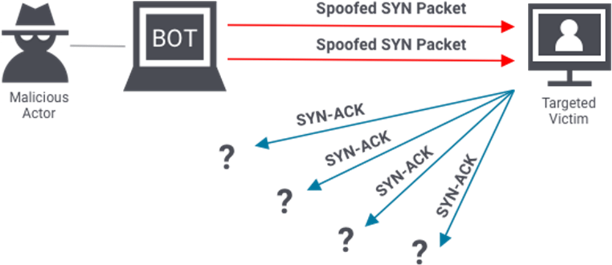
**Activity 4**

**Denial-of-Service Attack Simulation and Analysis**

Using various virtual machines, be able to perform “Denial-of- Service Attack Simulation and Analysis” for possible targeted virtualized machines in the network. Also conduct a thorough analysis of a captured network traffic.

# Activity Resources

Virtual Machines: Kali Linux, Ubuntu, Metasploitable Network Traffic Capture: [Activity4]NetCapture\_Scenario Tools: Nmap or ZenMap, Wireshark, hping3, Slowloris

*Disclaimer: Activity is for educational purpose only! Misuse or targeting other services outside the controlled or virtual environment is punishable by law and the University. The University and the Instructor has no liability on misuse of the tools used in this exercise.*

# Activity Procedure(s)

## Task 1 – Denial-of-Service Attack Simulation

In your workstation, open/run Oracle VirtualBox Manager and configure virtual machines (Kali Linux, Ubuntu and Metasploitable) network adapter using the following configurations:

## Adapter No. 1 Network Configurations

* Enable Network Adapter: YES (checked)
* Attached to: Host-Only Adapter
* Name: Virtual Host-Only Ethernet Adapter (note: choose network that is DHCP server enabled)
* Promiscuous Mode (Advanced): Deny
* Reset MAC Address (press the refresh button)

Run/Start virtual machine simultaneously (make sure all virtual machines are loaded and running). In your Kali Linux virtual machine, perform Network Scanning and Reconnaissance using Nmap or ZenMap tools to identify possible vulnerable target machines (Metasploitable). Next, perform any TCP Flood attack (DoS) technique on the target machine using Hping3 or Slowloris tool. While performing the attack, run Wireshark in Kali Linux to capture the network packet (observe and analyze the results). Also, in your Ubuntu virtual machine, open a browser and access the website hosted by the targeted webserver. Finally, observe and analyze the captured network traffic in Wireshark.

## Task 2 – Network Traffic Examination and Analysis

Open Wireshark and load the network capture file ([Activity4]NetCapture\_Scenario). Perform the necessary network investigation of the captured network traffic using various examination techniques (filtering, statistics analysis, and expert information analysis).

# Submission Note (Individual Activity)

Use file name convention (LASTNAME\_CTAINASL\_SECTION\_TERM\_AY\_Activity4.pdf). Submit/upload Softcopy (PDF file) in MS Teams

Submit a PRINTED activity rubric.

**ACTIVITY DOCUMENTATION**

|  |  |  |
| --- | --- | --- |
| **Group Name** | Ctrl+Z | Tuesday, April 22, 2025 |
| **Members Surname, First Name MI. (Alphabetical)** | |  |
| Cano, Kaide M. | |  |
| Cuenca, Sophia T. | |  |
| Dionela, Terrence A. | |  |
| Umengan, Darwin F. | |  |
| Click or tap here to enter text. | |  |

Instruction(s): Provide the appropriate screenshot/screen capture of your workstation.

|  |
| --- |
| **Network Scanning and Enumeration Simulation** |
| **Nmap/ZenMap Report**  Display here the result of the Nmap/ZenMap report. |
|  |

|  |
| --- |
| **Wireshark Report**  Display here the result of the captured network traffic using Wireshark. |
|  |
| Q1. What is/are the IP Address of the attacker machine(s) in the network?  *[Answer Format: IP Address, …, IP Address]*  Answer: 192.168.56.104  Q2. What is/are the IP Address of the target machine(s) in the network? [Hint: Except machines in ignored states]  *[Answer Format: IP Address, …, IP Address]*  Answer: 192.168.56.102 |

|  |
| --- |
| **Network Traffic Examination and Analysis** |
| **Wireshark Capture**  Display here the Wireshark capture file. |
|  |
| Display here the Wireshark capture file properties information. |
|  |

|  |
| --- |
| **Wireshark Filtering**  Display here the result of the Wireshark capture using various Denial-of-Service detection filter commands. |
|  |
| Observation and Findings: What do the filter result suggest? Explain!  Based on the filter result, the result shows that the IP address 192.168.31.181 sends many messages to the IP address 192.168.31.214. |

|  |
| --- |
| **Wireshark Statistics (IPv4 Conversations)**  Display here the statistics report. |
|  |
| Observation and Findings: What do the statistics result suggest? Explain!  The statistic shows that 192.168.31.181 sends a large packet to 192.168.31.214. leading for the 192.168.31.214 to run slow. |

