



ספר קורס



אבטחת נקודת קצה

עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

מידע על ספר לימוד זה

מסמך זה הוא ספר לימוד עבור הקורס תשתיות וטכנולוגיית סייבר בשלמותו. הוא מכיל את כל המידע שהמנחה יציג בכיתה.

ספר הלימוד מלווה את הקורס כולו, לפי סדר כרונולוגי, משלב ההתחלה ועד לחומר המתקדם של הקורס.

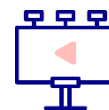
מקרא

קטעי טקסט צבעוניים מופיעים לאורך מסמך זה כדי להפנות את הקורא למקור ספציפי, או להעשיר אותו במידע נוסף.

קטעי הטקסט הצבעוניים כוללים את הנושאים הבאים:

משימת מעבדה

יש לעיין בקבצי המעבדה התואמים כדי לתרגל את מה שנלמד עד כה. תיבת טקסט זו כוללת גם שאלות ספציפיות לתרגול.



טוב לדעת

מידע נוסף או תובנות לגבי הנושא. מידע זה נועד לצורך העשרה בלבד ואינו חלק מהחומרים עליהם תיבחנו.



טיפ

מידע שימושי שיש בו כדי לסייע לתלמידים ללמוד את החומר או לעבוד עם כלים מסוימים.



מידע נוסף

קישורים או הפניות לחומר חיצוני שניתן להשתמש בהם כדי להרחיב את הידיעות שלכם לגבי הנושא.



אבטחת נקודת קצה (Endpoint Security)

פרק זה מציג את הרעיון וההתפתחות של פתרון אבטחת נקודות הקצה, מדוע הוא נחוץ, אילו שירותים הוא מספק וכיצד שירותים אלו פועלים. חקירה של ClamAV, הנתמכת בדוגמאות ותרגילים מעשיים.

פרק זה כולל את הנושאים הבאים:

- מבוא לאבטחת רשת ונקודת קצה
- תקלות וסיכונים
- רכיבי אבטחת נקודת קצה
- איתור ותגובה של נקודת קצה
- מבוא ל-ClamAV
- כללים וחתימות של YARA
- מסד נתונים ליצירת רשימת היתרים (Whitelist)

חלק 1: מבוא לאבטחת רשת ונקודת קצה

חלק זה מספק רקע על אבטחת סייבר בארגון ומסביר את הצורך בפתרונות אבטחת נקודות קצה. הוא גם מלמד את היסודות של תוכנות אנטי-וירוס וכיצד הן פועלות.

מה הוא פתרון אבטחת נקודת קצה?

חשבו על היקף אבטחת הסייבר של ארגון ממוצע, שהוא קו ההגנה הראשון מפני פולשים זדוניים. בדרך כלל יש לו נקודת כניסה אחת, **הנתב או חומת האש בנקודת הקצה**. מאחוריהם, נמצאים המתגים (switches) והמארחים (hosts). נתב נקודת הקצה הוא הנקודה היחידה שדרכה עוברת כל התעבורה אל הרשת הארגונית וממנה. מודל זה מייצג את היקף אבטחת הסייבר המסורתי.

עם זאת, התוספת של מחשוב ענן וטכנולוגיה ניידת, לצד הרגלי עבודה כגון BYOD (Bring Your Own Device) מוסיף למעשה את היקף אבטחת הסייבר המסורתי, כך שעלה צורך בגישה חדשה לגמרי לאבטחת סייבר עבור ארגונים.

וכאן נכנס הנושא של פתרונות לאבטחת של נקודות קצה.

פתרונות אבטחת נקודות קצה הם חבילה של כלים המגנים באופן אקטיבי על תחנות עבודה או מכשירי משתמשי קצה בעלי גישה למשאבי החברה (מחשבים שולחניים, מחשבים ניידים, מכשירים ניידים אישיים), מפני רוב וקטורי ההתקפה. הכלים כוללים פתרונות אנטי-וירוס, מערכות זיהוי פריצה מבוססות מארח (HIDS), מערכות למניעת פריצה מבוססות מארח (HIPS), בקרת יישומים, בקרת מכשירים ומניעת דליפת נתונים מבוססת מארח (DLP).

