CYBER SECURITY

W E S S A M A L K H U S H M A N

SPECIALIST

ABOUT ME

I'm Wessam Alkhushman, a cybersecurity enthusiast with a passion for ethical hacking, digital forensics, and network defense. I've built hands-on experience through intensive training programs like **Nashama 7 Bootcamp** and **Cyber Shield**, where I worked on real-world labs in:

- 🔐 Penetration Testing (Web, Mobile, Wireless)
- 🧠 Digital Forensics & Malware Analysis
- 🛡️ Active Directory Exploitation & Incident Response
- 📊 SIEM Monitoring & Threat Detection

I've used tools like **Burp Suite**, **Metasploit**, **Wireshark**, **MobSF**, **Volatility**, and **Splunk** to conduct assessments and build practical cybersecurity skills.

📫 Let's connect and collaborate on something meaningful!

Contact Information:
Email: wessamalkhushman@yahoo.com
Linkedin | Github | Phone: [+962776433171]

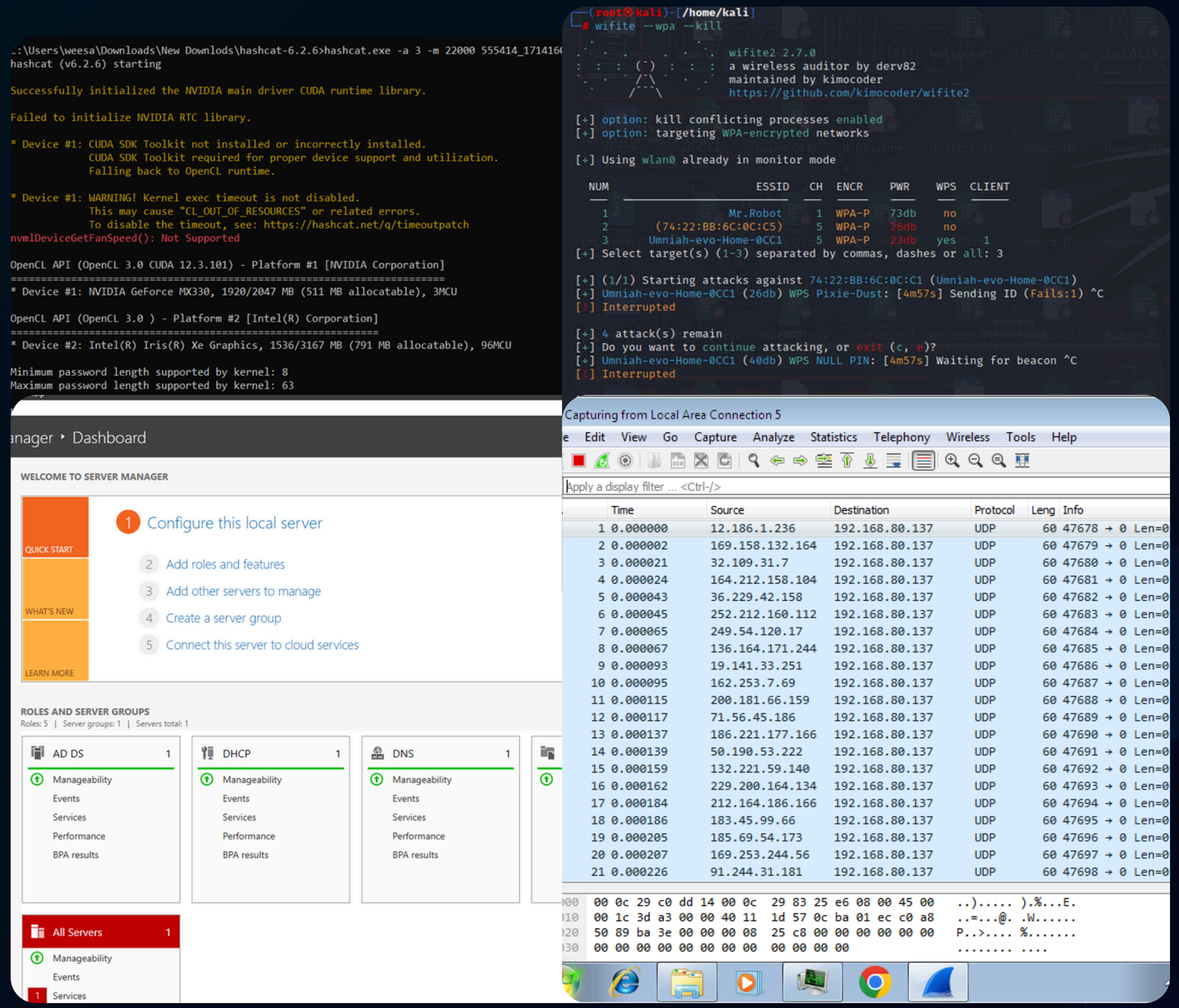
PROJECT

01 • Building and Analyzing a Vulnerable Website

02 • Active Directory

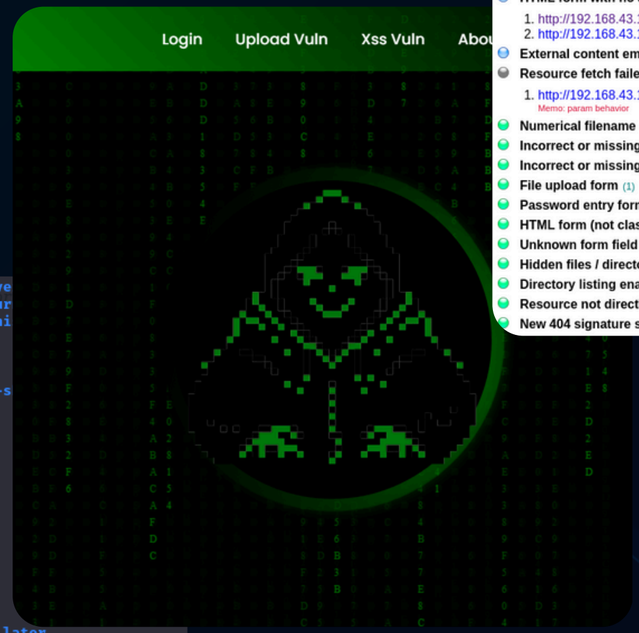
03 • Crack WIFI password

04 • Method of Attacks



BUILDING AND ANALYZING A VULNERABLE WEBSITE

My friends helped me create a website with vulnerabilities.
The website has vulnerabilities such as XSS, SQL injection, and file upload
I've exploited and tested them.

