מטלת התקפות

דור לבקוביץ – 203565015

DDOS

1.

A) שולחים בקשות פינג רבות על מנת להעמיס על השרת ולגרום לסירובו לבקשות משמעותיות יותר. כיום התקפות כאלו נדירות יחסית מכיוון שמרבית השרתים שהותקפו חוסמים את אפשרות הפינג.

B) במסגרת ההתקפה התוקף שולח רצף של חבילות SYN למחשב המותקף ובכך מאלץ אותו לפתוח במקביל חיבורים רבים עד שלא נותרים לו משאבים לקבלת חיבורים חדשים. בכך התוקף מונע מהמחשב המותקף להעניק שירות למשתמשים אחרים ומשיג את מבוקשו. הצפת SYN היא התקפה מוכרת ביותר ולרוב אינה אפקטיבית כנגד שרתים ורכיבי רשת מודרניים שכן אמצעי התמודדות רבים כבר שולבו באלו על מנת שיוכלו להתמודד איתה.

C) ברשתות אלחוטיות אפשרית חסימה אלקטרונית של הרמה הפיזית במטרה למנוע מעבר מידע תקין על גבי אותו התווך בין הצמתים ברשת. בניגוד להתקפות מניעת שירות אחרות, התקפת שיבוש אינה מכוונת לצמתים ברשת, אלא לתווך הפיזי המקשר ביניהם שהוא גם משותף במרבית המקרים לכל מי שנמצא במרחק פיזי מסוים מהרשת.

FUZZING

2. אז מה זה בעצם פאזינג? שיטת בדיקה אוטומטית שעיקרה בהזנה של קלטים אקראיים ו\או לא צפויים עבור תוכנה מסוימת בציפייה לגרום לה לקריסה, שבמקרה שלנו, תוביל למציאת חולשת אבטחה .

השיטה הוצגה לראשונה באוניברסיטת וויסקונסין שבארה"ב ע"י פרופ' ברטון מילר, יש הטוענים שהעבודה במקור החלה בעקבות השראה שהתקבלה מקריסה של תוכנות בשעת סופת ברקים בעקבות רעשי קו שנוצרו בעת חיבור מודם.

הקלטים אותם אנו שולחים אל התוכנית יכולים להיות מסוגים שונים, בין אם קבצים בפורמטים שונים (כגון PDF) או מבוססי רשת, למשל SNMP או FTP.

בעוד השלבים האחרונים הם טכניים לחלוטין, השלב הראשון של יצירת מקרי הבדיקה הוא בעצם השלב המכריע שבו מתרכז המאמץ, שכן הצלחה או כישלון במאמץ לחשוף חולשת אבטחה טמונה ביצירת מקרה הבדיקה "הנכון" שיחשוף את הבאג, הפאזר צריך להצליח היכן שהמפתח והבודקים של התוכנה במקור בעצם נכשלו.

SQLi (SQL Injection)

3. היא שיטה לניצול פרצת אבטחה בתוכנית מחשב בעזרת פניה אל מסד הנתונים.

השם נובע מכך שהמשתמש מכניס קוד SQL לשדה הקלט אליו אמורים היו להיכנס נתונים תמימים. באופן זה יכול משתמש זדוני לחרוג לחלוטין מן התבנית המקורית של השאילתה, ולגרום לה לבצע פעולה שונה מזו שיועדה לה במקור. הזרקת SQL היא מקרה פרטי של קבוצה רחבה של פרצות אבטחה הנקראות הזרקת קוד, שמתרחשות כאשר תוכנה כלשהי יוצרת קוד בזמן ריצה ע"פ הקלט ובלי לבדוק את תוכן הקלט תחילה.

כל תוכנית שבונה שאילתות SQL תוך שילוב של נתונים מן המשתמש, עלולה להיות פגיעה להזרקה, עלולה לחשוף נתונים שהמתכנת חשב שלא יוכלו להיחשף ועלולה לגרום נזק לנתונים עצמם ומכיוון שכך, היא עלולה להיות פגיעה ללוחמת סייבר.

על מנת להיות בטוחים שקוד לא יהיה חשוף להזרקה, אפשר לנקוט בשימוש במבנה קשיח יותר של שאילתה – שפות התכנות השונות מציעות פתרון עדיף לבעיה, ע"י כך שהמתכנת יכול להכין שאילתה מובנית ולשים "שומרי מקום" (placeholder) במקומות שאליהן יוכנס אחר כך הנתון הנקלט מהמשתמש.

XSS (Cross Site Scripting)

4. היא התקפה נגד גולש אינטרנט המנוצלת באמצעות פגיעות ביישומי אינטרנט ומאפשרת לתוקף להזריק סקריפט זדוני שמטרתו לרוץ בדפדפנים של משתמשי מערכת אחרים.

