צוות אדום ותפקידו במבדקי חדירות

מאת רועי שרמן

הקדמה

במאמר זה אסביר את המושג "צוות אדום", איך מתבצע פרוייקט צוות אדום ומה התועלת שלו ולמה יותר ויותר ארגונים בוחרים לבצע בדיקה מסוג זה.

מהי ההגדרה לצוות אדום?

צוות אדום הינו קבוצה של אנשים, אשר תפקידם לשחק את תפקיד האויב ובכך באמת לתרגל את הכוחות הפועלים בארגון (ארגון צבאי, ממשלתי, פרטי או עסקי). לעומתם קיים הצוות הכחול, אשר אמון על הגנת הארגון ותגובה למקרי תקיפה. צוות אדום הינו מושג אשר נקשר להמון פעילויות במגוון רחב של תחומים (צבאיים, מודיעיניים, ועוד). במאמר זה אנו נתמקד במשמעות המושג "צוות אדום" בהקשר של מבדקי חדירות וייעוץ.

מה הם מבדקי חדירות?

מבדקי חדירות הינם בדיקות למערכות מידע, אפליקציות, תשתיות ושאר רכיבי הטכנולוגיה בארגון, על ידי הדמיה של תקיפה על ידי האקרים, תיעוד התהליך והמצאת דוח מפורט אשר כולל את פרטי החולשות שגולו, הוכחה ליכולת שימוש בחולשות אלו והמלצות לתיקונם. בדיקות אלו מתבצעות על ידי יועצי אבטחת מידע (ידועים גם כפנטסטרים, האקרים כובע לבן והאקרים אתיים).

בעולם מבדקי החדירות ישנם שלוש מתודולוגיות עיקריות: קופסא לבנה, אפורה ושחורה. בקופסא הלבנה, הבודקים מקבלים את כל הפרטים האפשריים על המטרה, כולל קוד-מקור (אם קיים), מבנה המערכת ומגבלות ולאחר מכן מתחילים לנסות לפרוץ את המערכת. בקופסא האפורה, הבודקים מקבלים חלק מפרטים אלו ובקופסא השחורה הם אינם מקבלים פרטים כלל, למען הפרטים ההכרחיים (שם האפליקציה, הלקוח, וכד'). בנוסף ישנם סוגי בדיקות רבים, הקשורים לתחום הבדיקה, כגון אתרי אינטרנט, תשתיות, מוּדָעוּת (פישינג), בדיקות מוצר, ארכיטקטורה ועוד. בכל סוגי הבדיקות הללו, הגורמים בארגון אשר קשורים לפיתוח ו\או תחזוקת המערכת מודעים לביצוע הבדיקה. במאמר זה נתמקד בסוג בדיקה מסוים, הנקרא צוות אדום.

מה המגבלות של מבדקי חדירות "רגילים"?

כיום רוב הארגונים מבינים את הערך הקיים בבדיקות חדירות, אשר מקנים לארגון את האפשרות לקבל את זווית הראייה של האקרים כובע-לבן בנוגע למוצרים ולמערכות בארגון, חשיפה של חולשות אבטחה בהן (הנובעות מגורמים שונים) ואפשרות לתקן אותם (ולתקן נכון) על מנת למנוע ניצול שלהם על ידי גורמים זדוניים.

בדיקות אלה ברובן מוגבלות יותר מסוגן, ומתרכזות במערכת ספציפית, או מרכיב שלה ובכך הבדיקה אינה יכולה לכלול השפעות של מערכות או רכיבים שונים בסביבתה אשר יכולים לשנות את פני התמונה. למשל, יכול להיות שאחד מאתרי החברה נבדק ובסוף הפרויקט לא נמצא שום ממצא אשר יכול להעיד על יכולת להיכנס לתוך שרתי החברה, אך אם הייתה נבדקת הרשת בכללותה, או כלל השרתים החשופים לאינטרנט, אולי שרת הדואר היה מציג תמונה שונה?

