דו״ח מעבדה- תרחיש מס׳ 04

פרטים:

מגיש: אוראל מרדכי

תאריך: 20.12.18

שם התרחיש: Sql Injections

תהליך ההתקפה:

התוקף הגיע לשרת ,עשה סריקה, ואז עשה הרבה דרישות (רואים זאת בלוגים), הזין ״11111111״ הגיע לשלב של Contact text ואז גילה שיכול להזריק דברים. התוקף הזריק שמה פקודת SHELL שמייצרת טבלאות שמקבלת את כל ה SERVICES עשה reconfigure לשרת שלנו מה - Domain controller וקיבל הרשאות בשרת ה SQL. התוקף עשה זה enabling conditions (פתח גישה לביצוע פעולות בשרת).

תהליך הזיהוי:

קיבלנו התראה ב- ARCSIGHT על WebSite Crewling לאתר www.tech.com (172.16.100.4 בצד הלקוח) כולל כתובת התוקף (199.203.100.86). ניסינו בהתחלה להבין מה זה אומר בכלל ולבדוק בנתיים את האתר לראות שהוא בסדר וגם לבצע התחברות דרך ה- MSTSC לשרת. ראינו כי האתר, אך כאשר פתחנו את ה- Zenoss ראינו כי ישנם שלושה Services שנעצרו (ה-services שנעצרו הם: DNS,NTFRS,KDC). ביצענו התחברות באמצעות MSTSC (חלק התחברו דרך ה- VSphere) והתחלנו לבצע פעולות שיכולות לעזור לנו לאתר דברים חשודים (שעברנו מתרחישים קודמים) כגון מנהל משימות שנתקע, חיפוש שינויים שנעשו באותם שרתים שבהם בוצע עצירת ה-Services, שימוש בפקודה NETSTAT לבדוק את הרשת. לאחר שניסינו לחפש ב- last modify במחשבים שהותקפו ,לא מצאנו משהו (כי לא ידענו בדיוק מה אנחנו צריכים לחפש), דין בשלב זה כיוון אותנו לתיקייה (שנמצאת ב: c:\netpub\logs\logFiles) W3SYC1 ששמה ניתן לראות את קובץ ה- log של האתר (u_ex181219.log) שמתעדכן כל הזמן (ניתן גם ב DATE MODIFY לראות שזה הקובץ הכי מעודכן בתיקייה).בשלב זה דין ביקש שנרשום כל מיני דברים באתר לראות אם אכן זה מעדכן את הפעולות שאנחנו עושים בקובץ Log של האתר. פתחנו את קובץ ה-log וניסינו לבצע פעולות בתיבת הטקסט באתר ולעשות שליחה של הטקסט, זאת על מנת שנוכל לראות את השינויים בקובץ ולוודא שאכן אנחנו מסתכלים בקובץ הנכון, ואכן זה עדכן לנו קובץ ה Log. בלחיצה על ctrl+F רשמנו את שמות ה- services שנעצרו וגילינו דבר מעניין מאוד. גילינו כי נעשו כל מיני פעולות GET לשרת ה SQL ובכל פעולה מופיע לנו כתובת התוקף וכתובת היעד.

תהליך הגנה:

בשלב זה התברר לנו כי נעשה עלינו SQL INJUCTION מה שהוביל אותנו לבדוק אילו שינויים התוקף ניסה לעשות ואיך הוא קיבל גישה לבצע זאת. אורם רשם בקובץ טקסט חדש את כל הפעולות שביצע התוקף לפי שם האובייקט ואת אופן הביצוע שהתוקף ביצע את ההזרקה ע"י שימוש במספרים "11111111" ו –"2222222" וכך סינן לנו את כל מה שנעשה. לאחר שעברנו על הסינון שאלנו את עצמנו איך הוא קיבל גישה לבצע את הזרקה. התוקף באמצעות הזרקה של פקודה שביצעה Reconfigure (הגדרה מחדש),הצליח לקבל הרשאה. כל הדברים שנמצאים בשרת ה IIS כאשר אני זורק שאילתה הולך ל-msSql שנמצא בשרת Windows (192.168.214.4). כאשר ניגשנו ל Events viewer עברנו על הלוגים בשרת ושמנו לב לאחר כמה לוגים כי יש מילה שחוזרת על עצמה המילה Reconfigure (מתוך קובץ הטקסט שאורם יצר). ראינו כי נעשה שינוי של מספרים מאפס לאחד ומאחד לאחד וככה זה המשיך אך לא ידענו בוודאות מה זה אומר רק שזה קשור לפעולות שביצע התוקף אצלנו בשרת.

