**מטלת התקפות**

איתי הראל 316123892

מטלה זו יש להגיש ביחידים. פורמט הגשת המטלה הינו PDF ששמו הוא ת.ז. המגיש.

במטלה זו תתבקשו לחקור ולהסביר על התקפות ידועות

לכל התקפה יש לרשום פסקה(בעברית) המסבירה עליה שתכלול את מהלך ההתקפה, מה נתקף(איזו פירצה מנוצלת) ודרך אחת לפחות להתמודד עם ההתקפה

DDOS

התקפה זו היא הניסיון לגרום לשרת, אתר אינטרנט או שירותים אחרים להפוך ללא זמינים על ידי ניצול מרבי של אחד מהמשאבים של השירות לדוגמא : מעבד, זיכרון, רוחב פס. הסיבה שקוראים להתקפות האלו התקפת מניעת שירות מבוזרת מכיוון שתנועת הגולשים המזויפת מגיעה מכמות עצומה של מחשבים שונים. התקפות DDoS משתמשות ב- Botnet שהוא אוסף של הרבה מחשבים או מכשירים בעלי אפשרות גלישה באינטרנט הנשלטים מרחוק בעזרת [תוכנות זדוניות](https://he.safetydetectives.com/blog/best-malware-removal-software/) בכדי לבצע מתקפה. המטרות להתקפות מניעת שירות הן לצורך שעשוע, דרך פשיעה, עבור בטרור וכלה בלוחמת סייבר.

Fuzzing

בדיקת Fuzzing היא טכניקת שעושה בדיקת תוכנה אוטומטית כאשר יש בה אספקת נתונים לא חוקיים, בלתי צפויים או אקראיים. לאחר מכן יש מעקב אחר התוכנית בשביל לאתר חריגים כגון קריסות, קביעות קוד מובנות כושלות או דליפות זיכרון אפשריות. בדרך כלל משתמשים Fuzzing לבדיקת תוכניות שלוקחות תשומות מובנות.

SQLi

התקפת הזרקת SQL מורכבת מהכנסה או "הזרקה" של שאילתת SQL דרך נתוני הקלט מהלקוח ליישום. התקפת הזרקת SQL מוצלחת יכולה לקרוא נתונים רגישים מהמאגר כגון סיסמאות, פרטי כרטיס אשראי או מידע אישי על המשתמש, לשנות את נתוני בסיס הנתונים ולבצע פעולות ניהול במסד הנתונים ובמקרים מסוימים מוציאים פקודות למערכת ההפעלה.

דרך להתמודדות:

XSS

זוהי אחת ההתקפות הנפוצות כיום שתוקפת משתמשי אתרי אינטרנט על ידי הסתננות לתוך יישום האינטרנט. ההתקפה פוגעת בפרטיות הגולש כאשר פרטיו נגנבים או מטופלים על ידי גורמים עבריינים. בהתקפת XSS יש שלושה צדדים: התוקף, הקורבן והאתר האינטרנט.במהלך ההתקפה סקריפטים זדוניים מוזרקים לתוך האתרי האינטרנט והתוקף מצליח לעלות קוד זדוני הפועל בצד הדפדפן וקוד זה מורד ומופץ בדפדפנים של קורבנות.התקפה כזאת מתאפשרת במקום בו יישום האינטרנט משתמש בקלט משתמש ללא אימות ואינו מזהה שהועלה לאתר קוד ולא נתונים כקלט הקורבן לא מודע שנשלח אליו סקריפט זדוני שיכול לגשת לכל העוגיות הנשמרות בדפדפן ויכול להגיע לכל מידע רגיש שנשמר על הדפדפן מול האתר המותקף.

Phishing

**בדואר-** נעשה בדרך כלל בדואר זבל אלקטרוני, כלומר באמצעות פנייה למספר רב מאוד של נמענים, כך שמבחינתו של השולח, אחוז קטן מאוד של נופלים בפח כדי להשיג את המטרה. הפנייה בהודעות אלה בדרך כלל אינה אישית (למשל: "לקוח יקר"), אך לעיתים מתבסס השולח על רשימת שמות שנפלה לידיו, כגון רשימת כל העובדים או הלקוחות בארגון מסוים, ופונה באופן אישי לכל נמען, צעד המגביר את אמינותה של הודעת PHISHING . בנוסף, לעיתים מציין השולח כתובות ושמות של חברות, ארגונים ואנשים אמיתיים (שמות וכתובות של משרדי עורכי דין, מספרי חשבון בנק אמיתיים) לצורך הגברת אמינות ההודעה.

