JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Information Security Institute

EN.650.624, Network Security, Spring 2020 Instructor: Reuben Johnston, reub@jhu.edu

Homework 3

See Blackboard for grade %

Due Date

See Blackboard for date

Summary

In this homework exercise, students will use penetration testing and intrusion detection tools on a server running Nginx to explore HTTP-based denial of service (DoS) attacks and defenses.

Part 1

- Run HTTP server in Docker container on raspberry pi (RPI) or VM (running Ubuntu server) using default settings
- Setup Kali virtual machine (VM) on same network with HTTP server and prepare Wireshark to capture a network sequence
- Use hping3 (https://tools.kali.org/information-gathering/hping3) to perform DoS attacks on Nginx from another RPI or VM; capture the network sequence between hping3 and Nginx using Wireshark

Part 2

- Modify the Nginx settings to improve defenses against DoS attacks
- Repeat the DoS attacks from part 1 and capture the network sequence

Part 3

- Install Suricata in another Docker container and configure it to detect the attack
- Repeat the DoS attacks and ensure Suricata detects the attack promptly; gather reporting details from Suricata that show it detected the attack

Part 4

- Answer the questions

Requirements

Executive summary report

The report must contain an overview of the project, the project goals, project execution highlights (i.e., what was performed, with pertinent technical highlights), what goals were accomplished (and any that were not achieved), and what was learned from the project (2-3 pages). For the report format, groups shall use the IEEE format (see here). The report is intended to be reference material for when you are performing threat modeling in practice.

Groups will begin the project with the creation of a project backlog and by assigning tasks in the backlog amongst the team. For each task in the backlog, groups should include exit conditions and schedule milestones.

For this assignment, place supplementary code and documentation in the specified locations on the course GitHub. Submit supplemental *.pcap files in a single *.zip archive using BB. Turn in the executive summary report, via TurnItIn assignment on BB, and your supplemental *.zip in the separate BB assignment for supplemental material. Please include team member last names in the filenames for all files submitted (e.g., "hw3-execsum-name1-name2-name3.docx" or hw3-supplemental-name1-name2-name3.zip).

Deliverables

Part 1

1. Describe the sequence used
2. Provide a python script that executes your attack
3. Provide *.pcap network capture file from traffic between attack host and target running the application server
4. Describe the results of the attack

Part 2

1. Provide the details for updated Nginx settings
2. Provide *.pcap network capture file from traffic between attack host and target running the application server
3. Describe the results of the attack

Part 3

1. Provide the details used to install and configure Suricata so that it could be replicated by someone else
2. Provide reporting details from Suricata that show it detected the attack

Part 4

4. Discuss what else could be performed to defend against these attacks

Grading Rubric

Threat modeling deliverables (50% overall)

Part 1 – 25%

- Description of attack sequence
- Python script
- *.pcap file capturing DoS attack
- Description of results from the attack

Part 2 – 25%

- Details for updated Nginx settings
- *.pcap file capturing DoS attack
- Description of results from the attack

Part 3 – 25%

- Suricata installation and configuration details
- Reporting details from Suricata

Part 4 – 25%

- Discussion

Executive summary report (50% overall)

Table 1-Executive summary grading rubric (2006, Leydens, Santi)

Objective	**1 - Exemplary**	**2 - Proficient**	**3 - Apprentice**
Format / layout / organization	Report is very clear, coherent with excellent transitions	Report is clear and coherent, strong throughout	Report has some gaps, some weak sections
Writing mechanics	Report is virtually error-free, and contains few if any reader distractions	Report is logical and easy to read, and may contain a few errors causing minimal reader distraction	Report is generally clear, but distracting errors and flow make it difficult to follow at times
Figures / Tables	All figures and tables are easy to understand, and are clearly linked to the text.	All figures and tables can be understood with information given and are linked to	Figures and/or tables are hard to understand, are not all

	Story can be told almost entirely through figures.	text. One or more need improvement. May need more figures to tell the story.	linked to text. Several need improvement. Several more figures are needed to tell story.
References	All sources identified and referenced appropriately. Evidence of careful and thorough research for outside information.	All sources identified and referenced appropriately. Includes mostly readily available works.	All sources identified. Only readily-available works included. Some weaknesses in referencing, such as missing publisher information.
Typical Grade (average):	90-100%	80-90%	70-80%

References and useful resources

- https://github.com/jhu-information-security-institute/NwSec/wiki
- 2006, Leydens, Santi, “Optimizing Faculty Use of Writing as a Learning Tool in Geoscience Education” (provided the rubric specified for the executive summary report)