פרוטוקולים ופורטים חשובים לSOC

פרוטוקול TCP (Transmission Control Protocol)

מה זה TCP?

הוא פרוטוקול תקשורת ברשת המתפקד כחלק מה-Internet Protocol Suite. הוא מבוסס על חיבור (connection-oriented protocol), כלומר לפני העברת הנתונים יש צורך בהקמת חיבור בין המחשב השולח למחשב המקבל.

מה השימוש?

משמש להעברת נתונים בצורה אמינה ואחראית. הוא התשתית למספר שירותים באינטרנט כגון גלישה באינטרנט (HTTP/HTTPS), דואר אלקטרוני (SMTP, IMAP, POP3), העברת קבצים (FTP) ועוד.

איך הוא עובד?

מתחיל בתהליך של "שלוש פעימות" (Three-Way Handshake) שמוודא את יצירת החיבור:

1. **SYN**: המחשב השולח שולח הודעת SYN (synchronize) לשרת כדי להתחיל את החיבור.
2. **SYN-ACK**: השרת מגיב בהודעת SYN-ACK (synchronize-acknowledge) כדי לאשר את קבלת הבקשה.
3. **ACK**: המחשב השולח משיב בהודעת ACK (acknowledge) שמאשרת את קבלת ההודעה מהשרת. לאחר מכן, הנתונים מחולקים לקטעים, מסומנים ומועברים בצורה מסודרת, תוך כדי שליחת אישור (ACK) על כל קטע שהתקבל.

על איזה פורט הוא רץ?

- פורטים משתנים לפי השירותים, לדוגמה:
  - **HTTP**: פורט 80 (TCP)
  - **HTTPS**: פורט 443 (TCP)
  - **FTP**: פורט 21 (TCP)

יתרונות:

- **אמינות גבוהה**: מבצע אישור קבלה של כל חבילה, מה שמבטיח שהנתונים הגיעו בשלמותם.
- **שליטה בשגיאות**: כולל מנגנון תיקון שגיאות כדי להבטיח שהמידע לא יאבד.
- **סדר במידע**: החבילות מתקבלות ומסודרות בסדר הנכון.

חסרונות:

- **אטיות יחסית**: התהליך של הקמת חיבור והבקרה על העברת הנתונים גורם ליותר זמן שליחה.
- **צריכת משאבים**: נדרשים משאבים נוספים לניהול החיבור ותהליכי האישור.

- **עומס על הרשת**: עלול להעמיס על הרשת במצבים של העברת נתונים רבים.

פרוטוקול UDP (User Datagram Protocol)

מה זה UDP?

הוא פרוטוקול תקשורת ברשת שאינו מבוסס על חיבור (connectionless protocol). הוא מאפשר שליחת נתונים מבלי לבדוק אם הם הגיעו ליעד או באיזה סדר.

מה השימוש?

מתאים להעברת נתונים בקצבים גבוהים ובזמן אמת, כמו סטרימינג של וידאו, שיחות VoIP, משחקים מקוונים, עדכוני GPS ואפליקציות שדורשות זמן תגובה קצר.

איך הוא עובד?

שולח חבילות מידע (datagrams) מבלי לבדוק את המצב של היעד או לספק מנגנון אישור. החבילות נשלחות על ידי הלקוח לשרת, אך אין הבטחה שהן יגיעו או יגיעו בסדר הנכון.

על איזה פורט הוא רץ?

- פורטים משתנים לפי היישום, לדוגמה:
  - **DNS**: פורט 53 (UDP)
  - **NTP**: פורט 123 (UDP)
  - **VoIP (SIP)**: פורטים 5060, 5061 (UDP)

יתרונות:

- **מהירות גבוהה**: העברת נתונים מהירה יותר מאשר TCP, כי אין צורך במנגנוני אישור.
- **פשטות**: קל יותר ליישום ומחייב פחות משאבים.
- **מתאים לסטרימינג ויישומים בזמן אמת**: מספק חיבור עם זמן תגובה מהיר.