תהליך הגנה מונעת:

ביצענו בתחילת התרחיש חסימה ב firewall לתוקף את דרכי הכניסה והיציאה (למרות שזה לא נתן לנו הרבה כי כבר נעשה ההתקפה). לאחר שהבנו איך נעשה ההתקפה לא עשינו פעולה מיוחדת לעצירה רק הבנו איך התבצע התקיפה , איך הוא השיג את ההרשאות לביצוע ההזרקה ואת הServices שנפלו הרמנו בחזרה.

הפרצות באבטחת הארגון

Domain controller שגיאה של תוך הארגון שלנו, זה ש ב-Domain controller יש הרשאת אדמין לשרת ה- SQL . בעצם אפשר לעצמו דרך הפרצה הזאת לעשות שינוי אדמין ולקבל גישה לבצע Sql Injections לשרת.

כלים שפיתחנו

אין

אופן עבודת הצוות

ראש צוות- אוראל
אורם, קיריל ורע היו כל אחד מהם מחוברים לשרת אחר על מנת לבדוק פעולות חשודות וכן חיפוש בלוגים של האתר IIS, השרת DC1 והשרת db-mysql.
ינאי ורועי היו צמודים לאורם וקיריל במטרה לעזור וללמוד מהם כמה דברים.

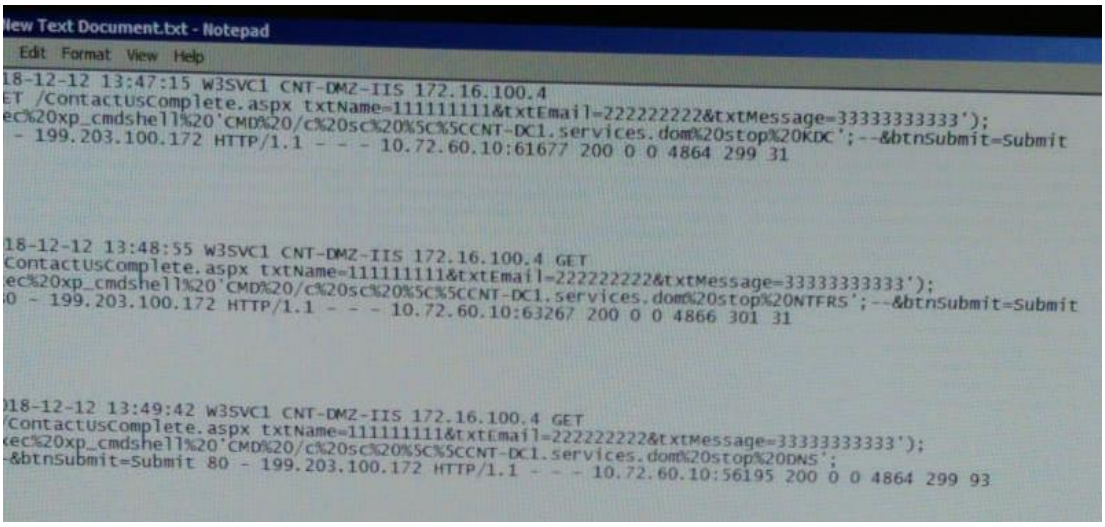
חוסרים/קשיים

התרחיש היה יותר מורכב מהקודמים , הרגשתי שאנחנו לא באמת מבינים מה אנחנו צריכים לעשות ואיך לגשת לזה למרות שכבר עברנו מספר תרחישים. בחלק הראשון של התרחיש ללא הכוונה לא היינו מגיעים לתיקייה שמכילה את קובצי הלוג של השרת.

