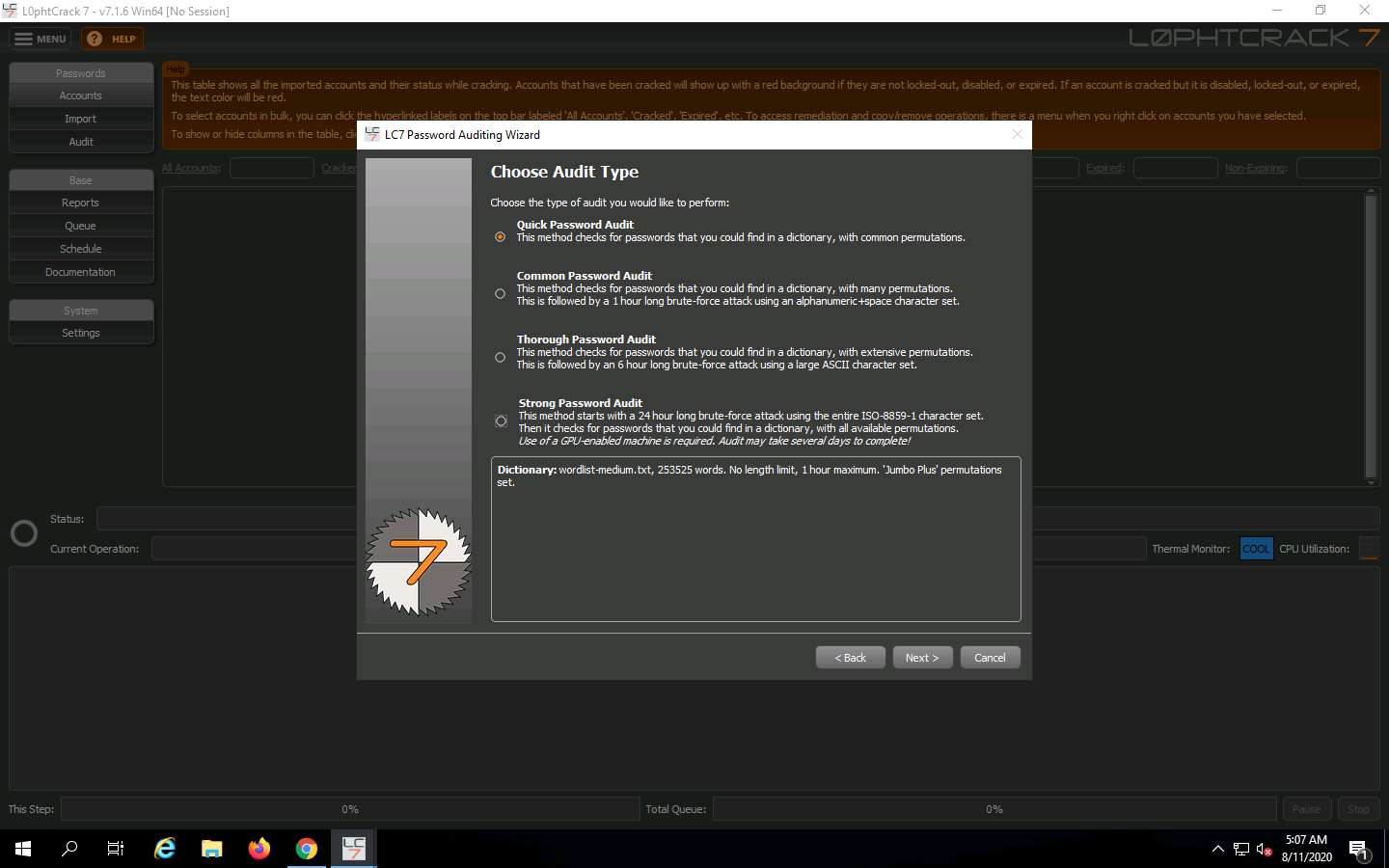
1. In the **Windows Import** window, select **A remote machine** radio button and click **Next**.



