פרוטוקולים:

## TCP- transmission control protocol. פרוטוקול הנמצא בשכבת התעבורה. כל ייסוד קשר בין שני מחשבים תופס מספר פורט באופן בלעדי ולא ניתן לתקשר בין מספר מחשבים במקביל על אותו פורט. העברת המידע נעשה בצורה מבוקרת בעזרת יצירת חיבור מקושר הפועל על פי מנגנון three way handshake\*. הפרוטוקול מפרק את ההודעות שעוברות לחלקים קטנים הנקראים segments הממוספרים לפי סדר ומועברים לפרוטוקול IP כדי להרכיב מהם חבילות בהגעתם ליעד. פרוטוקולים רבים רוכבים על פרוטוקול TCP לשם שלמות העברת המידע.

\* three way handshake- מנגנון שפרוטוקול TCP משתמש בו להקמת קשר בין היעד למקור. למנגנון שלושה שלבים: 1.syn- תחנת המקור שולחת הודעה לתחנת היעד ובה הרצון שלו לפתיחת קשר. 2.syn-ack- תחנת היעד מקבלת את ההודעה שולחת בחזרה הודעה על אישור קבלה ופתיחת הקשר מצידה. מרגע זה תחנת היעד יכולה להתחיל לשלוח נתונים. תחנת היעד בנוסף מוסרת כי היא מתחילה מספור התחלתי של חתיכות המידע שישלחו. 3.ack- תחנת המקור מיידעת את תחנת היעד על סיום מיסוד הקשר ועל המספור ההתחלתי שלה.

## UDP- user datagram protocol. זהו פרוטוקול משכבת התעבורה הדוגל בשטית "שגר ושכח". שיטה זו מספק מעבר מידע במהירות מבלי ביצוע בדיקת פלט ואמינות המקור. שימושו העיקרי מתבצע בשיחות וידיאו, סרטוני וידיאו והזרמת שמע ובמקרים נוספים בהם רצוי שהמידע יגיע מיד. חבילות המידע עלולות להגיע בסדר שונה מזה שבו הן נשלחו, להגיע מספר פעמים או ללכת לאיבוד ולא להגיע בכלל. בפרוטוקול UDP יכול מחשב לתקשר עם מספר מחשבים על אותו פורט במקביל. התכונה העיקרית של הפרוטוקול היא שהוא אינו יוצר חיבור לפני העברת הנתונים.

QUIC- פרוטוקול משכבת התעבורה. הפרוטוקול מהווה יותר ממחצית מכל החיבורים של דפדפן הCHROME אל שרתי הGOOGLE. דפדפנים רבים תומכים בו ביניהם: safari, Firefox, chromium ועוד. השם של הפרוטוקול הוא אינו ראשי תיבות אך מקורו היה : "Quick UDP Internet Connections". הפרוטוקול מהווה שיפור לביצועים של יישומי האינטרנט המשתמשים בפרוטוקול TCP וזאת באמצעות יצירת מספר חיבורים בין שתי נקודות קצה באמצעות פרוטוקול UDP. בין תפקידיו הנוספים של הפרוטוקול ישנם: הפחתת זמן החיבור והשינוע והערכת רוחב פס לכל כיוון למניעת עומסים.

TLS/SSL- transport layer security/secure sockets layer, פרטוקול בשכבת התעבורה המהווה מאחד מפרוטוקולי האבטחה החשובים והפוצים ביותר של האינטרנט. מטרתו לאבטח שיחות שרת/לקוח בשיטות קריפטוגרפיות חזקות ובכך למנוע זיוף/חבלה או ציתות של המידע שעובר בין השרת ללקוח. הפרוטוקול מאפשר התחברות אנונימית, אימות חד/דו צדדי עם שמירה על דיסקרטיות ושלמות המסר. הרבה פרוטוקולים שאינם מאובטחים משתמשים בפורט ייעודי ובתוספת (S) לשם הפרוטוקולים הם מאובטחים ובכך המידע שעובר בהם מוצפן על ידי פרוטוקול TLS/SSL.

IPSEC- internet protocol security. חבילת פרוטוקולים המספקים שירותי אבטחה בשכבת הרשת. הוא מגדיר את האלגוריתם לשימוש המערכת, ומשתמש ב-"מפתח" מוצפן כדי לספק תקשורת מאובטחת בין מחשבים או רשתות. הפרוטוקול פותח כדי להגן על חבילת ה-IP, מבלי לשנות את פרוטוקול ה-IP עצמו. IPsec מספק זיהוי של השולח, וידוא שלמות של חבילות, IP הצפנת תוכן החבילות, מניעת שליחה מחדש של חבילות ישנות והגנה נגד ניתוח התעבורה ברשת ובנוסף לכך, IPSec יכול להגן על כל חבילת ה-IP (התוכן הפנימי-DATA והחלק החיצוני HEADER) או רק על החלק הפנימי שלה.