בנוסף, בבדיקות של מערכת או חלק ייעודי מהרשת לא נלקח בחשבון הצוות הכחול אשר אמון על ניטור הרשת ותקריות ותפקידו להגיב במידה ומתבצעת תקיפה, ליידע ולהזניק את הגורמים הרלוונטיים ובמידת הצורך לחסום את התוקף. יתרה מזאת, במידה ומותקנות בארגון מערכות הגנה מתקדמות לזיהוי איומים, או אפילו מערכות הונאת תוקפים (Deception), האפקטיביות שלהם אינה נלקחת בחשבון בבדיקות מהסוג שתואר למעלה, אך בבדיקות צוות אדום, התמונה משתנה לחלוטין ובכך הצוות האדום, מעבר לבדיקה של בגרות האבטחה הארגונית, גם עוזר לתרגל ולמדוד את יעילות המערכות והצוותים הכחולים.

בנוסף, ההבנה הכללית של תועלת בדיקות החדירות עזרה לרתום חברות רבות לתהליך ולהירשם לתוכניות Bug Bounty, או מקימות תכניות מקבילות משלהן, על מנת למשוך חוקרים עצמאיים לבדוק את המערכות שלהם, למצוא פרצות אבטחה ולדווח עליהן לארגון על מנת שיוכל לתקן אותם ולמנוע שימוש לרעה בהן על ידי גורמים זדוניים. בתוכניות אלו ניתן למצוא חברות ענק (Facebook, Google), סטארט אפים קטנים ואפילו סוכנויות ממשלתיות (USA Department of Defense) וניתן גם למצוא תוכניות אשר מתקיימות על ידי מתווכחים כמו: HackerOne, Bugcrowed ונוספים.

לפני שנפנה לסקור את צורת הפעולה של צוות אדום ותפקידו במבדקי חדירות, יש להבין את אורח החיים של תקיפה סטנדרטית (לשם כך נדמה בדיקה של ארגון פיקטיבי בשם "גיבסון", אשר המטרה שהוגדרה על ידיו היא לגנוב מסמכי פטנטים):

1. **מחקר ואיסוף מודיעין (Research & Reconnaissance) -** השלב הקריטי ביותר. בשלב זה התוקף מתחיל לאסוף מידע על המטרה שלו ומשתמש בעצם בכל מקור מידע אפשרי, בין אם זה על בעלי תפקידים ברשתות חברתיות (לינקדאין, פייסבוק וכו'), כתובות מייל של הארגון, סוגי מערכות ההגנה בשימוש (על ידי סקירה של מודעות דרושים), מיפוי שרתים ונכסים אשר זמינים מהאינטרנט, רישום בעלי תפקידים עיקריים ודרכי יצירת קשר איתם, מיקומים של משרדים ועוד.

בבדיקה שלנו, אנו נתחיל לחפש באינטרנט את שם הארגון ולנסות לאתר עובדים שהזינו את שם הארגון כמעסיק בלינקדאין. נריץ כלים (The Harvester לדוגמא), עם שם הארגון, כדי לייעל את החיפושים ולאסוף כתובות אי מייל של עובדים ותוצאות ממנועי חיפוש שונים. את כל התוצאות נתעד ונשמור להמשך התהליך. במקביל, נשתמש במנועי חיפוש ייעודים, כמו Shodan ו-Censys על מנת לנסות לאתר נכסים של "גיבסון" שחשופים לאינטרנט ואיזה פורטים פתוחים בהם. למשל שרת SMTP שפורט 25 פתוח וניתן להשתמש בו ל-Mail Relay.

2. **תקיפה ראשונית (Initial Attack) -** כאן וקטור התקיפה ישתנה בהתאם למידע אשר נאסף בשלב הקודם. התוקף, לאחר שיסקור את המידע שנאסף, יבחר וקטור תקיפה ויתאים את כליו על מנת לנצל את הפרצה במלואה. למשל, אם זוהו אתרי אינטרנט אשר פגיעים לחולשה, אולי יבחר לנצל אותה? אולי יעדיף לבחור בפישינג, אם בחר בפישינג, יבחר אם להוסיף קובץ זדוני למייל, אולי מייל עם לינק שיבקש מהמשתמש את הסיסמא שלו ואולי בכלל יבחר לנסות לקרבת המשרד ולפרוץ את הרשת האלחוטית?