חסרונות:

- **אין ביטחון באמינות**: נתונים יכולים לאבד מבלי שהלקוח יידע על כך.
- **ללא תיקון שגיאות**: אין מנגנון לתקן טעויות בהעברת המידע.
- **חוסר סדר**: חבילות עלולות להגיע בסדר שונה ממה שנשלחו

פרוטוקול Kerberos

מה זה Kerberos?

פרוטוקול לאימות משתמשים ברשת מבוזרת, המיועד להבטיח תקשורת מאובטחת בין מחשבים ואפליקציות.

מה השימוש?

נמצא בשימוש במערכות כמו Microsoft Active Directory ובמערכות Unix/Linux לצורך אימות והענקת גישה מאובטחת לשירותים ברשת.

איך הוא עובד?

מבצע אימות על ידי שימוש ב"Tickets" (כרטיסים). התהליך כולל שלושה שלבים עיקריים:

1. **התחברות לשרת Kerberos**: הלקוח מבקש כרטיס גישה (TGT - Ticket Granting Ticket).
2. **בקשה לשירות ספציפי**: הלקוח שולח את ה-TGT לשרת Kerberos כדי לקבל כרטיס גישה לשירות מסוים.
3. **גישה לשירות**: הלקוח מציג את כרטיס השירות לשרת השירות על מנת להתחבר.

על איזה פורט הוא רץ?

- **פורט 88 (TCP/UDP)**

יתרונות:

- **אימות חזק**: משתמש בהצפנה מתקדמת ואימות דו-שלבי.
- **יעילות**: אפשרות להתחבר לכמה שירותים שונים לאחר אימות אחד.
- **הגנה מפני התקפות**: מנגנון מוגן מפני התקפות כמו זיוף זהות.

חסרונות:

- **מורכבות בהתקנה**: דורש תכנון והגדרה מוקדמת.
- **תלות בשעון**: סנכרון זמן מדויק בין הלקוח לשרת קריטי לפעולה.
- **סיכון של כרטיסים גנובים**: גניבת כרטיסים עלולה לסכן את האבטחה.

פרוטוקול VPN (Virtual Private Network)

מה זה VPN?

רשת פרטית וירטואלית המאפשרת למכשירים להתחבר לרשת פרטית דרך האינטרנט באמצעות חיבור מוצפן.

מה השימוש?

משמש להגנה על פרטיות המשתמשים, חיבור מאובטח לרשתות ציבוריות, גישה מרחוק לרשתות ארגוניות ועקיפת מגבלות גאוגרפיות.

איך הוא עובד?

מקים מנהרה מוצפנת בין המחשב לשרת ה-VPN, כך שכל התעבורה בין המחשב לשרת מוצפנת ומוגנת. כאשר המחשב מחובר ל-VPN, כתובת ה-IP שלו מוסתרת , והנתונים שהוא שולח נשארים פרטיים.

על איזה פורט הוא רץ?

- פורטים משתנים לפי פרוטוקול ה-VPN:
  - **PPTP**: פורט 1723 (TCP)
  - **L2TP**: פורט 1701 (UDP)
  - **IPsec**: פורטים 500 ו-4500 (UDP)
  - **OpenVPN**: פורט 1194 (UDP/TCP)

יתרונות:

- **הצפנה ואבטחה**: מגן על המידע ומונע מעקב של צדדים שלישיים.
- **גישה מרחוק**: אפשרות להתחבר לרשתות ארגוניות מכל מקום.
- **עקיפת מגבלות גאוגרפיות**: מאפשר גישה לתכנים באתרים חסומים.

חסרונות:

- **פחות מהיר**: חיבור מוצפן עלול להאט את החיבור.
- **תלות בספק ה-VPN**: השירות תלוי בביצועים של ספק ה-VPN.
- **סיכון למתקפות**: VPN שאינו מוגן כראוי עלול להיות יעד למתקפות.

פרוטוקול Syslog

מה זה Syslog?

פרוטוקול לאיסוף וניהול יומני מערכת (log files) במערכות מחשוב לצורכי אבחון, ניטור ותחזוקה.

