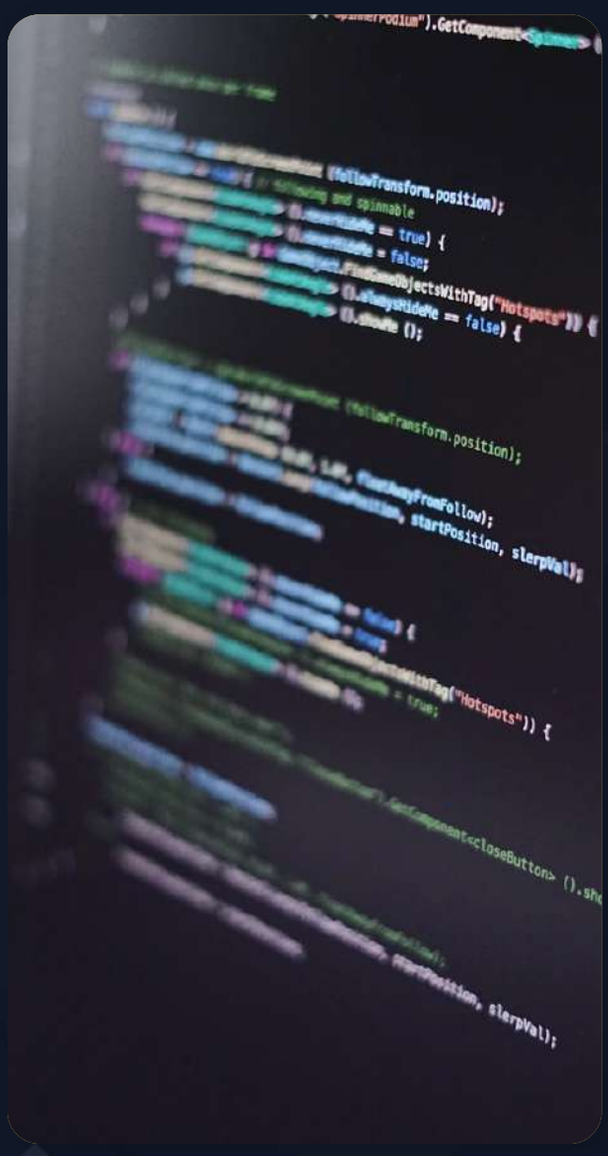
ECOM SCHOOL

המכללה למקצועות הדיגיטל וההייטק

קורס אבטחת מידע וסייבר בהתמחות מבדקי חדירה (PT)

הקורס כולל מבחנים פנימיים
ומכין להסמכות בינלאומיות



מבנה הקורס

קורס אבטחת מידע וסייבר

בדיקת חדירה (הידועה בשם Penetration Testing או בקצרה PT) הינה תהליך מורכב המתבצע על ידי ההאקר על מנת לבדוק האם היישומים והשירותים של החברה פגיעים לליקויי אבטחה. בדיקת חדירה הינה תהליך חשוב ביותר עבור ארגונים בארץ ובעולם ומתבצעת על ידי האקר מיומן אשר משתמש באותן השיטות בהן ישתמש ההאקר הזדוני, כדי לגלות האם הוא יכול לפגוע באפליקציות, אתרים או בתשתיות של החברה ולנצל ליקויי אבטחה על מנת לגרום לנזק. לאחר סיום הבדיקה ההאקר יספק דוח לחברה אשר יציג את כלל ליקויי האבטחה שאיתר וכמו כן פתרונות כיצד לתקן את ליקויי האבטחה האלו. החברה יכולה לבקש מגוון רחב של בדיקות חוסן ולכן על ההאקר להיות בקיא במגוון רחב של תחומים, כגון: בדיקות חוסן ליישומי האינטרנט (האתרים והמערכות) של החברה, בדיקות חוסן לאפליקציות שמפתחת החברה הן לאנדרואיד והן לאייפון, בדיקות חוסן לתשתיות של החברה ברמה הרשתית ועוד. עקב הידע הרב הנדרש לביצוע בדיקות חוסן והחוסר בתוכניות הכשרה מסודרות קיים מחסור רב בבודקי חוסן הן בארץ והן בעולם וכאן נכנס לתמונה קורס סייבר בדיקות חוסן ופיתוח מאובטח. קורס בדיקות חוסן ופיתוח מאובטח הינו הקורס המקיף ביותר בתחום מבדקי החוסן המתבסס על מחקרים שביצעו מרצי הקורס תוך כדי עבודתם כבודקי חוסן / חוקרי סייבר בכירים בחברות בארץ. במהלך הקורס המרצה יציג את הממצאים אשר מצא לאורך הקריירה שלו, ימקד את התלמיד ויפתח אצלו חשיבה יצירתית לצורך מבדקי חוסן. כך התלמיד יזכה לראות כיצד מתבצע מבדק חוסן על ידי מומחה בתחום. במהלך הקורס התלמיד עובר התמקצעות בתחום ה- LINUX וה- PYTHON.