FTP- file transfer protocol. פרוטוקול תקשורת המבוסס על TCP להעברת קבצים בין מחשבים. הפרוטוקול נמצא על פורט 21 ו-20, כאשר מעוניינים לבצע התחברות (Login) נשתמש בפורט 21 של פרוטוקול ,TCP ולאחר האימות ייפתח סשן (שיחה) חדש לשם העברת הקבצים בפורט 20. השימוש בפרוטוקול נפוץ באופן יחסי, ושירותי אחסון הקבצים "בענן" שגם הם מתבססים על FTP בגלל הקלות של שיתוף המידע ולעיתים קרובות האבטחה המוגברת. לפרוטוקול אין אבטחה והצפנה, הפתרון המקובל לבעיה זו הוא שימוש ב-SFTP וב-FTPS, המוסיפים הצפנה (בעזרת פרוטוקול SSH) לפרוטוקול.

SMB- Server Message Block. פרוטוקול בשכבת האפליקציה הנמצא על פורט 445.שימושו העיקרי הוא למטרת סיפוק גישה משותפת אל קבצים, מדפסות ומשאבים בין מחשבים ברשת. בנוסף הפרוטוקול מסםק מנגנון תקשורת מאומת בין תהליכים. הפרוטוקול עובד בשיטת שרת-לקוח ומספק ליישומי הלקוח שיטה מאוטחת ומבוקרת לפתיחה, קריאה, העברה, יצירה ועדכון של קבצים בשרתים מרוחקים.

SSH- secure shell. פרוטוקול המאפשר התחברות מרוחקת למחשב לאחר אימות חזק, ואפשור ביצוע פעולות מרוחקות תוך ביצוע תקשורת מאובטחת ומוצפנת בין מחשבים לא תלויים ברשתות לא מאובטחות.הפרוטוקול נמצא על פורט 22 בשכבת התעבורה. הגרסה הראשונה שיצאה התבססה על תוכנה פתוחה וחופשית וספריות GNU. הפרוטוקול הוא הגרסה המאובטחת של פרוטוקול TELNET. פרוטוקול SSH משתמש בהצפנה כדי לאבטח את החיבור בין לקוח לשרת. כל אימות המשתמש, הפקודות, הפלט והעברת הקבצים מוצפנים כדי להגן מפני התקפות ברשת.

TELNET- TELecommunication NETwork. פרוטוקול המשמש לתקשורת בין שרתים ברשת האינטנרט ו/או ברשתות מקומיות. החיבור נעשה בעזרת שורת פקודה בין המחשבים ברשת. בעזרת הפרוטוקול ניתן להרית תוכנות, לעבוד עם מערכות קבצים, להעביר קבצים, להפעיל/להפסיק פעולה של שירותים ולברר אם פורטים פתוחים. הפרוטוקול ברוב המקרים משומש מול שרתי לינוקס מאחר והוא ממשק קרקטריאלי. הפרוטוקול אינו מאובטח והפקודות שעוברות בו אינן מוצפנות כך שניתן לצותת למידע הרגיש , לפתרון בעיה זו נוצר פרוטוקול SSH המצפין את תעבורת המידע.

 IMAP- internet messaging access protocol. פרוטוקול המשמש לגישה לדואר אלקטרוני שנמצא על שרת מרוחק ממחשב מקומי. מהווה אלטרנטיבה מתקדמת יותר מפרוטקוך pop3. פרוטוקול זה נותן למשתמש יכולת לנהל את תיבות הדואר שלו ולעבוד עם מספר תיבות דואר, אך הוא קשה לעבודה ולכן אינו פופלרי כל כך. זהו פרוטוקול טקסטואלי בלבד ובעת הורדת דוא"ל הוא מוריד רק את הכותרת והתוכן הטקסטואלי וכך חוסך בנפח ההורדה ונפח המקום. רץ על פרוטוקול TCP ונמצא על פורט 143. הגרסה המאובטחת של הפרוטוקול (בעזרת פרוטוקול SSH) משוייך לפורט 993.