במקרה של גיבסון, בחרנו לשלוח פישינג. אנו יוצרים מסמך פרסומת, של הנחה לעובדי הארגון בבית הקפה שפועל ליד המשרד, הקופון נשמר בקובץ PDF שמצורף לאימייל ומכיל קוד מאקרו זדוני, שבעת ההרצה מתחבר לשרת שליטה של הצוות האדום.

3. **דריסת רגל (Initial Foothold) -** זהו השלב בו התוקף הצליח לחצות לראשונה את מערכות ההגנה של הארגון ולהיכנס לתוכו. בין אם נכנס לרשת הארגונית דרך הרשת האלחוטית, בין אם גרם לעובד להריץ קובץ עם קוד זדוני, או אולי אפילו, נכנס למשרדים לתוך חדר ישיבות וחיבר מכשיר לאחד מחיבורי הרשת בקירות.

מזל טוב! מנהלת המשרד של גיבסון פתחה את המייל ופתחה את הקובץ המצורף! יש לנו חיבור לתוך רשת הארגון, ברמת ההרשאות של מנהלת המשרד.

4. **תמידיות (Persistency) -** בשלב זה התוקף יחפש כיצד הוא יכול לייצר מצב שבו לא יאבד את הגישה שהשיג. בין אם זה לשתול קוד אצל המשתמש, בשרתים, אולי מפתחות ברג'יסטרי, משימה מתוזמנת או כל דרך אחרת, כך שהחיבור שנוצר יישמר והוא יוכל להמשיך לפעול לאורך זמן ומתחת לרדאר.

בתוך החיבור שנוצר, אנו נריץ פקודה על מנת לרשום משימה מתוזמנת (Scheduled task) שתריץ פקודה שתיצור חיבור חדש כל יום ב-12 בצהריים. כך שאפילו אם המשתמשת תתנתק מהאינטרנט, או תבצע ריסטארט, כל יום יווצר לנו חיבור חדש.

5. **איסוף מודיעין פנימי (Internal Reconnaissance) -** השלב הזה מאוד דומה לשלב הראשון, אך ההבדל העיקרי הוא שהוא מתבצע פנימה, אל תוך מערכות הארגון. התוקף ינסה למפות את הארגון והרשת מבפנים, איפה ממוקמים שרתים ואיזה תפקידים הם ממלאים, לאיזה משתמשים יש הרשאות גבוהות ועל איזה חלקים מהרשת וכמובן, באיזה מהשרתים נמצא מידע שיועיל לו להשלים את המשימה שלו.

בשלב זה נתחיל לתשאל את ה-DC של הארגון על מנת לנסות לאתר את הכתובת שלו, נבדוק את רמת ההרשאות של המשתמשת שפתחה את הקובץ, ננסה לאתר שרתים נוספים ברשת, נבדוק מה הגדרות ה-GPO שחלות בארגון, מורכבות הסיסמאות (לפריצה עתידית של Hashes) ומיקומים של תיקיות רשת והמידע שנמצא בהם.

6. **העלאת הרשאות (Privileges Escalation) -** בשלב זה התוקף ירכז את מאמציו על מנת לקבל עמדת שליטה חזקה וגבוהה יותר על הרשת ועל הארגון, על ידי גניבת סיסמאות או האשים, ניסיון לנצל חולשות אבטחה פנימיות בחלק מהמערכות ואולי אפילו על ידי ניצול משתמש חלש שהוא הצליח להשתלט עליו, כדי לתקוף משתמשים חזקים יותר.