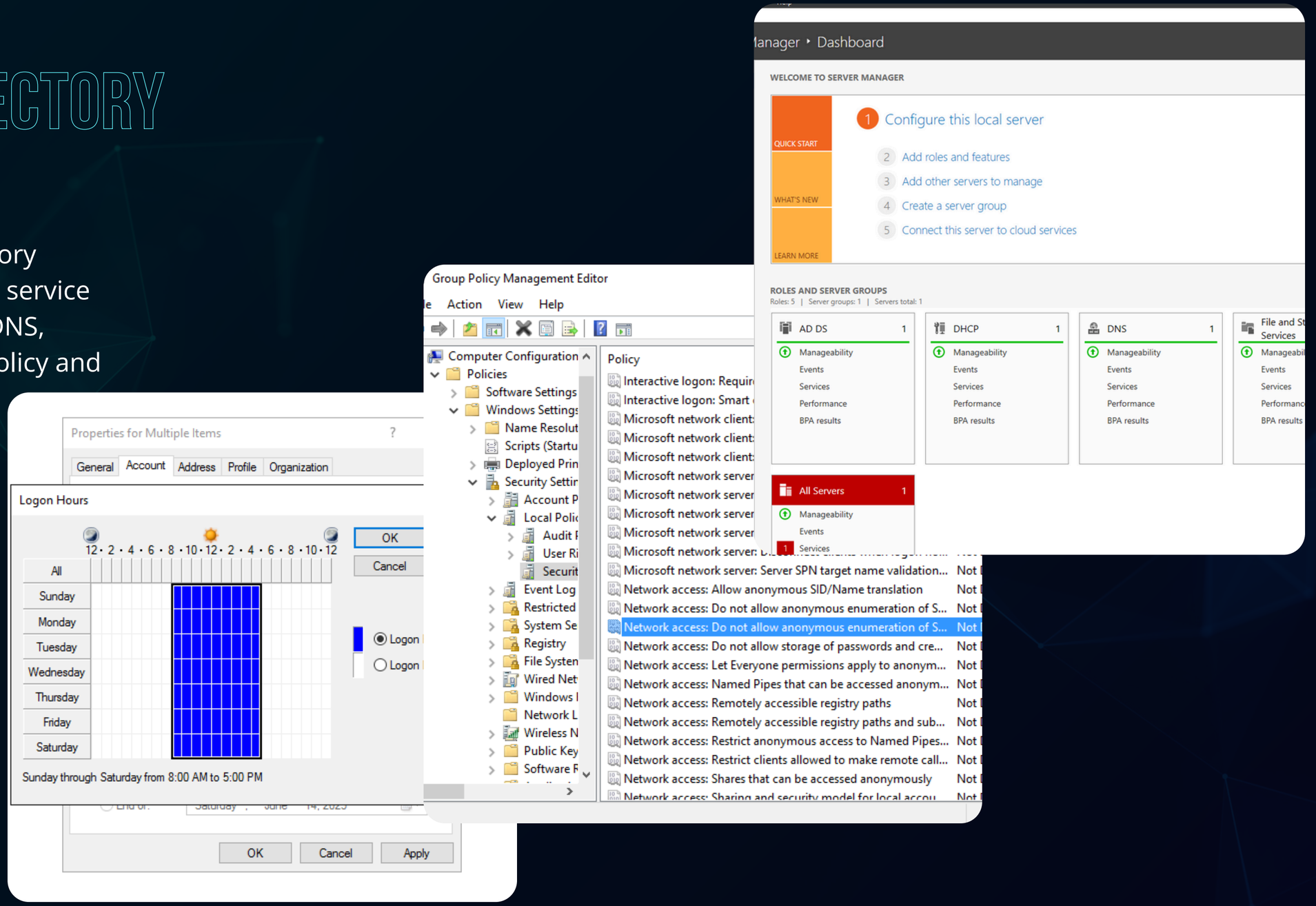


penetration test and a series of tests were conducted on vuln web Site, a vulnerable website built for security testing purposes using testing tools and manual testing techniques, to identify actual or potentially exploitable security vulnerabilities, which if exploited could result in direct or indirect damage.

