סילבוס הכשרת Firewall Check Point

ברוכים הבאים לקורס המקיף והמעשי של מכללת Umbrelix ללימוד ופיתוח מיומנויות מתקדמות בתחום Firewall Check Point. קורס זה מיועד לסטודנטים ומקצועי דו המעוניינים להעמיק את הבנתם בתשתיות רשת ואבטחת מידע ברמה המקצועית הגבוהה ביותר.

במהלך הקורס תרכשו כלים מעשיים וידע תיאורטי מוצק הדרושים לניהול, תחזוקה ואבטחה של רשתות ארגוניות מורכבות. הקורס בנוי מארבעה מודולים מקיפים המשלבים בין תיאוריה לתרגול מעשי במעבדות מתקדמות.

מודול 1: יסודות ותשתיות רשת

הכרת האינטרנט

בסיס להבנת תקשורת ואבטחת מידע מודרנית

פרוטוקולי תקשורת

מבוא מקיף ל-IP/TCP ו-OSI - מודלים בסיסיים

כתובות IP ו-Subnetting

יסודות הכתובות ברשת וחלוקת תת-רשתות

המודול הראשון מניח את היסודות החיוניים להבנת עולם האבטחה הדיגיטלית. נתחיל בהכרת תפקיד ה-Firewall באבטחת המידע ונכיר את סוגי Firewalls השונים ותכונותיהם הייחודיות. בנוסף, נכיר פתרונות אבטחה נוספים כמו WAF ו-IPS.

חלק משמעותי מהמודול יוקדש להכרת מערכת הפעלה לינוקס, עולם ה-Virtualization ושימוש מעשי ב-VMware Workstation. נסיים בהתקנה מעשית של סביבת מעבדה עם מערכת ניהול ושרת קצה של Check Point.

סביבת המעבדה והתקנות מערכת

מבוא למערכת הפעלה לינוקס

הבסיס ל-Command Line Interface (CLI) ופקודות חיוניות

הכרת עולם ה-Virtualization

שימוש מתקדם ב-VMware Workstation והתקנת סביבות וירטואליות

התקנת Security Management

הקמת מערכת ניהול של Check Point במעבדה

התקנת Security Gateway

התקנה והגדרה של שרת קצה Check Point

במסגרת זה נלמד שימוש בטופולוגיה ובאובייקטים של הרשת, הבסיס לעבודה מקצועית עם מערכות Check Point.

מודול 2: ניהול מדיניות אבטחה

המודול השני מתמקד בניהול מתקדם של מדיניות אבטחה באמצעות כלי הניהול המתקדמים של Check Point. נתחיל בהכרת SmartConsole ו-WebUI - הכלים המרכזיים לניהול המערכת.

1 יצירה וניהול אובייקטים (Objects)

הכרת סביבת העבודה ב-SmartConsole ויצירת אובייקטים שונים לניהול הרשת

2 ניהול רכיבי NAT

התמחות במערכת Check Point וניהול מתקדם של Network Address Translation

3 יצירה וניהול חוקי Firewall Policy

פיתוח מדיניות אבטחה מקיפה וניהול חוקי Clean-Up

4 התקנת מדיניות אבטחה

יישום והטמעת Policy במערכת ומעקב אחר ביצועים

לוגים, דוחות וניהול משתמשים

ניהול משתמשים וקבוצות

- יצירת Users and Groups במערכת
- הקצאת הרשאות ופריבילגיות
- ניהול Access Control מתקדם

ניתוח לוגים ודוחות

- מבוא ללוגים ולדוחות במערכת Check Point
- ניתוח לוגים באמצעות SmartLog
- זיהוי דפוסי התקפה ואיומים

נלמד שימוש מתקדם באובייקטים של שירות (Service Objects) ובאובייקטים של זמן (Time Objects) ליצירת מדיניות אבטחה דינמית ויעילה. בנוסף, נתמחה בביצוע שינויים ב-Access Control Policy ושימוש ב-Time Objects במדיניות אבטחה.

המודול כולל גם הכרת Zone Based Security של Check Point ושימוש ב-Inline Layers במדיניות אבטחה להגנה מרובת שכבות מתקדמת.