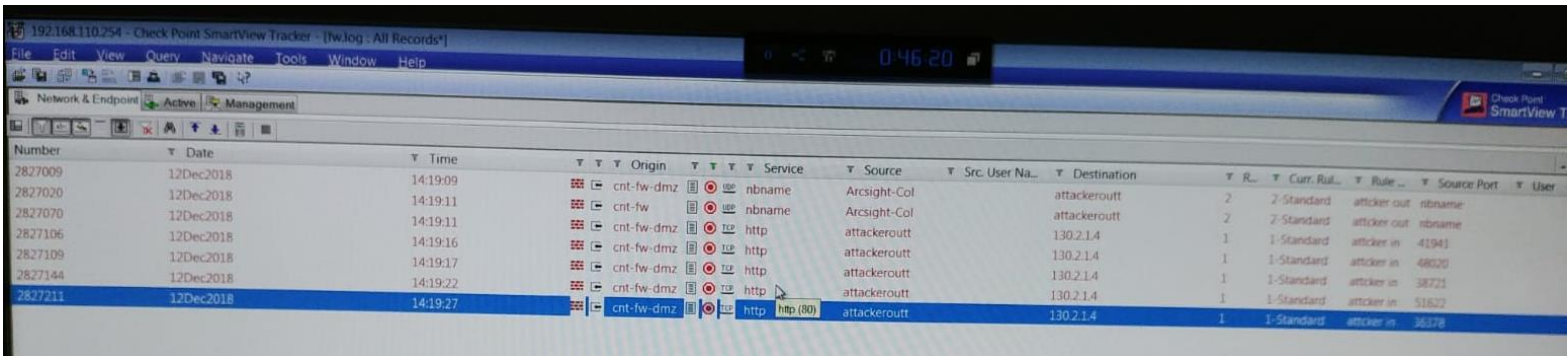
לדעתי לאחר התדרוך בסוף השיעור מראה לי אישית כי חסר לנו הרבה ידע על מנת לגשת לתרחיש כזה שדורש מאיתנו דברים שלא למדנו במהלך לימודינו באריאל ויוצר מצב לא נעים לחלק ניכר מחברי הקבוצה.

<u>תמונות מהאירוע :</u>

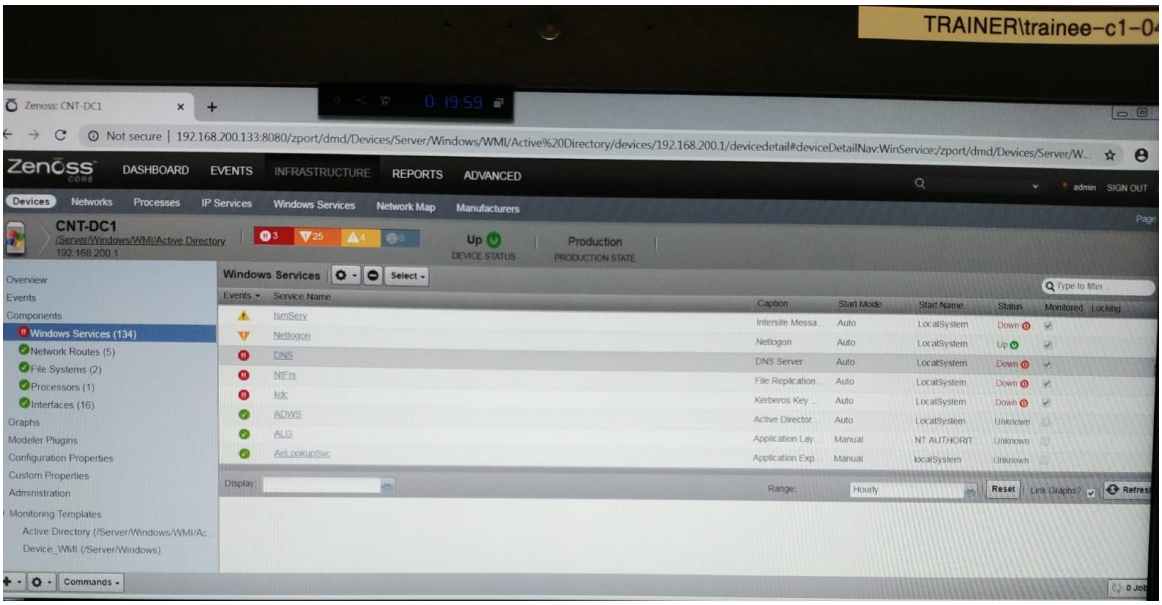
קובץ עם הפקודות שהתוקף ביצע בשרת (לא מה שאורם עשה)