Tools I used:
OWASP ZAP, Skipfish and Manual Testing

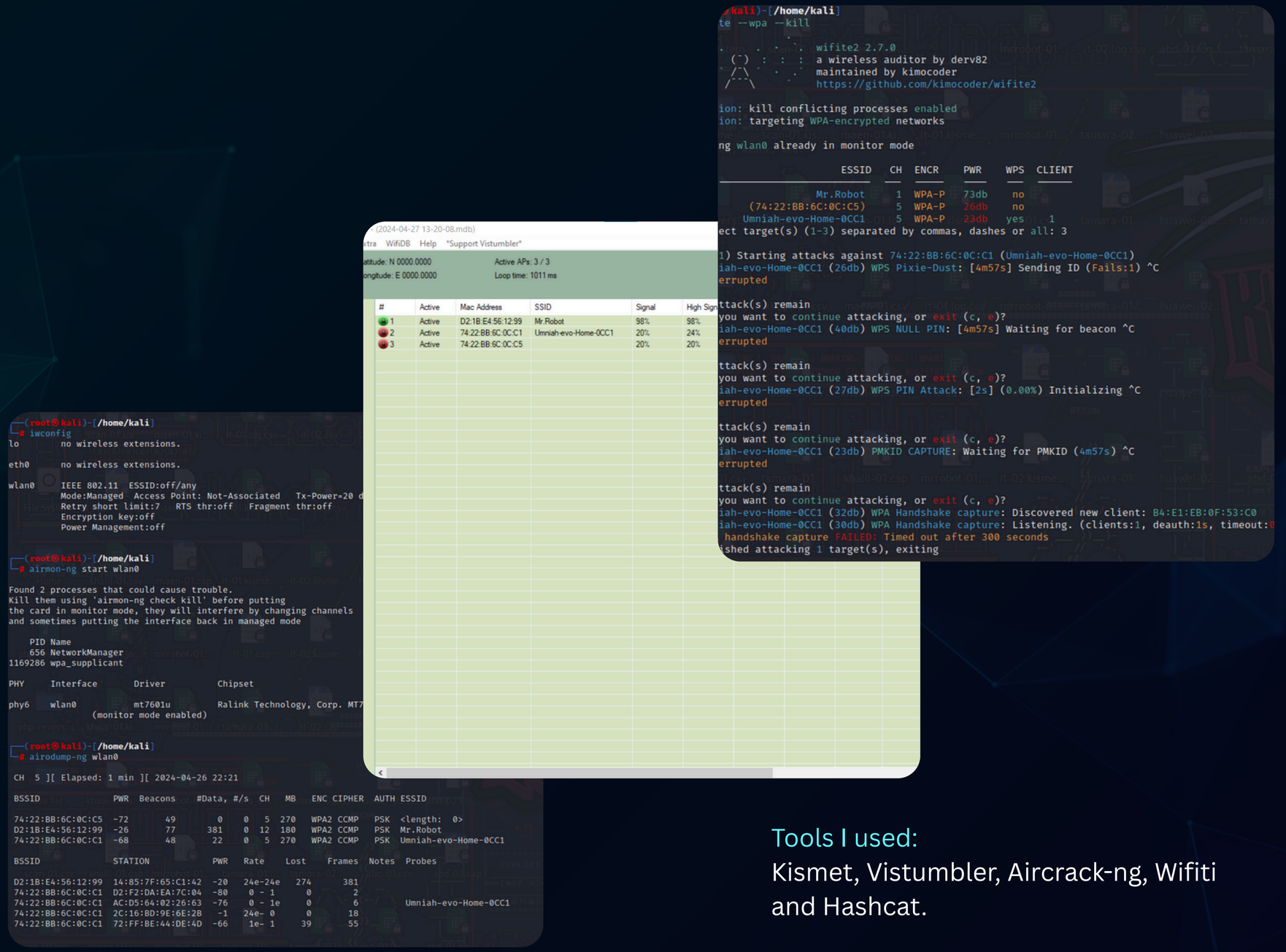
ACTIVE DIRECTORY

Setting up Active Directory Environment, Then add service such as DHCP, IIS and DNS, Then Applying Group Policy and Access Control



CRACK WIFI PASSWORD

Use different tools to scan the network and obtain the SSID and MAC address. Then, use a brute-force attack and a dictionary attack to hack the target.

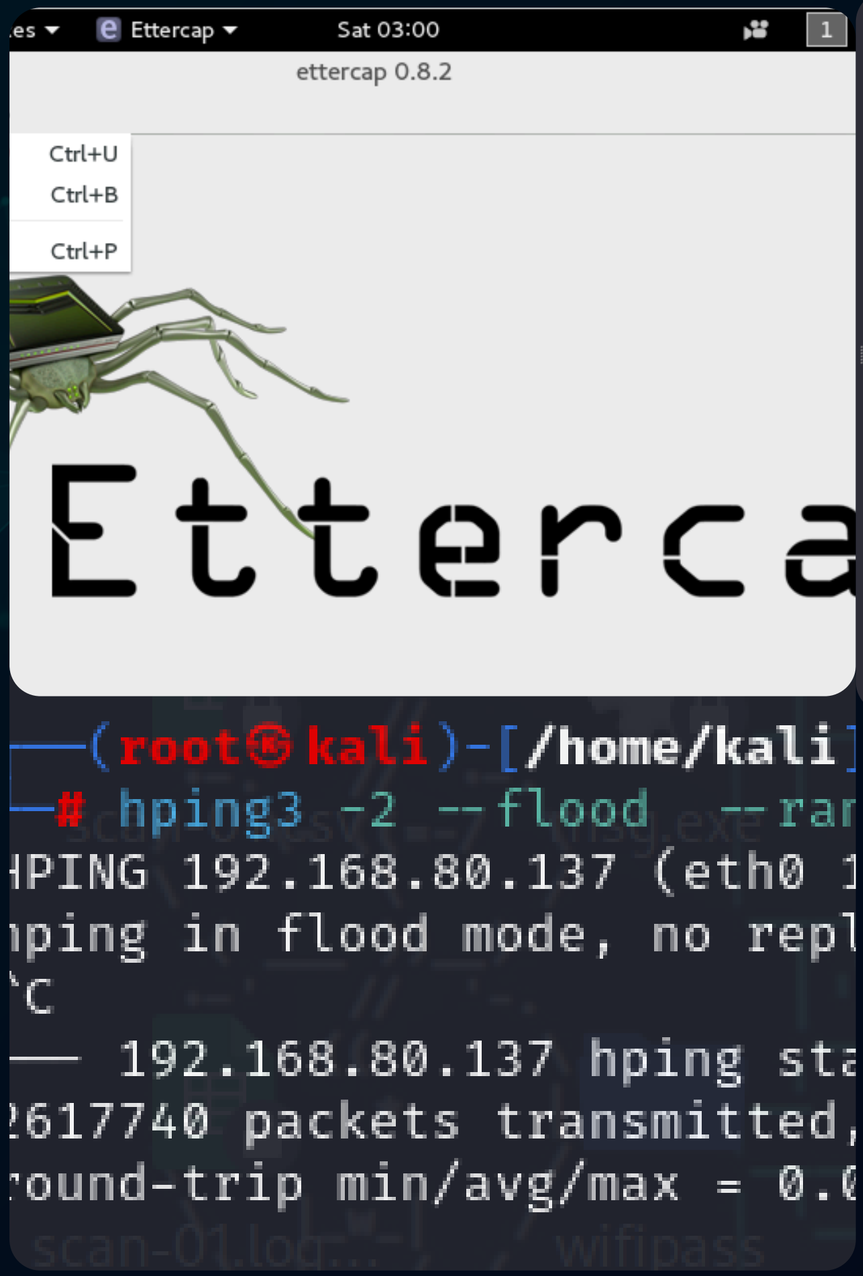


Tools I used:
Kismet, Vistumbler, Aircrack-ng, Wifiti and Hashcat.