לפני שמתירים למכשירים שלא הונפקו על ידי הארגון לקבל גישה למשאבים ממיקומים חיצוניים לרשת הארגונית, יש ליצור תקשורת מוצפנת נאותה בצורה של רשת פרטית וירטואלית.

בנוסף, אם עובדים מסוגלים להוריד למכשירים שלהם חומר שעשוי להיות מסווג (כונני פלאש, mass storage וכו'), חייבת להיות מערכת להקשחת האבטחה במכשירים אלה. המערכת צריכה להיות אפליקציית בקר התקנים שהיא חלק מאבטחת נקודות הקצה, המאפשרת הטמעת מדיניות ממסוף ניהול מרכזי.

חבילת אבטחת נקודת קצה

➤ **תוכנות אנטי-וירוס/נגד תוכנה זדונית:** הן פתרון האבטחה הנפוץ ביותר הקיים ברוב המחשבים הביתיים והארגוניים. תוכנות אלה פועלות על ידי השוואת חתימות קבצים מול מסד נתונים של קבצים זדוניים ידועים, וניתוח התנהגות של תוכנות המכונה זיהוי היריסטי.

➤ **מניעת אובדן נתונים (DLP - Data Loss Prevention):** ערכת כלים המשמשים לסיווג ולמניעת אובדן, שימוש לרעה או גישה בלתי מורשית של נתונים רגישים.

סוגי הכלים כוללים:

מבוססי-אסימון: משתמשים במילות מפתח קבועות לצורך זיהוי.

מבוססי-ביטויים נפוצים דפוסים גנריים מאפיינים משפחות של נתונים רגישים, כגון מידע זיהוי אישי (PII).

מבוססי חתימה מותאמת אישית למשתמש: חתימות ספציפיות הקשורות לצרכי הלקוח.

➤ **בקרת יישום/רשימות היתרים:** ממפה רשימה של יישומים בנקודת קצה ושולטת בשימוש בהם. ניתן לחסום, לאפשר או להגביל יישומים על ידי חסימת שירותים או תהליכי יישום מסוימים בלבד.

מערכת מבוססת-מארח למניעת חדירות/גילוי (HIPS/HIDS): מאחסנת מוד נתונים של אובייקטי מערכת ותכונותיהם.

המערכת יוצרת סיכומי ביקורת (checksums) של האובייקטים (בדרך כלל MD5 או SHA1) ומאחסנת אותם במסד נתונים מאובטח לבדיקה מאוחרת יותר כדי לזהות או למנוע שינויים שנעשו על ידי ישויות לא ידועות, ואולי אף זדוניות. פתרונות HIPS עשויים לעקוב אחר שינויים במערכת הקבצים שאינם מרמזים בהכרח על קוד זדוני. הם יכולים לנתח קבצי יומן ולבדוק רכיבי מערכת כדי לזהות אי סדרים וחריגות. מבוססי-אסימון: משתמשים במילות מפתח/ hashes קבועים כדי לזהות התקפות זדוניות ידועות. מבוססי ביטויים נפוצים: משתמשים בדפוסים גנריים שונים כדי לאפיין התקפות ידועות כמו WannaCry. מבוססי חתימה מותאמת אישית למשתמש: משתמשים בחתימות ספציפיות הקשורות לצרכי הלקוח.

הצפנת תקשורת: היכולת להקים VPN (רשת פרטית וירטואלית) דרך IPsec או שיטת תקשורת מוצפנת אחרת, כאשר כל צד רוצה להתחבר לרשת הארגונית, בין אם מסניף אחר של הארגון ובין אם ממכשיר משתמש קצה.