קהל יעד:
אנשים המגיעים ללא רקע לעולם הסייבר, המעוניינים בהסבת מקצוע עם זיקה לשינוי ופיתוח עצמי והתקדמות נרחבת בתחום. מפתחים אשר רוצים לבצע הסבה מקצועית לתחום בדיקות החוסן עם התמקצעות בתחום הלינוקס והפייתון או להעשיר את הידע שלהם בתחום. בודקי חוסן מתחילים שרוצים להשתפר בתחום בדיקות החוסן ולעלות מדרגה לשלב הבא. תלמידי מדעי המחשב/ הנדסת תוכנה מאוניברסיטאות/ מכללות שרוצים לשפר את הסיכויים שלהם לעבוד בתחום מבדקי חוסן עם התמקצעות בתחום הלינוקס והפייתון.
תלמידים שעברו קורסי סייבר בעבר ועדיין מרגישים שאינם מסוגלים לעבור ראיון עבודה בתחום בדיקות חוסן עם התמקצעות בתחום ה- LINUX וה- PYTHON.
כל מי שרוצה ללמוד לבצע בדיקת חוסן מקצועית מא' ועד ת' עם התמקצעות בתחום הלינוקס והפייתון ובעל ניסיון מעשי בתחום טכנולוגי כגון ניהול רשת, Devops ו-QA.

משך הקורס:
משך הקורס הינו 360 שעות אקדמיות המתקיימות במסגרת 72 מפגשים, פעמיים בשבוע בין השעות 17:30 ועד 21:30.

חומר עזר:
מערך דיגיטלי שמטרתו לעזור ולקדם את התלמיד, לצפייה חוזרת, במידת הצורך, ללא הגבלת זמן. בקורס תתרגלו את כלל הנושאים על מערכת אתגרים מבוססת מחקרים אמיתיים שבוצעו על ידי המרצים של הקורס!
לרשות התלמידים מערך סרטונים דיגיטליים ללימוד אנגלית ברמה בסיסית ומתקדמת.

תנאי סף:
הקורס הותאם לתלמידים אשר התנסו בחומר וגם תלמידים אשר מגיעים ללא רקע קודם. כל הנושאים נלמדים החל מהבסיס ועד לרמה המקצועית ביותר. הקורס דורש אנגלית ברמה בסיסית.

בסיום הקורס:
עם סיום הקורס התלמיד ידע לבצע בדיקות חוסן בצורה הטובה והיסודית ביותר, הכוללת כתיבת דו"ח בדיקות חוסן. תלמידים שהגישו את כל מטלות הקורס ועברו את הקורס בהצלחה עם ממוצע ציונים של 85 ומעלה, יקבלו תעודת סיום ועזרה בהשמה בתחום הסייבר ובדיקות החוסן. בנוסף הקורס מכין את התלמיד למבחני ההסמכה החיצוניים: LINUX , PYTHON . במידה והתלמיד רוצה לגשת למבחני הסמכה חיצוניים ניתן לגשת באופן עצמאי.