METHOD OF ATTACKS

This project demonstrates different methods of hacking and contains:

- Gain Access to a Remote System.
- Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities.
- Perform a DoS Attack on a Target Host.
- Perform a Man-in-the-Middle (MITM) attack.
- Perform Social Engineering using Various Techniques




```
Listening on [any] 1234 ...
connect to [10.17.124.149] from (UNKNOWN) [10.10.21.131] 37686
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 21:37:18 up 13 min,  0 users,  load average: 0.00, 0.44, 0.63
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ sudo -l
sudo: no tty present and no askpass program specified
$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ find / -user root -perm /4000
find: '/home/rootme/.cache': Permission denied
find: '/home/rootme/.gnupg': Permission denied
find: '/home/test/.local/share': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/fuse/connections/48': Permission denied
find: '/run/lxcfs': Permission denied
find: '/run/sudo': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/lvm': Permission denied
find: '/run/systemd/unit-root': Permission denied
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/root': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
```

Tool used:
namp, Gobuster, Metasploit, Armitage, hping3, Ettercap, Cain & Abel, wireshark and The Social-Engineer Toolkit (SET)

CERTIFICATIONS

The Hope International Company

CERTIFICATE
OF ATTENDANCE

THIS IS TO CERTIFY THAT

Wessam Mohammad Alkhushman

HAS SUCCESSFULLY COMPLETED A COURSE IN

Certified Ethical Hacker

AND IN RECOGNITION THEREFORE IS AWARDED THIS CERTIFICATE

FOR A TOTAL OF 50 HOURS - FROM 12/5/2023 TO 07/08/2023

Eng.Sami Almashaqbeh — Instructor
16/09/2023 — Issue Date
Jacob Hamash — General Manager

SHAI — Share Artificial Intelligence

TRAINING CERTIFICATE

TO WHOM IT MAY CONCERN

Date: 16/9/2022

Wessam Mohmmed khaleel Alkhushman has been awarded this certification for successfully completed 35- hours of our Artificial intelligence training program in coding with python course. Powered by SHAI company During the training period, his character and conduct was very good. We wish him a successful and good career.

Trainer: Abdullah Abuelayyan

CEO: Tasnim Ali

Tasnim Ali

zain ZINC

Certificate
OF ATTENDANCE

THIS CERTIFICATE IS PROUDLY PRESENTED TO

WESAM MOHAMMAD AL KHASHMAN

For successfully completing the requirements of

Python Training

In 25 hours in 09/08/2022

STEAM CENTER

CYBER SHIELD ACADEMY

This Certificate Of Achievement is Presented to

Mr Wissam Khashman

In Recognition of Attending

Upskilling Program in Cybersecurity

Held On 26 Nov 2023 to 9 Jan 2024

Academy Manager: Ahmad Tarawneh

Trainer: Eng. Ali Bani Bakar

شهادة

يشهد مكتب الإرشاد الوظيفي ومتابعة الخريجين / عمادة شؤون الطلبة في جامعة مؤته وصندوق الملك عبدالله الثاني للتنميه

بأن الطالب

وسام محمد الخشمان

قد شارك في الدورة التدريبية التي نظمها المكتب بعنوان

(أمن المعلومات والشبكات)

بواقع 30 ساعة تدريبية خلال الفصل الدراسي الاول 2022/11/1 إلى 2022/12/7

وبناء عليه منح هذه الشهادة

المدرب — ر.ش تدريب الطلبة — مدير مكتب الإرشاد الوظيفي ومتابعة الخريجين — عميد شؤون الطلبة

Cisco Networking Academy — Corporate Social Responsibility

Certificate of Course Completion

Introduction to Cybersecurity

For completing the Cisco Networking Academy® Introduction to Cybersecurity course, and demonstrating the ability to explain the following:

- Global implications of cyber threats
- Ways in which networks are vulnerable to attack
- Impact of cyber-attacks on industries
- Cisco's approach to threat detection and defense
- Why cybersecurity is a growing profession
- Opportunities available for pursuing network security certifications

Wessam Alkhushman — Student

ITTI-JAF — Academy Name

Jordan — Location

12 Feb 2024 — Date

Ali Bani bakar — Instructor

Instructor Signature

UPSKILLING IN CYBERSECURITY

Understand information systems, networks, security and protection systems. I learned about the basics of Networks - Cyber Security - Kali Linux - OS and an introduction to hacks, how to implement them, frameworks for their implementation, and international principles and laws. And how to do network scan and its programs to be able to find ports servers firewalls and protection systems, then learn how to record all the information obtained by network scan and protocols for collecting passwords for devices and mail accounts and other important matters to collect private information from the network to successfully carry out the hacking process. Then learn about Social Engineering and how to deceive people in order to obtain information or carry out a hacking operation, in addition to learning the basics of encryption and the mechanism of its work, and managed to make a hack in order to know the gaps in the network in order to address them.

PYTHON

I have taken two certificates from different centers in learning Python and have extensive experience in it

TRAINING

Nashama 7 Cybersecurity Bootcamp(240 hours)

is a training program of the National Cybersecurity Center (NCSC) and has completed 240 hours in the following topics:

1. Ethical Hacking: Learn techniques for penetration testing and discovering security vulnerabilities in a legal and ethical manner.
2. Network Security: Understand how to protect networks against cyber threats and attacks.
3. Secure Coding: Learn to write secure code that minimizes security flaws and exploits.
4. Digital Forensics: Gain skills in analyzing digital evidence and investigating cybersecurity incidents.
5. Application Security: Understand how to secure applications from common vulnerabilities and threats.
6. Incident Response: Learn how to effectively detect, respond to, and recover from security incidents.
7. Cloud Security: Understand the security challenges of cloud environments and how to address them.
8. Operating System Security: Learn how to secure different operating systems against potential threats.
9. Mobile Security: Explore techniques for securing mobile devices and mobile applications.
10. Security Analysis Using Advanced Tools: Practice using tools like Wireshark, Metasploit, and Burp Suite for security testing and analysis.

