תשובות מאמן סייבר

1) ברגע שאני ארצה להיכנס למכונה אני אצליח להיכנס למכונה ובזמן שחברי יעבוד תוך כדי לא יקרה כלום ונוכל לעבוד יחד על אותה מכונה

2) netstat -na | grep -i established

הפקודה הזאת מציגה את כל החיבורים הפעילים

3) device address היא מיקום זיכרון שממנו רכיב מחשב יכול לקרוא נתונים או לשלוח נתונים.

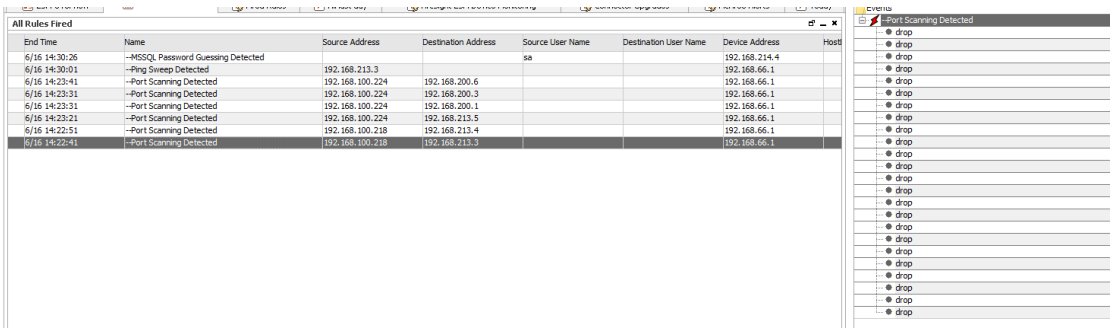
Destination address היא הכתובת אליה שולחים מסגרת או חבילת נתונים ברשת. כתובת היעד משמשת hosts ברשת כדי לקבוע אם החבילה או המסגרת מיועדים להם או ל hosts אחרים.

ההתראה מציינת פעולה חשודה שמתרחשת ברשת ה device address זיהה את הפעילות החשודה מהכתובת 192.168.66.1 וה destination address זו הרשת שבוצעה בו הפעולה החשודה בכתובת 213.0.0.220

4) (dst 172.16.100.21 OR dst 172.16.100.22) AND action:drop

חלק ב'

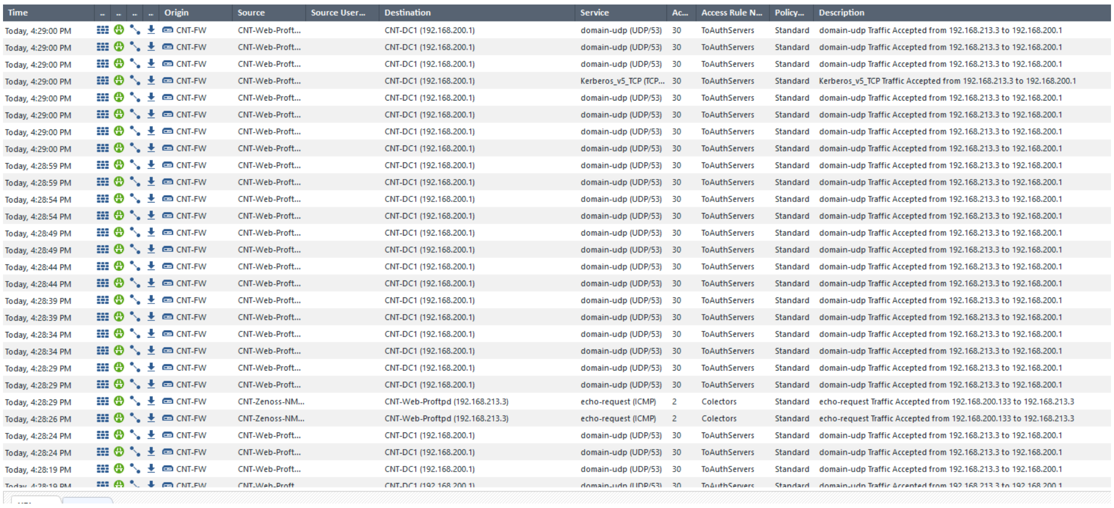
החל משעה 14:22 arcSight הודיע על שורת התראות של סריקות פורטים של המכונות 192.168.213.X לאחר מכן בשעה 14:23 הודיע על סריקות פורטים על המכונות 192.168.200.1, 192.168.200.3, 192.168.200.6 הנמצאות בתוך הארגון, לאחר מכן בשעה 14:30 הודיע על זיהוי sweep ping מהמכונה 192.168.213.3 והתראה על MSSQL Password gussung detected



סריקת פורטים - "משמשת לבירור אילו פורטים פתוחים במחשב מסוים המחובר לרשת מחשבים .הסריקה מבוצעת בדרך כלל על ידי האקר בשלב איסוף המידע על מחשב היעד או איש אבטחת מידע כדי לדאוג לסגור פורטים פתוחים. באמצעות רשימת הפורטים הפתוחים יכול התוקף להסיק אילו שירותי רשת רצים על המחשב הנסרק ובהתאם לכך להפעיל התקפות מתאימות Wikipedia - ".בלשונית בצד ימין של הממשק, תחת הכותרת Inspect\Edit->Event Inspector->Description->Eventאנו רואים פירוט יותר מורחב על ההתראה שזוהתה, רואים אילו פורטים זוהו כפתוחים -accept(הבקשה לפורט מסוים

התקבלה - הפורט פתוח(ו אילו פורטים זוהו כסגורים) - dropהבקשה לפורט מסוים הודחה - הפורט סגור.)

כמובן שזו היא רק דגימה שלפיה ה arcSight זיהה את ההתנהגות החשודה, ובשביל לראות את התמונה המלאה אנו יכולים להתבונן ברשומות של חומת האש עבור כל מכונה לדוגמא המכונה 192.168.213.3:



Time	...	...	...	...	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	Kerberos_v5_TCP (TCP...	30	ToAuthServers	Standard	Kerberos_v5_TCP Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:29:00 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:59 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:59 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:54 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:54 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:49 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:49 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:44 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:44 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:39 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:39 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:34 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:34 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:29 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:29 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:29 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Zenoss-NM...		CNT-Web-Proftpd (192.168.213.3)	echo-request (ICMP)	2	Colectors	Standard	echo-request Traffic Accepted from 192.168.200.133 to 192.168.213.3
Today, 4:28:26 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Zenoss-NM...		CNT-Web-Proftpd (192.168.213.3)	echo-request (ICMP)	2	Colectors	Standard	echo-request Traffic Accepted from 192.168.200.133 to 192.168.213.3
Today, 4:28:24 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:24 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:19 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1
Today, 4:28:19 PM	▦	⊕	↘	⬇	CNT-FW	CNT-Web-Proft...		CNT-DC1 (192.168.200.1)	domain-udp (UDP/53)	30	ToAuthServers	Standard	domain-udp Traffic Accepted from 192.168.213.3 to 192.168.200.1

אנו יכולים לראות שסריקת הפורטים הייתה רחבה בהרבה ממה שראינו בדגימה של הארקסייט