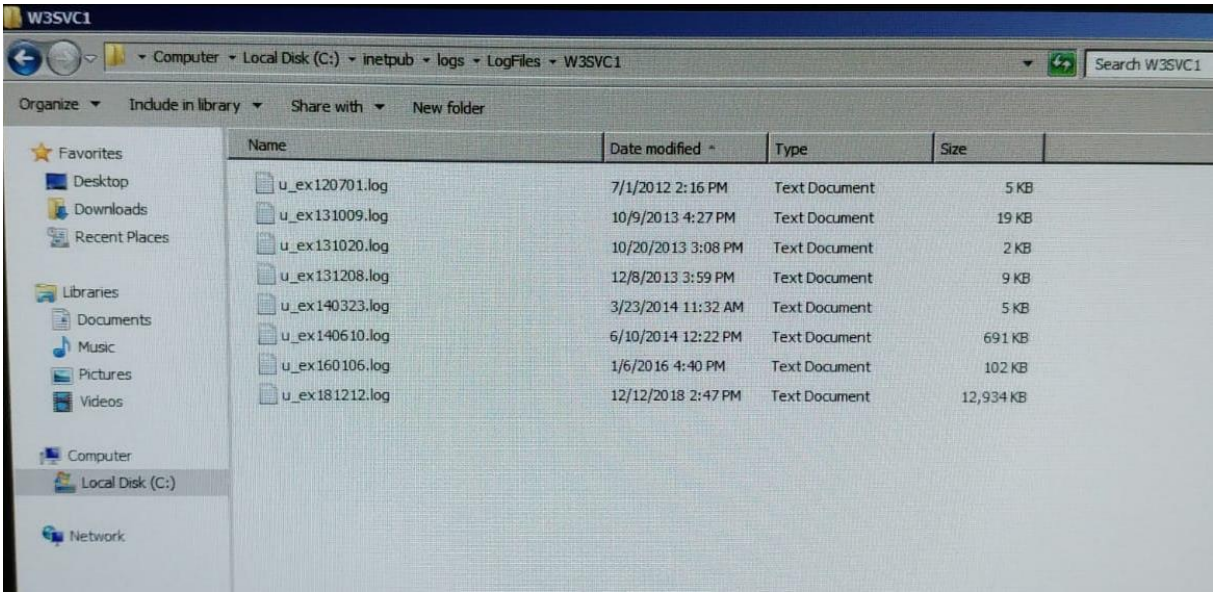
חסימת דרכי כניסה ויציאה של התוקף ב FIREWALL