In addition to technical topics, the bootcamp also includes:

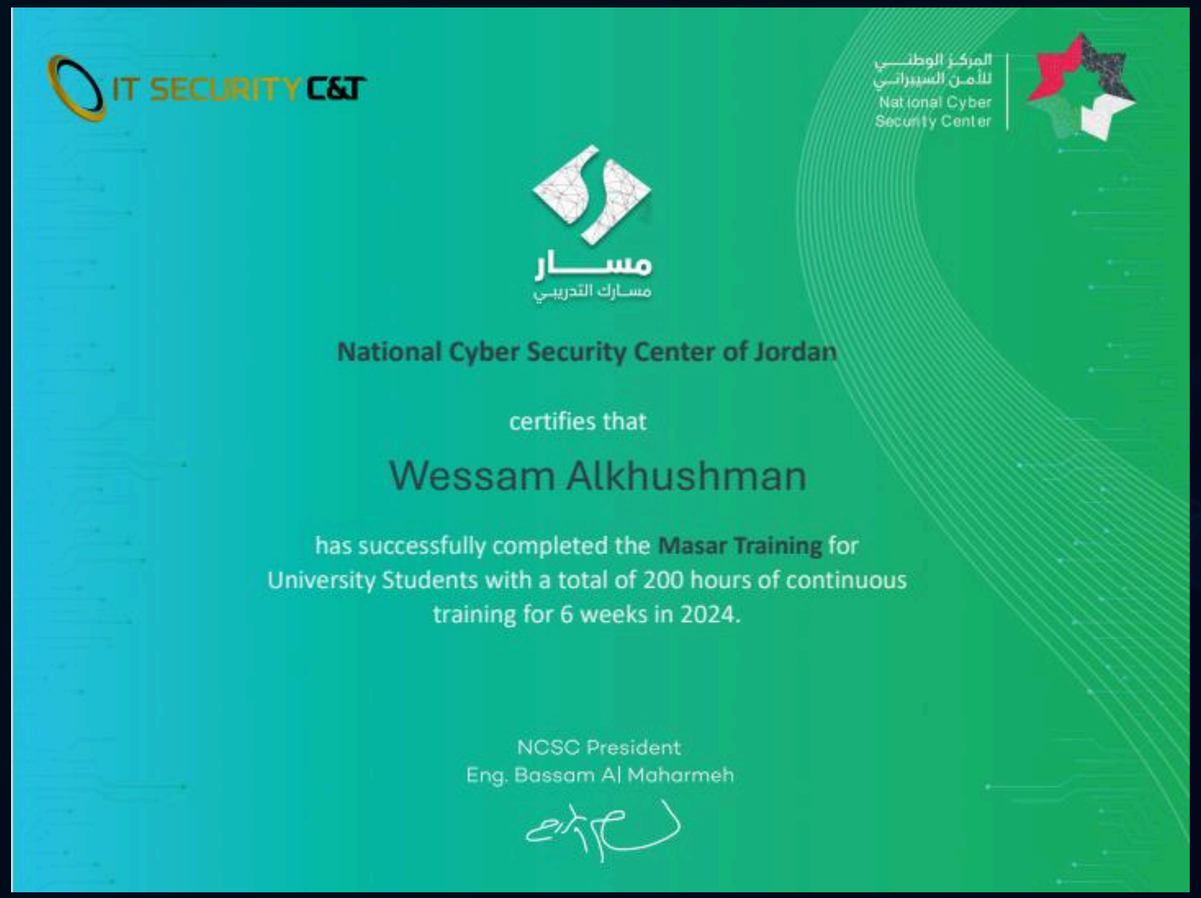
- 100 hours of English language training: To improve professional and technical communication.
- 60 hours of soft skills training: Focused on teamwork, problem-solving, and critical thinking.

TRAINING

Masar cybersecurity training program (200 hours)

is a training program of the National Cybersecurity Center (NCSC) and has completed 200 hours in the following topics:

- Ethical Hacking
- Web Hacking
- Digital Forensics and Incident Response
- Mobile Hacking



TRAINING

Upskilling in Cybersecurity(180 hours)

Purpose of the program:
This program was built with the aim of rapidly upskilling trainees with a technical background in the fields of system administration, information security, programming, and ultimately penetration testing and digital forensics.

Course Outline:

- Linux Administration.
- Python Programming.
- Practical Applications on python.
- Cybersecurity foundation.
- Introduction to Ethical Hacking and Digital Forensics.

SKILLS ACQUIRED

01

System and Security Management: I learned how to configure and enforce security policies using tools like Group Policy in Windows and iptables in Linux.
I gained practical knowledge in securing environments and enhancing protection across different systems.

02

4-Vulnerability Analysis: I gained extensive experience in security analysis by studying the OWASP Top 10 and performing both active and passive reconnaissance.
I learned how to identify vulnerabilities and apply appropriate mitigation measures.

03

5-Certifications in Cybersecurity: I have obtained recognized certification in the field like CEH and I am currently preparing for OSCP, CSA and CHFI certification . These certifications have bolstered my technical expertise and increased my credibility in the cybersecurity domain.

04

6-Project and Team Management: I was captain of the technical team of several student teams and vice president of the science club at my university .
I was responsible for coordinating work and ensuring smooth operations, which honed my leadership and organizational skills.

05

8-System Administration in Windows and Linux: I gained expertise in managing systems in both Windows and Linux environments, including setting up BitLocker and implementing access control policies and time-based restrictions.

06

9-Technical Report Writing: I developed my skills in writing technical reports by documenting challenges and solutions in my cybersecurity projects.
I always ensure that my reports clearly explain the procedures followed and the outcomes achieved.

TECHNICAL KNOWLEDGE

01

Operating Systems:

- Windows: I am proficient in managing Active Directory, configuring Group Policies, and securing Windows environments. I have hands-on experience in Windows Server administration, configuring user permissions, and managing security settings in both client and server editions.
- Linux: I have solid experience in user management, file system management, and configuring iptables for network security. I am comfortable with command-line tools and have worked with distributions such as Kali Linux, Ubuntu, and CentOS.

02

Programming Languages:

- Python: I have developed custom security tools and automation scripts in Python, including tools for network scanning, vulnerability scanning, and data extraction. Python has been instrumental in automating various cybersecurity tasks.
- Bash: I am proficient in writing Bash scripts for automating system administration tasks, including file management, process management, and user permissions on Linux systems.
- C++: I am proficient in using C++ and doing tasks and operations through it and its advantage is that it is fast compared to other languages

03

Cybersecurity Tools:

Wireshark: I use Wireshark for network traffic analysis, capturing packets, and inspecting them for vulnerabilities and suspicious activities in both local and remote networks.