POP3- Post Office Protocol version 3. פרוטוקול לשליפת וקריאת הודעות דואר אלקטרוני משרת דואר מרוחק. הפרוטוקול עובד בשיטת שרת-לקוח בשכבת האפליקציה על פורט 110. הפרוטוקול נועד למשתמשים שאין להם חיבור קבוע לשרתי דואר. הפרוטוקול כעצמו אינו מצפין את ההודעות ושולח אותן כהודעת טקסט גלוי, אך עם הרחבות שונות ניתן לפתור בעיה זו. השימוש בפרוטוקול פשוט מאחר ומתכנתיו בנו אותו עם תכונות דלות יחסית. קריאת הדואר על ידי הלקוח מתבצעת באמצעות הפרוטוקול.

DNS- domain name system. פרוטוקול המשמש לתרגום כתובות IP לשמות תחום (כתובות URL) ולהיפך. זהו פרוטוקול משכבת האפליקציה הנמצא על פורט 53. על שרתי הDNS נמצאות טבלאות המכילות שמות מחשב וכתובות IP, כאשר לקוח שולח בקשת DNS, השרת מחפש תחילה בטבלה הנמצאת בזיכרון הcache שלו. במידה ולא נמצאה כתובת ה-IP/שם התחום מהשאילתה יתבצע תהליך הDNS. פרוטוקול הDNS רץ כברירת מחבל על פרוטוקל UDP שמקנה לו מהירות אך פוגע באבטחה ובאמינות שלו. הפרוטוקול מאפשר גישה למסד נתונים מבוזר זאת כדי שיחידות קצה ברשת האינטרנט יוכלו לתרגם שמות תחום לכתובות IP. תהליך התרגום מתבצע כך: שרת הDNS פונה לרמה ההיררכית הראשונה שנקראת רמת השורש “root level” רמה זו כוללת את סיומת שם הדומיין הנקודה, לאחר שזיהה את הסיומת הוא עובר לרמה הבאה שהיא רמת הtop level domain שם השרת יזהה את שם סיומת כתובת האתר (למשל אם זה ארגון/מדינה וכו), לאחר הזיהוי הוא ימשיך לרמה הבאה שהיא second level domains שבה השרת יזהה לפי הרמה הקודמת את המאגר ממנו יקח את הכתובת (אם הסיומת היא IL השרת יחפש במאגר של כלל הכתובות של אתרים מסחרים בישראל). לבסוף תתקבל כתובת שלמה לאתר שאליו בקשת הDNS רצתה לגשת.

LLMNR- link local multicast name resolution. פרוטוקול משכבת האפליקציה ונמצא על פורט 5355. הפרוטוקול משומש במקום פרוטוקול DNS לצורך תרגום שמות תחום של מחשבים סמוכים ברשת המקומית (LAN). הפרוטוקול מבית מייקרוסופט, כך שהוא פועל רק בסביבת WINDOWS. שאילתות LLMNR נשלחות ומתקבלות דרך פרוטוקול UDP בעיקר למרות שניתן להשתמש גם בפרוטוקול TCP. השאילתות נשלחות כהודעות MULTICAST לכל המחשבים ברשת הLAN ורק המחשב שרלוונטי אליו הבקשה עונה ישירות למחשב המתשאל. פרוטוקול LLMNR מבוסס על פרוטוקול DNS.

NetBIOS (NBNS)- network basic input/output system. פרוטוקול משכבת האפליקציה הנמצא על פורט 137, בדרך כלל הפרוטוקול משתמש בפרוטוקול UDP ולעיתים רחוקות בפרוטוקול TCP. הפרוטוקול הוחלף על ידי פונקציות DNS שונות. הפרוטוקול משומש בעיקר ברשתות מקומיות לצורך איסוף מידע על שמות NETBIOS באותה הרשת. הנתונים נאספים למסד הנתונים שדרכו הנתונים מצטלבים בין עמדות קצה, מאחר והפרוטוקול אינו היררכי ישנו קושי בהבדלה בין עמדות קצה של ניהול, שרת ומשתמש.

HTTP1.X- hypertext transfer protocol. HTTP הוא פרוטוקול המשמש להעברת היפר טקסט (הכוונה היא להעברת דפי html של האתרים, בין אם מדובר בתמונות, קבצי קול או סרטונים). פרוטוקול HTTP מספק תקשורת בין מערכות תקשורת שונות. כאשר המשתמש מבקש להיכנס לאתר כלשהו, שרת האינטרנט שולח את הנתונים המבוקשים למשתמש בצורה של דפי אינטרנט. כך שלמעשה, פרוטוקול HTTP מאפשר לנו להעביר את הנתונים מהשרת ישירות ללקוחHTTP .  הוא פרוטוקול משכבת האפליקציה ונמצא על פורט 80. פרוטוקול זה אינו מאובטח. לאורך השנים יצאו גרסאות מעודכנות וחדשות לפרוטוקול, השינויים העיקריים היו: הוספת שיטות בקשה, קוד מיוחד שמציין את תוצאות הבקשה, , יעול השליטה על המטמון, ייעול אופן הפעלת הפרוטוקול, שינוי ושיפור מנגנון שליחת הבקשות ואופן מעבר המידע.