המכללה ליזמות, מקצועות הדיגיטל והייטק

איקום היא מיזם חברתי – קהילתי, שנוסדה במטרה לייצר שינוי תודעה בכל הקשור לשיטות לימוד, בדרכים קריאטיביות יוצאת דופן, אשר חלקן אפילו מעוגנות כפטנט עולמי!
הכיתות הוירטואליות , הרשת החברתית והקשר ההדוק בין המכללה לתלמידים גם לאחר סיום הקורס.
לימודי מקצועות העתיד יתנו לכם את האפשרות להשתלב בתעשיית ההייטק והדיגיטל כשכירים או עצמאיים בליווי צמוד לאורך כל הדרך.

ברשותינו רישיון השמה מטעם משרד העבודה והרווחה,
כמו כן אפשרות לייעוץ עסקי, בהקמת מערך אופרטיבי ראשון באינטרנט.

מכללת איקום היא היחידה בישראל
אשר נמצאת במאגר תוכניות הלימוד של משרד החינוך.

אנחנו זמינים עבורכם 24/7, ONLINE & OFFLINE , לקבלת מידע מקצועי ומהימן ממיטב אנשי המקצוע בתחום הדיגיטל וההייטק המתקדם, עם כל החידושים והעדכונים בזמן אמת ומענה חי וזמין.

הרשת החברתית האקדמאית הראשונה והיחידה מסוגה בישראל
עולם שלם של קהילה שלא הכרתם!

מעל 300 שיעורים דיגיטלים מעודכנים ומתעדכנים, פרופיל אישי, צ'אט עם מדריכים, הכרות עם סטודנטים באיקום, פורומים ממוקדים, פורטל ענק ועוד.

תקשורת

23 שיעורים מוקלטים
250 דקות צפייה
6 מפגשים
30 שעות אקדמיות
מעבדות תרגול

מבוא לסייבר

- אודות המרצה
- ציפיות מהקורס
- חשיבות החשיבה והעבודה הקשה
- סייבר וחוקיות
- המונח סייבר לתולדותיו
- סוגי האקרים
- אירועים אחרונים
- ציפיות לעתיד ומציאת עבודה
- חומרה, תוכנה ו-Kernel

מבוא לווירטואליזציה:

- יסודות ווירטואליזציה
- יתרונות הווירטואליזציה
- שימושים בתעשייה
- השימושים בסייבר
- סוגי קבצים חשובים
- המונח "ענן"
- השימוש ב-Virtual Box והגדרותיו

יסודות התקשורת

- תקשורת מחשבים
- מדוע יש צורך ברשת במחשבים
- יתרונות התקשורת
- מונחי יסוד בתקשורת
- מוצרי תקשורת וכיצד הם עובדים
- סוגי תקשורת – Unicast, Multicast, Broadcast, Anycast
- המונחים – שירות, שרת ופרוטוקול

יסודות התקשורת חלק שני:

- מודל שבע השכבות – OSI
- מודל ארבע/חמש השכבות – TCP/IP
- תהליך ה-Encapsulation וה-Decapsulation
- היכרות בסיסית עם Cisco Packet Tracer

יסודות התקשורת חלק שלישי:

- ספירה בינארית
- היכרות עם בסיסי הספירה – דצימלי, אוקטלי, בינארי והקסדצימלי
- כתובות IP ושימושן
- מסיכת רשת ומחלקותיה
- נתב ושער ברירת המחדל
- תהליך ניתוב חבילות רשת
- שירותים בסיסיים כגון DHCP, DNS וכן היכרות עם המונח VLAN

יסודות התקשורת חלק רביעי:

- ICMP
- IPV6
- TCP
- תהליך לחיצת היד המשולשת
- היכרות עם מספרי פורטים לוגיים
- מהי חומת האש
- הרכבת כלל הידע ושימושו בעולם הסייבר – IPS & IDS, DOS וכיו"ב

הידעת ?