|  |
| --- |
| **Wireshark Expert Information**  Display here the Expert Information summary report. |
|  |
| Observation and Findings: What do the expert information result suggest? Explain!  This shows the vulnerabilities and the severity of the server. |

|  |
| --- |
| **Question and Answer** |
| What is the IP Address of the attacker and the target machine(s) in the captured network traffic?  Answer (Attacker’s IP Address) : 192.168.31.181 Answer (Target’s IP Address) : 19.168.31.214 |
| What is the MAC Address of the attacker and the target machine(s) in the captured network traffic?  Answer (Attacker’s MAC Address) : 08:00:27:1e:c5:ec  Answer (Target’s MAC Address) : 80:00:27:a8:ab:c7 |
| What Denial-of-Service attack technique was used by the attacker in the captured network traffic?  Answer: SYN Flood |
| **Mitigation and Recommendations**  What are the necessary countermeasures to avoid or prevent Denial-of-Service attacks. |
| Mostly do not connect to any free Wi-Fi in any place because someone could attack your pc and may lead to an attack from someone you don’t know. |

**ACTIVITY RUBRICS**

|  |  |  |
| --- | --- | --- |
| **Group Name** | Click or tap here to enter text. | Tuesday, April 22, 2025 |
| **Members Surname, First Name MI. (Alphabetical)** | |  |
| Click or tap here to enter text. | |  |
| Click or tap here to enter text. | |  |
| Click or tap here to enter text. | |  |
| Click or tap here to enter text. | |  |
| Click or tap here to enter text. | |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | | **Activity Rubrics** | | | | | | | **Points** |
| **Not**  **Attempted (0 points)** | | | **Beginning (1 point)** | **Developing (2 points)** | **Proficient (3 points)** | **Exemplary (4 points)** |
| Use of Tools & Techniques | | No attempt to use relevant tool(s). | | | Incorrect or unsuitable tool(s) selected. | Tool(s) used is/are somewhat suitable but not optimal. | Selected appropriate tool(s) with minor mismatches to the scenario. | Selected the most appropriate tool(s) for the task based on scenario. |  |
| Execution of Simulation | | No attempt to execute attack simulation. | | | Poorly executed; goals unmet; major safety/ethical concerns. | Execution had flaws; goals only partially met; some safety concerns. | Attack executed with minor issues; met most goals; adhered to safety. | DoS attack executed safely, ethically, and effectively within controlled environment; met all goals. |  |
| **Use of Wireshark Filters and Features** | | No attempt to perform filtering of network traffic data. | | | Filters not used or configured incorrectly, leading to large irrelevant data. | Basic filters applied; excessive or irrelevant data captured. | Capture filters set up correctly with minor inefficiencies. | Capture filters configured accurately; unnecessary data excluded effectively. |  |
| No attempt to use Wireshark features. | | | Wireshark features not used effectively; manual analysis  dominates. | Limited use of Wireshark features; investigation hindered by inefficiency. | Basic features used effectively; advanced features used with some errors. | Advanced features used effectively (e.g., filters, color coding, statistics) |
| **Analysis, Interpretation and Mitigation** | | No attempt to conduct analysis and interpretation. | | | Minimal or incorrect analysis; important information overlooked. | Basic analysis performed, but some important findings are missed or misinterpreted. | Results analyzed accurately but with some minor gaps in interpretation. | Detailed and accurate analysis of results; clear identification of open ports, services, and potential vulnerabilities. |  |
| No attempt to provide recommendations for mitigation. | | | Incorrect recommendations for mitigation. | Generalized or incomplete recommendations; lacks actionable steps. | Mostly accurate and actionable recommendations with minor omissions. | Accurate and actionable recommendations tailored to the  scenario. |
| **Documentation** | | No attempt to provide report documentation of findings. | | | Poor documentation of findings; lacks structure or critical details. | Basic report provided with significant omissions or unclear explanations. | Detailed report provided; minor gaps in methods or findings. | Comprehensive report including methods, findings, and recommendations. |  |
| **Total Score and Feedback** | | | | | | | | **TOTAL POINTS EARNED**  **(20 max points)** |  |
| * Exemplary | 20 | | Exemplary work demonstrating mastery of Wireshark features, thorough investigation, analysis, and comprehensive reporting. | | | | |
| * Proficient | 16-19 | | Solid performance with minor gaps in technical skills or documentation. | | | | |
| * Developing | 12-15 | | Basic understanding of Wireshark and investigation concepts; several significant gaps in execution. | | | | |
| * Beginning | 8-11 | | Minimal effort or understanding; critical errors or omissions in the capture, analysis, or reporting. | | | | |
| * Not Attempted | 0-7 | | Indicates failure to perform network investigation and analysis. | | | | |
| Evaluated by:  Name of Course Instructor | | | | **Remarks/Comments** | | | | | |