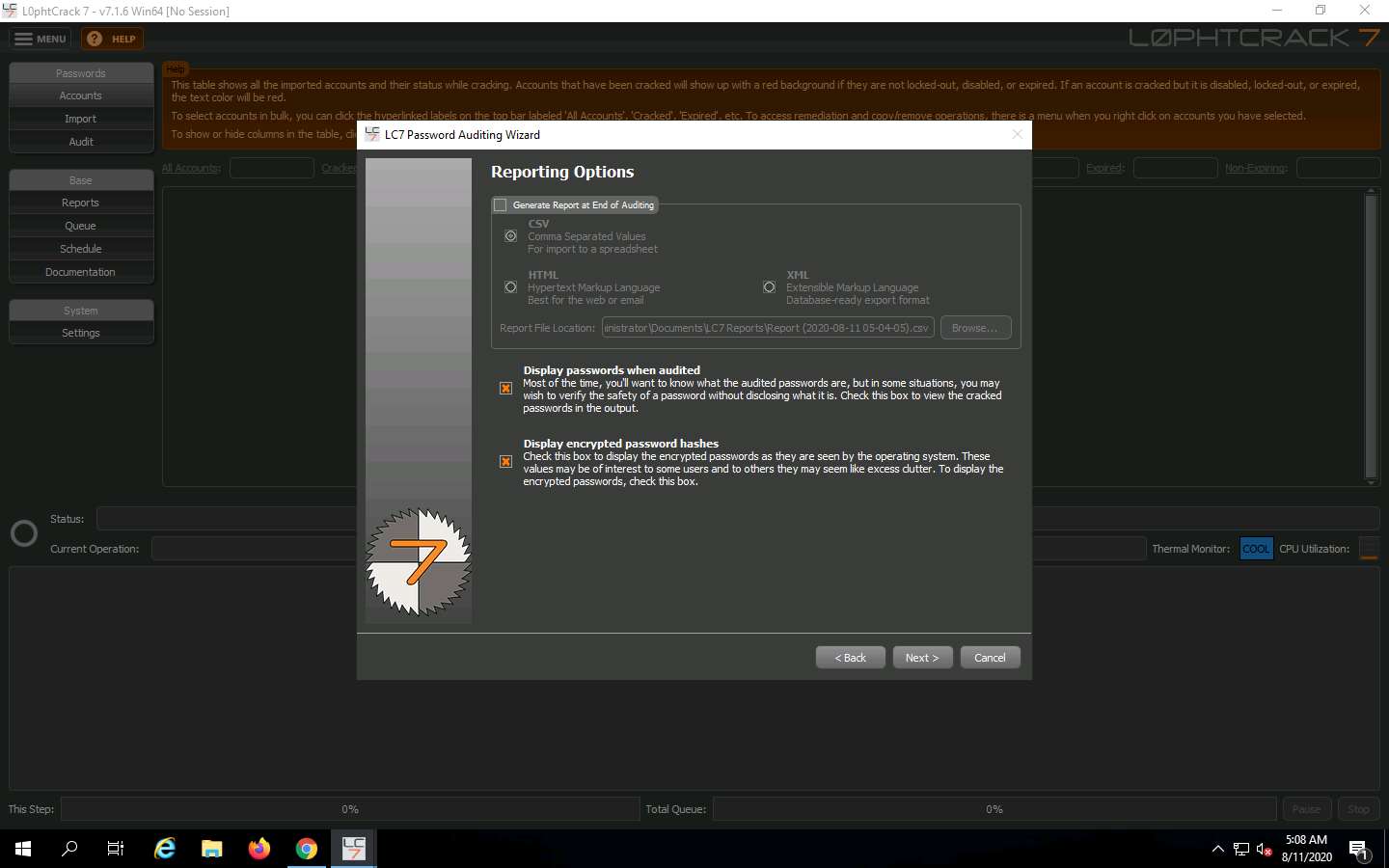
1. In the **Host** field of **Windows Import From Remote Machine (SMB)** window, provide the IP address of **Advertisement Dept.** machine and click **Next**. Here, the IP address of **Advertisement Dept.** is **172.19.19.15**.



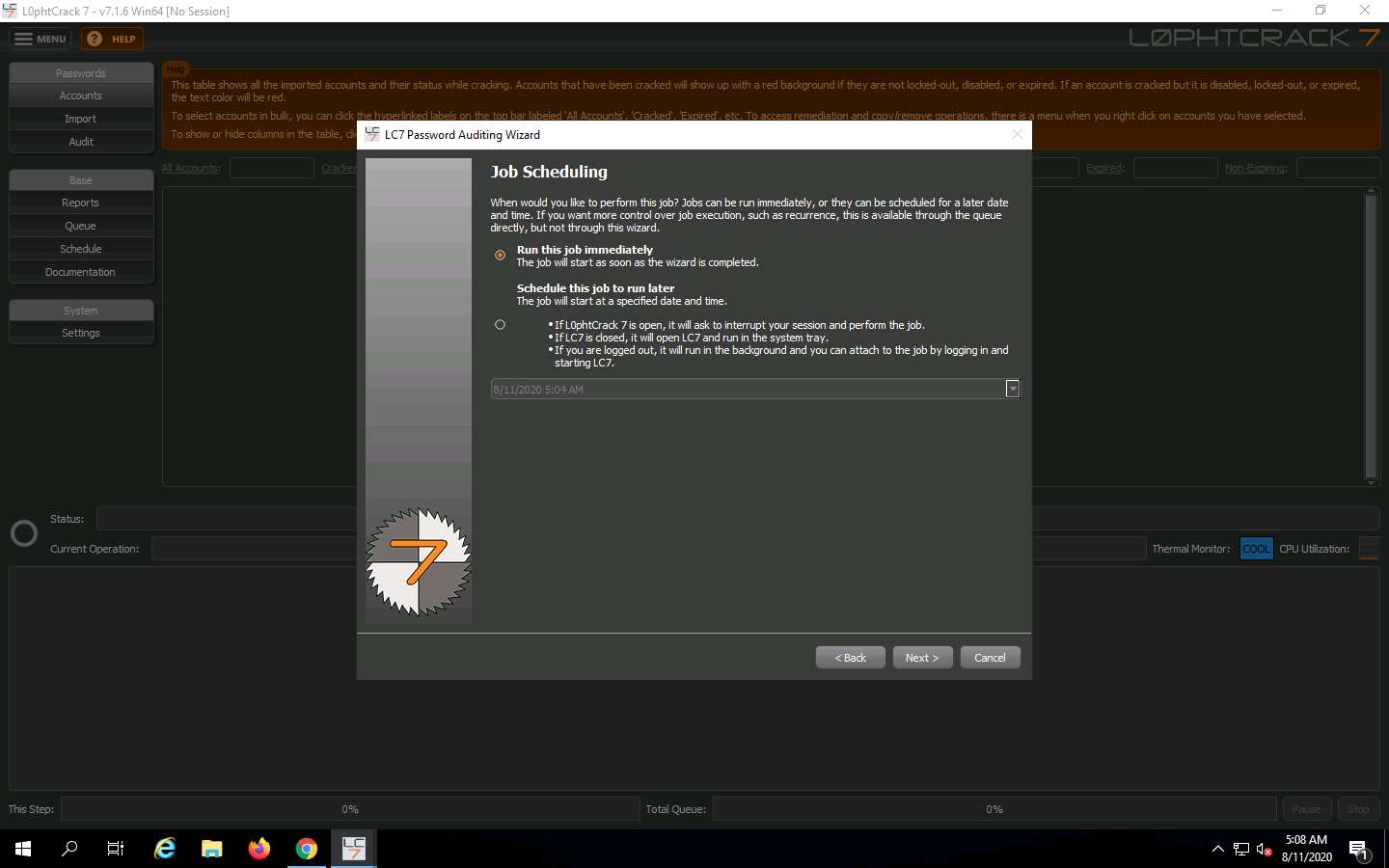
1. In the **Choose Audit Type** window, select **Quick Password Audit** option and click **Next**.