"מספר מקומות העבודה בסייבר עומד לזנק פי 10 בעשור הקרוב."

עיתון גלובס

Linux

22 שיעורים מוקלטים
7 מפגשים
מעבדות תרגול
250 דקות צפייה
35 שעות אקדמיות

מבוא למערכת Linux

- היסטוריית מערכות ההפעלה
- Windows VS. Linux
- מהו קוד פתוח
- רישיונות קוד פתוח
- גרסאות מערכות הפעלה מסוג Linux
- פלטפורמות המשתמשות ב-Linux
- היכרות עם FHS
- GUI VS. CLI
- Shell Types

Linux Terminal:
- Standard Streams
- File Descriptors
- How to find files using the terminal
- Basic commands

Advanced Terminal:
- Text Processing
- Piping
- Operators
- Useful commands

הידעת ?

"90% מהשרתים בעולם הינם שרתי לינוקס"

Linux

קבצים והרשאות:
- סוגי קבצים במערכות הפעלה
- סיומות קבצים מוכרות
- זיהוי דפוסים באמצעות הטרמינל
- משתמשים והרשאות – Root, Regular User ו-SUDO
- UID & GID
- יצירת משתמשים
- החלפת משתמשים
- מנגנון הרשאות
- הרשאות לקבצים

מבוא לכתיבת Script ואוטומציה:
- Script VS. Program
- Bash Scripting
- Variables
- Environment Variables
- Scheduling tasks – Crontab
- Docker technology and challenge

Bash Programming:
- Input & Output
- If statement
- Nested if
- Boolean Operators
- Loops – For & While

System Services:
- מהו שירות
- ניהול והגדרת שירותים ב-Linux
- Systemctl
- Commonly used services – Telnet, SSH & FTP
- Hacking Demo

Python

23 שיעורים מוקלטים
12 מפגשים
מעבדות תרגול
300 דקות צפייה
60 שעות אקדמיות

Python

מבוא לחשיבה תכנותית:
- מהו pseudo קוד
- קונספט של תנאי ולולאה
- מהו אלגוריתם
- שימוש באלגוריתמים בתכנות
- תכנון אלגוריתם תכנותי בסיסי

מבוא לתכנות ב-Python:
- איך מעבד עובד בהקשר של תכנות
- מבנה שפות Interpreter אל מול Compiled
- מדוע השימוש כה נרחב בשפת Python
- ניהול גרסאות בשפה
- שימוש ב-IDE וכן התנהלות אל מול PyCharm

משתנים ומבנה נתונים חלק ראשון:
- היכרות עם קונספט של משתנים
- היכרות עם סוגי משתנים
- היכרות עם ניהול משתנים בשפה
- היכרות עם מבני נתונים מוכרים
- שימוש בפונקציה type
- היכרות עם מחרוזות ופונקציות ייעודיות
- פעולות על מספרים

המשך מבנה נתונים:
- ניהול רשימות ופונקציות ייעודיות
- ניהול מילון ו-Set וכן מתי יתבצע שימוש בכל אחד

תנאים בסיסיים ומורכבים:
- היכרות עם הקונספט של If
- מהו תנאי ומהו משתנה בוליאני
- טבלאות אמת ולוגיקה בסיסית
- שימוש בתנאי מורכב
- If-Else

לולאות:
- היכרות עם הקונספט של לולאות
- ההבדל בשימוש של לולאות For & While
- לולאות בשפות תכנות אחרות

פונקציות:
- מהי פונקציה
- יצירת פונקציה
- ההבדל בין פונקציות Void (כקונספט) לבין פונקציות Return

ספריות ושימוש בספריית OS ו-SubProcess:
- מהי ספרייה
- השימוש בפונקציות הכתובות בספרייה
- השימוש ב-__main__ משתנים מיוחדים
- היכרות עם הפונקציה dir ו-help
- פונקציונליות שימושית ב-OS ו-SubProcess