**מאקרו-**שימוש בקובץ וורד המצורף להודעת אימייל, אשר בכדי לקרוא את תוכנו מתבקשים הנמענים לאפשר הפעלת מאקרו. מרגע ההפעלה מתחיל באופן מידי תהליך של התקנת קוד עויין מסוג סוס טרויאני על המחשב. הודעת האי-מייל נראית כהודעה פנים ארגונית תמימה, אשר מכילה צרופה (Attachment) בקובץ וורד אשר שמו Financial Statement.doc. לאחר שמורידים את הקובץ ופותחים אותו לצפייה התוכן נראה מטושטש ובלתי קריא, ובראש הדף מופיעה הודעה אשר מציינת כי הטקסט טושטש במכוון לצורך אבטחה, ובמידה ומעוניינים לקרוא את המסמך ולהסיר את הטשטוש יש לאפשר הפעלת מאקרו במסמך ע"י לחיצה על הכפתור המתאים בוורד, אשר נמצא מתחת לסרגל הכלים.

**העתקת אתרים-**לחיצה על הקישור עשויה להוביל משתמש לדף מזויף הנראה כמו דף של אתר לגיטימי. כאשר המשתמש מכניס את פרטיו הדף מפנה אותו באופן אוטומטי לאתר האמיתי ומכניס עבורו את הפרטים כך שהמשתמש אינו יודע שמסר את פרטיו לאתר מזויף.

MITM & Poisoning

**רשמו פסקה המסבירה על התקפת התאום המרושע.**

התקפת תאומים מרושעת היא התקפת גרזן שבה האקר מקים רשת Wi-Fi מזויפת שנראית כמו נקודת גישה לגיטימית לגנוב פרטים רגישים של הקורבנות. לרוב, הקורבנות של התקפות כאלה הם אנשים רגילים כמוך וכמוני. ההתקפה יכולה להתבצע כהתקפת אדם באמצע (MITM). נקודת הגישה המזויפת של Wi-Fi משמשת לציתות למשתמשים ולגנוב את אישורי הכניסה שלהם או מידע רגיש אחר.

**רשמו פסקה המסבירה על התקפת הרעלת ARP**

שיטה לפריצה של רשתות Ethernet שנותנת אפשרות לפורץ לנטר את הנתונים שעוברים ברשת המקומית או לעצור את התעבורה. העיקרון של ההתקפה הוא לשלוח הודעות ARP מזויפות ברשת המקומית שמכילות כתובות MAC שקריות ובכך מטעה משאבי רשת וגורם לתעבורת המידע לעבור בתצורה שונה מהמקור. לדוגמה ברשת ניתן לקבוע Gateway למחשב קצה ותחת פעולה זו לאלץ את המחשב להאמין כי הכתובת המדומה החדשה תואמת את ה-Gateway המקורי ובכך התעבורה היוצאת תישלח אל המחשב בעל הכתובת המזויפת, כך הוא יכול לבצע פעולות ניטור לרשת ובכך לחשוף מידע רב העובר בתצורה בלתי מוצפנת ברשת. העמדה המזויפת יכולה לאחר מכן להעביר את השדרים אל התחנה האמיתית ובכך להטמיע את עצמה בצורה שקופה למשתמש או לחלופין לגרום לכלל התעבורה להינתב למיקום רשת אחד ובכך להעמיס על משאביו ולגרום לקריסתו (התקפת מניעת שירות - Denial of Service).

**רשמו פסקה המסבירה על התקפת הרעלת DNS.**

תקיפת הרעלת DNS או הרעלת מטמון DNS היא תיאור לתקיפה שבאמצעותה המחשב המותקף מופנה על ידי שרת DNS אל כתובת איי-פי (IP) פיקטיבית. לרוב תקיפה זו היא תקדים לתקיפת פישינג. תקיפת הרעלת DNS מתבצעת בשני שלבים וישנן שתי שיטות עיקריות לביצוע השלב הראשון של תקיפת הרעלת DNS:

* התוקף מקים שרת DNS פיקטיבי ופונה אליהם דרך פורט תקשורת לוגי 53/UDP מחכה לפניות ממחשבים.
* התוקף חודר אל שרת DNS ומשחית רשומות NS קיימות כדי שמחשבך יופנה אל אתר פיקטיבי.

**Ransomware**

**רשמו פסקה המסבירה על התקפות כופר והביאו דוגמא אחת להתקפה כזו**

היא נוזקה שמגבילה גישה למערכות המחשב הנגוע בדרך מסוימת, ומשמשת לסחיטה מהמשתמש תשלום כסף (דמי כופר) כדי שתוסר מגבלת הגישה. חלק מתוכנות הכופר מבצעות הצפנה לקבצים על הכונן הקשיח, וכך הופכות את תהליך הסרת ההצפנה לקשה מבלי לשלם כופר עבור מפתח ההצפנה,. לרוב, חודרת תוכנת הכופר למחשב כסוס טרויאני, המוסווה כקובץ תמים.

דוגמא להתקפה כזו היא המתקפה שהייתה בחברת ביטוח שירביט כאשר התוקפים השתלטו על המאגר נתונים ובכך הם רצו המון כסף בשביל להסיר את הגישה שלהם.