מה השימוש?

משמש לניטור, ניתוח ותיעוד של פעולות ואירועים במערכות מחשוב, כולל שרתים, נתבים, חומות אש ואפליקציות.

איך הוא עובד?

מכשירים ויישומים שולחים הודעות Syslog לשרת Syslog מרכזי, שם הנתונים נאספים, מאוחסנים וניתנים לניתוח על מנת לזהות בעיות או לעקוב אחר פעילות.

על איזה פורט הוא רץ?

- **פורט 514 (UDP/TCP)**

יתרונות:

- **ניהול מרכזי**: מאפשר איסוף וניתוח יומני מערכת ממקורות שונים.
- **יכולת ניתוח**: מאפשר לאתר בעיות ולזהות מגמות במידע.
- **פשטות בהטמעה**: קל להטמעה ומאפשר הפקת דוחות מותאמים.

חסרונות:

- **אבטחה נמוכה**: מידע מועבר בטקסט גלוי ולכן יש סיכון לדליפת מידע אם לא מוגן.
- **חוסר סנכרון**: ייתכן שהודעות יגיעו באיחור או יתפספסו.
- **כמות נתונים גדולה**: דורש ניהול נכון של כמות נתוני הלוגים.

==פרוטוקול(FTP (File Transfer Protocol ==

- ## מה זה FTP?

הוא פרוטוקול תקשורת שנועד להעברת קבצים בין מחשבים ברשת. זהו אחד הפרוטוקולים הוותיקים ביותר להעברת נתונים, והוא פועל על בסיס מודל לקוח-שרת.

- ## שימושים של FTP

1. **העלאת קבצים**: מאפשר למשתמשים להעלות קבצים מלקוח (מחשב המשתמש) לשרת.
2. **הורדת קבצים**: מאפשר למשתמשים להוריד קבצים משרת למחשב.
3. **ניהול קבצים**: מאפשר פעולות נוספות כמו מחיקה, שינוי שמות, יצירת תיקיות וכו'.

- ## איך FTP עובד?

1. **חיבור**:
   - הלקוח מתחבר לשרת באמצעות שם משתמש וסיסמה (או בצורה אנונימית ללא הזדהות).
   - נעשה שימוש בפרוטוקול TCP כדי להבטיח העברת נתונים אמינה.
2. **מצבי עבודה**:
   - **Active Mode**: הלקוח פותח פורט אקראי ומאזין לשרת שיחזור אליו דרך פורט 20 לצורך העברת נתונים.
   - **Passive Mode**: השרת פותח פורט אקראי ומודיע ללקוח להתחבר אליו לצורך העברת נתונים.
3. **שני ערוצי תקשורת**:
   - **ערוץ הפקודה** (Control Channel): רץ על פורט 21 ומשמש להעברת פקודות (כמו העלאת קובץ, הורדת קובץ וכו') ותגובות השרת.
   - **ערוץ הנתונים** (Data Channel): משמש להעברת הקבצים עצמם. בפורט 20 (ב-Active Mode) או פורט אחר שנבחר ב-Passive Mode.

- ## יתרונות:

  - פשוט לשימוש.
  - פרוטוקול ותיק ותומך במגוון מערכות.

- ## חסרונות:

  - **חוסר אבטחה**: FTP שולח את הנתונים (כולל שם משתמש וסיסמה) בצורה שאינה מוצפנת, מה שמהווה סיכון אבטחה.
  - ניתן להתגבר על בעיות אבטחה על ידי שימוש בגרסאות מאובטחות כמו SFTP (Secure File Transfer Protocol) או FTPS (FTP Secure).

פרוטוקול SSH (Secure Shell)

מה זה SSH?

הוא פרוטוקול תקשורת מאובטח המשמש בעיקר לשליטה מרחוק במחשבים ולניהול רשתות.
הוא מספק ערוץ מוצפן לתקשורת ברשת לא מאובטחת, ומחליף שיטות לא בטוחות כמו Telnet או FTP רגיל.

