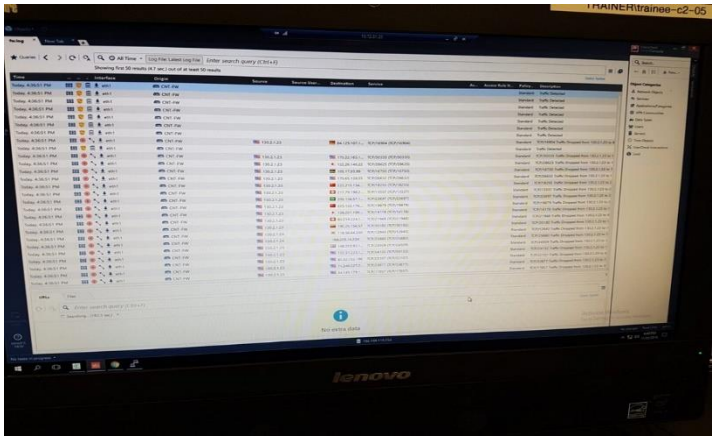
דוח אירוע

מגיש: דור לבקוביץ – 203565015

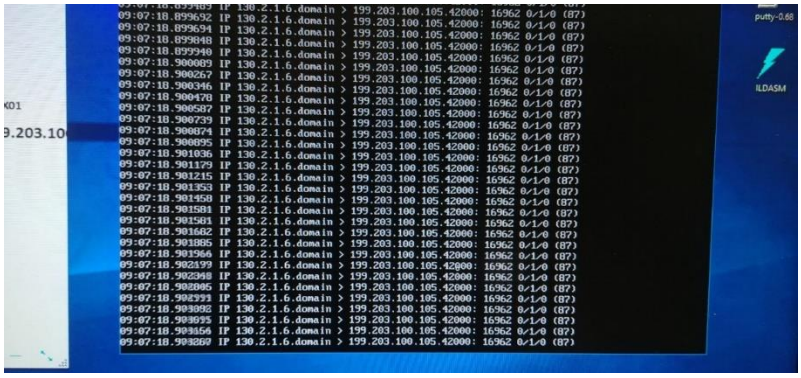
שם תרחיש: DNS AMPLIFICATION

<u>תהליך ההתקפה:</u> התוקף זייף את הכתובת אייפי של ארגון אחר ושלח בקשות לשרת ה- DNS שלנו בארגון מה שגרם לשרת שלנו לשלוח תשובות לכתובת המבוקשת (לכתובת האייפי של הארגון שהתוקף התחזה אליה) לאחר זמן מה הארגון המדובר התלונן בפנינו שאנחנו מעמיסים אותו בתעבורה.

