LOG BOOK OF NASIBU MAULIDI OMARY

T21-03-01972 (BSC.CNISE 3)

DIRECTORATE OF ICT / DODOMA (2023/2024)

#	Week	Day	Date	Work Hours	Activity
1	2	Monday	2024/07/29	8	Installing Proxmox VE on bare metal provides a solid foundation for building a virtualization infrastructure that can efficiently manage your workloads. Proxmox Virtual Environment (VE) is a powerful, open-source platform for managing virtual machines (VMs) and containers. It combines two virtualization technologies, KVM (Kernel-based Virtual Machine) for virtual machines and LXC (Linux Containers) for lightweight containerization
2	2	Tuesday	2024/07/30	8	Today I installed DVWA (Damn Vulnerable Web Application) and Wazuh on an Ubuntu server. This builds on the work I did yesterday, setting up a lab environment to practice and test various security tools and techniques. The installation of DVWA will allow me to practice finding and exploiting vulnerabilities in a controlled environment, while Wazuh will help in monitoring and analyzing security events
3	2	Wednesday	2024/07/31	8	Today, I tackled the first DVWA challenge on this practical training by attempting a brute force attack with Burp Suite and Hydra. I tried this on all security levels: low, medium, high, and impossible, to see how the defenses change. This exercise helped me learn about different security measures and how to adapt my attack methods. It's an essential part of my training in cybersecurity, giving me hands-on experience with web application security
4	2	Thursday	2024/08/01	8	Today,I tested a web application called DVWA for command injection vulnerabilities at low, medium, and high security levels. I compared how different security measures affected the application's resistance to these attacks. This helped me understand how to find and prevent command injection, which is a valuable skill for cybersecurity.

#	Week	Day	Date	Work Hours	Activity
5	2	Friday	2024/08/02	8	Today, I worked on the DVWA file inclusion challenge, testing it across three security levels: low, medium, and hard. I examined how each level handles file inclusion vulnerabilities and used various commands to explore the system, such as including sensitive files and directories. This exercise helped me understand the risks associated with file inclusion and how different security measures can mitigate these threats. This hands-on practice is essential for my cybersecurity training, giving me practical experience in identifying and addressing web application vulnerabilities.
Supervisor Name :					
Signature :					
Date					