שימושים של SSH:

1. **שליטה מרחוק**: מאפשר חיבור לשרתים או מחשבים אחרים לצורך ביצוע פעולות ניהול ושימוש.
2. **העברת קבצים**: באמצעות כלים כמו SCP (Secure Copy Protocol) או SFTP (Secure File Transfer Protocol).
3. **מנהור (Tunneling)**: יצירת חיבור מוצפן בין מחשבים, אפילו עבור פרוטוקולים אחרים.
4. **הרצת פקודות**: מאפשר להריץ פקודות באופן מאובטח על מחשב מרוחק.
5. **ניהול מפתחות**: ניתן להשתמש במפתחות ציבוריים ופרטיים לאימות ולא רק בשם משתמש וסיסמה.

איך SSH עובד?

פועל על בסיס מודל לקוח-שרת:

1. **חיבור**:
   - הלקוח (לדוגמה: תוכנה כמו `ssh` בלינוקס או Putty ב-Windows) יוצר חיבור לשרת באמצעות פרטי הזדהות (שם משתמש וסיסמה או מפתח ציבורי-פרטי).
   - ההתחברות מאובטחת בעזרת הצפנה.
2. **הצפנה**:
   - בשלב הראשון מתבצע **החלפת מפתחות** (Key Exchange) בין הלקוח לשרת כדי ליצור ערוץ מאובטח.
   - לאחר יצירת הערוץ המאובטח, כל הנתונים המועברים מוצפנים.
3. **אימות**:
   - האימות יכול להתבצע באמצעות סיסמה או מפתחות ציבוריים ופרטיים.
   - השיטה המומלצת היא מפתחות ציבוריים-פרטיים שמונעים גניבת סיסמאות.
4. **תקשורת מאובטחת**:
   - לאחר החיבור, ניתן להשתמש בפרוטוקול כדי לשלוט בשרת, להעביר קבצים, או לבצע פעולות אחרות בצורה מוצפנת.

על איזה פורט SSH רץ?

- ברירת המחדל של SSH היא **פורט 22**, אך ניתן לשנות זאת לצורכי אבטחה או ניהול.

יתרונות:

1. **אבטחה גבוהה**: הצפנה חזקה שמונעת האזנה לנתונים המועברים ברשת.
2. **רב-תכליתיות**: מאפשר מגוון רחב של פעולות (שליטה מרחוק, העברת קבצים, מנהור ועוד).
3. **אמינות**: משתמש בפרוטוקול TCP שמבטיח העברת נתונים אמינה.
4. **אימות חזק**: אפשרות לשימוש במפתחות ציבוריים ופרטיים לאימות.

חסרונות:

1. **סיכון בהגדרות שגויות**: הגדרות שגויות (כמו סיסמאות חלשות או הרשאות פתוחות) עלולות לחשוף את המערכת לסיכונים.
2. **מורכבות**: דורש מיומנות טכנית בסיסית להגדרה ושימוש נכון.
3. **מטרה לפורצים**: פורט 22 עלול להיות מותקף לעיתים קרובות, ולכן מומלץ לשנות אותו.

פרוטוקול SMTP (Simple Mail Transfer Protocol)

מה זה SMTP?

הוא פרוטוקול תקשורת שנועד לשליחת דואר אלקטרוני (Email) בין שרתים וממשתמשים לשרת. הוא מהווה את הסטנדרט המרכזי לשליחת הודעות דואר אלקטרוני באינטרנט.

שימושים של SMTP:

1. **שליחת מיילים**: שולח הודעות מלקוח הדואר האלקטרוני (לדוגמה: Outlook, Thunderbird) לשרת הדואר.
2. **העברת מיילים בין שרתי דואר**: משמש לשליחת מיילים משרת אחד לאחר באינטרנט.
3. **שליחה דרך אפליקציות ושירותים**: אפליקציות ותוכנות שונות משתמשות ב-SMTP לשליחה אוטומטית של מיילים (לדוגמה: התראות או אישורי רכישה).

איך SMTP עובד?