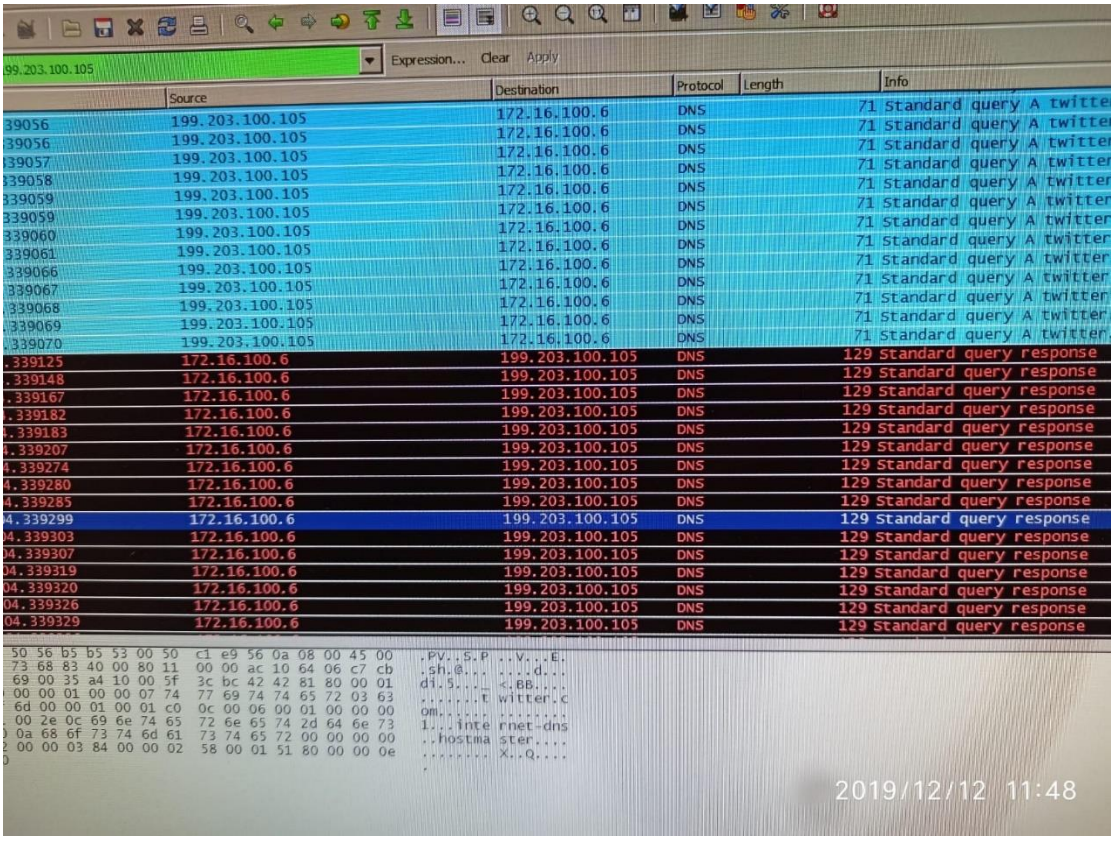
<u>תהליך הזיהוי:</u> הארגון שאליו התחזה התוקף התלונן שאנחנו מציפים אותו בתעבורה מהארגון שלנו. לאחר בדיקה מעמיקה בתוכנה SMART CONSOLE שמנו לב שאכן יש תנועה גדולה לאותו אייפי של הארגון המתלונן (199.203.100.105).



לאחר בדיקה מעמיקה נכנסנו לשרת האחראי על חומת האש באמצעות ה- PUTTY ושם הרצנו את הפקודה tcpdump שמטרתה לנתר את התנועה ברשת ושם גילינו ששרת ה- DNS הוא זה שמבצע את שליחת הפינגים לאייפי.



לאחר מכן התחברנו לשרת דרך תוכנת vsphere והרצנו בשרת תוכנה בשם WIRESHARK שתפקידה לנתח את כל התנועות ברשת (גם מוסתרות ומוצפנות).



כך גילינו בעצם שנשלחות לשרת בקשות לאתר טוויטר מכתובת ה- IP של הארגון וה- DNS בעצם מקבל את הבקשות ושולח בחזרה תשובות.

<u>תהליך ההגנה הראשוני:</u> לא עשינו פעולות על מנת למנוע את התקיפה אבל ידענו מה קרה.

תהליך הגנה מונעת: לעצור את התנועה החשודה באותו הרגע ולהגדיר חוקים נוקשים יותר ב SNORT ובכך למנוע או לפחות להקשות על פעולה שכזאת בעתיד

<u>הסבר מפורט על אופן ההתקפה (התמקדות בחולשות):</u> התוקף בעצם התחזה לכתובת אייפי תמימה ובכך בעזרתנו הצליח להציף את אותו ארגון. השרת DNS לא ידע לזהות את כמות והתזמון ופשוט שלח תשובות בלי הפסקה לארגון והציף אותו

<u>כלים חדשים שפיתחתם/השתמשתם:</u> VSPHERE שזאת מערכת לשליטה מרחוק למערכות הפעלה ווינדוס, WIRESHARK מראה ניתוח של מפורט של כל התנועה ברשת.

אופן עבודת הצוות: בהתחלה היה קצת חוסר סינכרון אבל בסוף היה איפוס בין כולם והגענו לפיתרון בסוף.

<u>חוסרים/קשיים/בעיות:</u> לקח לנו הרבה זמן לקלוט מה קורה בהתחלה עד שהתעשתנו והצלחנו לעלות על המקרה