Metasploit: I have hands-on experience with Metasploit for penetration testing, vulnerability exploitation, and conducting ethical hacking assessments. I have used it to identify and exploit security weaknesses in systems and applications.

Burp Suite: I am proficient in using Burp Suite for web application security testing. This includes scanning for vulnerabilities, intercepting HTTP/HTTPS traffic, and identifying issues like SQL injection, XSS, and CSRF.

Nmap: I regularly use Nmap for network discovery, port scanning, and vulnerability scanning. It helps me gather critical information about hosts, services, and potential risks within a network.

Volatility: I use Volatility to analyze memory dumps and uncover hidden processes, injected code, and other artifacts that help in detecting advanced malware and investigating security incidents.

John the Ripper: I have used John the Ripper for password cracking and analyzing password hashes. This tool has helped me assess the strength of authentication mechanisms.

Kali Linux Tools: I am highly familiar with the Kali Linux suite of tools, including Hydra, Aircrack-ng, Netcat, and others, for penetration testing, password cracking, and network analysis.

Snort: I have experience configuring and using Snort for intrusion detection and prevention. It helps me monitor network traffic and detect potential security threats in real-time.

04

Other Skills:

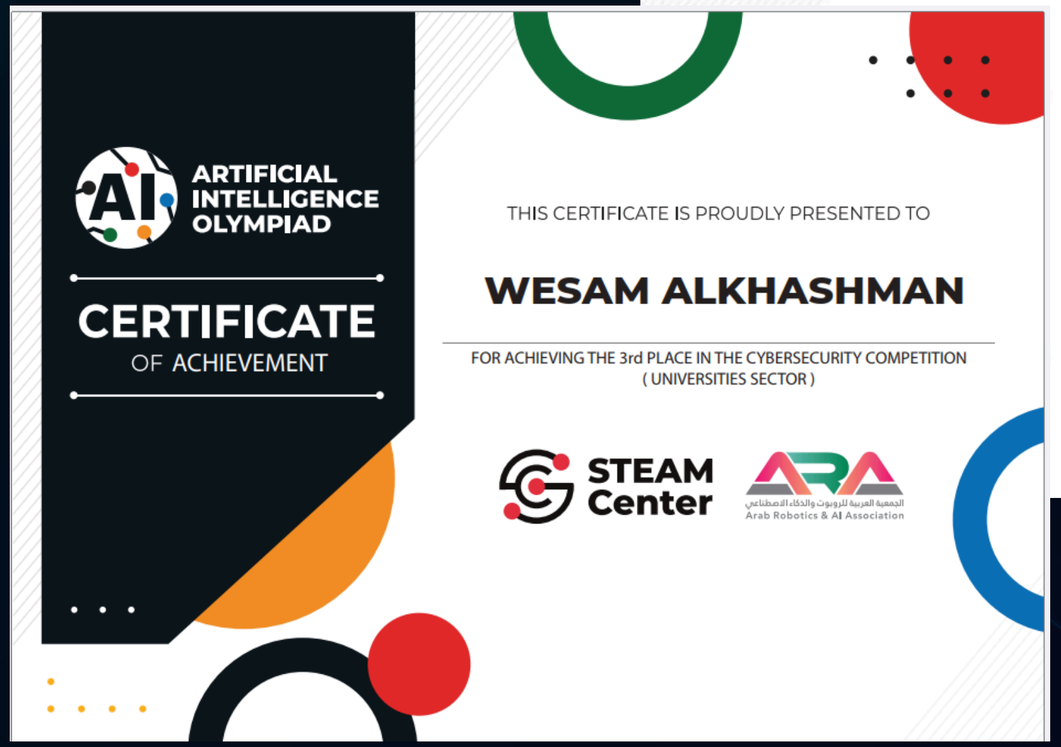
Network Management: I have a strong understanding of network configuration and management, including configuring firewalls, VPNs, DNS, and DHCP. I am also experienced with network troubleshooting tools like Ping, Traceroute, and Netstat.

Vulnerability Analysis: I have hands-on experience with vulnerability scanning tools like OpenVAS, Nessus, and Qualys. I can identify, assess, and mitigate security weaknesses in both systems and web applications.

COMPETITIONS

01

3rd place in the Cybersecurity track of the Arab Olympiad for Artificial Intelligence.



COMPETITIONS

02

Cyber Hero (CTF JO)

CERTIFICATE OF PARTICIPATION

GREEN CIRCLE

Green Circle Company & Cyber Shield Academy

Certify that

(Wessam Mohammad Al-khushman)

has participated in

Cyber Hero Competition (CTFJO 2024)

His team (Zero Zone) has qualified to the Final Round

They have attained an excellent rank of 8th out of 80 teams

Therefore, it was decided to grant him this certificate

GC CEO

Mohammed Al-Khudari

GREEN CIRCLE

be aware. be secure

COMPETITIONS

03

MUCPC (Problem Solving)