פועל על מודל שרת-לקוח, ונעשה בו שימוש במערכת שלבים לשידור הודעות:

1. **חיבור**:
   - הלקוח (Client) יוצר חיבור לשרת SMTP.
   - החיבור נעשה בדרך כלל בפורט ברירת המחדל (פורט 25 או אחרים, כפי שמוסבר בהמשך).
2. **שליחת ההודעה**:
   - ההודעה מורכבת ממטא-נתונים (כתובת שולח, כתובת נמען) ותוכן (כותרת גוף המייל, תוספות).
   - התקשורת מתבצעת באמצעות פקודות טקסטואליות כמו:

- **HELO**: מציג את הלקוח לשרת.
- **MAIL FROM**: מציין את כתובת השולח.
- **RCPT TO**: מציין את כתובת הנמען.
- **DATA**: מתחיל את העברת תוכן המייל.
- **QUIT**: מסיים את החיבור לשרת.

3. **העברת ההודעה לשרת היעד**:
   - אם השרת אינו השרת של הנמען, הוא מעביר את המייל לשרת SMTP אחר, עד שהמייל מגיע לשרת המתאים לנמען.
4. **אחסון ההודעה**:
   - לאחר שהמייל מגיע לשרת של הנמען, הוא מאוחסן זמנית עד שהנמען מוריד אותו באמצעות פרוטוקולים כמו IMAP או POP3.

על איזה פורט SMTP רץ?

יכול לרוץ על כמה פורטים:

1. **פורט 25**: ברירת המחדל ההיסטורית להעברת מיילים בין שרתים. עם זאת, הוא נחסם לעיתים קרובות ברשתות מסוימות כדי למנוע שימוש לרעה (כמו ספאם).
2. **פורט 587**: משמש לשליחה מאובטחת של מיילים (משמש לקוחות דואר).
3. **פורט 2525**: לעיתים נבחר חלופי על ידי ספקי שירותי דואר, במיוחד כאשר פורט 25 חסום.

יתרונות:

1. **פשטות וסטנדרטיזציה**: פרוטוקול ותיק ונפוץ, שתואם את רוב מערכות הדואר האלקטרוני.
2. **תמיכה רחבה**: כל שרתי הדואר והלקוחות תומכים ב-SMTP.
3. **שילוב קל במערכות אוטומטיות**: מתאים לשליחה אוטומטית של מיילים מאפליקציות ושירותים.

חסרונות:

1. **אבטחה מוגבלת במקור**: גרסתו הבסיסית של SMTP אינה כוללת הצפנה, ולכן רגיש להאזנות וסיכוני אבטחה.
   - ניתן להתגבר על כך באמצעות גרסאות מאובטחות כמו SMTPS או שימוש בהצפנת TLS.
2. **תלות בשרתים מתווכים**: אם שרת כלשהו בתהליך השליחה אינו פועל, המייל עלול להתעכב.
3. **סיכון לשימוש לרעה**: שרתי SMTP פתוחים (Open Relays) עלולים להיות מנוצלים לשליחת ספאם.

פרוטוקול DNS (Domain Name System)

מה זה DNS?

הוא פרוטוקול חיוני ברשת האינטרנט שתפקידו לתרגם שמות דומיין (כמו `www.example.com`) לכתובות IP (כמו `192.0.2.1`). מכיוון שמחשבים מתקשרים באמצעות כתובות IP, DNS משמש כ"ספר הטלפונים" של האינטרנט.

שימושים של DNS:

1. **תרגום שמות דומיין לכתובות IP**: כדי שמשתמשים יוכלו לגשת לאתרים או שירותים באמצעות שמות קלים לזכירה.
2. **הפניית תעבורה**: מאפשר ניהול הפניות לדומיינים שונים, כמו הפניות לשרתי דוא"ל, אתרים או שירותים אחרים.
3. **שירותי איזון עומסים**: מאפשר הפניית בקשות לכתובות שונות כדי להפחית עומס.
4. **שירותי אימות דואר אלקטרוני**: שימוש ברשומות DNS לאימות מקור המייל (SPF, DKIM, DMARC).