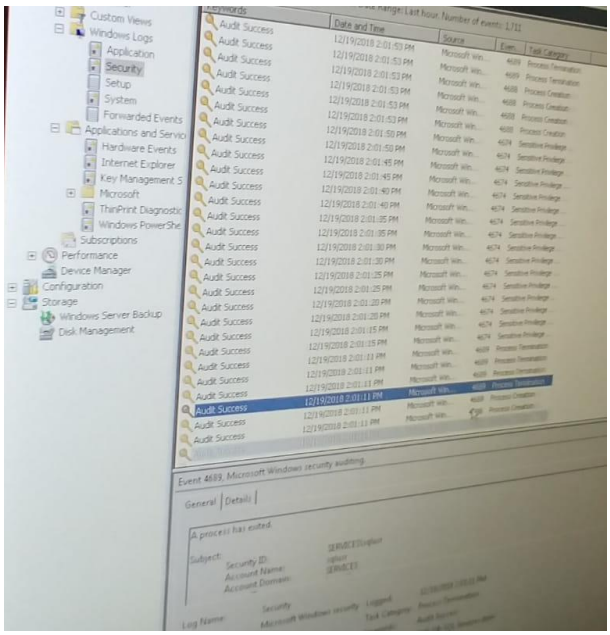
ה-Services שהתוקף עצר בשרת DC1

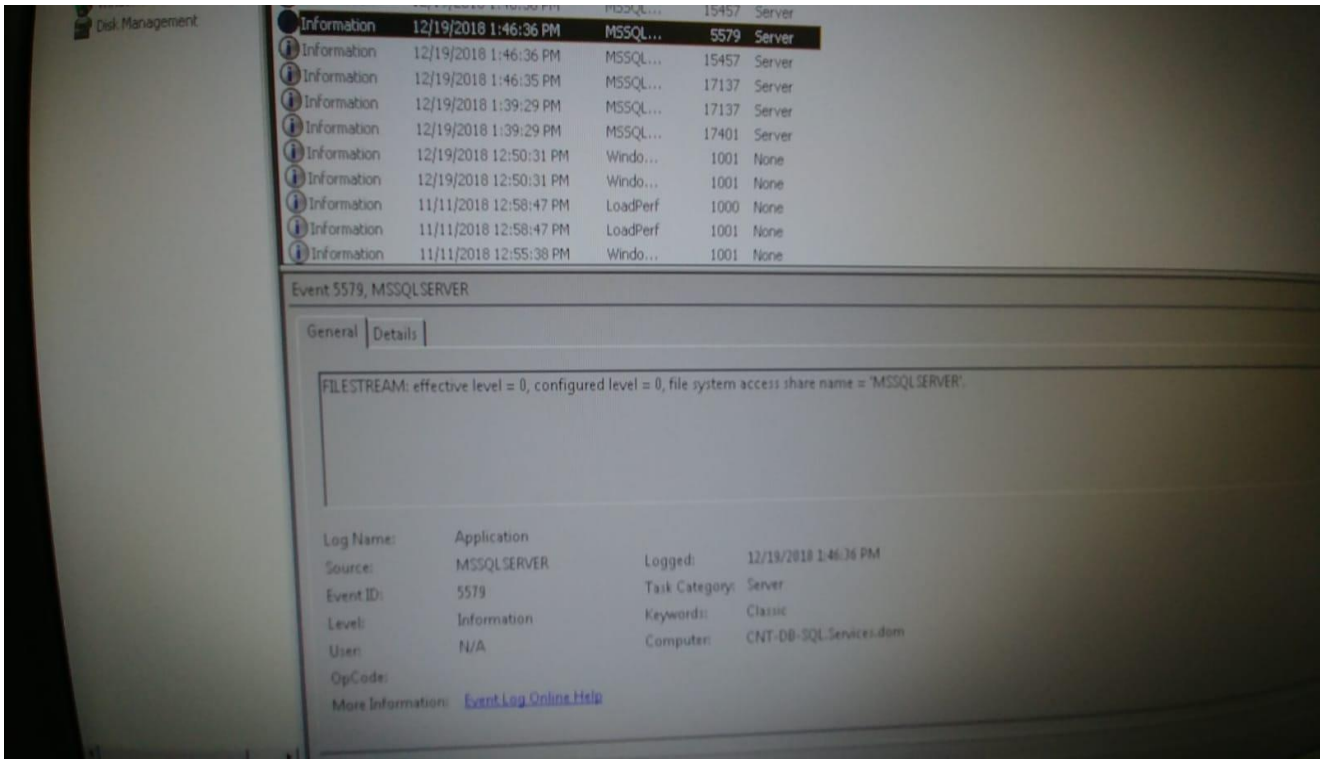


התיקייה שמכילה את קבצי הלוגים בשרת



כאן נמצא כל התמונות שמראות את ה Reconfigure שביצע התוקף:





Information	12/19/2018 1:39:29 PM	MSSQL...	17137	Server
Information	12/19/2018 1:39:29 PM	MSSQL...	17401	Server
Information	12/19/2018 12:50:31 PM	Windo...	1001	None
Information	12/19/2018 12:50:31 PM	Windo...	1001	None
Information	11/11/2018 12:58:47 PM	LoadPerf	1000	None
Information	11/11/2018 12:58:47 PM	LoadPerf	1001	None
Information	11/11/2018 12:55:38 PM	Windo...	1001	None

Event 15457, MSSQLSERVER

General | Details

Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.

Log Name:	Application		
Source:	MSSQLSERVER	Logged:	12/19/2018 1:46:36 PM
Event ID:	15457	Task Category:	Server
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	CNT-DB-SQL.Services.dom
OpCode:			
More Information:	Event Log Online Help		

