דו"ח מעבדה- תרחיש מס 4

פרטים:

מגיש:יגאל נאמן

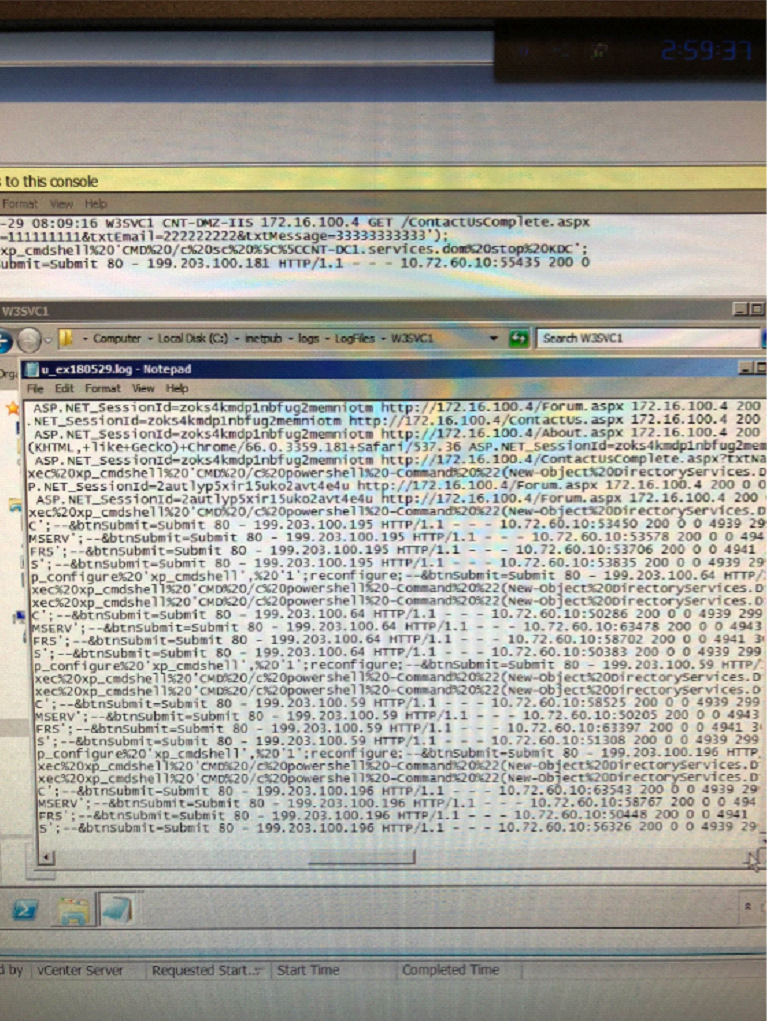
שם התרחיש:SQL injection

תהליך ההתקפה:

תהליך ההתקפה הינו שבו התוקף מבקש את כל האובייקטים מהאתר כלומר עושה לו crawling ובכך אוסף מידע על האתר עצמו ויכול לזהות חולשות שבהם הוא יכול לתקוף איזורים שהם פגיעים ברגע שהתוקף מזהה כי ישנו איזור בו הוא יכול לתקוף לאחר איסוף המידע שבמקרה שלנו התוקף זהה כי יוכל להזריק קוד זדוני דרך איזור ההרשמה contact us shell זוהי הפקודה אותה מריצים שבעזרתה ניתן לכתוב שאילתות למסד נתונים וניתן לבצע פקודות גם לכתיבה לקבצי sql sql injection

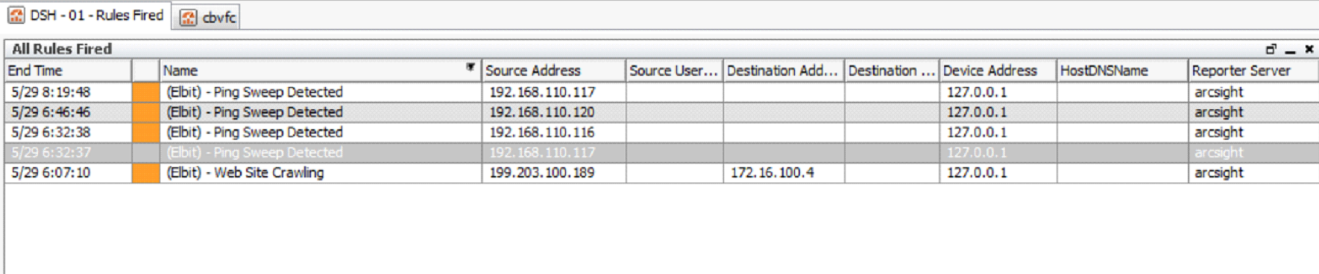
שתי פעולות שניתן לבצע עם CMD SHELL

* Create a SQL Job with a Task Step having a type of PowerShell or OS CmdExec
* Use Windows Task Scheduler and batch files