שימוש ב-Socket וניהול תקשורת ב-Python:
- היכרות עם ספריית Socket
- בניית שרת ולקוח בשפת Python
- כיצד מתבצע העברת תוכן בין שרת ולקוח
- ניהול שרת רב משתמשים

שימוש בספריית Requests:
- התקנת ספריות בשפה
- מהי ספריית requests
- היכרות בסיסית עם פרוטוקול HTTP
- בניית תוכניות שימושיות לעתיד בהקשר של התקפות Web

המשך שימוש בספריית Requests ופרסור מידע:
- היכרות עם הקונספט של פרסור מידע
- היכרות עם BeautifulSoup
- בניית תוכניות שימושיות

היכרות עם Scapy והתקפות רשת פנימית:
- בניית חבילת מידע לרשת באמצעות השפה
- היכרות עם מנגנון של Scapy ושימושו הנרחב
- בניית WireShark בסיסי באמצעות השפה

הידעת ?

"פייתון היא שפת התיכנות
המבוקשת ביותר בשנים האחרונות"

print("Hello, World!")

"Hello, World!"

התקפות תשתית

23 שיעורים מוקלטים
23 מפגשים
מעבדות תרגול
200 דקות צפייה
115 שעות אקדמיות

מבוא להתקפות תשתית:
- מבנה המודול – External VS. Internal
- מהו שרת ומבוא ל-Windows Server 2019
- Workgroup VS. Domain
- התקנת DC
- היכרות עם הקונספט והטרמינולוגיה:
- Active Directory, Forest, Domain, Organizational Unit, Computers VS Users

היכרות עם שירותים מהותיים:
- DNS, DHCP (and APIPA), Global catalog, more roles and features

ניהול משתמשים והרשאות בשרתים:
- משתמשים:
  - delegated admin
  - domain admin
  - enterprise admin
- ניהול GPO and ADDS components:
- NTDS.DIT
- RODC
- GROUPS - Group VS. OU
- RSAT
- Kerberos בסיסי

היכרות עם רכיבי הגנה:
- NAC
- Device Control
- EDR:
- EDR & AV
- Firewall
- IPS & IDS
- NOC & SOC
- SIEM
- VPN & PROXY
- Dnssec
- Ipsec
- Macsec

Wi-Fi Hacking:
- היכרות עם עולם ה-Wi-Fi:
- IEEE
- 802.11

Encryptions:
- WEP
- WPA & WPA2 & WPA3
- WPS + Attacks

Authentication Process:
- RC4 -> TKIP -> EAPOL -> AES -> CCMP
- Brute-Force and Well known attacks
- Routersploit

data sniff:
- Special NIC – ALFA
- Client mode
- Managed mode
- Monitor mode
- Injection mode
- Wifite2

aircrack-ng:
- airemon-ng
- airodump-ng
- aireplay-ng

Additional hardware:
- pine apple
- Rogue AP attack
- Evil portal
- Evil twin

היכרות עם הצפנות וקריפטוגרפיה:
- Hash
- Cipher:
- Symetric:
- XOR cipher
- AES
- A-Symetric:
- RSA
- טכניקות התמודדות:
- local brute force:
- GPU VS. CPU brute-force
- Wordlist:
- Cupp
- Rainbow table
- Seclists

OSINT – Open-Source Intelligence:
- GHDB & Google Dorks
- FOCA & Metadata
- Shodan
- have I been pwned
- the hashed
- Linkedin enum
- The harvester
- Build your own fake identity
- Social Enum
- OSINT framework as a concept
- Whois
- Maltego

"במהלך הקורס המרצה יציג ממצאים שמצא לאורך הקריירה וימקד את התלמיד לפיתוח חשיבה יצירתית"

התקפות תשתית

Phishing והנדסה חברתית:
- SMS phishing
- Website phishing:
- spear phishing
- how to buy a domain
- URL obfuscation
- Site mirror
- Hiddeneye
- Setoolkit

Mail phishing:
- SPF, DKIM & DMARC
- Gophish
- How to build a phishing infrastructure
- Mail spoofing

