דו"ח מעבדה - תרחיש מס' 3

פרטים:

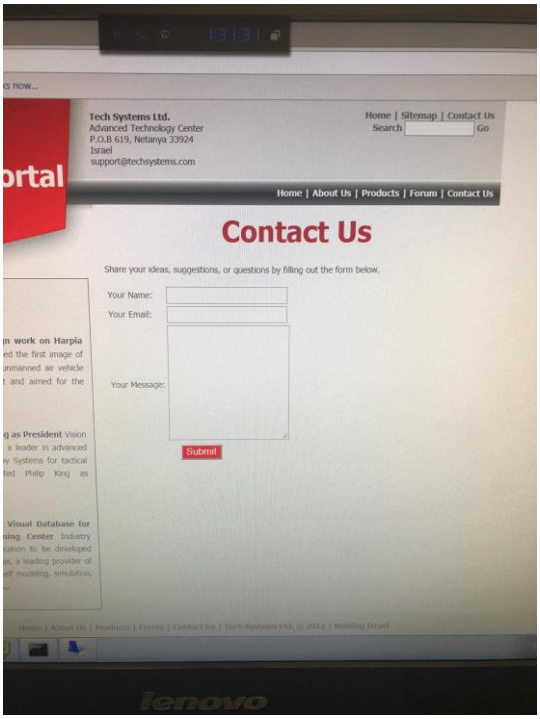
מגיש: דביר ברזילי

תאריך: 10.5.2018

שם התרחיש: SQL Injection

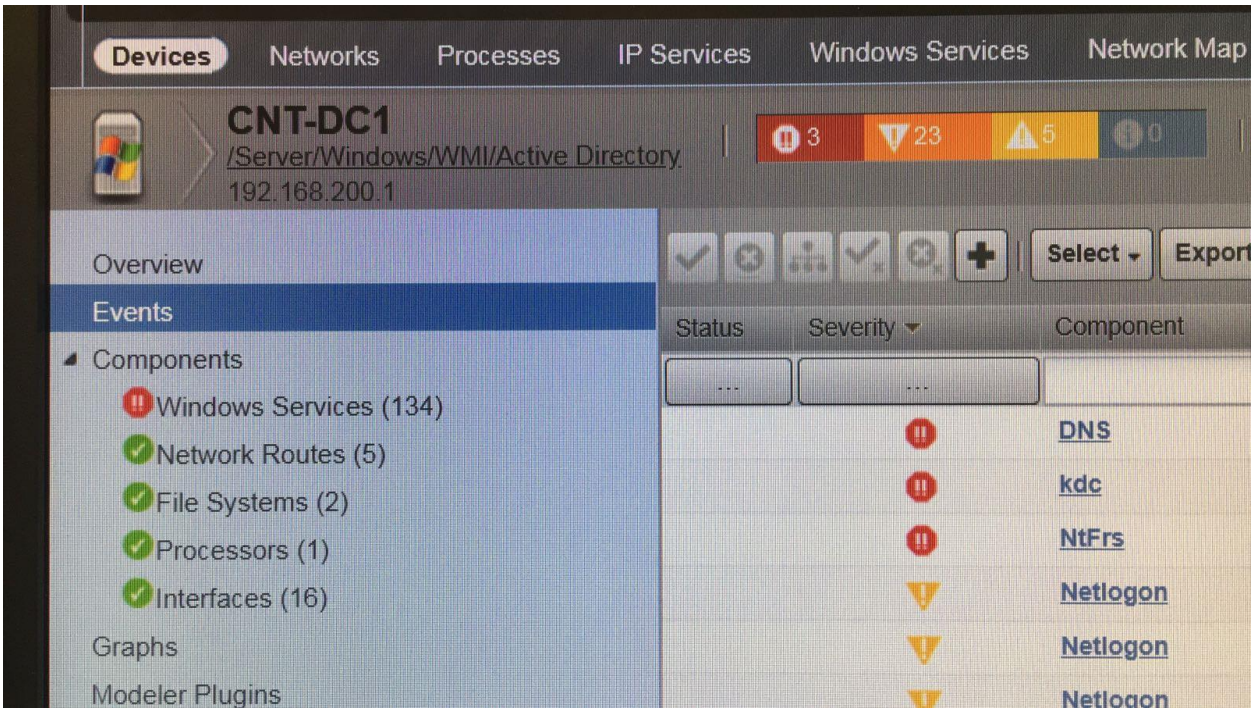
תהליך ההתקפה:

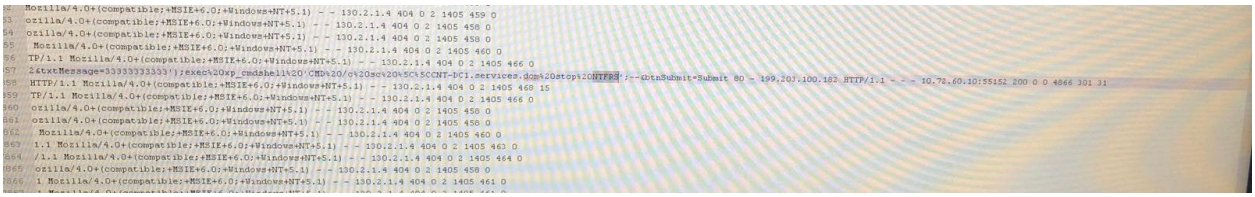
התוקף ביצע web crawling בתוך האתר tech.com על מנת ללמוד אם קיים שדה למילוי משתמש שחשוף לגניבת נתונים על ידי SQL Injection. לאחר שזיהה שניתן לתקוף דרך השדה message בדף contact us שבאתר, התוקף השתמש בשדה הזה כדי להפעיל shell מרוחק (xp_cmdshell), וע"י כך הריץ פקודות שהפילו את השירותים DNS, kdc ו- NtFrs.



תהליך הזיהוי:

קיבלנו התראה על web crawling, וראינו שהתקבלו למעלה מ- 50,000 בקשות GET לשרת שלנו, כמות שאינה אופיינית. כמו כן ראינו שהשירותים DNS, NtFrs ו- kdc נפלו. חיפשנו בין כל השאילתות שהתקבלו לשרת הDB שלנו שאילתות ארוכות מהרגיל, או שאילתות שבהן ניתנה הפקודה להפיל שירותים כגון kdc. מצאנו שאילתות שבהן התוקף הפיל את השירותים ע"י הפעלת shell מרוחק.





תהליך הגנה:

חסמנו את הכתובת של התוקף ב-FireWall מתעבורה נכנסת ויוצאת. בפעולה זו מנענו מהתוקף להמשיך להעביר פקודות לשרת בתקיפת ה-SQL Injection ולהפיל שירותים.

תהליך הגנה מונעת:

אילו היינו דואגים לחטא כל קלט שאנו מקבלים מהמשתמש באתר ע"מ לוודא שהקלט נקי מפקודות שאינן אמורות להופיע שם, מגבילים את אורך השדה ואת סוג התווים שניתן להכניס כקלט, כנראה שכך היינו נמנעים מהתקפה כזו. כמו כן, מן הראוי שכאשר משתמש מבצע כל כך הרבה שאילתות GET בתווח זמן כה קצר (50,000 שאילתות GET) המשתמש היה מקבל חסימה אוטומטית, ולא לאפשר לו להמשיך את הפעילות באתר.

הגנה מונעת נוספת היא שבביצוע פקודות שמפילות שירותים חשובים (או פקודות חשובות כלשהן באופן כללי) המשתמש היה נדרש לאמת שהוא בעל הרשאות מתאימות ע"י הזנת סיסמא.

הפרצות באבטחת הארגון

אין בקרה על הקלט שמגיע דרך האתר מהמשתמש. זו פירצת אבטחה מפני שאנו נותנים יד חופשית למשתמש להזין מה שהוא רוצה, ועל ידי כך לפגוע בארגון שלנו.

אופן עבודת הצוות

מכיוון שהשרת היה עם מערכת הפעלה של Windows, רק חבר צוות אחד יכל לעיין בשרת ולבדוק מה קורה בתוכו. בנתיים שאר חברי הצוות ניסו לתחקר את האירוע, לחקור את התקשורת שהייתה בזמן התקיפה, ונסיונות להבין מה פשר נפילת השירותים בשרת שוב ושוב. לאט לאט חיברנו את החלקים השונים שהיו בהתקפה ולבסוף קיבלנו את התמונה המלאה.

חוסרים/קשיים

התרחיש זה היה קושי להבין כיצד התרחשה ההתקפה. מבין למעלה מ50,000 פניות לשרת, רק בודדות היו ה-SQL Injection עצמו. אחרי שמצאנו את השאילתות שבהן הייתה התקפה של ממש, השאילתות שהפילו את השירותים ופגעו בארגון, לקח לנו זמן להבין איך ע"י שאילתת SQL התוקף מצליח להפיל שירותים בשרת. הושקע זמן רב בקריאת קבצי לוגים.

קושי נוסף היה בכך שרק חבר צוות אחד יכל לעבוד על השרת מכיוון שהוא הריץ מערכת Windows.