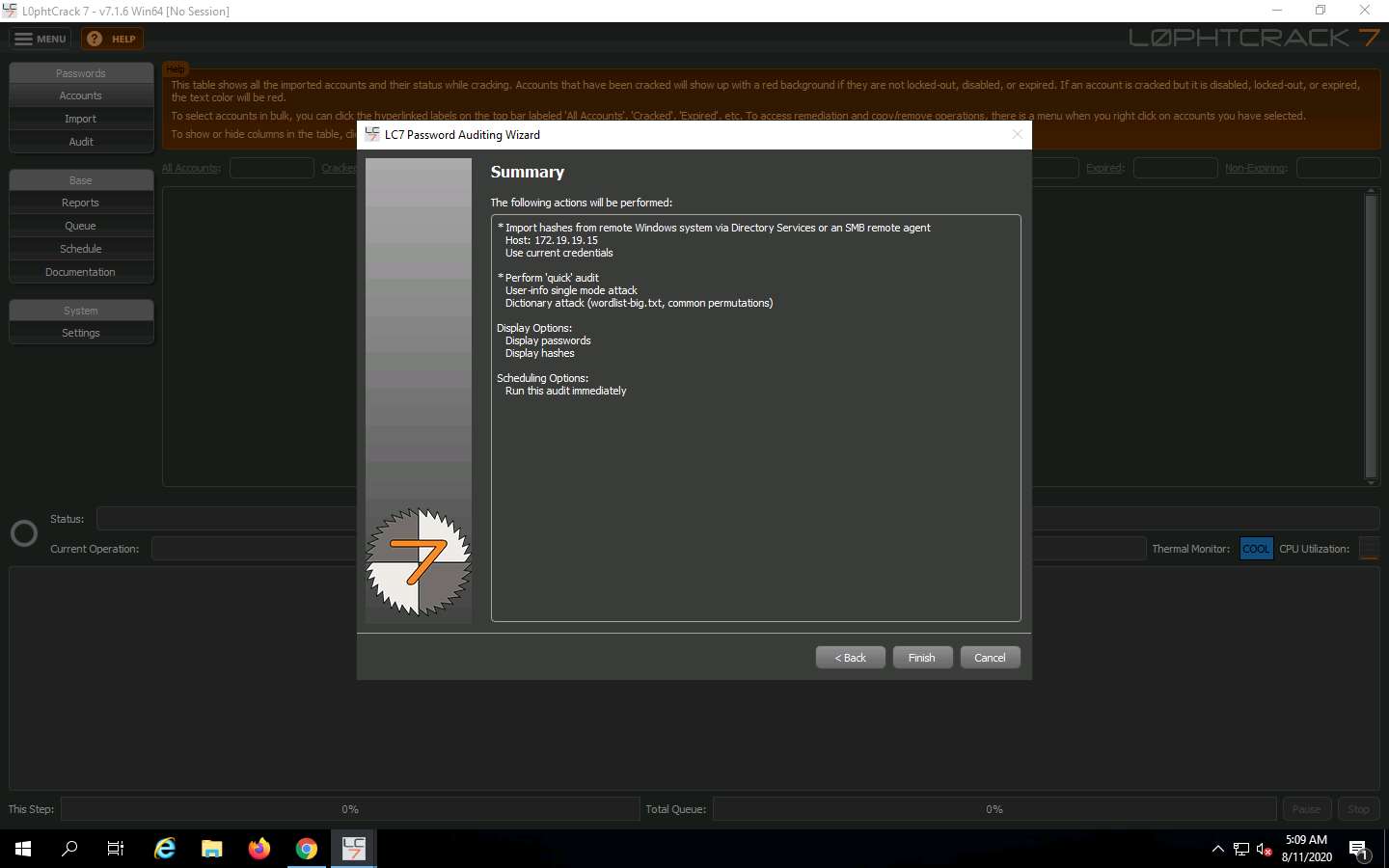
1. In the **Reporting Options** window, leave the options set to default and click **Next**.