מודול 3: טכנולוגיות מתקדמות ואינטגרציות

המודול השלישי מתמקד בטכנולוגיות מתקדמות ופתרונות אינטגרציה מורכבים של Check Point. נתחיל עם Hide NAT (Dynamic NAT) והגנה מפני זיוף כתובות (Anti-Spoofing) - כלים חיוניים לאבטחת הרשת.

Shared Policy Management

שימוש ב-Shared Policy לניהול מדיניות משותפת ויעיל במספר מערכות Check Point במקביל

HTTPS Inspection

בדיקת תעבורה מוצפנת מתקדמת וטכניקות פיענוח לזיהוי איומים נסתרים

Application & URL Filtering

סינון אפליקציות וכתובות URL מתקדם עם הגדרות מותאמות אישית

Content Awareness I-Identity Management

1

Content Awareness

זיהוי וניהול תכנים ברשת - מניעת דליפת מידע ושליטה על תכנים רגישים העוברים ברשת הארגונית

2

Identity Awareness עם פורטל משתמש

הטמעת מערכת זיהוי משתמשים מתקדמת עם פורטל ייעודי לניהול הרשאות ואימותים

3

Identity Awareness באמצעות Agent

התקנה והגדרה של Agent במערכת Check Point לניטור ובקרה מתמדת של פעילות משתמשים

נלמד הגדרות מתקדמות ל-URL & Application Filtering ב-Check Point, כולל יצירת רשימות מותאמות אישית ומדיניות סינון דינמית המותאמת לצרכי הארגון השונים.

IPS, ו-VPN הגנה מתקדמת

מבוא מקיף למערכת מניעת חדירות (IPS) ב-Check Point - הכלי המתקדם ביותר להגנה מפני איומים מתקדמים ומתקפות סייבר מורכבות.

Cyber Attack Protection	IPS Bypass	IPS Protections
הגנה מפני מתקפות סייבר באמצעות IPS	חריגת תעבורה מ-IPS במקרים מיוחדים	הגנות IPS מתקדמות והתמודדות עם איומים חדשים

Anti-Virus ו-Anti-Bot

הגנה מפני וירוסים ובוטים במערכת Check Point ברמה הארגונית

Data Loss Prevention (DLP)

מניעת דליפת מידע רגיש מהארגון באמצעות טכנולוגיות מתקדמות של Check Point

המודול מסתיים במנגנוני יצירת והגדרת VPN מסוג IPsec ב-Check Point - פתרון מאובטח לחיבור מרחוק ותקשורת מוצפנת בין אתרים.

מודול 4: תחזוקה, גיבויים ותחקור תקלות

המודול הרביעי והאחרון מתמקד בהיבטים המעשיים של תחזוקת מערכת Check Point ברמה הארגונית. נתחיל בביצוע גיבויים ושחזורים במערכת - הליך קריטי לשמירה על המידע והמערכת.

גיבויים ושחזורים

ביצוע גיבויים מתוכננים ושחזור מערכת במקרה של תקלות

ניהול Package Repository

ניהול מאגר חבילות ושדרוג גרסת Check Point לגרסאות עדכניות

Log Exporter

שימוש ב-Log Exporter לייצוא לוגים והעברתם למערכות אחרות

Troubleshooting

פקודות מתקדמות לתחקור תקלות ופתרון בעיות מורכבות

סיכום הקורס והתמחות מעשית

בסיום הקורס תרכשו הסמכה מקצועית מטעם מכללת Umbrelix ויהיו לכם כל הכלים והידע הנדרשים לניהול מערכות Check Point ברמה המקצועית הגבוהה ביותר.

4

מודולים מקיפים

מיסודות הרשת ועד לטכנולוגיות המתקדמות ביותר

+40

שעות למידה

תיאוריה ותרגול מעשי במעבדות מתקדמות

100%

התמחות מעשית

עבודה עם מערכות אמיתיות וסביבות מעבדה

ערך מוסף מיוחד: הקורס כולל פקודות לינוקס שימושיות למנהלי Check Point - ידע חיוני לעבודה יעילה ומקצועית עם המערכת.

מכללת Umbrelix מזמינה אתכם להצטרף לקורס המוביל בתחום ולרכוש מיומנויות מבוקשות בשוק העבודה הישראלי והבינלאומי. ההרשמה פתוחה עכשיו!