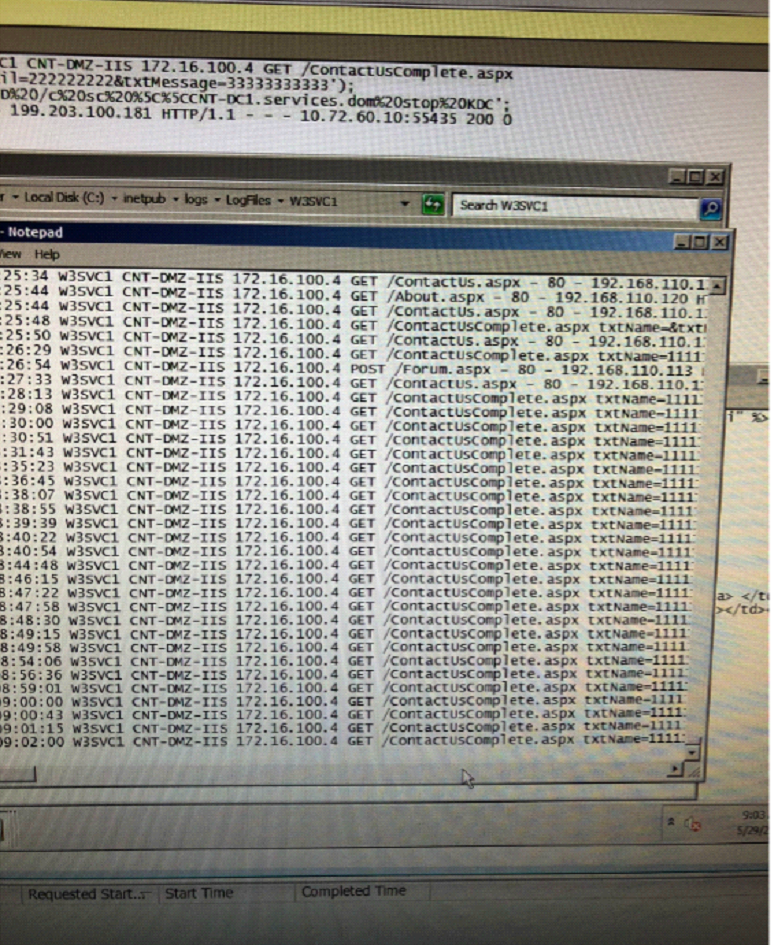
תהליך הזיהוי:

בתהליך הזיהוי תחילה קיבלנו התראה ב arcsight שיש crawling attack



ניתן לראות שההתקפה מגיעה מכתוהת ip חיצונית 192.168.110.117 אל שרת ה **iis** server שבארגון שכתובתו 172.16.100.4

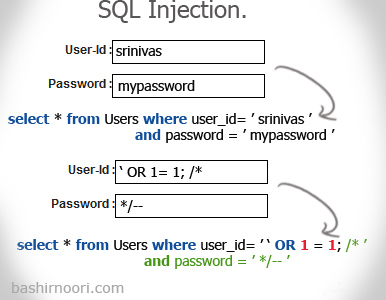
לאחר מכן נכנסו לשרת ה Iis אשר נמצא בארגון שלנו ובדקנו בקבצי הlog איזהם חריגיות וזיהנו כי יש הרבה בקשות **get** מצצד אותו כתובת Ip שזיהנו כתוקפת וניתן לראות זאת בתמונה שלהלן



הזרקת נתונים ל contact us ולאחר מכן ביצוע הפקודה בשורת הפקודה CMD שאיתה ניתן ליצור שאילתות או לייצר איזשהו תהליך אשר קשור ל sql מסד הנתונים של אתר זה נפגע בכך שהוא חשוף לגורם חיצוני

**דוגמאה נוספות שמתאר כיצד מתבצעת ההתקפה SQL injection**

**1. איך מתבצעת ההתקפה בטופסי ההרשמה**



בטבלת ה-USERNAME התוקף למעשה מנסה להזין משתמש ב בתנאי שמחזיר TRUE הוא פשוט שואל IF 1==1 למעשה אם לא חסמנו את התגיות הנ"ל בטיבלת הטקסט, אנחנו עלולים להיות מותקפים, כיוון שהמחשב יחזיר 1 לתוקף וייצור בתוקף הטבלאות שלי שם משתמש כזה, ולאחר מכן התוקף יותר להתחבר ל- DATABASE שלי בעזרת השם משתמש שהוא ייצר לעצמו.....(התקפות מסוג זה חוזרת על עצמן ברוב המקרים בוורציות שונות ומשונות) שכן מומלץ מאד לשים עין על ה- SYNTAX כשכותבים את הקוד , וכדאי למנוע ולא לייצור לעצמו בטעות חוריי אבטחה שאחר כך ייעלו בתור "VULNIRABILYS" בסריקת ה- NMAP במחשב של התוקף...

תהליך הגנה:

תהליך ההגנה המיידי הוא לחסום כרגע כל תקשורת מכתובת ip שתקופת

להגידר חוק שברגע שיש תנועה חריגה מאותו גורם יש להשהות את פעולתו לאלתר

תהליך הגנה מונעת:

תהליך הגנה לטווח הרחוק הוא לייעץ לארגון לבצע בקרת קלט כלומר שלא יוכלו להזין ערכים שאינם חוקיים לדוגמא ;

הפרצות באבטחת הארגון

הפרצה באבטחת הארגון הינה שמסד הנתונים היה חשוף לביצוע פרוצדורות , שאילתות בעזרת הפקודה CMDשניתן דרכה לבצע זאת

כלים שפיתחנו

לא פיתחתי כלים

אופן עבודת הצוות

במהלך התרחיש חלקנו תפקידים כך שכל אחד עבד על עמדה מסוימת כאשר אחד ניהל את האירוע

חוסרים/קשיים

להבין את מהלך ההתקפה