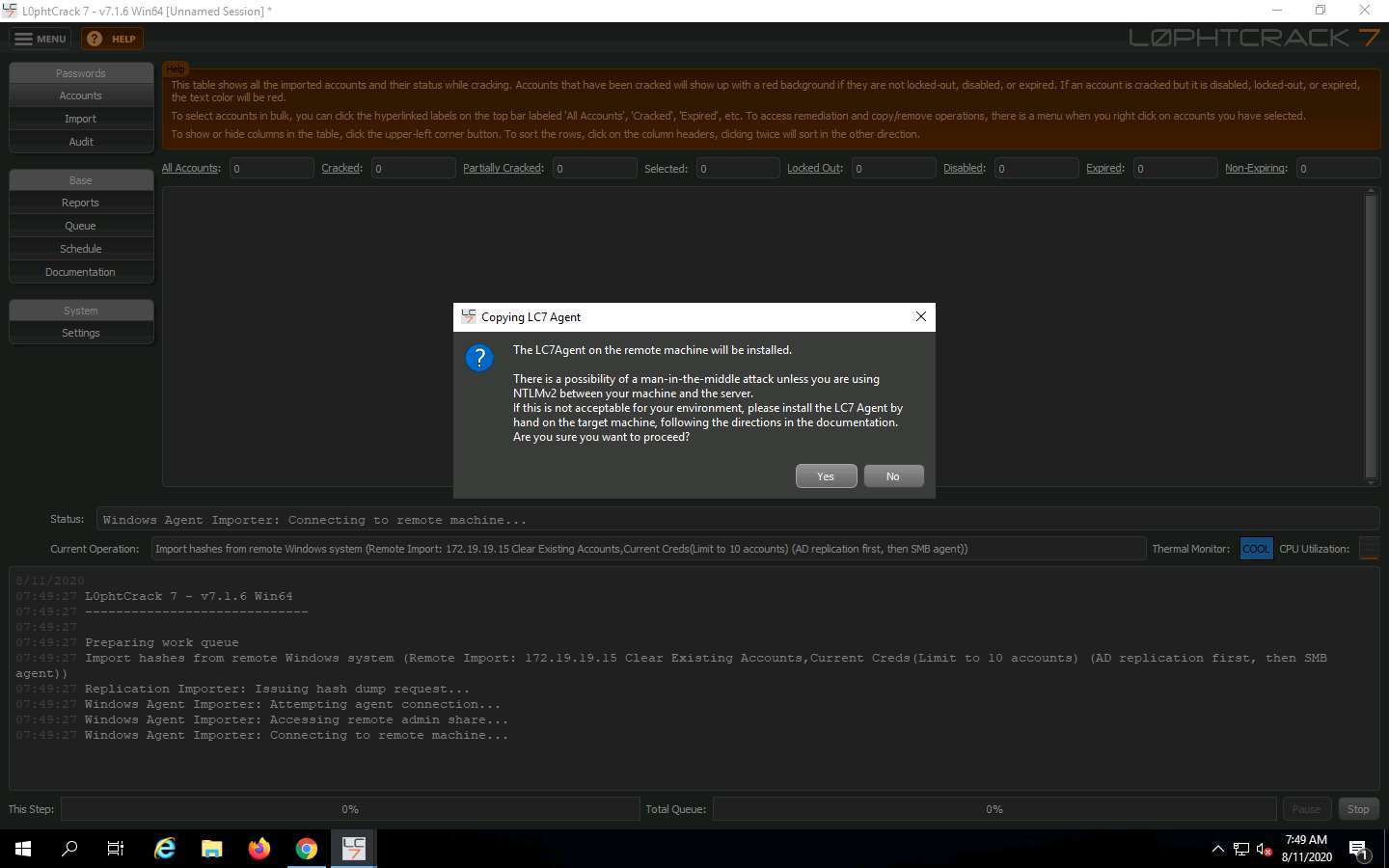
1. In the **Job Scheduling** window, select **Run this job immediately** and click **Next**.



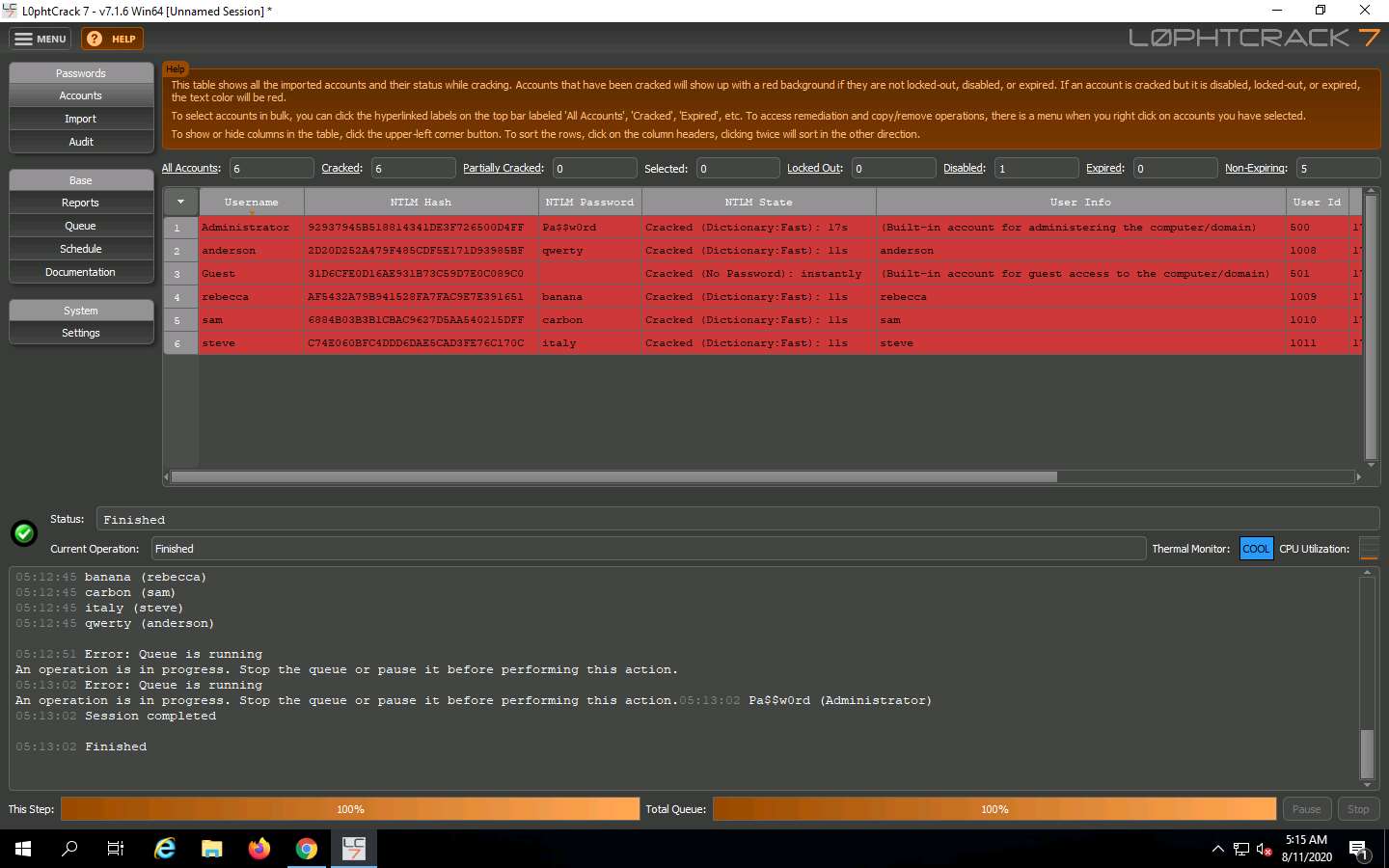
1. In the **Summary** window, read the summary and click **Finish**.