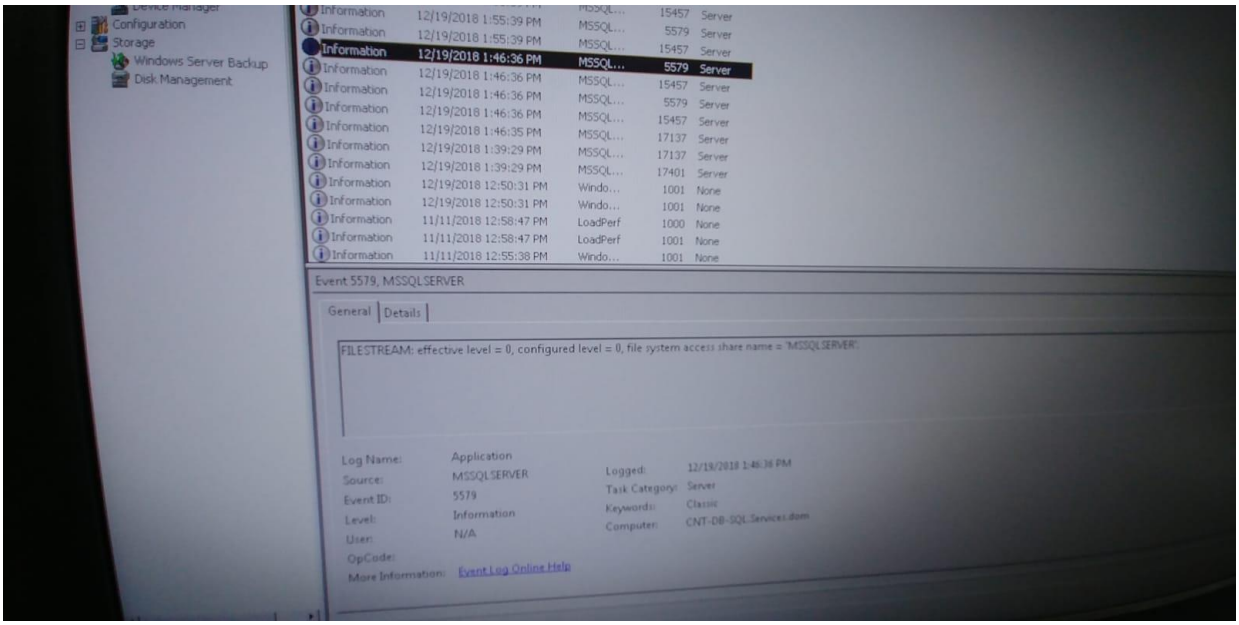
Information	12/19/2018 1:39:29 PM	MSSQL...	17137	Server
Information	12/19/2018 1:39:29 PM	MSSQL...	17137	Server
Information	12/19/2018 12:50:31 PM	Windo...	1001	None
Information	12/19/2018 12:50:31 PM	Windo...	1001	None
Information	11/11/2018 12:58:47 PM	LoadPerf	1000	None
Information	11/11/2018 12:58:47 PM	LoadPerf	1001	None
Information	11/11/2018 12:55:38 PM	Windo...	1001	None