COMPETITIONS

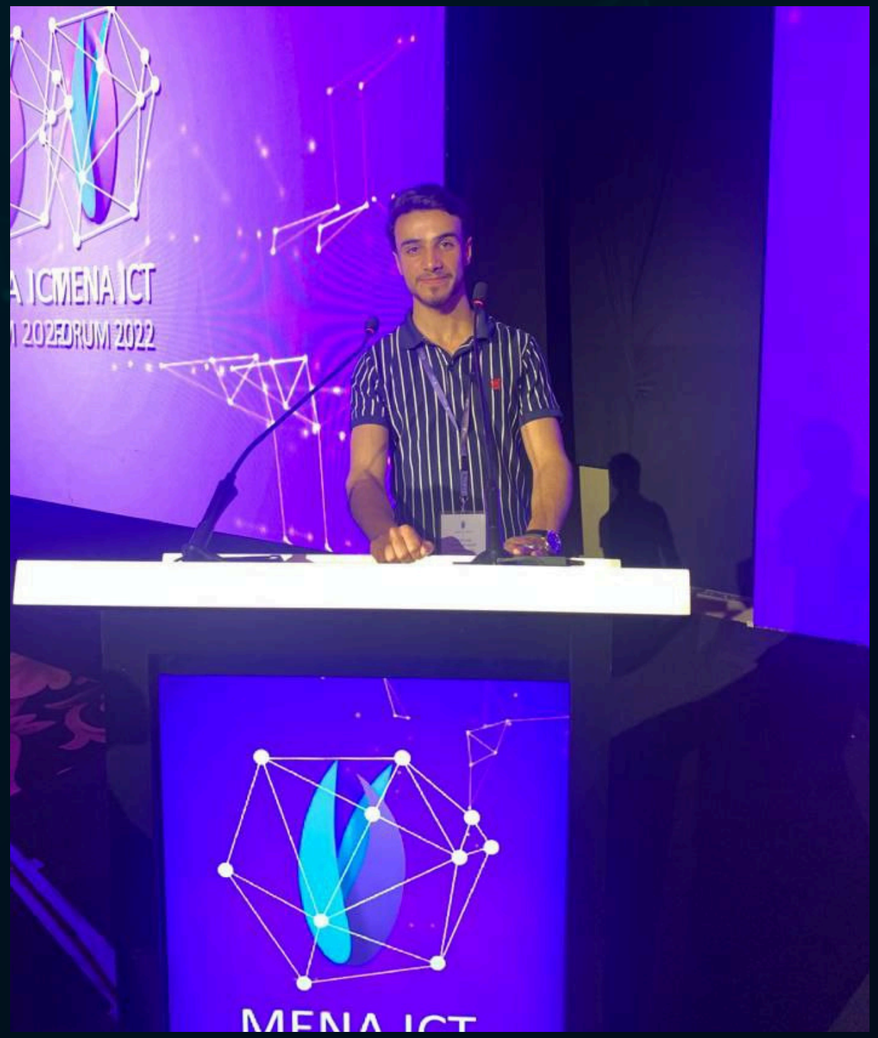
04

JCPC (Problem Solving)

CONFERENCES AND FORUMS

01

MENA2022



CONFERENCES AND FORUMS

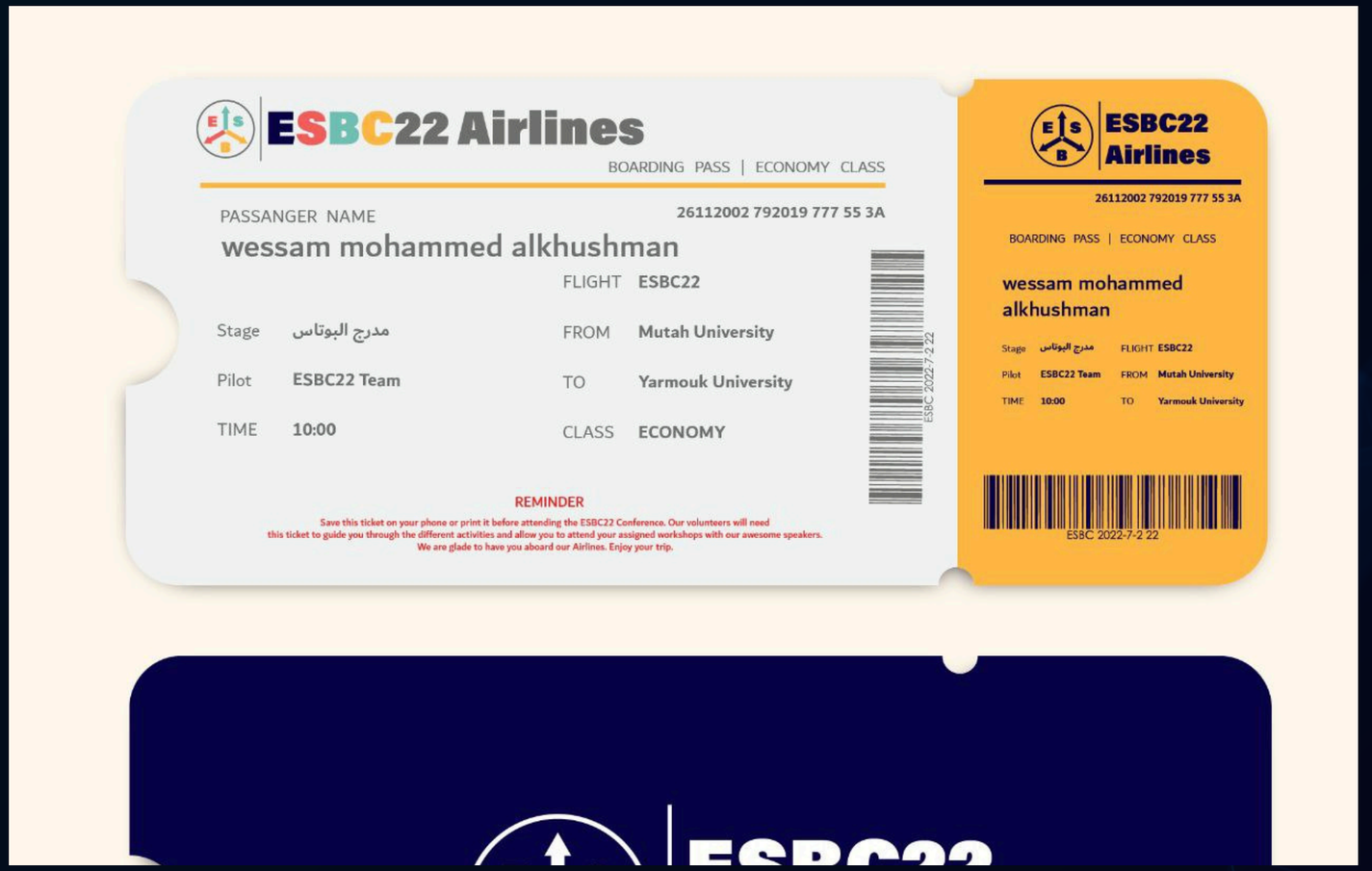
02

المؤتمر الدولي الاول حول الاتجاهات الناشئة في تطبيقات الحوسبة والهندسة.