בעת הרצת הקוד יוכל התוקף לבצע פעולות בשמו של המשתמש בשירות ע"י ניצול מגבלות בפרוטוקול HTTP ואף לגנוב את מזהה המשתמש.

הגנה אמינה מפרצות XSS דורשת קידוד של כל תגי ה- HTML המיוחדים הקיימים במידע שעלול להכיל קוד זדוני (למשל כזה המגיע מהמשתמש). לרוב פעולה זו מתבצעת לפני ההצגה עצמה של התוכן, ולשפות תכנות רבות יש ספריות המספקות שירות זה(נקרא בהקשר הזה לרוב quoting או escaping).

הצורה המקודדת תיראה בתוך עמוד HTML בדיוק כמו המחרוזת שהמשתמש הכניס, אולם הקוד (שבמקרה זה מקפיץ חלון עם הכתובת "XSS") לא ירוץ.

הבעיה הגדולה ביותר עם הגנה מפני פרצות XSS היא שהגנה בצורה המתוארת למעלה, למעשה מונעת מהמשתמש להכניס כל דבר שאינו טקסט פשוט אל תוך עמודי HTML. אם נדרש לאפשר למשתמש הכנסת תוכן מעבר לטקסט פשוט, יש להפריד בין תגי HTML חוקיים לכאלו שאינם חוקיים, ומשימה זו היא קשה הרבה יותר, מכיוון שכל מקרה דורש טיפול לגופו.

PHISHING

באבטחת מידע, דיוג או פישינג הוא ניסיון לגניבת מידע רגיש ע"י התחזות ברשת האינטרנט. המידע עשוי להיות, בין היתר, שמות משתמש וסיסמאות או פרטים פיננסיים. פישינג מתבצע באמצעות התחזות לגורם לגיטימי המעוניין לקבל את המידע. לרוב שולח הגורם המתחזה הודעת מסרים מידיים או דואר אלקטרוני בשם אתר אינטרנט מוכר, בה מתבקש המשתמש ללחוץ על קישור. לאחר לחיצה על הקישור מגיע המשתמש לאתר מזויף בו הוא מתבקש להכניס את הפרטים אותם מבקש המתחזה לגנוב.

5. **דואר אלקטרוני –** פעולות דיוג נעשות בדרך כלל בדואר זבל אלקטרוני, כלומר באמצעות פנייה למספר גדול מאוד של נמענים, כך שמבחינתו של השולח, די באחוז קטן מאוד של נופלים בפח עדי להשיג הצלחה. 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 הדיוג. בנוסף, לעיתים מציין השולח כתובות ושמות של חברות, ארגונים ואנשים אמיתיים (שמות וכתובות של משרדי עורכי דין, מספרי חשבון בנק אמיתיים וכו') לצורך הגברת אמינות ההודעה.

6. **מאקרו –** בכדי לקרוא את תוכנו מתבקשים הנמענים במייל לאפשר הפעלת מאקרו. מרגע ההפעלה מתחיל באופן מידי תהליך של התקנת קוד עוין מסוג סוס טרויאני על המחשב. הודעת המייל נראית כהודעה פנים ארגונית תמימה, אשר מכילה צרופה (Attachment) בקובץ וורד.

לאחר שמורידים את הקובץ ופותחים אותו לצפיה התוכן נראה מטושטש ובלתי קריא, ובראש הדף מופיאה 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.

באם המשתמש אכן מאפשר את פעולת המאקרו , מתחילה התקנת הקוד העוין על גבי המחשב – הפעלת המאקרו מפעילה בתורה סקריפט ב- visual basic אשר בהמשך מפעיל סקריפט נוסף ב- powershell אשר עם הפעלתו מוריד את קובץ הקוד העוין מכתובת ייעודית באינטרנט ומתקין אותו על גבי המחשב.

טכניקה זו מקטינה מאוד את הסיכוי לזיהוי הקוד העוין ע"י מערכות ההגנה הארגוניות ואלו אשר מותקנות על המחשב, זאת מכיוון שמערכות אנטי-וירוס מתקשות לזהות קוד עוין אשר נמצא בתוך פקודות מאקרו אשר נמצאות בתוך קובץ וורד.

הקוד העוין עצמו הינו סוס טרויאני בעל יכולות keylogging והעתקת תוכן ה-clipboard, ונראה שמטרתו העיקרית הינה להשיג גישה למערכות נוספות ברשת באמצעות השגת המשתמש וגניבת זהותו.

7. **העתקת אתרים –** לחיצה על קישור 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. שיטות מסוג זה נקראות "אדם באמצע" (man in the middle).

