# Cybersecurity

# **Activity 3.2.5 Exploring Security Frameworks**

Copy and paste screenshots and/or answer questions from the activity.

#9 For the Quick Scan Plus:

* 1. What does this scan provide about this specific host that isn’t available in the Quick scan (used in Activity 3.2.3)?

It has the version.

* 1. Record the detailed information for the required services on PumpPLC.

ProFTPD 1.3.5

OpenSSH 6.6.1p1 Ubuntu 2Ubuntu2.11

* 1. For the essential services, which of these, if any, should be accessible from outside the firewall?

Neither should be accessible from the firewall

* 1. How would unethical hackers use information from these scans to their advantage in developing an attack plan?

MAC Address

Specific 7 hosts that are up

#20 While Nessus is scanning, research an example of a plug-in and the impact an exploit of its service may have on a system.

4. Describe this plug-in and its severity. What is the potential impact of exploiting this vulnerability?

Graphical user interface, text, application, email

Description automatically generated

#22 Save a screenshot of the Vulnerabilities page that include the first few entries.

Graphical user interface, application, table

Description automatically generated

#23 Select the ProFTPD vulnerability and save a screenshot of its details. (If necessary, you can select the Vulnerabilities tab again to return to the list of vulnerabilities.)

Graphical user interface, application

Description automatically generated

#24 Using your screenshot, review the plug-in details.

* 1. What is the service and software (version) exploited in the vulnerability?
     1. ProFTPD version 1.1
  2. What port(s) and protocol(s) are affected?
     1. 21 / tcp / ftp
  3. When was the plug-in published?
     1. June 16, 2015
  4. When was it last modified?
     1. March 27, 2020
  5. What are the solutions? What will they achieve?
     1. Upgrade your version

#39 As the pen tester, you have found and confirmed a major vulnerability on your network!

* 1. What were the effects of launching the exploit?

We had access to the entire system (files etc)

* 1. What are the ethical consequences and responsibilities of testing this vulnerability?

Damage a network or expose passwords

#41 Join a cyber team as directed by your teacher.

Refer to your iptables commands in your notebook to answer the following questions:

1. How do you designate the protocol used by FTP and SSH?
   1. Zenmap
2. What is the port designation for FTP and SSH?
   1. 21 & 22
3. How do you establish the source of inbound traffic for each service?
   1. zenmap
4. What is the general policy you want to create?
   1. Security

Then, denote which iptables commands you will use to provide remediation for PumpPLC.

* Clear rules for current inbound traffic:
  + sudo iptables -F INPUT
* Allow .....
  + sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
* Allow SSH traffic
  + sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
* Allow FTP traffic only from PumpMonitor
  + sudo iptables -A INPUT -p tcp --dport ftp -s 10.2.0.6 -j ACCEPT
* Deny all other traffic
  + sudo iptables --policy INPUT DROP
* Confirm the rules
  + sudo iptables -L INPUT
* Save
  + sudo iptables-save

#44 Take a screenshot of your results as evidence

Text

Description automatically generated with medium confidence

#46 Take a screenshot of your results as evidence

