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	1	Wednesday	2024/07/24	8	Today&#039;s task was to identify, evaluate, and prioritize potential security threats to the system (stafftest.udom.ac.tz). This process helps security professionals understand the attack surface and assess vulnerabilities of the system
2	1	Thursday	2024/07/25	8	Today we&#039;re focusing on identifying potential SQL injection vulnerabilities within the system (staff test.udom.ac.tz) using tool like Burpsuite and sqlmap in Kali linux
3	1	Friday	2024/07/26	8	Installation of Ubuntu server and Wazuh.Wazuh is popular open source which is designed to help organisations to monitor and manage their security posture more effectively by collecting, analysing and correlating security related data from various sources across their network infrastructure
4	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
5	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

#	Week	Day	Date	Work Hours	Activity
6	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&#039;s an essential part of my training in cybersecurity, giving me hands-on experience with web application security
7	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&#039;s resistance to these attacks. This helped me understand how to find and prevent command injection, which is a valuable skill for cybersecurity.
8	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.
9	3	Monday	2024/08/05	8	Today, I engaged in a practical exploration of file upload vulnerabilities by manipulating the DVWA environment at low, medium, and high security settings. Through these experiments, I developed a strong grasp of the attack surface and the importance of implementing stringent security controls to prevent malicious file uploads.
10	3	Wednesday	2024/08/07	8	Today, I delved into the insecure capture challenge on DVWA, systematically testing its vulnerabilities across low, medium, and high security levels. By experimenting with various techniques to intercept and manipulate sensitive data, I gained insights into the potential risks of inadequate data protection. This hands-on experience underscored the importance of robust security measures in preventing data breaches and reinforced my cybersecurity skill set.
11	3	Thursday	2024/08/08	0	Farmers&#039; Day

#	Week	Day	Date	Work Hours	Activity
12	3	Friday	2024/08/09	8	Today, I worked on the DVWA SQL injection challenge, testing it across three security levels: low, medium, and hard. I used different SQL commands to try and access the database, such as retrieving usernames and passwords by injecting SQL queries into the input fields. This exercise helped me understand how SQL injection works and how security measures at each level can prevent or reduce the risk. This hands-on practice is an important part of my cybersecurity training, giving me real experience in finding and fixing web application vulnerabilities.
13	4	Monday	2024/08/12	8	Today, I practiced finding security holes in a website called DVWA. This website lets you try hacking at different levels of difficulty. I used a special tool called SQLmap to look for a type of security hole called blind SQL injection. This means I couldn&#039;t see the results of my attacks right away, so I had to use tricks to figure out if I was successful. I tested the website at easy, medium, and hard levels. SQLmap helped me learn how to break into a website’s database without being noticed by looking at things like how long it took the website to respond. This is important for protecting websites from hackers.
14	4	Tuesday	2024/08/13	8	Today,I tested a website&#039;s security against a specific type of attack called DOM-based XSS on DVWA as my demo website. I tried different levels of difficulty to understand how the website was protected. This helped me learn how to find and fix this kind of problem in websites.
15	4	Wednesday	2024/08/14	8	Today,I conducted a penetration test on the staff system at test.udom.ac.tz today. My objective was to identify vulnerabilities and evaluate the system&#039;s resilience against various attacks. This practical exercise enhanced my understanding of the system&#039;s security posture and sharpened my ability to detect potential threats. It&#039;s a crucial component of my cybersecurity education, providing hands-on experience in safeguarding web applications from malicious activities.
16	4	Thursday	2024/08/15	8	Today, I conduct search engine discovery reconnaissance for information leakage and fingerprint web server hosting stafftest.udom.ac.tz

#	Week	Day	Date	Work Hours	Activity
17	4	Friday	2024/08/16	8	As part of my ongoing penetration testing on the staff test.udom.ac.tz system, I continued the information-gathering phase. I focused on identifying hidden paths and functionalities by analyzing metadata files. Through this analysis, I was able to extract and map additional details within the scope of the test, providing a deeper understanding of the system&#039;s structure and potential weak points. This step is crucial for building a comprehensive profile of the system, which will guide the next phases of the security assessment.
18	5	Monday	2024/08/19	8	Today,I testing for session management schema in order to gather session tokens,for the same user and for the different users where possible -And analyse and ensure that enough randomness exists to stop session forging attack
Supervisor Name :					
Signature :					
Date					