דוא"ל והגנה מפני פשינג: צורה הכרחית נוספת של הגנה על תקשורת היא היכולת לסרוק את כל הודעות הדוא"ל הנכנסות והיוצאות לאיתור עומסים זדוניים אפשריים בכל חלק של הדוא"ל עצמו (כותרת, גוף וכו') ובקבצים מצורפים. מכיוון שהודעות דוא"ל פשינג הופכות ליותר ויותר חכמות, וקשה יותר להבחין ביניהן לבין הודעות דוא"ל אמיתיות, אפילו המשתמשים הערניים ביותר יכולים ליפול בפח ברגע של הסחת דעת.

רישום וניטור: איסוף יומני אבטחה כגון הפרת גישה ואימות כושל לניטור התקני משתמש קצה וזיהוי איומים בזמן אמת או לניתוח במועד מאוחר יותר. פתרון אבטחת נקודות קצה צריך לכלול חלק מהטכנולוגיות שהוזכרו לעיל או את כולן, בנוסף לאמצעי אבטחה אחרים.

אנטי-וירוס - מבט מקרוב: סריקה

אנטי-וירוס (AV) פועל על ידי סריקת קבצים והשוואת חתימותיהם למסד נתונים של חתימות קבצים זדוניים. תהליך זה נקרא זיהוי ספציפי, והוא מחפש מספר דברים:

➤ **חתימות מחרוזת/בייט:** קבצי הפעלה מורכבים מביטים או מחרוזות של ביטים בדפוסים ספציפיים. הדפוסים משתנים בין קבצי הפעלה השונים. מסד נתונים של תוכנות אנטי-וירוס זדוניות מורכב מתבניות של דפוסים אלה. על ידי השוואת הדפוס שנשרק לתבניות במסד הנתונים שלו, אנטי-וירוס יכול לזהות דפוסים זדוניים.

➤ **חתימות Hash:** אלגוריתם hash הוא פונקציה חד-כיוונית שלוקחת קלט בכל אורך וממירה אותו למחרוזת בגודל קבוע של תווים ייחודיים באמצעות פונקציה מתמטית. ישנם שלושה רכיבים המשמשים בתהליך גיבוב (hashing), **הקלט** (מה שאנו מנסים לגבב), **פונקציית ה-hash** (אלגוריתם הגיבוב שבו אנו רוצים להשתמש), ו**ערך ה-hash** (מחרוזת הטקסט המתקבלת). זה כמעט בלתי אפשרי לייצר אותו ערך hash מקלט שונה. השינוי הקל ביותר בקלט יכול לייצר ערך hash שונה לחלוטין. המשמעות היא שלכל אלגוריתם גיבוב יש רק גיבוב אחד אפשרי עבור אותו קובץ. זה מאפשר לאנטי-וירוס להשוות חתימות hash זדוניות ידועות לקבצים שהוא סורק.

עד כה, סקרנו את הדרכים שבהן אנטי-וירוס סורק ומזהה תוכנות זדוניות ידועות. לספקי אנטי-וירוס יש מסדי נתונים עצומים של חתימות מוכרות, ומסדי הנתונים ממשיכים לצמוח בין היתר בשל קהילת מומחי אבטחת הסייבר שמספקים דוגמאות של תוכנות זדוניות חדשות שמצאו.

עם כל מדגם חדש, מסד הנתונים גדל, ומתגלים קווי דמיון בין תוכנות זדוניות. קווי דמיון אלה מובילים ליצירת משפחות של תוכנות זדוניות, קבוצות של תוכנות זדוניות שחולקות בסיס קוד משותף. ממידע זה נוצר גם **זיהוי גנרי (generic detection)**, שמחפש תוכנות זדוניות שהן גרסה של משפחות מוכרות.

זיהוי היוריסטי (Heuristic detection) מחפש וירוסים לא ידועים על ידי חיפוש אחר התנהגות חשודה ידועה או מבני קבצים ידועים. איתור היוריסטי בוחן קבצים כדי לזהות כל דבר חריג. הוא מחפש אחר פרמטרים כמו מבנה מוזר או התנהגות שונה מזו של קובץ תמים. זיהוי היוריסטי פועל גם באזורים אפורים כדי לבחון קבצים עם כמה תכונות שליליות וכמה חיוביות.