CONFERENCES AND FORUMS

03

ESBC2022



CONFERENCES AND FORUMS

04

AHU ATE

CONFERENCES AND FORUMS

05

From Venus To Universe (FVTU2)

CONFERENCES AND FORUMS

06

مؤتمر الخريجين 2024

EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

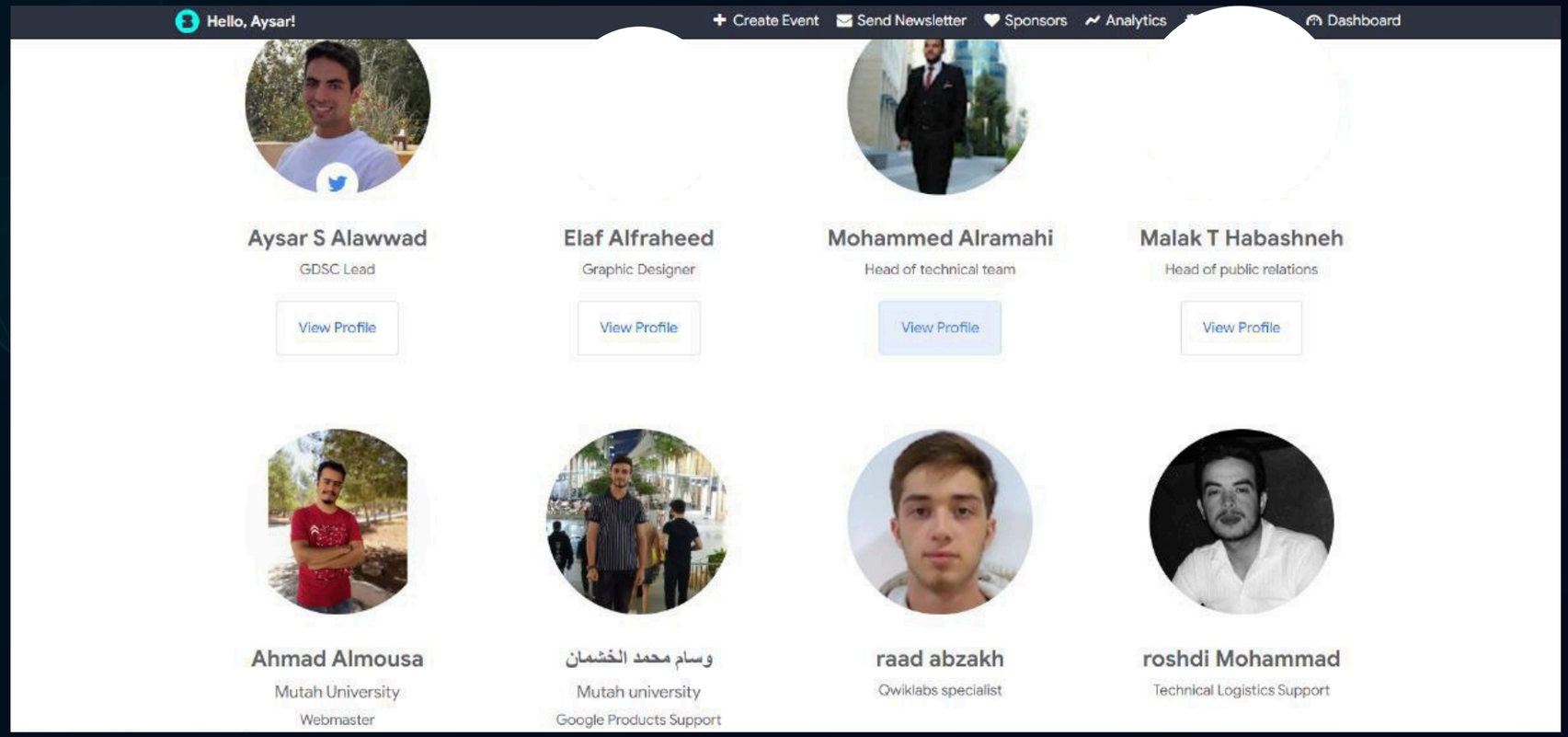
IEEE student club in Mutah university

EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

Google Developer Student Clubs (GDSC)



EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

MutahVerse:
A student group that I was one of the founders of

EXPERIENCE AND VOLUNTEERING

02

Vice President of the Scientific Club at Mu'tah University

EXCERPTS

MENA 2022

The second day of the forum, in which we learned and benefited from the expertise of IT specialists and got to know and consult with IT companies

IOT Workshop

Learn to program embedded systems and refactor robots

AIO

It was a very special experience in the ctf competitions and I made a breakthrough in it

EXCERPTS

مجلس اتحاد طلبة جامعة مؤتة

التاريخ: ٢٠٢٣/٠٩/٢٦

مرحبًا بأعضاء الإرشاد!

تحية طيبة وبعد،،،

تم اختياركم لتمثيل جامعة مؤتة في نشاط الإرشاد للطلبة المستجدين في العام الجامعي ٢٠٢٣/٢٠٢٤.

نحن سعداء جدًا بانضمامكم إلى هذا الفريق المميز، أنتم العنصر الحيوي الذي سيساعد الطلبة في تجاوز تحدياتهم والتكيف في الحرم الجامعي، نثق تمامًا بأنكم ستقدمون الدعم والمساعدة المهمة للطلبة المستجدين، وستكونون لهم مصدرًا قويًا للمعلومات والإرشاد.

نرجو منكم تأكيد الحضور في كافة أيام الإرشاد التي ستحدد لاحقًا؛ ليتم التواصل معكم تباعًا على برنامج الـ WhatsApp وإعلامكم بالخطوات التالية.

.....

مع أطيب التمنيات،،،

رئيس مجلس الاتحاد

راشد عبدالله العديلات

مسؤول نشاط الإرشاد

محمد رضا الطراونة

New Student Orientation

It was a great experience. It's nice to help if you can.

Organizing a MUCPC 2023 contest

This contest was all about problem solving.

Review

Training and review work for students

EXCERPTS

X Competition and Alumni Conference

IOT Workshop

SHAI representative at the AHU ATE conference

EXCERPTS

IOT workshop

While organizing an event at the university

Students organizing an event for the College of Information Technology

EXCERPTS

Karama Scout Camp

Dibbin Scout Camp

Delegate in parliamentary elections

CONTACT INFORMATIOM

+962776433171

GitHub

wessamalkhushman@yahoo.com

www.linkedin.com/in/wessam26

Shobak-Ma’an-Jordan

THANK YOU

**Thank you for taking the time to explore my portfolio. i am eager to contribute to
future projects and take on new challenges in the cybersecurity field.
if you would like to discuss how my skills can support your
organization's cybersecurity goals or need
additional information, please feel free to**

CONTACT ME DIRECTLY.