1. A caution box appears regarding changed LC7Agent on the remote machine as shown in the screenshot. Click **Yes**.

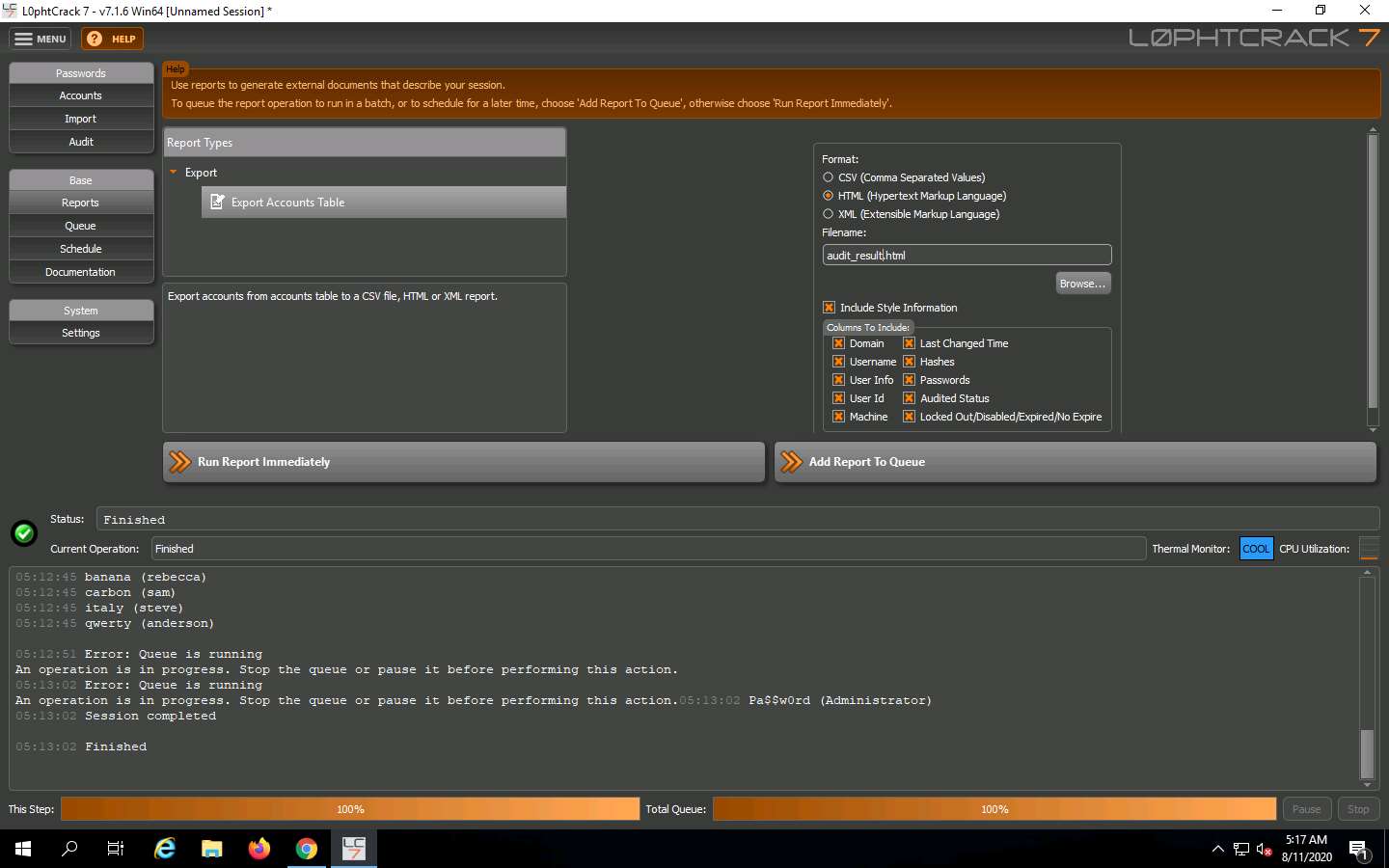


1. L0phtCrack will begin to decode the hashes. You can see the Progress bar in the lower right-hand corner of the window. Once done with the password auditing, it displays the weak passwords set for the respective user accounts present in **Advertisement Dept** machine as shown in the screenshot.

