

# OMRI HERMAN

Phone number: 0522-959002

Home address: Or-Yehuda

E-mail address: [omh\\_il@yahoo.com](mailto:omh_il@yahoo.com) ID: 061212932

To whom it may concern,

I am a certified ethical hacker seeking experience in any position that will advance my career in cyber-security.

I'm a diligent and responsible worker seeking to prove the value of my work and willing to commit to long term jobs.

## Credentials & Certificates

### "Certified Ethical Hacker"

Earned by successfully passing the official "ECC-Council Certified Hacker" (CeH) exam.

### Cyber-Security Course, "Hacker-U" College, Ramat-Gan

Successfully completing the six-month long cyber-security course, and meeting all of its requirements.

### "Linux Essentials" certification by the "Linux Professional Institute"

Earned by successfully passing the official "Linux Essentials" online exam of the LPI.

## Education

01/2019 - 07/2019

### Information security and ethical hacking course, "Hacker-U" college, Ramat-Gan

590 academic hours. Successfully completed the six-month long cyber-security course, and met all of its requirements.

2021 **Some practical experience with various CTF challenges** (These include 40 "TryHackMe" challenges which I have completed and many of Hacker U's "Cywars" system challenges which I have completed.)

### 2014 EMT certificate, Magen David Adom

Volunteered during the year at the MDA Bney Brak branch.

2000 **"Ironi Alef" high school, earned a full Bagrut certificate**

## Professional skills:

### Penetration Testing of Computer Networks & Individual Systems' Infrastructure

**LAN attacks** such as various MITM (Man in the Middle) techniques and DNS spoofing methods, sniffing of network traffic, Nmap techniques, extraction of sensitive data, such as the systems credentials and the cracking of said data's hashing.

**Remote attacks** using Nmap scanning and scripts, known vulnerabilities, password spraying, reconnaissance (including SMTP recon, DNS transfers/recon and Google hacking), and social engineering.

**Privilege escalation** (both remote and local) on both Linux/Unix & Windows systems and on Active directory managed domains.

### Penetration testing of web-applications and their underlying systems

**Knowledge of various web attacks and vulnerabilities**, such as: SQL Injection, XSS, Command injection, Local file inclusion, URL tampering, etc.

### Operating Systems

Proficiency in **Linux** OS working environments.  
Proficiency in **Microsoft Windows** OS working environments.  
Familiarity with **Microsoft Windows Server** OS environments, including knowledge of basic windows network administration.

English & Hebrew at a native tongue level | Speaks basic Spanish

### Programming

Some programming/scripting knowledge of:

Python  
Java-Script  
PHP  
Powershell  
Batch scripting.  
Bash scripting

## Work experience

### 2019-2021 NOC Engineer for "Motorola Solutions Israel"

The Job consisted of management and monitoring of several closed networks for Motorola's clients as well as managing Motorola's worldwide wifi networks.

The work entailed:

- The planning of the wifi infrastructures and placements of the Access points on the work sites based upon maps provided by our on sites contact persons. The actual planning utilized the Ekahau program which is designed to simulate the physical conditions on the location and foresee the quality of wifi transmissions based upon the APs' placement and other parameters.
- Assistance in the Wifi settings configurations after the physical connection of the AP's to the switches on the site locations.
- Remote configuration of the AP's through various controllers using the SSH protocol. The configuration included the preparation of profiles and logical groups which were associated with the sites' AP's, and the designation of IP ranges to the different sites. These profiles determined various network settings, Vlans, Radio channels activity, SSID's etc. Additionally, there was sometimes a need to initiate the communication between the AP's and the controllers by logging in remotely into the AP's and configuring it.
- Configuration of outbound and inbound access lists, management of Wifi networks security settings, ongoing monitoring and maintenance by performing routine checkups and addressing problems and complaints from workers around the world by troubleshooting the issues (while using systems such as Splunk and Nsight).
- Continuous monitoring of networks of projects for the company's clients while utilizing various monitoring systems and real time reporting of malfunctions to the proper contact persons.
- A SOC project as a backup team for one of the company's clients. The work consisted of the monitoring, investigation and reporting of events while utilizing the system's interface. I've also learned to prepare filters and rules on the system, associating them to active channels, navigating the different menus and more.
- The work also required familiarity and knowhow (both in the monitoring as well as the maintenance and configuration aspects) of the following monitoring and management systems: SolarWinds, Zabbix, Splunk, Nsight and Arcsight

2018

### Helpdesk, "YaYasoft", a software development company

The work consisted of providing **technical support** to the company's clients.