לאחר שמיפינו את הרשת הפנימית, אנו רוצים לחזק את השליטה והיכולות שלנו. נבדוק את רמת ההרשאות של המשתמשת שלנו. היא לא אדמין לוקאלי על העמדה. נחפש פירצת אבטחה שתאפשר לנו להעלות הרשאות (אפליקציה פגיעה שרצה בהרשאות גבוהות או חולשה במערכת ההפעלה, מה שנוצל, יתועד לטובת הדוח בסוף הפרוייקט) וכרגע רמת ההרשאות שלנו היא אדמין על העמדה הלוקאלית. עכשיו נשתמש בכלי אחר, על מנת לגנוב סיסמאות של משתמשים אחרים שהתחברו לעמדה הזו בעבר, אחד מהם הוא דומיין אדמין. כרגע יש לנו שליטה מלאה על הרשת.

7. **תנועה רוחבית (Lateral Movement) -** בשלב זה התוקף מנסה לנוע בין מערכות ו\או רשתות ברשת, על מנת לנצל את המידע ורמת ההרשאות שהושגו בשלבים קודמים כדי להגיע ולהשתלט על מערכות ורשתות נוספות ובמידת הצורך, יחזור בהן על השלבים הקודמים (איסוף מידע פנימי והעלאת הרשאות).

לאחר שהעלנו את רמת השליטה שלנו ומיפינו את הרשת הפנים-ארגונית, אנו יודעים מה הוא שרת הקבצים. נבצע תנועה רוחבית על מנת ליצור חיבור נוסף מתוך השרת הזה, תוך שימוש בשם המשתמש והסיסמא של הדומיין אדמין וכרגע יש לנו שליטה מלאה על שרת הקבצים.

8. **איסוף והצפנת מידע (Gather & Encrypt Data) -** כאן כבר התוקף הצליח להשיג את המידע שחיפש (לרוב זה יהיה מידע סודי ו\או מסווג, PII Personally Identifiable Information), מידע עסקי,

מידע מפליל (עסקי או אישי) וסודות ארגוניים. התוקף יאסוף את המידע והזה ויצפין אותו על מנת לסחוט את החברה, או על מנת להוציא אותו החוצה מהחברה ולהימנע מזיהוי של המידע בעת ההעברה.

נתחיל לחפש שמות של קבצים ותיקיות שמכילים את המילה "פטנט", נאסוף את כולם לתיקייה אחת, נכווץ ונצפין אותה.

9. **הוצאת המידע (Exfiltration) -** לאחר שהמידע נאסף והוצפן, במידה וסחיטה אינה אחת ממטרות התוקף, הוא ינסה להוציא את המידע החוצה מגבולות הארגון, למקור אחר אשר תחת שליטתו ואשר יאפשר לו לעבור על המידע מאוחר יותר ולסנן אותו ואולי אף למכור או להעביר אותו לגורמים אחרים.

לאחר שסיימנו לאסוף את כל המסמכים שרצינו, נוציא את המידע מהארגון למחשב בשליטה שלנו, שממוקם מחוץ לארגון.

10. **ניקיון והסרת ראיות (Evidence cleanup) -** התוקף ינסה להסיר כל עדות לפעילות שלו, על מנת למנוע זיהוי של המתקפה ובעיקר למנוע זיהוי של התוקף והכלים בהם השתמש. כך יוכל להסתיר את עקבותיו ועקבות המתקפה, לשמור על זהותו ואף לשפר את הסיכויים שהארגון לא יצליח לתקן את פרצות האבטחה.

כעת נמחק עדויות. נסיר את הקבצים שהעתקנו ואת התיקייה שיצרנו, נסיר את המשימה המתוזמנת שיצרנו אצל מנהלת המשרד. נסיר לוגים שרלוונטיים לפעולות שלנו, נמחק את מייל הפישינג, נתנתק מהחיבור. לסיום, נמחק וננתק לחלוטין את השרת שהשתמשנו בו לשליטה במהלך הפרוייקט.