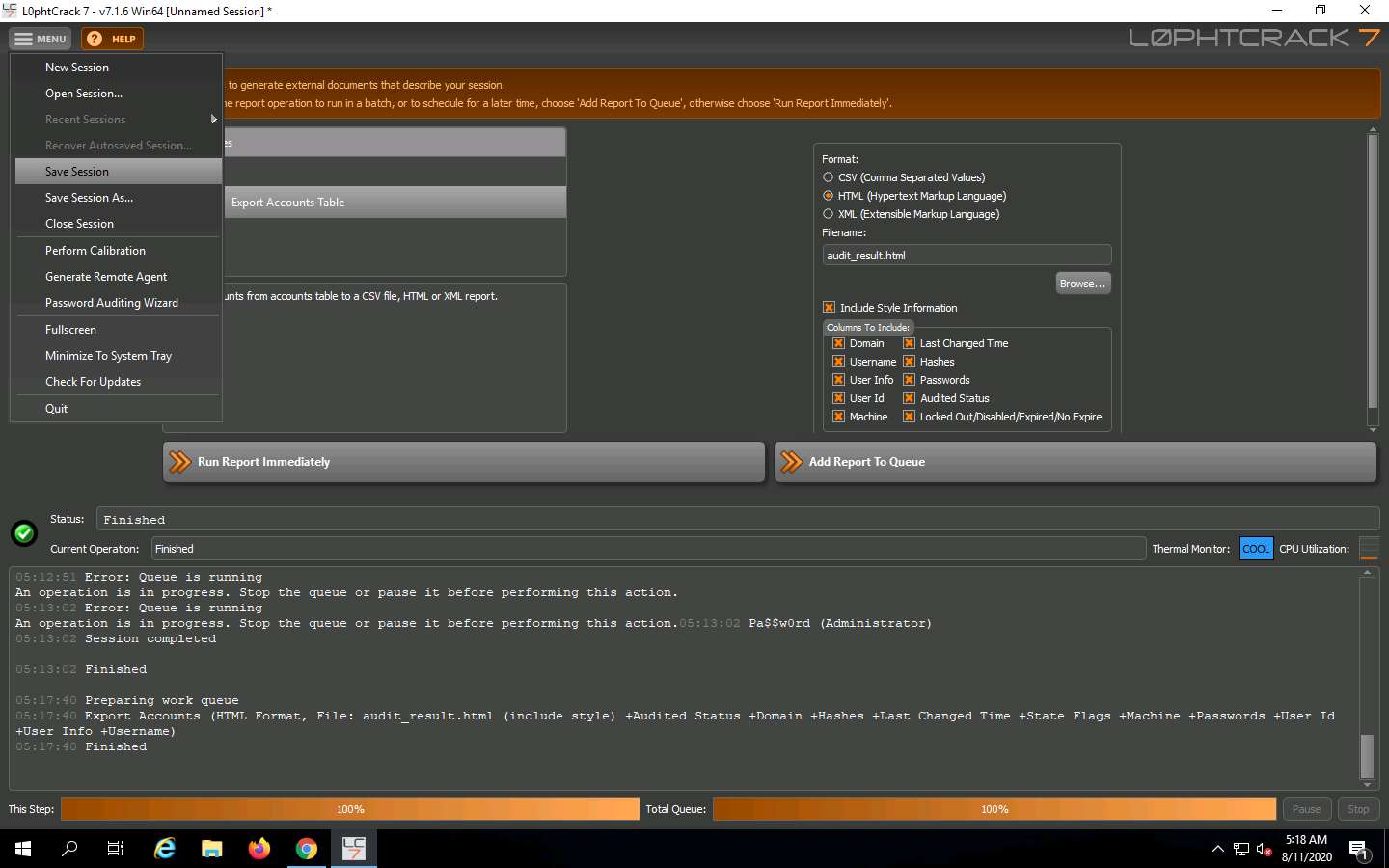


1. Click **Reports** tab on the left-pane and click **Export Accounts Table** in the **Report Types** box. Select **HTML (Hypertext Markup Language)** under **Format:** box and provide a name for the file and click **Run Report Immediately**.