להלן תכונות מפתח של זיהוי היוריסטי:

- הוא מבוסס על ציון אינדיקציה לסיכון (IOC) עבור כל פעילות תהליך בנקודת הקצה. המנוע מאפיין את הזרימה בכל תחנת עבודה וקובע ציון של אמון, שעשוי לכלול למשל תקשורת למטרות או משאבים לא ידועים.
- כל לקוח יכול להגדיר את רמת הרגישות (נמוכה, בינונית, גבוהה).
- ככל שרמת הרגישות גבוהה יותר, כך מיושמות יותר הגבלות.

ספקים נפוצים וכיסוי

לפתרונות האבטחה של נקודות הקצה המפורטים להלן יש יכולות דומות והבחירה ביניהם היא עניין של העדפה אישית וניסיון. לכל ספקי האנטי-וירוס הגדולים יש מגוון שירותים שיכולים להגן על המחשב לא רק מפני וירוסים הנכנסים באמצעות הורדות, אלא גם מפני תוכנות זדוניות שמתפשטות מכונן נייד או מהרשת. אלו הם רק חלק מהשירותים העקביים בין McAfee, Kaspersky, Check Point, Symantec:

- הגנה בזמן אמת
- חומת אש של המארח
- בקרת יישומים
- בקרת מכשירים
- הגנת רשת
- הצפנת דיסק מלאה
- הגנת USB
- EDR
- ארגז חול (Sandbox)
- אנטי-ספאם ואנטי-פשינג
- הגנת יום אפס
- אנטי-כופרה
- ניהול מרכזי

סריקת אנטי-וירוס מרובת מנועים

כל תחנת עבודה צריכה לכלול אנטי-וירוס אחד בלבד. יש לציין כי התקנת יותר מתוכנת אנטי-וירוס אחת במערכת תצרוך יותר מדי משאבים ועלולה ליצור התנגשויות בין הספקים. תוכנות אנטי-וירוס שונות משתמשות במתודולוגיות וברשימות שחורות שונות, והתקנת תוכנות אנטי-וירוס שונות עלולה להוביל להתנגשויות בין רשימות שחורות ולתחזוקה מורכבת.

חלק 2: תקלות וסיכונים

בחלק זה, נבחן סיכונים פוטנציאליים נפוצים, בעיות בתוכנת אנטי-וירוס ודרכים לצמצם אותן.

False Negative ו- False Positive

תוצאות חיוביות כוזבות (false positives) קיימות בכל מנגנון בדיקה. בדיקה שמצביעה על כך שתנאי מתקיים (true) כשהוא לא באמת מתקיים, יוצרת תוצאה חיובית כוזבת. תוצאה שלילית כוזבת (false negative) היא כאשר תוצאת הבדיקה מעידה באופן שקרי על היעדר קיומו של תנאי.

תוצאות כוזבות באבטחת סייבר עלולות להוביל להשלכות משמעותיות על ארגון. בין אם כתוצאה מתוצאה חיובית כוזבת המעידה על תוכנה זדונית, הדורשת זמן וכסף לתיקון, או שלילית כוזבת המאפשרת לפורץ להיכנס לרשת החברה, הנזקים עלולים להיות חמורים.

הגורמים לתוצאות חיוביות ושליליות כוזבות

תוצאות חיוביות כוזבות יכולות להיות תוצאה של מספר גורמים:

היוריסטיקה (כללי אצבע)

ספקי אנטי-וירוס משדרגים כל הזמן את המוצרים ואת מסדי הנתונים של תוכנות זדוניות כדי לעמוד בקצב השוטף של התוכנות הזדוניות המתפתחות. האקרים כל הזמן מחפשים דרכים להסוות את התוכנה הזדונית שלהם על ידי חיקוי ההתנהגות הלגיטימית של משתמש או של מערכת. בניסיון ללכוד את כל הפעילות הזדונית, לעתים מייצרת היוריסטיקה תוצאות חיוביות שגויות. רוב ספקי האנטי-וירוס מספקים אפשרות להעלות או להוריד את רמת הרגישות של תוכנת האנטי-וירוס. ככל שהרמה גבוהה יותר, כך גדל הסיכוי לספק תוצאות חיוביות שגויות.