HTTPS- hypertext transfer protocol secure. פרוטוקול המאפשר מעבר נתונים באופן מאובטח. העברת הנתונים נעשת בצורה מאובטחת ומונעת העברה של מידע לצד אחד. פרוטוקול HTTPS הוא הגרסה המאובטחת של פרוטוקול HTTP זאת באמצעות הוספת פרוטוקול SSL ויישום מודל TLS המשמשים כמנגנון לאבטחה והצפנה אסימטרית. זהו פרוטוקול משכבת האפליקציה והוא נמצא על פורט 443. הפרוטוקול מוסיף הזדהות בעת ההתחברו לאתר, הצפנה דו כיוונית על תעבורת המידע בין הלקוח לשרת, והבטחה כי הלקוח יגיע לאתר שאליו מבקש לגשת.

RPC- remote procedure call. פרוטוקול המאפשר לתוכנית שרצה במחשב אחד לבקש שירות מתוכנית הרצה על מחשב אחר ברשת באופן שקוף, ללא צורך ביישום פרטני של פרוטוקול תקשורת. הפרוטוקול מבוסס על מודל של שרת לקוח. התוכנית המבקשת שירות היא הלקוח והתוכנית שמספקת את השירות היא השרת. הפרוטוקול נמצא על פורט 135 בשכבת האפליקציה. במידה והרצת הפונקציה מרחוק נכשלה, המחשב המוקמי שהריץ אותה אינו יודע אם היא בוצעה או לא. RPC מבצע Session ראשוני בפורט 135 אך המשך העבודה מתבצע בפורט גבוה (1024-65535) דבר היוצר אתגר לאבטחת המידע.

RDP- Remote Desktop Protocol. פרוטוקול מבית מייקרוסופט המאפשר למשתמש גרפי להתחבר בצורה מלאה לשולחן עבודה מרוחק דרך חיבור רשתי. הפרוטוקול נמצא על פורט 3389 כברירת מחדל אך בעזרת הregistry ניתן לשנות זאת. יתרונו של הפרוטוקול הוא שאין דרישה לVPN ברשת המקומית. RDP מאפשר לשני מכשירים מרוחקים להחליף מידע בבטחה בערוץ תקשורת מאובטח ומוצפן. כדי להבטיח שכל המידע שנשלח בין המכשירים יישאר מאובטח, RDP מצפין את כל הנתונים המועברים. נתונים אלה כוללים הקשות, תנועות עכבר, תצוגות שולחן עבודה ומידע חיוני אחר.

NTP- Network Time Protocol. פרוטוקול המאפשר להתקני רשת לקבל את השעה המדויקת מהתקני רשת אחרים המשמשים כ-Time Server. הפרוטוקול משמש כמערכת סנכרון זמן עבור שעוני מחשב דרך רשת האינטרנט. הפרוטוקול מבטיח דיוק וסנכרון של זמן בין מכשירים, רשתות ומדינות. אי התאמה של אפילו מעיט שניה עלול לגרום לבעיה. הפרוטוקול חינמי וזמין לציבור דרך האינטרנט. מחשבים המיועדים להיות שרתי זמן מצויידים במקלט המיועד לכך, אליו מתחברים המחשבים ובעזרת הפרוטוקול הם מסנכרנים את זמני השעון של המחשבים.

SNMP- Simple Network Management Protocol. פרוטוקול לניהול רשת המשמש לניהול וניטור של מכשירים המחוברים לרשת. הפרוטוקול מוטמע בהתקנים מקומיים כמו: switch, router, חומות אש, שרתים ונקודות גישה אלחוטיות. הפרוטוקול מספק מנגנון נפוץ עבור התקני רשת להעברת מידע ניהול בתוך סביבות LAN או WAN יחידות ומרובות ספקים. הפרוטוקול הוא משכבת האפליקציה ונמצא על פורטים 161 ו-162. הפרוטוקול בדרך כלל מיושם באמצעות פרוטוקול UDP. למרות יכולותיו, השימוש בפרוטוקול ברוב המקרים הוא לקבלת נתונים ולא לשינוי הגדרות תצורה.