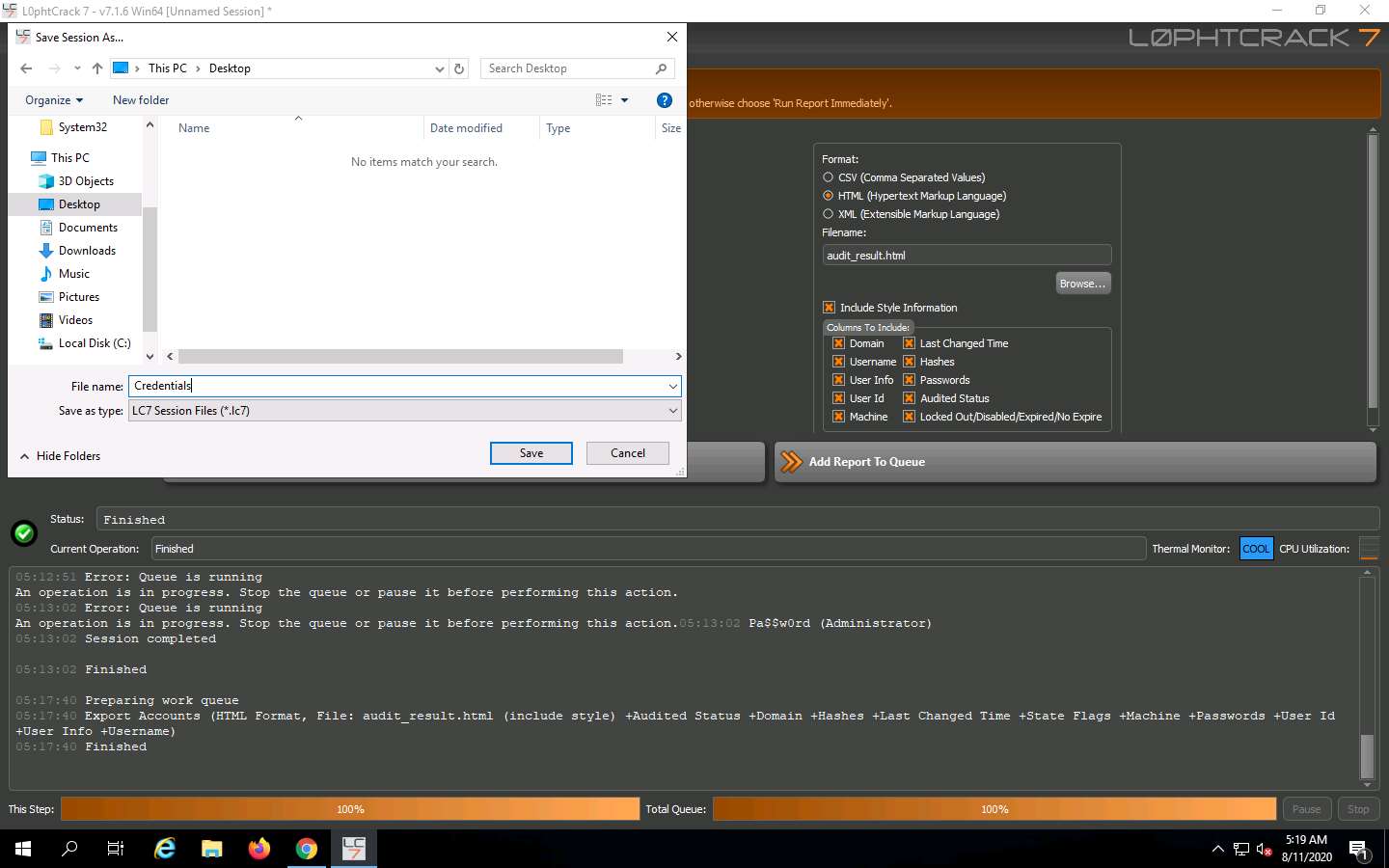
After clicking the **Run Report Immediately** button, a **Warning** pop-up window appears. Click **Yes**.



1. To save this session, navigate to **MENU** icon at the top left corner of the window and click **Save Session** option.



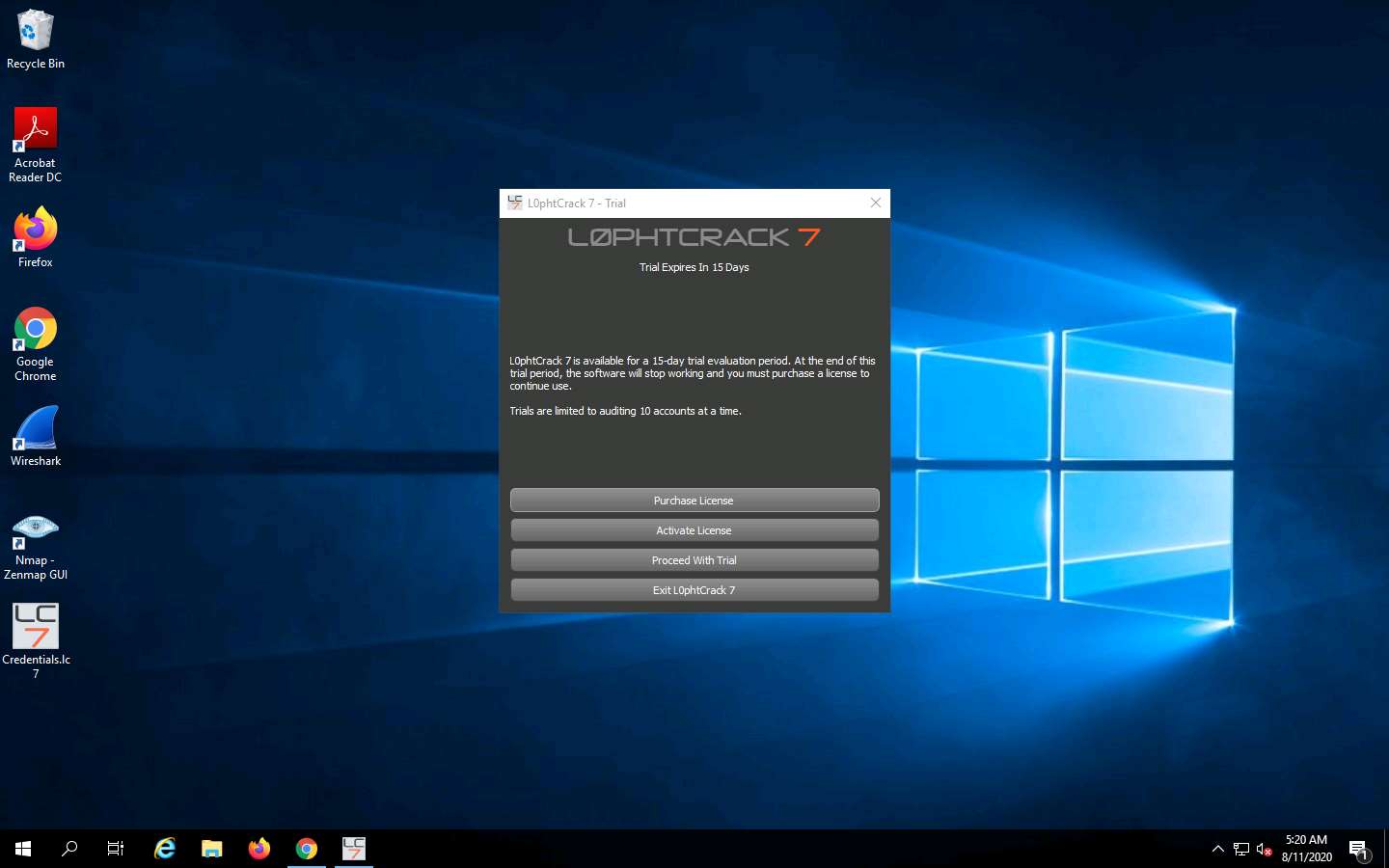
1. A **Save Session As** window appears on the screen. Select the destination location (here, **Desktop**), specify the file name as **Credentials** and click **Save**. Now close the **L0phtCrack** window.