שיטות מתוחכמות יותר כוללות את שינוי הכתובת בשורת הכתובת של הדפדפן והצגת תמונה של הכתובת הנכונה, או סגירת שורת הכתובת האמיתית והצגת שורת כתובת מזויפת בדפדפן או שימוש בדומיין שנכתב בשפה אחרת אך האותיות שלו דומים לאותיות שבאנגלית שיטות XSS מאפשרות לאתר להפעיל תוכנה במחשב הקורבן כך שניתן למעשה לבצע כל פעולה מתוך המחשב בהרשאות המשתמש. שיטה זו קשה מאוד לזיהוי על ידי מי שאינו מומחה.

8. **שימוש בווב 2.0 -** עבריני דיוג משתמשים בטכנולוגיית ווב 2.0 כדי ליצור דפי אינטרנט המובילים לדיוג. אחסון הדפים על שרתי ווב 2.0 אמינים (כמו ויקיפדיה ומערכת בלוגים) והוספת תוכן לגיטימי יחד עם תוכן מטעה מגבירים את אמינות הדף, וגורמים לגולשים להיכנס אליו. מפעילי הבלוג משתמשים בטכניקות קידום במנועי חיפוש כדי לשפר את דירוג הבלוג ומעדכנים אותו באופן תדיר. מכיוון שהחברות המציעות שירותי בלוגים לרוב אינן מפקחות על תוכנם (משיקולי עלות-תועלת), תרי ווב 2.0 העוסקים בדיוג שורדים זמן רב יותר משיטות הדיוג המסורתיות.

קיימות דרכים שונות להילחם בתופעת הדיוג, החל מחקיקה מתאימה וכלה באמצעיטכנולוגיים. שיטות אלה נקראות "אנטי־פישינג". ניסיונות דיוג באמצעות דואר אלקטרוני יכללו בדרך כלל פנייה כללית או יפנו למקבל הדואר באמצעות כתובת האימייל שלו ולא בשמו; קישור לכתובת IP במקום לכתובת אתר ושגיאות כתיב הן שיטות נפוצות להתחמקות

ממסנני דיוג, ולרוב הן יכולות להזהיר את המשתמש מפני ניסיון דיוג. בשנים האחרונות התפתחה שיטת דיוג הנקראת "דיוג ממוקד". הודעות אלה מופנות לאדם מסוים או לקבוצה מצומצמת של אנשים ונראות כאילו הן מגיעות מאדם מוכר או בעל סמכות. מטרתן של הודעות אלה היא בדרך כלל לפגוע בחברה המותקפת. דפדפנים מכילים אמצעים טכנולוגיים המיועדים לזהות כניסה לאתר חשוד. בגרסאות ישנות של הדפדפן אינטרנט אקספלורר הופיע סימן המנעול (PadLock) שהראה שהחיבור הוא לאתר מאובטח באמצעות פרוטוקול SSL. בדפדפן פיירפוקס הופיעה כתובת מאובטחת בצבע צהוב. חיבור SSLמצריך תעודה דיגיטלית (Certificate) כדי לוודא את מהימנותו של האתר אליו מתחברים. הדפדפן בודק שהתעודה בתוקף ושהיא חתומה על ידי רשות מוסמכת.

MITM & Poisoning

9. **התאום המשוגע -** הרצת נקודת גישה "תאום מרושע" שמתחזה לאמיתי ושואב מידע או עושה פישינג. פריצת סיסמאות כניסה לרשת אלחוטית עוד.

10. **הרעלת ARP –** התוקף שולח לכל המחשבים ברשת הודעת ARP המודיעה שכתובת ה-MAC שלו, היא מתאימה לכתובת ה-IP של הנתב, כלומר גורם לכך שרוב התעבורה תעבור דרכו (כולם חושבים שהוא הנתב).

11. התוקף מכניס לשרת ה-DNS רשומות שגויות, בכך גורם למשתמשים לבקש כתובות IP של אתרים, משרתי DNS מזוייפים. למשל מגדיר בשרת ה-DNS שכאשר יבקשו את הכתובת google.com, למעשה יקבלו כתובת IP של אתר הגונב את פרטי המשתמש, ולא כתובת ה-IP של אתר google.com.

Ransomware

היא נוזקה מגבילה גישה למערכות המחשב הנגוע בדרך מסוימת, ומשמשת לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה. חלק התוכנות הכופר מבצעות הצפנה לקבצים על הכונן הקשיח, בכך הופכות את תהליך הסרת ההצפנה לקשה מבלי לשלם כופר עבור מפתח ההצפנה, בעוד תוכנות כופר אחרות פשוט נועלות את המערכת ומציגות הודעת שווא כי לא ניתן לגשת לקבצים, על מנת לרמות את המשתמש ולהמריצו לשלם. לרוב, חודרת תוכנת הכופר למחשב כסוס טרויאני, המוסווה כקובץ תמים.

דוגמה: סיפור על מישהי מפורסמת בישראל שמישהו פרץ לה לטלפון והצפין לה שם תמונות עירום שלה ודרש כופר על מנת לשחרר את התמונות ואם לא תשלם הוא יפיץ את התמונות.