איך DNS עובד?

כאשר משתמש מקליד כתובת URL בדפדפן, תהליך ה-DNS מתרחש בשלבים הבאים:

1. **שליחת בקשה (Query)**:
   - המחשב שולח בקשה לשרת DNS כדי לקבל את כתובת ה-IP של הדומיין המבוקש.
2. **בדיקת Cache**:
   - המחשב או שרת DNS קרוב בודק אם התשובה כבר שמורה בזיכרון המטמון.
   - אם כן, התהליך מסתיים במהירות.
3. **שימוש בשרתי DNS היררכיים**:
   - אם הכתובת אינה במטמון, השרת פונה לרשומת ה-DNS לפי הסדר הבא:
     - **Root Server**: נותן מידע על ה-TLD (לדוגמה, `com.`).
     - **TLD Server**: מספק את הכתובת של שרת ה-DNS הספציפי לדומיין (לדוגמה, `example.com`).
     - **Authoritative Name Server**: מספק את כתובת ה-IP של האתר.
4. **החזרת תשובה**:
   - כתובת ה-IP מוחזרת ללקוח, והוא משתמש בה כדי להתחבר לשרת המבוקש.

סוגי רשומות DNS:

1. **A (Address)**: מקשרת דומיין לכתובת IPv4.
2. **AAAA**: מקשרת דומיין לכתובת IPv6.
3. **CNAME (Canonical Name)**: יוצרת שם דומיין אלטרנטיבי (Alias).
4. **MX (Mail Exchange)**: מגדירה את שרתי הדוא"ל של הדומיין.
5. **TXT**: מכילה מידע טקסטואלי, משמשת לאימות כמו SPF, DKIM, ו-DMARC.
6. **PTR (Pointer)**: תרגום הפוך מכתובת IP לשם דומיין.
7. **NS (Name Server)**: מגדירה את שרתי ה-DNS האחראיים לדומיין.

על איזה פורט DNS רץ?

- **פורט 53**:
  - משמש להעברת בקשות ותשובות DNS.
  - תומך בשני סוגי פרוטוקולים:

1. **UDP**: ברירת המחדל לבקשות DNS, קל ומהיר יותר, רגילות.
2. **TCP**: משמש להעברות נתונים גדולות יותר או במקרים של אמינות גבוהה יותר.

יתרונות:

1. **פשטות למשתמשים**: מאפשר שימוש בשמות דומיין במקום כתובות IP מורכבות.
2. **גמישות ניהולית**: מאפשר לנהל ולכוון תעבורה ברשת בקלות.
3. **אופטימיזציה באמצעות מטמון**: שיפור ביצועים וחיסכון בזמן חיפוש כתובות.

חסרונות:

1. **פגיעות להתקפות**:

- **DNS Spoofing/Cache Poisoning**: מניפולציה על רשומות ה-DNS במטמון כדי להפנות משתמשים לאתרים זדוניים.
- **DDoS על שרתי DNS**: מתקפות עומס שמטרתן להפיל שרתי DNS קריטיים.

2. **חוסר הצפנה במקור**: DNS רגיל מעביר מידע בטקסט גלוי, מה שיכול לחשוף פרטי גלישה.
- פתרונות כמו DNS over HTTPS (DoH) או DNS over TLS (DoT) מספקים הצפנה.

פרוטוקול HTTP (Hypertext Transfer Protocol)

מה זה HTTP?

הוא פרוטוקול תקשורת המשמש להעברת מידע ברשת האינטרנט בין דפדפן (לקוח) לשרת. הוא מאפשר הורדה של דפי HTML, קבצי מדיה, ותוכן נוסף, ומהווה את הבסיס לתקשורת ברשת ה-World Wide Web.

שימושים של HTTP:

1. **טעינת דפי אינטרנט**: מאפשר למשתמשים לגשת לאתרי אינטרנט דרך דפדפנים.
2. **שליחת בקשות וקבלת תשובות**: העברת נתונים בין הלקוח לשרת (GET, POST, PUT, DELETE וכו').
3. **שירותי API**: שימוש בפרוטוקול HTTP לתקשורת בין שירותים ואפליקציות.