The support entailed helping the clients operate the company's **web based CRM** program and its **mobile applications**.

## קורות חיים: עומרי הרמן

עיר מגורים: אור יהודה מספר פלאפון: 0522-959002

מ.ז.: 061212932 כתובת מייל: [omh\\_il@yahoo.com](mailto:omh_il@yahoo.com)

שלום רב, אני עובד כטכנאי NOC מזה שנתיים, בוגר קורס אבטחת מידע של מכללת האקר יו ומוסמך ceH על ידי ה-EC-Council. אני מחפש כל משרה שתקדם את ההתמקצעות שלי בתחום אבטחת המידע. אני חרוץ ואחראי בעבודתי ומוכן להתחייב לעבודה לטווח ארוך.

## תעודות:

**תעודת הסמכה "Ce|H - Certified Ethical Hacker"**, לאחר מעבר מבחן ההסמכה הרשמי של ארגון Ec-Council.

**תעודת הסמכת "Linux Essentials"** לאחר מעבר מבחן ההסמכה הרשמי של ארגון LPI.

**תעודת סיום קורס אבטחת מידע במכללת "האקר יו" ברמת גן.**

בוגר מסלול אבטחת מידע, לאחר שהשלמתי בהצלחה את המסלול בן ששת החודשים ועמדתי בכל הדרישות של הקורס.

## מסלול מקצועי:

- 2000 - סיים תיכון "עירוני א" עם תעודת בגרות מלאה.
- 1/2019 – 7/2019 קורס אבטחת מידע במכללת "האקר-יו", 590 שעות אקדמיות.
- 2019 – 2021 התנסות מעשית באתגרי CTF שונים הכוללים את האתגרים של מערכ' Cywars של האקר יו, ואתגרים של האתר "TryHackMe".

## כישורים מקצועיים:

בדיקות חדירות לרשתות מחשבים ותשתיות של מערכות בודדות.

- **התקפות ב-LAN**, כגון טכניקות שונות של MITM (האדם שבאמצע), ושיטות הרעלת DNS. סריקות רשת, סניפינג (ניטור מידע העובר ברשת), שליפת מידע רגיש, כמו פרטי זיהוי ופיצוח ההאשינג של המידע הנ"ל.
- **התקפות מרחוק**, תוך שימוש בסריקות וסקריפטים של תוכנת Nmap, טכניקות איסוף מידע מגוונות (הכוללות תשאול DNS, תשאול שרתי SMTP, וחיפושים בגוגל באמצעות אופרטורים מתקדמים), מינוף פגיעויות ידועות, והנדסה חברתית.
- **העלאת הרשאות** (גם מרחוק, וגם מקומית), על מערכות לינוקס ווינדוס ובסביבות דומיין המנוהלות על ידי אקטיב דיירקטורי.

בדיקת חדירות לאפליקציות רשת והתשתיות שבבסיסן.

- ידע בטכניקות שונות של התקפות שרתי ווב וחולשותיהם. הטכניקות כוללות בין השאר, הזרקת SQL, הזרקת XSS, הזרקת פקודות PHP, הכללת קבצים לוקאליים, מניפולציות על פרמטרים בURL וכו'.

### מערכות הפעלה:

- בקיאות ברמה גבוהה בסביבת מערכות הפעלה של לינוקס.
- בקיאות ברמה גבוהה בסביבת עבודה של מערכות הפעלה "חלונות" של מייקרוסופט.
- התמצאות במערכות הפעלת שרתים "ווינדוס סרבר" של מייקרוסופט, כולל ידע בסיסי בניהול רשתות ווינדוס.

