# Cybersecurity

**Activity 3.2.4 Analyze and Defend Network Attacks**

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

#11 On TargetWindows01, open File Explorer and navigate to where your stored your two large capture files. Compare the two file sizes.

How do the sizes differ? What might this indicate?

The baseline file size is much smaller than the unknown file’s size indicating malicious traffic.

#12 Copy and Paste your Zenmap table from Activity 3.2.3. In your Zenmap table, highlight the necessary services.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **My Zenmap Table** | | | | |
| **IP address** | **Hostname** | **# Open Ports** | **# Filtered Ports** | **# Closed Ports** |
| 10.2.0.8 | TagetWindows01 | 4 | 0 | 96 |
| 135 tcp open msrpc  139 tcp open netbios-ssn  445 tcp open Microsoft-ds  3389 tcp open ms-wbt-server | | | | |
| 10.2.0.5 | PumpPLC | 9 | 0 | 91 |
| Table  Description automatically generated  21, 22 | | | | |
| 10.2.0.6 | PumpMonitor | 2 | 0 | 98 |
| 21, 22 | | | | |
| 10.2.0.7 | Web01 | 6 | 0 | 94 |
| Table  Description automatically generated  21, 80, 3389 | | | | |

#13 Use your notes, topology diagram and the operational requirements to fill out the following chart for allowed and expected traffic.

|  |  |  |  |
| --- | --- | --- | --- |
| **My Traffic Rules Table** | | | |
| **Protocol/Port** | **Source** | **Destination** | **Permission** |
| Remote Dekstop/3389 | ANY | 10.2.0.8 | ALLOW |
| ftp/21 | 10.2.0.6 | 10.2.0.5 | ALLOW |
| ftp/21 | 10.2.0.5 | 10.2.0.7 | ALLOW |
| Ssh/22 | 10.2.0.8 | 10.2.0.5 | ALLOW |
| Ssh/22 | 10.2.0.8 | 10.2.0.6 | ALLOW |
| http/80 | 10.2.0.8 | 10.2.0.7 | ALLOW |
| Remote Desktop/3389 | 10.2.0.8 | 10.2.0.7 | ALLOW |
| ANY | ANY | ANY | DENY |
|  |  |  |  |
|  |  |  |  |

#14 *Hints:* *How could you use your first filter to analyze traffic between PumpMonitor and Web01? Between TargetWindows01 and Web01?*

*What protocols might be of interest?*

* FTP between PumpPLC and PumpMonitor
  + Filter: **ftp and ip.addr == 10.2.0.5 and ip.addr == 10.2.0.6**
  + First FTP packet: 42
  + Last FTP packet: 270
  + Notable activity:
    - Vagrant logged in, ftp connection opened, mode set to binary, pump\_log.txt transferred, ftp connection quit
* FTP between PumpMonitor and Web01
  + Filter: : **ftp and ip.addr == 10.2.0.7 and ip.addr == 10.2.0.6**
  + First FTP packet: 352
  + Last FTP packet: 504
  + Notable activity:
    - Anonymous logged in, ftp connection established, pump\_log.txt transferred, ftp quit
* HTTP between TargetWindows01 and Web01
  + Filter: http **and ip.addr == 10.2.0.7 and ip.addr == 10.2.0.8**
  + First FTP packet: 555
  + Last FTP packet: 584
  + Notable activity: http request, css request, favicon request

1. Confirm that PumpMonitor did not exchange HTTP data with any host. What filter did you use?

Graphical user interface

Description automatically generated with medium confidence

1. Confirm that PumpPLC did not FTP with Web01. What filter did you use?

Graphical user interface, application, table, Excel

Description automatically generated

#15 Load your full unknown capture file in Wireshark and analyze all of your unexpected network traffic.

*Hints:*

* *What are the addresses of the hosts you want to analyze?*
* *Do you want to limit your analysis to a source and/or destination address?*
* *What protocols might you be interested in?*
* *Is there useful information in the packet details?*

Network Scan

* Filter: ip.src == 10.2.0.8
* Suspicious Activity:
  + zenmap scan

Browse Web01 from PumpMonitor

* Filter: http and ip.addr == 10.2.0.6 and ip.addr == 10.2.0.7
* Suspicious Activity:
  + Someone is illegally browsing Web01 from pump monitro

FTP from Web01 to PumpPLC

* Filter: ftp and ip.addr == 10.2.0.6 and ip.addr == 10.2.0.5
* Suspicious Activity:
  + ftp connection opened, my\_web\_file.txt transferred from web01 to PumpPLC

#27 Screenshot of your inbound new rules

#28 Retry the “attacks” on PumpPLC.(finish the phrase for a, b, and c based on the results)

1. Using Zenmap on TargetWindows01, scan PumpPLC.

The Zenmap scan shows…

Table

Description automatically generated

ONLY SSH IS OPEN

1. From PumpMonitor, browse to Web01.

Browsing to Web01 from PumpMonitor still worked, because…

Text

Description automatically generated

1. Transfer a file from Web01 to PumpPLC

FTP from Web01 to PumpPLC failed with a timed-out session because…

We disabled FTP between Web01 and PumpPLC

Text

Description automatically generated

#29 Place the following table in your Cybersecurity Notebook…