לאחר הבנה של השלבים של תקיפה סטנדרטית, אנו יכולים לראות כי מבדקי חדירות למערכות ייעודיות או לחלקים מן הרשת, לעולם לא יוכלו לדמות תוקף אמיתי וכאן נכנס לתמונה צוות אדום. תפקידו של צוות אדום הוא להוות הדמיה הקרובה ביותר האפשרית לתקיפה אמיתית, על פי השלבים שתוארו לעיל. אך למרות זאת, ישנן מספר מגבלות על צוות אדום (אשר משתנות מפרויקט לפרויקט, על ידי הלקוח המזמין את הבדיקה):

- **מגבלת הזמן -** תוקף אמיתי יוכל להקצות מספר חודשים (ואף שנים) לכל שלב בתקיפה, אך פרויקט צוות אדום תחום בזמן עקב המגבלות הכלכליות והעסקיות של מזמין הבדיקה.

- **מגבלת כלים -** לעיתים קרובות, הלקוח אשר מזמין את הבדיקה, לא יוכל להקצות סביבה ייעודית לבדיקה ולכן לא יוכל לקחת סיכון על המערכות הקיימות ולכן יגביל את הצוות בשימוש בכלי פריצה

מסוימים, אשר עלולים לגרום למערכת אי יציבות כגון אקספלויטים אשר מתבססים על Buffer Overflow וכד'.

- **מגבלות עסקיות -** ישנם לקוחות אשר תוחמים את הבדיקה, בין אם זה במטרות המאושרות למשלוח פישינג (לרוב לא מאפשרים לשלוח פישינג לבעלי תפקידים והנהלה), מגבלות במרחב התקיפה כגון רשתות מחוץ לתחום.

- **מגבלות אזוריות -** לעיתים לקוח יזמין בדיקה אשר לא כוללת הגעה פיזית לאתרי הארגון ובכך מבטל את הווקטור של השארת מדיה נגועה, פריצת מנעולים, התחזות לנותני שירות, גישה דרך הרשת האלחוטית וכדו'.

מהו הצוות האדום במבדקי חדירות?

הצוות האדום מורכב ממספר של יועצי אבטחת מידע, בעלי ניסיון hands-on בשלל מערכות וטכנולוגיות, בהן גם איכויות לא טכנולוגיות כגון גישה פיזית (פריצת מנעולים), הנדסה חברתית ובעיקר יצירתיות ומבצעיות. צוותים אלו קיימים לעיתים לא רק כחלק מחברות ייעוץ, לעיתים גם ניתן למצוא אותם כצוות אשר הוקם פנימית בחברה, על מנת לבצע את הבדיקות.

חברות רבות היום פונות לבדיקות של צוות אדום עקב העובדה כי כך הארגון יכול לקבל תמונה אמינה של מצב ורמת אבטחת המידע (ואולי גם האבטחה הפיזית) שלו. בעת הזמנת הבדיקה הגורמים היחידים המודעים לבדיקה, הינם מספר בודד של אנשים בארגון, כך בעצם מובטח כי הבדיקה אינה מסויגת וכי התרחישים אשר יופעלו נגד הארגון יגררו את התגובות אשר הגורמים הרלוונטיים יגיבו בתרחישי אמת. בנוסף ניתנת להנהלה האפשרות להגדיר בעצמה את היעדים לצוות האדום, את הנכסים הקריטיים ביותר ולהצביע על הנקודות הרגישות ביותר עבורן, במידה ותוקף ייכנס לארגון ובכך למדוד את רמת האבטחה המיועדת למידע ספציפי או מערכת ספציפית ואת העמידה שלו אל מול תוקפים חיצוניים.

מהם היתרונות של צוות אדום?

עקב העובדה כי צוות אדום לרוב יכלול תרחיש של גישה פיזית, ניסיון לנצל את החולשה האידיאלית (בני אדם) בפישינג או שיחות טלפון מפוברקות, מתאפשר לארגון לא רק להבין היכן נמצאות הבעיות הטכניות שלו, אלא להרגיש ולראות מה עלול לקרות לארגון במידה וגורם זדוני יחליט לנצל את זה. בעבר פרצות אבטחה היו מסתכמות בתרחישים תיאורטיים ("המשתמש לחץ על לינק באימייל פישינג, אז התוקף **יכול** להשתלט על המחשב"), כאן ישנה הדגמה חיה של התרחיש ("המשתמש לחץ על הפישינג, הנה סקרינשוט מהמסך שלו כשהוא במערכת הכספים") רכישת הרשאות גבוהות, גניבת מידע רגיש והתחמקות ממערכות שליטה והגנה בארגון. יתרה מכך, התוצאות של בדיקת צוות אדום מהוות כלי בידי מנהלי אבטחת מידע על מנת להציג להנהלה את הסיכונים מולם מתמודד הארגוואת הצורך במתן כספים