### שפות תוכנה/סקריפטינג:

#### ידע מסוים בשפות הנ"ל:

- פייתון.
- ג'אבה סקריפט.
- PHP
- באש סקריפטינג.
- באץ' סקריפטינג
- פאוורשל.

### ניסיון תעסוקתי:

- **2019-2021 אנליסט NOC במוטורולה ישראל.** מהות העבודה היה ניטור וניהול מס' רשתות סגורות של לקוחות מוטורולה ורשתות הוויי פיי של מוטורולה ברחבי העולם.

#### העבודה כללה:

- תכנון תשתית הוויי פיי ופרישת נקודות הגישה באתרים השונים על סמך מפות אשר סופקו על ידי אנשי הקשר באתר ובהסתייעות בתוכנת EKAHAU. תוכנה זו נועדה לסייע בהדמיית התנאים הפיסיים באתר ולנבא את איכות תשדורת הוויי פיי בהתאם לפרישת נקודות הגישה ופרמטרים אחרים.
- סיוע בהגדרת אתרי הוויי-פיי השונים לאחר החיבור הפיסי של נקודות הגישה למתג באתר. הטמעת ההגדרות מרחוק באמצעות הקונטרולרים השונים דרך פרוטוקול SSH. ההגדרות כללו הכנת פרופילים וקבוצות לוגיות אשר שויכו לכל אתר על פי צרכיו והקצאת טווחי איי פי. הפרופילים קבעו הגדרות רשת שונות, וילאנים, פעילות ערוצי רדיו הן באופן עצמאי והן בתיאום עם נקודות הגישה האחרות, רשתות וויי פיי וכו'. בנוסף היה לעיתים צורך ביצירת התקשורת הראשונית בין נקודות הגישה לקונטרולרים על ידי התחברות לנקודות הגישה מרחוק והגדרתן.
- הגדרות רשימות גישה יוצאות ונכנסות, ניהול אבטחת הרשתות, ניטור ותחזוקה שוטפים על ידי בדיקות שגרתיות ומענה לתקלות ותלונות ברחבי העולם באמצעות תחקור הבעיות (תוך שימוש במערכות שונות כמו ספלאנק Nsighti).
- ניטור מתמיד של רשתות בפרוייקטים נוספים בעבור לקוחות שונים על תוך שימוש במערכות הניטור השונות ודיווח בזמן אמת לגורמים המתאימים על התקלות.

- פרוייקט SOC כצוות גיבוי בעבור אחד הלקוחות של החברה. העבודה כללה ניטור, תחקור ודיווח על אירועים תוך שימוש והיכרות בממשק המערכת. כמו"כ למדתי להכין פילטרים וחוקים במערכת, לשייכם לערוצים אקטיביים, לנווט במערכת בין התפריטים השונים ועוד.
- במסגרת העבודה, שימוש במערכות זאביקס, סולרווינדס, ספלאנק, ארקסייט Nsighti אשר דרש התמקצעות והתמצאות בכל אחת מהן (הן בניטור ובשימוש השוטפים והן בהגדרת ותחזוק אופן פעולתן).

- **2018 - עבודה כתומך טכני בהלפדסק של חברת פיתוח התוכנה "יאסופט".**  
העבודה כללה סיוע ללקוחות החברה בתפעול מערכת הCRM מבוססת הווב שפיתחה "יאסופט", והאפליקציות הסלולאריות התממשקות עמה.
- **2015-2019 - אסיסטנט במרפאה וטרינרית "וטרינר בכיכר".** העבודה כללה מתן טיפול וטרינרי לחיות מחמד וכללה עזרה לרופאים בנייתוחים והפעלת טכנולוגיות רפואיות (כמו למשל מכונת צילום רנטגן).
- **2009-2015 - עוזר אדמיניסטרטיבי לרופא במרפאה פרטית.**
- **2009 - חובש במרפאת מתאדון לנפגעי סמים.**

#### כישורים נוספים:

- דובר עברית ואנגלית ברמת שפת אם.
- דובר ספרדית ברמת תקשורת בסיסית.