Malwares:
Msfvenom:
- Trojan payload
- Demonstrate how to hack a windows machine

MSF Suite:
- General handler
- Meterpreter and additional payload types
- Encoders
- Bind & Reverse shell

התקפות באמצעות Microsoft Office:
- Macro
- VBS
- CSV Injection
- PowerPoint exploitation
- SFX
- Macro obfuscation
- PDF Shell – History

מציאת פגיעויות:
Metasploit Suite:
- Exploit
- Vulnerability
- ExploitDB
- Searchsploit

Well known exploits:
- Etternal blue
- Nightmare
- Bluekeep
- Zero logon
- Smbghost
- Sigred

הסלמת הרשאות מקומית ב-Windows:
Windows local:
Local users:
- Regular user
- Local admin
- NT Authority

Boot process:
sethc.exe attack:
- net user
- net localgroup
- bitlocker
- ATP protection bypass

Windows post exploitation:
Hiding a user:
- Hide from net user
- Hide from logon screen

חיפוש אחר סיסמאות מקומיות:
- Browser
- Wi-Fi
- Registry
- SAM & SYSTEM
- lsass.exe

Mimikatz:
- hide from event viewer
- Procdump
- Rundll
- Manual dump
- PPL bypass

הסלמת הרשאות ע"י חיבור מרוחק ב-Windows:
- Unquoted services
- DLL hijacking

services exploitation:
- winpeas
- Bitlocker bypass
- Kernel issues

סריקות רשת והתקפות לשירותים חיצונית:
- רשת חיצונית ורשת פנימית
- שימוש ב-NMAP
- Masscan
- RustScan

Service brute force:
- hydra
- password spray

Attacks:
- DNS zone transfer
- DOS
- Ping Of Death
- BSOD
- Smurf attack
- Additional DOS techniques
- SMTP attacks

התקפות תשתית

הסלמת הרשאות מקומית ומרוחקת ב-Linux:
- GRUB Exploitation:
- Boot Process
- Encrypting the GRUB
- Shadow and Passwd:
- JtR Brute Force
- Remote Exploitation:
- CRON abuse

הסלמת הרשאות ע"י חיבור מרוחק ב-Linux:
- Kernel issues:
- dirty cow
- Sudo exploits:
- Sudo version exploits
- Wrong permissions
- SUID abuse
- Wrong permissions for sensitive files
- Process exploitation
- Linpeas

הסלמת הרשאות ע"י חיבור מרוחק ב- Windows:
- Unquoted services
- DLL hijacking
- Services exploitation:
- winpeas
- Bitlocker bypass
- Kernel issues

Wireshark:
- Sniffing
- Promosicous mode
- Passive enum
- Pcap
- Statstics
- TCP flow
- Filtering:
- Display filtering
- Hard filtering
- Packets analysis
- Exporting data
- Pcap challenge
- Tcpdump & Tshark
- How to discover if Wireshark exists in the organization

Man in the middle – MITM:
- Arp poisoning
- DNS spoofing
- Bettercap
- Internal:
- ipv6 attacks
- mitm6
- ipv6 neighbors
- ipv6 toolkit
- LLMNR & Responder

סריקות פנימיות ב-Domain:
- Bloodhound & SharpHound
- Ldap enum
- SMB enum
- RPC enum
- Ping castle
- PowerView

שימוש ב-PowerShell כנשק:
- PowerShell Introduction
- IEX bypass
- MSI bypass
- PowerShell to exe
- PowerShell modules
- Turn off firewall
- Turn off ATP
- PowerSploit
- Download files
- Mimikatz Obfuscated
- Nmap
- Keylogger
- Winpwn
- Death star
- Empire

דילוג בין מחשבים:
- Lateral Movement
- תזכורת לשימוש במתקפת Brute Force ושימוש ב-Well known exploits
- Cme
- Printersploit
- Impacket
- SMB relay
- SMB signing
- Psexec
- Wmiexec