להכשרה, רכישת מערכות, או שינוי ארגוני. כמו כן, בדיקת הצוות האדום מסייעת לארגון לבחון את עצמו ואת צוותי הניטור והבקרה שלו, המערכות אשר הוטמעו בו ואת הצורך במערכות נוספות ו\או שונות לטובת הגנה, בקרה, ניטור ותגובה.

<u>מה עושים לאחר שמסתיימת הבדיקה?</u>

בסוף הבדיקה מתקיים דיון, אשר בו הצוותים (האדום, והכחול אם קיים), מסבירים כל שלב בתהליך, מה בוצע וכיצד ניתן היה לפתור\למנוע את זה וכיצד נכון היה להגיב לאותו מקרה. בנוסף מתקיים דיון עם הנהלת הארגון בנוגע לפעולות אשר מומלץ לבצע בסוף הבדיקה, על מנת לשפר את רמת האבטחה של הארגון. ואם בדיקת צוות אדום לא יכולה להבטיח חסינות כנגד מתקפות אחרות, היא בהחלט תשפר את עמידות הארגון אל מול תקיפות מתקדמות, תוכל להצביע על נקודות כשל טכנולוגיות ואנושיות ולהדגים בפועל את הנזקים אשר עלולים להיגרם עקב התקפת סייבר.

תחום הצוות האדום תופס תאוצה בשנים האחרונות, עד כדי כך שארגונים מזמינים בדיקות לתשתיות מדיניות (https://www.youtube.com/watch?v=pL9q2lOZ1Fw&feature=youtu.be).

התפתח המושג Red Teaming וסביבו חוקרי אבטחה ויועצים אשר מפתחים כלים ייעודיים וטקטיקות ייעודיות לשלב התקיפה, שלב איסוף המודיעין, תשתיות התקיפה ואפילו טקטיקות להקמת התשתית. נוצרו באינטרנט דיונים רבים כיצד לפעול בבדיקה שכזו על מנת להתחמק מהצוות הכחול ובנוסף לייעל את יכולות הבדיקה, לשמור על דממה מבצעית ולהשלים את הפעולה בהצלחה.

סיכום

עולם הטכנולוגיה והמחשבים בשנים האחרונות, הבין שכדי להגן על עצמו בצורה הטובה ביותר מתוקפים זדוניים, עליו לאמץ את שיטותיהם וכליהם ולשם כך יש לגייס (או לשכור) שירותים של תוקפים "לגיטימיים" ולבצע מבדקי חדירות, על מנת לשפר את המצב של אבטחת המידע בארגון. עם זאת, מבדקי החדירות הסטנדרטיים אינם מתאימים למתן של תמונה מלאה על יכולות חדירה לארגון ומתאימים לתמונה מוגבלת יותר, שתחומה להיקף הבדיקה והמערכת הנבדקת, לשם כך התחילו בדיקות של צוות אדום. צוות אדום יודע היום להתמודד עם חדירה לארגון בכללותו, על ידי ניצול של כל הדרכים האפשריות ולהתמודד אקטיבית מול צוותי הגנה וכל זאת על מנת לשפר את מצב הארגון בהיבט של אבטחת המידע ברשתות והמערכות והמצב של הארגון להתגונן אקטיבית ולהגיב לאירועי חדירה ותקיפות.

על המחבר

רועי שרמן, יועץ אבטחת מידע בכיר ו-Red Teamer ב-Ernst and Young ASC Israel. לשאלות, הערות, הארות ושאר ירקות ניתן למצוא אותי ב-Roei.sm@gmail.com