Assignment 3

Mercy Ikem Ogechi

8859960

PROG8291

Sajjad Shahid

3rd July 2024

Table of Contents

[**Assignment 3** 2](#_Toc170385848)

[**DESCRIPTION** 2](#_Toc170385849)

[**PREPARATION** 2](#_Toc170385850)

[**OBSERVATION** 2](#_Toc170385851)

[**SCREENSHOT** 3](#_Toc170385852)

[**REFLECTION** 6](#_Toc170385853)

# **Assignment 3**

# **DESCRIPTION**

The lab document shows how to use ZAP Proxy and Nessus for system Vulnerability testing. Start with host discovery scans in Nessus, and then run a basic network scan with the Metasploitable system as the target. I perform an automated scan on DVWA using Zap Proxy, then configure authenticated scans and brute-force credentials.

# **PREPARATION**

* I install ZAP Proxy and Nessus on Kali Linux to get ready for the lab.
* I verified the Metasploitable VM is up and operational.
* A wordlist for ZAP Proxy, network connectivity between the systems, and a browser for interaction.

# **OBSERVATION**

Throughout the lab, I observed how well vulnerability scanning tools such as Nessus and ZAP Proxy detect potential security vulnerabilities in the network and online applications. Pay attention to how easy it is to use the tools, how accurate the scans are, and how many vulnerabilities were discovered. Note any issues that arise during the process, such as issues with authentication or configuring scans, so that future testing procedures can be improved.

# **SCREENSHOT**

A screenshot of a computer

Description automatically generated

Figure 1 shows i performed a Nessuss vulnerability scan on the local NetworA screenshot of a computer

Description automatically generated

Figure 2 shows results of the Fuzz Attack on the dvwa login.php.

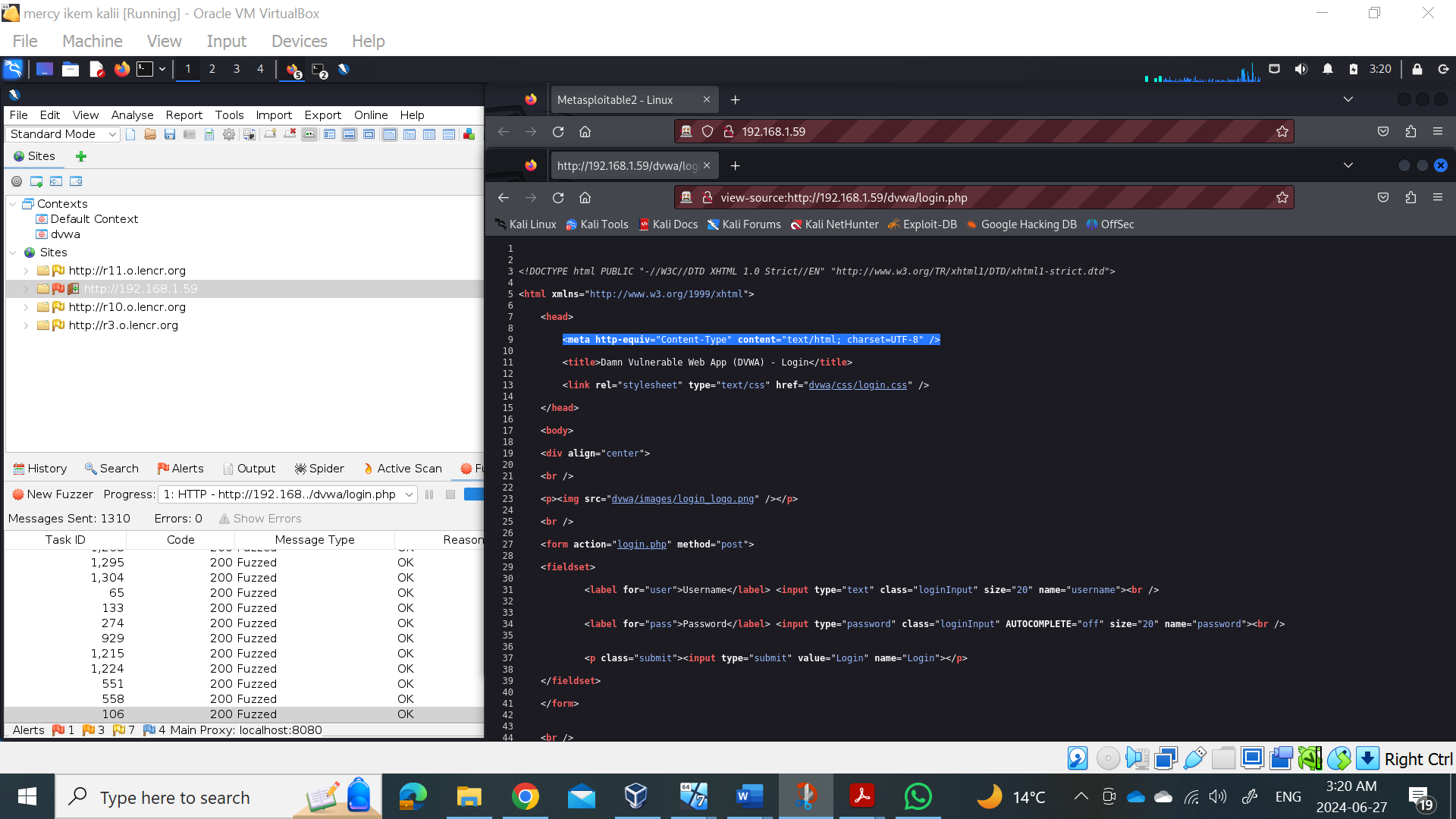


Figure 3 shoes the page source code.

A screenshot of a computer

Description automatically generated

Figure 4 show spider scan performed on the dvwa instance.

# **REFLECTION**

Taking part in this lab highlights the significance of proactive security measures in safeguarding network infrastructure. It highlights how crucial it is to identify potential vulnerabilities using trustworthy vulnerability scanning tools like Nessus and ZAP Proxy. The real-world experience also emphasizes how important careful planning and rigorous testing protocols are.

Thinking back on this procedure, one can gain understanding of how cybersecurity is changing, and the ongoing work needed to successfully counter new threats.