השתלטות פנימית בסביבת Domain:
- introduction to Internal Takeover
- DC attacks:
- Golden ticket
- Silver ticket
- Kerberos attacks:
- Kerberoasting:
- SPN
- SREP
- Kerbrons
- Pass the hash & Pass the ticket

Domain Post Exploitation:
- DPAPI exploitation
- Domain replication including shadow copies
- Tunneling and firewall bypass including domain jumping and forest

שיעור תרגול מאסיבי:
- HackTricks
- מוצרים לשימוש

התקפות
Web Applications

30 שיעורים מוקלטים
19 מפגשים
מעבדות תרגול
300 דקות צפייה
95 שעות אקדמיות

מבוא לפיתוח אפליקציית Web:
HTTP protocol:
- Structure
- Status codes
- Methods
- Headers

Client & Server Web technologies:
Client side:
- HTML & CSS & JS & JS Framework

Server side:
- PHP, Python, .NET, JAVA, Node.js
- Web server (engine) OWASP

Developer Attitude:
- SPA
- DOM ROUTING
- Regular routing
- HTML basics

JavaScript:
- JS basics
- JS obfuscation & de-obfuscation

Burp Suite and XSS:
- Burp Introduction
- Thinking of censorship – filtering
- Regex - server side

XSS:
- Stored
- DOM
- Reflected
- Self – xss

Advanced XSS:
- Cookies and Insecure cookies
- Localstorage concept
- Session hijacking
- CSP protection bypass

Databases:
- SQL Concepts
- Database management
- SQL storage
- Massive training

SQL injection:
Sqli concept:
- Error Based
- Boolean Based
- Identification
- Sqlmap

Advanced SQL injection:
- Time Based sqli
- Sqli to RCE
- Blind Sqli

Cross Site Request Forgery – CSRF:
- CSRF concept using GET and POST

CORS & SOP:
- PREFLIGHT
- SAME SITE Cookie

Server Side Request Forgery – SSRF:
- SSRF Identification
- Protection Bypass

XML injection & XXE:
- XML Concept
- The usage of XML
- XML Injection
- OOB and Blind XXE

LFI, RFI, Arbitrary file read & RFD:
- Local file include introduction
- LFI to RCE using log poisoning
- Directory traversal
- Remote File Download
- RFI to RCE

HTTP Smuggling:
- Proxy usage
- Abusing the proxy

Three different techniques of smugglings

Remote Code Execution – RCE:
- RCE as a concept
- Arbitrary file upload
- Command injection
- Code injection

CMS vulnerabilities:
- WordPress exploitation
- Jumla exploitation

חלק ראשון – SSO vulnerabilities:
- SAML

JWT Concept:
- JWT vulnerabilities

OAuth 2.0 exploitation:
- Abusing the usage of JWT
- The combination of CSRF, XSS, etc

חלק ראשון – Minor vulnerabilities:
- Broken authentication

Broken authorization:
- MFA usage
- Usage of default credentials
- lack of anti-automation mechanism
- User enumeration
- Open redirect
- Sensitive information leakage

חלק שני – Minor vulnerabilities:
- Clickjacking
- Information disclosure
- Improper cache handling
- Improper error handling
- Lack of security headers
- Insecure communication channel
- Lack of AV solution
- Response split
- Directory listing

Penetration Testing & Report:
- PT attitude
- Business logic bypass
- Parameter tampering
- Vulnerability scanners
- Sub-domain enum
- Reverse DNS enum
- Juice shop PT

Mobile - חקירת אפליקציות אנדרואיד

15 שיעורים מוקלטים
5 מפגשים
מעבדות תרגול
100 דקות צפייה
25 שעות אקדמיות

מבוא למובייל ואנדרואיד

- מבנה מערכת ההפעלה אנדרואיד
- היכרות עם Android Open Source Project
- היכרות עם אימולטורים המשמשים לחקירה
- היכרות עם ADB
- חקירת מבנה APK

