מטלת סיום – רשתות תקשורת

חלק ראשון:

1.

- עומס ברשת (Network Congestion) המאט את קצב ההעברה
- איבוד פקטות (Packet Loss) המוביל לשידורים חוזרים
- זמן השהיה גבוה (Latency) שמשפיע על רוחב הפס
- הפרעות של חומת אש או אנטי-וירוס המעכבים חבילות מידע
- הגבלות רוחב פס על ידי ספק האינטרנט / תשתית
- פתרון: שימוש ב Wireshark-לניטור רשת, בדיקת רוחב פס, והתאמת גודל חלון TCP

2.

- בקרת זרימה מונעת הצפה של המקבל על ידי ויסות קצב השידור
- כאשר השולח חזק בהרבה מהמקבל, הוא חייב להאט את הקצב
- יתרון: מונע איבוד נתונים
- חסרון: עלול לגרום לזמני המתנה ולירידה ביעילות

3.

- קיצור מסלול מפחית זמן השהיה
- שימוש במסלול בעל רוחב פס גבוה משפר ביצועים
- עומס רשת גורם להאטה במסלול מסוים
- איזון עומסים (Load Balancing) משפר ביצועים
- QoS מסייע בתיעדוף תעבורה חשובה

4.

- שימוש במספר נתיבים במקביל מגביר תפוקה
- מספק יתירות במקרה של כשל נתיב
- מפחית עומסים על ידי פיזור תעבורה
- דוגמה: מכשיר נייד המשתמש ב WiFi-וב LTE-במקביל

5.

- עומס רשת ותורים מלאים בנתבים
- שגיאות ניתוב או בחירת מסלול לא אופטימלית
- כשל במנגנון TCP שגורם לשידורים חוזרים מיותרים
- פתרון: ניטור רשת עם ,Wireshark בדיקת עומסים, התאמת ניתוב ושיפור תשתית

חלק שני:

FlowPic זיהוי תעבורה מוצפנת באמצעות זיהוי תמונה:

- תרומה מרכזית :מציג שיטה הממירה זרמי נתונים לתמונות לזיהוי בעזרת.CNN
- מאפייני תעבורה בשימוש :

  גודל מנות וזמני הגעה

  דפוסי תעבורה מוצפנים
- מסקנות :דיוק גבוה בזיהוי שירותים שונים גם ב VPN-ו.Tor-

מיון מוקדם של תעבורה עם ClientHello מוצפן

- תרומה מרכזית :שימוש בהודעות ClientHello של TLS לזיהוי תעבורה מוקדם.
- מאפייני תעבורה בשימוש :

  חתימות.TLS

  מערכות הצפנה ומידע על אישורים.
- מסקנות :מאפשר זיהוי תעבורה מוצפנת בדיוק גבוה.

ניתוח תעבורה מוצפנת ב HTTPS-לזיהוי מערכת הפעלה ודפדפן

- תרומה מרכזית :זיהוי מערכת ההפעלה, הדפדפן והאפליקציות דרך ניתוח.HTTPS
- מאפייני תעבורה בשימוש :

  פרמטרים של ידית TLS

  פרטי תעודות SSL

  דפוסי חיבור ייחודיים.
- מסקנות :דיוק גבוה בזיהוי מערכת ודפדפן גם ללא גישה למידע מפוענח.

חלק שלישי:

מהתשובות בפורום הקורס הבנתי שניתן לבצע את הגרפים באמצעות Wireshark אז זה מה שעשיתי והם מצורפים להגשה. **ההקלטה של zoom גדולה מידי אז הקטנתי אותה מספיק שאני אוכל לעלות אותה ושלחתי אותה בנפרד משאר הקבצים.**

בנוסף לפי ניתוח הגרפים ניתן להבין שיש חתימה לכל אפליקציה במדגם שלנו כגון: הTTL של zoom אינה מאוזנת ומשתנה עם הזמן לעומת YouTube שלאורך הזמן הייתה מאוזנת, בנוסף קבלת החבילות שהתקבלה בyoutube ממותנת יותר לעומת zoom שקופצת לאורך הגרף. וכן כמובן שאר האפליקציות ניתן להסיק הבדלים וככה גם חתימה לכל אפליקציה ולכן גם כשהתעבורה מוצפנת, דפוסי גדלים ותזמון של חבילות עשויים להספיק כדי לנחש באיזו אפליקציה או אתר מדובר – במיוחד אם ידוע לכל session מזהה כלשהו (כמו 4־tuple). ללא המידע על ה־4־tuple, הניתוח קשה יותר, אבל עדיין אפשר לעיתים לזהות סוגים כלליים של תעבורה. כדי למנוע זאת, מומלץ להשתמש בכלים כמו VPN/Tor וטכניקות Padding שמקשות על ניתוח תבניות התעבורה.

חלק רביעי:

מצורפת גם היא להגשת המטלה.