איך HTTP עובד?

מבוסס על מודל בקשה-תגובה:

1. **בקשה (Request)**:
- הלקוח שולח בקשה לשרת עם פרטים כמו סוג הבקשה (לדוגמה, GET לטעינת עמוד או POST לשליחת נתונים) ונתיב המשאב.
- הבקשה כוללת כותרות (Headers), נתוני מטא, ולעיתים גם גוף הבקשה (Body).
2. **תגובה (Response)**:
- השרת מחזיר תשובה הכוללת כותרות, קוד סטטוס (כמו 200 OK או 404 Not Found), ולעיתים תוכן (כמו HTML או JSON).
3. **תקשורת על גבי TCP**:
- משתמש בפרוטוקול TCP לערוץ תקשורת אמין.
- ברירת המחדל היא פורט 80.

פרוטוקול HTTPS (Hypertext Transfer Protocol Secure)

מה זה HTTPS?

הוא גרסה מאובטחת של HTTP, המשתמשת בהצפנה באמצעות פרוטוקול TLS (Transport Layer Security) או SSL (Secure Sockets Layer). הוא מספק סודיות, שלמות נתונים, ואימות בין הלקוח לשרת.

שימושים של HTTPS:

1. **אבטחת גלישה**: מגן על נתונים רגישים כמו סיסמאות, פרטי אשראי ונתוני משתמש אחרים.
2. **אימות זהות השרת**: מבטיח שהמשתמשים מתחברים לשרת הנכון ולא לשרת מזויף.
3. **שמירה על פרטיות**: מונע מהאקרים להאזין לתקשורת בין הלקוח לשרת.

איך HTTPS עובד?

משלב את פעולתו של HTTP עם שכבת אבטחה:

1. **תהליך Handshake**:
   - הלקוח והשרת מחליפים מפתחות קריפטוגרפיים כדי ליצור חיבור מאובטח.
   - תהליך זה כולל אימות תעודת SSL/TLS של השרת.
2. **הצפנת התקשורת**:
   - כל הנתונים המועברים בין הלקוח לשרת מוצפנים באמצעות המפתח שהוסכם עליו.
3. **שימוש ב-TCP**:
   - בדומה ל-HTTP, גם HTTPS משתמש ב-TCP, אך בברירת המחדל על פורט 443.

הבדלים בין HTTP ל-HTTPS:

מאפיין	HTTP	HTTPS
אבטחה	אין הצפנה, מידע נשלח בטקסט גלוי	מידע מוצפן באמצעות TLS/SSL
פורט ברירת מחדל	80	443
אימות	אין אימות זהות השרת	אימות זהות באמצעות תעודה דיגיטלית
שימושים	לרוב מתאים למידע ציבורי שאינו רגיש	מתאים לכל תוכן, בעיקר מידע רגיש

יתרונות HTTPS על פני HTTP:

1. **אבטחת נתונים**: הצפנה מונעת האזנה או גניבת נתונים על ידי צד שלישי.
2. **אימות זהות**: מבטיח חיבור לשרת הנכון ולא לאתר מתחזה.
3. **יSEO ושיפור אמינות**: מנועי חיפוש (כמו Google) נותנים עדיפות לאתרים עם HTTPS.
4. **מניעת שינויים בנתונים**: מבטיח שהמידע לא שונה במהלך ההעברה.

חסרונות:

יHTTP:

1. **חוסר אבטחה**: כל הנתונים נשלחים בטקסט גלוי, כולל סיסמאות ונתונים רגישים.
2. **פגיעות להתקפות**: קל להאזין לתקשורת או לשנות אותה.

יHTTPS:

1. **מורכבות הגדרה**: דורש התקנת תעודות SSL/TLS ותחזוקתן.

2. **עלות**: למרות שקיימות אפשרויות חינמיות (כמו Let’s Encrypt), תעודות מאובטחות יותר עשויות לדרוש תשלום.
3. **עומס על השרת**: הצפנה דורשת משאבים נוספים, מה שעלול להשפיע על ביצועים.