בניית אפליקציה ראשונה לאנדרואיד:
- היכרות עם פיתוח באמצעות Android Studio
- היכרות ראשונה עם JAVA
- בניית אפליקציה פשוטה למחקר

מחקר אפליקציה רשתי:
- ביצוע מחקר באמצעות BurpSuite
- עקיפת מנגנון SSL PINNING
- היכרות עם הכלי Frida

ביצוע מחקר סטטי ודינאמי לאפליקציה:
- מבוא לחקירה סטטית
- Mobsf
- Drozer and emulation
- ביצוע אתגרים

המעבר לתעשייה

- שיעור על בניית קורות חיים
- כיצד עוברים ראיון עבודה

הידעת ?

"אנדרואיד הינה מערכת ההפעלה הנפוצה ביותר בעולם עם 38.61% תפוצה"

נושאי הקורס

שעות אקדמיות (ש"א) בחלוקה לשבעה מודולים	
מודול 1 - מבוא - 10 ש"א	
מודול 2 - תקשורת - 20 ש"א	
מודול 3 - LINUX לינוקס - 35 ש"א	
מודול 4 - PYTHON פייטון - 60 ש"א	
מודול 5 - התקפות תשתית - 115 ש"א	
מודול 6 - התקפות Web Apps - 95 ש"א	
מודול 7 - התקפות Mobile (ניידים) - 25 ש"א	
סה"כ שעות לימוד אקדמיות	**360**

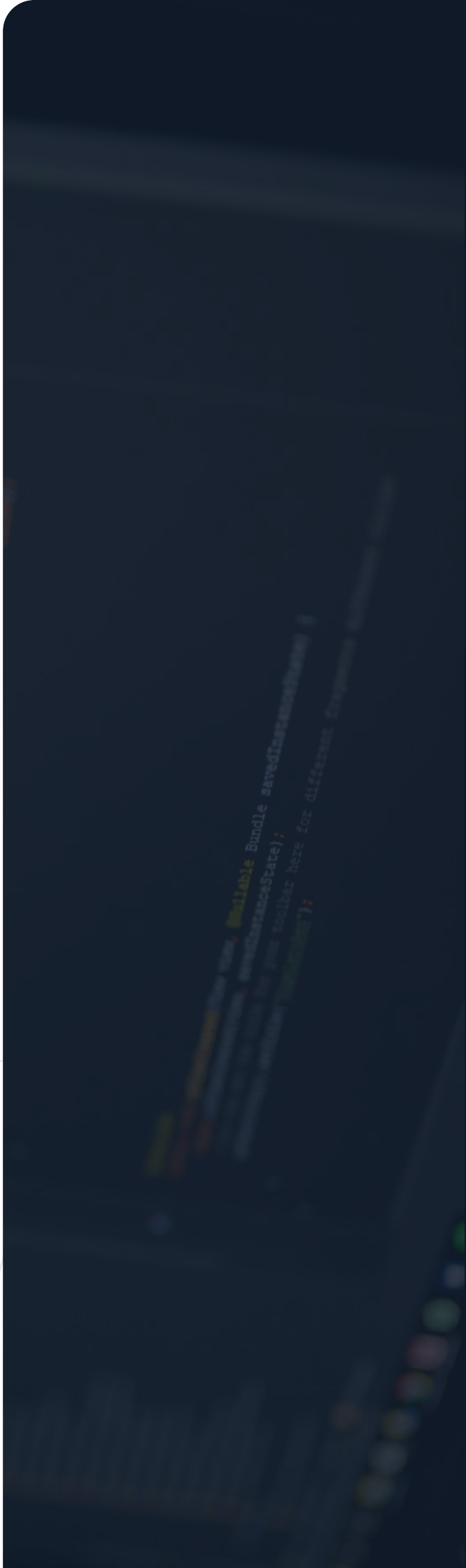
*3952

info@ecomschool.co.il

ecom school

ecom school

053-722-2921

SCAN ME

רמת החייל
ראול ולנברג 22