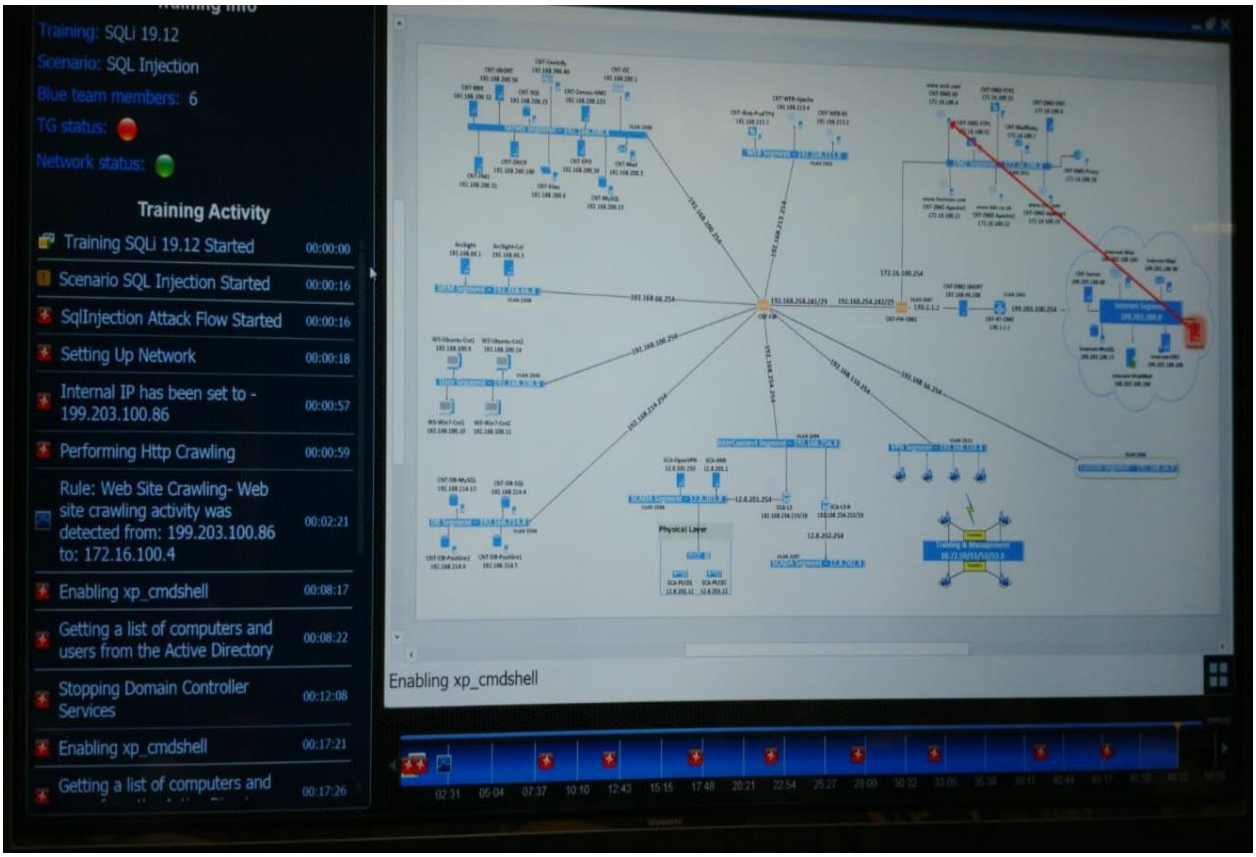
Event 15457, MSSQLSERVER

General | Details

Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.

Log Name:	Application		
Source:	MSSQLSERVER	Logged:	12/19/2018 2:17:27 PM
Event ID:	15457	Task Category:	Server
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	CNT-DB-SQL.Services.dom
OpCode:			
More Information:	Event Log Online Help		


Configuration
Storage
Windows Server Backup
Disk Management
Information 12/19/2018 1:55:39 PM MSSQL... 15457 Server
Information 12/19/2018 1:55:39 PM MSSQL... 5579 Server
Information 12/19/2018 1:46:36 PM MSSQL... 15457 Server
Information 12/19/2018 1:46:36 PM MSSQL... 5579 Server
Information 12/19/2018 1:46:36 PM MSSQL... 15457 Server
Information 12/19/2018 1:46:36 PM MSSQL... 5579 Server
Information 12/19/2018 1:46:35 PM MSSQL... 15457 Server
Information 12/19/2018 1:39:29 PM MSSQL... 17137 Server
Information 12/19/2018 1:39:29 PM MSSQL... 17137 Server
Information 12/19/2018 12:50:31 PM MSSQL... 17401 Server
Information 12/19/2018 12:50:31 PM Windo... 1001 None
Information 11/11/2018 12:58:47 PM Windo... 1001 None
Information 11/11/2018 12:58:47 PM LoadPerf 1000 None
Information 11/11/2018 12:55:38 PM LoadPerf 1001 None
Event 5579, MSSQLSERVER
General
Details
FILESTREAM: effective level = 0, configured level = 0, file system access share name = 'MSSQLSERVER'.
Log Name: Application
Source: MSSQLSERVER
Event ID: 5579
Level: Information
User: N/A
OpCode:
More Information: Event Log Online Help
Logged: 12/19/2018 1:46:36 PM
Task Category: Server
Keywords: Classic
Computer: CNT-DB-SQL.Services.dom


Training: SQLi 19.12
Scenario: SQL Injection
Blue team members: 6
TG status:
Network status:
Training Activity
Training SQLi 19.12 Started 00:00:00
Scenario SQL Injection Started 00:00:16
SqlInjection Attack Flow Started 00:00:16
Setting Up Network 00:00:18
Internal IP has been set to - 199.203.100.86 00:00:57
Performing Http Crawling 00:00:59
Rule: Web Site Crawling- Web site crawling activity was detected from: 199.203.100.86 to: 172.16.100.4 00:02:21
Enabling xp_cmdshell 00:08:17
Getting a list of computers and users from the Active Directory 00:08:22
Stopping Domain Controller Services 00:12:08
Enabling xp_cmdshell 00:17:21
Getting a list of computers and 00:17:26
Physical Layer
Enabling xp_cmdshell