ניתוח התנהגותי

למרות שאנטי-וירוס מזהה התנהגויות ספציפיות כזדוניות, עלולה להתרחש טעות בזיהוי, כגון אי יכולת להבחין בין תוכנת הצפנה לגיטימית לבין וירוס WannaCry, שגם מנסה להצפין תיקיות וקבצים של תחנת עבודה.

למידת מכונה

ספקים מזינים לתוכנות האנטי-וירוס נתוני הכשרה כדי שיוכלו ללמוד לזהות בעצמן תוכנות זדוניות חדשות. אולם, הכמות העצומה של הנתונים עלולה לגרום לטעויות או אי בהירות שיובילו לזיהוי שווא.

יום אפס

ניצול יום אפס הוא פגם בתוכנית שלא התגלה או שהתגלה אך לא תוקן. ניצול יום אפס יכול להיות רדום שנים לפני שיתגלה. שני הצדדים (התוקפים והמגנים) מעוניינים בסוג זה של ניצול באותה המידה, אך מסיבות שונות. האקרים מזהים נקודות תורפה שאינן ציבוריות ומנצלים אותן לפני שהספק יוכל ליצור תיקון.

שיטות לעקיפת אנטי-וירוס

אריזה והצפנה

אריזה היא שיטה המסייעת להימנע מזיהוי מבוסס חתימה על ידי הסתרת החתימה של קובץ ההפעלה המקורי באמצעות הקובץ הדחוס. מכיוון שבדרך כלל, קוד ההרצה מפורק בזיכרון זמני, ייתכן שהזיהוי יימנע. ההצפנה לא תאפשר לתוכנת האנטי-וירוס לגלות מה יש בתוך קובץ ללא המפתח הנדרש כדי לפענח אותו.

מוטציית קוד

מוטציות מוטמעות אוטומטית בקוד התוכנה הזדונית, ויוצרות וריאציות מעט שונות במטרה להימנע מזיהוי.

טכניקות התגנבות

בטכניקות התגנבות משתמשים כדי לשנות או להגביר את ההתנהגות של מערכת הפעלה, יישומים או תוכנות על ידי יירוט קריאות פונקציה, הודעות או אירועים המועברים בין רכיבי תוכנה. הקוד שמטפל ביירוטים נקרא Hook. רוב טכניקות ה-hooking מבצעות מניפולציה של סריקת API במוצרי אנטי-וירוס, וגורמים להם לא לכלול קבצים זדוניים כדי שלא ייסרקו בתחנת העבודה.

השבתת עדכוני אנטי-וירוס

תוכנת אנטי-וירוס תלויה במסד הנתונים של החתימות. כל וירוס מושווה לבסיס הנתונים, ואי עדכון האנטי-וירוס עלול לאפשר לו וירוסים חדשים שאינם רשומים במסד הנתונים הנוכחי להיכנס אל המערכת.

טוב לדעת

השבתת עדכון אנטי-וירוס מתבצעת על ידי שינוי הקובץ **hosts** כדי להפנות את שם הדומיין של ספק האנטי-וירוס אל ה-**localhost**.
דוגמה לשינוי בקובץ מארחים: 0.0.0.0 Eset.com



מתקפה נטולת קבצים

התקפות מסוג זה ידועות גם כמתקפות עם אפס טביעת רגל (Zero footprint attacks) או התקפות ללא תוכנות זדוניות. התקפות מסוג זה אינן מתקינות תוכנה חדשה במחשב, ולכן סביר להניח שכלי אנטי-וירוס יחמיצו אותן. לרוב, התקפות כאלה מריצות את המטען הזדוני מ-RAM.

משימת מעבדה: עקיפת אפליקציית אנטי-וירוס

יש להוריד קבצי EICAR ולהצפין אותם כדי למנוע זיהוי על ידי סורקי VirusTotal.

