**LESSON 3 – NETWORK SECURITY**

**ACTIVITY 3.2.4 – ANALYZE AND DEFEND NETWORK ATTACKS**

**ATTENTION -** *Download both full capture files to your school’s local machine.*

How do the sizes differ? What might this indicate?

|  |
| --- |
|  |

In your Zenmap table, change the necessary services text color to RED.

|  |
| --- |
| **MY ZENMAP TABLE** |
| **IP ADDRESS** | **HOSTNAME** | **#OPEN PORTS** | **#FILTERED PORTS** | **#CLOSED PORTS** |
| 10.2.0.8 | TargetWindows01 | 4 | 0 | 96 |
| 135 tcp open msrpc139 tcp open netbios-ssn445 tcp open microsoft-ds 3389 tcp open ms-wbt-server |

|  |
| --- |
| **MY ZENMAP TABLE** |
| **IP ADDRESS** | **HOSTNAME** | **#OPEN PORTS** | **#FILTERED PORTS** | **#CLOSED PORTS** |
| 10.2.0.5 | PumpPLC | 9 | 0 | 91 |
| 21 tcp open ftp 22 tcp open ssh 80 tcp open http 111 tcp open rpcbind139 tcp open netbios-ssn445 tcp open microsoft-ds 631 tcp open ipp 3306 tcp open mysql8080 tcp open http |

|  |
| --- |
| **MY ZENMAP TABLE** |
| **IP ADDRESS** | **HOSTNAME** | **#OPEN PORTS** | **#FILTERED PORTS** | **#CLOSED PORTS** |
| 10.2.0.6 | PumpMonitor | 2 | 0 | 98 |
| 21 tcp open ftp22 tcp open ssh |

|  |
| --- |
| **MY ZENMAP TABLE** |
| **IP ADDRESS** | **HOSTNAME** | **#OPEN PORTS** | **#FILTERED PORTS** | **#CLOSED PORTS** |
| **10.2.0.7** | **Web01** | **6** | **0** | **94** |
| 21 tcp open ftp 80 tcp open http 135 tcp open msrpc 139 tcp open netbios-ssn445 tcp open microsoft-ds 3389 tcp open ms-wbt-server |

Use your notes to fill out the following chart for allowed and expected traffic. The entries below are just examples and should be modified for your network topology and services. Use as many lines as you need. This table will be known as your "Traffic Rules" table.

*The traffic rules may be in any order other than the last DENY rule.*

|  |  |  |  |
| --- | --- | --- | --- |
| **My Traffic Rules** |  |  |  |
| **Protocol/Port** | **Source** | **Destination** | **Permission** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Recall the three baseline tasks you performed and refer to your network topology diagram:

Find the packets that represent your baseline traffic for each task. Record the filters you used to find the packets, identify the first and last packets of each baseline task, and record any notable activity related to the operational requirements of the network.

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?*

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

Recall the three suspicious tasks you performed. Load your full unknown capture file that you collected on Web01. Refer to your network topology diagram, your Zenmap table, and your Traffic Rules table. Find the packets that represent unexpected and/or suspicious traffic on your network. Record the filters you used to find the packets, compare the unknown packets to the baseline packets, and describe the suspicious 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?

|  |
| --- |
|  |

Record the iptables command and flags above; you will use variations of them throughout this activity and later in the course.

|  |
| --- |
|  |

Take a screenshot of your inbound new rules. HINT - retry the attacks after adding the host-based firewall rules and note their findings

|  |
| --- |
|  |

Thinking back to the CIA Triad, is it a good idea to still have some ports accessible on PumpPLC? Explain your reasoning.

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Step** | **Command / Translation** |
| 19 | sudo iptables -L INPUT |
|  |
| 20 | sudo iptables -F INPUT |
| Useful option:  |
| 21 | sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT |
| Operational Requirement:  |
| 23 | sudo iptables -A INPUT -p tcp --dport ftp -s 10.2.0.6 -j ACCEPT  |
| Operational requirement:  |
| 24 | sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT |
| Operational requirement:  |
| 25 | sudo iptables --policy INPUT DROP  |
| General Policy:  |
| 27 | sudo iptables-save |
| Useful option:  |

**CONCLUSION**

For any attack that was not affected by the iptables rules, recommend additional fix(es) to address those attacks.

|  |
| --- |
|  |

What is the role of a host-based firewall in network defense? What are its limitations?

|  |
| --- |
|  |