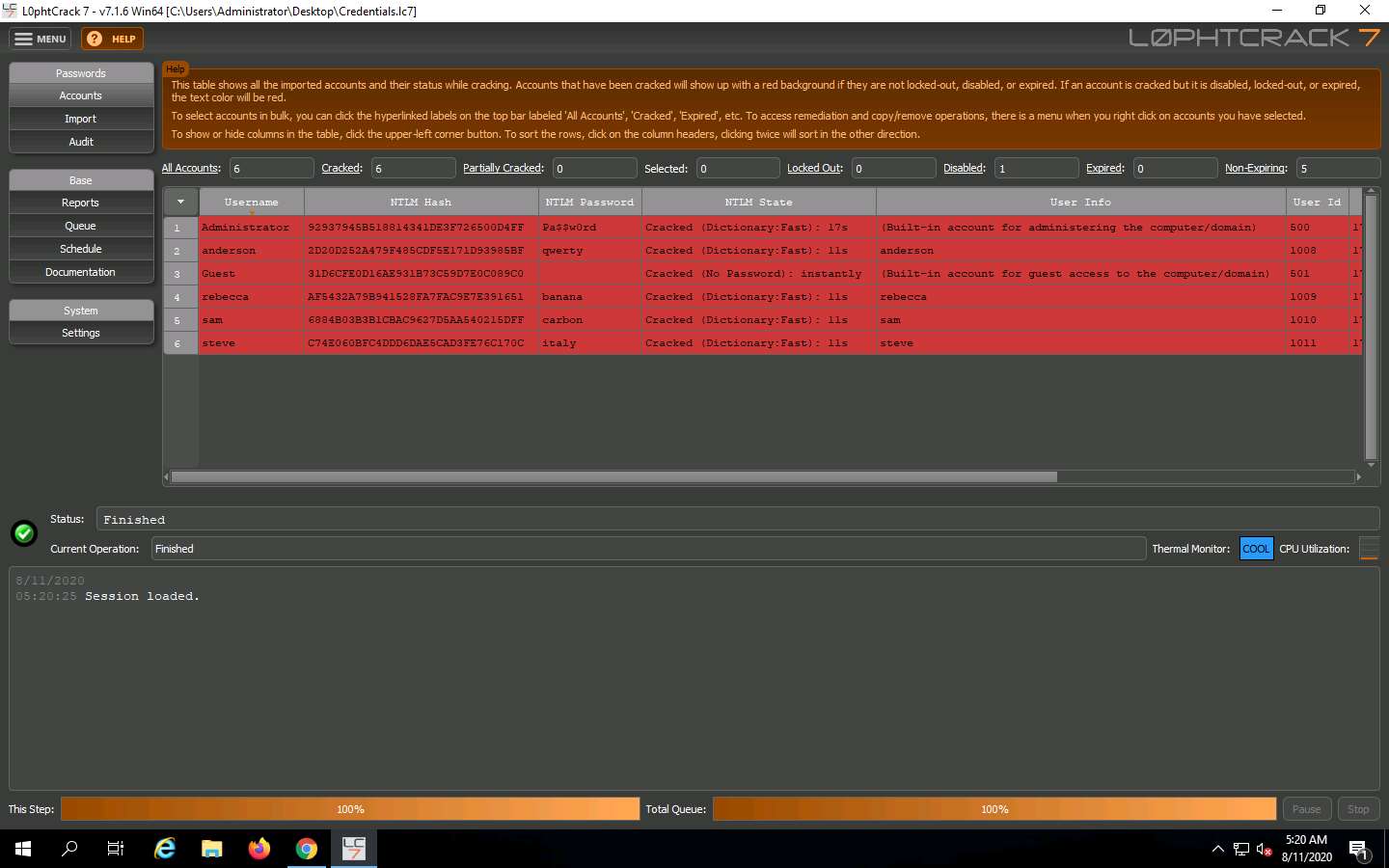
1. To open the saved result, navigate to **Desktop** and double-click the **Credentials.lcs** file to **view result**.



1. A **L0phtCrack 7 - Trial** reminder pop-up appears, click the **Proceed With Trial** button.



1. Now you can see the saved result in the **L0phtCrack** window.



1. Close all the open windows.

In this lab you have learnt how to extract the **Administrators** password using **L0phtCrack**.