פרוטוקול SMB (Server Message Block)

מה זה SMB?

הוא פרוטוקול תקשורת המשמש לשיתוף משאבים ברשתות מקומיות (LAN), כגון קבצים, מדפסות, פורטים ושירותים נוספים. הוא מאפשר למחשבים לתקשר ולשתף נתונים בצורה יעילה ובטוחה.

שימושים של SMB:

1. **שיתוף קבצים**: מאפשר למשתמשים לגשת לקבצים המאוחסנים על מחשבים אחרים ברשת המקומית.
2. **שיתוף מדפסות**: מאפשר לשתף מדפסות ברשת המקומית.
3. **ניהול משתמשים ומשאבים**: מאפשר לאדמיניסטרטורים לנהל גישה לקבצים ומשאבים לפי הרשאות.
4. **שיתוף פורטים ושירותים**: מעבר לשיתוף קבצים ומדפסות, SMB תומך גם בשיתוף התקנים שונים כמו פורטים.

איך SMB עובד?

1. **חיבור הלקוח לשרת**:
   - לקוח (Client) מבצע בקשה לגישה לשרת SMB (בדרך כלל מחשב אחר ברשת).
   - החיבור יכול להיות מאומת (באמצעות שם משתמש וסיסמה) או לא מאומת (Guest).
2. **ניהול בקשות**:
   - הלקוח מבקש פעולה מסוימת, כמו קריאה או כתיבה לקובץ, והשרת מבצע אותה בהתאם להרשאות.
3. **תקשורת דו-כיוונית**:
   - מאפשר תקשורת דו-כיוונית בין הלקוח לשרת, כולל שליחת הודעות ועדכון מידע בזמן אמת.

על איזה פורט SMB רץ?

משתמש בדרך כלל בפורטים הבאים:

1. **פורט 445**:
   - פורט ברירת המחדל לפרוטוקול SMB המודרני.
   - התקשורת מתבצעת ישירות מעל TCP/IP ללא צורך ב-NetBIOS.
2. **פורט 137, 138, 139**:
   - בשימוש גרסאות ישנות יותר של SMB שמשתמשות ב-NetBIOS.

שיפורי אבטחה ב-SMB:

1. **השבתת SMB 1.0**: מומלץ להשבית את SMB 1.0 ולהשתמש בגרסאות חדשות יותר (2.0 ומעלה).
2. **שימוש בהצפנה (SMB Encryption)**: זמין החל מ-SMB 3.0 להגנה על נתונים במהלך ההעברה.

3. **ניהול הרשאות קפדני**: הקפדה על הרשאות גישה בהתאם לצרכים בלבד.
4. **Firewall**: הגבלת גישה לפורטים 445 ו-139 רק לרשת המקומית.

יתרונות:

1. **שיתוף יעיל ברשת מקומית**: מאפשר שיתוף קבצים ומשאבים בקלות.
2. **תאימות רוחבית**: SMB נתמך על ידי מגוון מערכות הפעלה (Windows, macOS, Linux).
3. **ביצועים גבוהים**: במיוחד בגרסאות מאוחרות, SMB מספק מהירות ואמינות גבוהות יותר.
4. **אבטחה מתקדמת**: גרסאות מודרניות כוללות הצפנה ואימות חזקים.

חסרונות:

1. **פגיעות לגרסאות ישנות**: SMB 1.0 פגיע לאיומים כמו WannaCry ו-NotPetya, ולכן מומלץ להשביתו.
2. **שימוש ברוחב פס**: בתקשורת כבדה או רשת עמוסה, SMB עשוי לצרוך משאבים רבים.
3. **חשיפה ברשתות ציבוריות**: פורט 445 פתוח יכול להוות פתח להתקפות אם לא מוגן כראוי.
4. **תלות במערכת ההרשאות**: הרשאות לא נכונות עלולות לחשוף קבצים רגישים.

פרוטוקול DHCP (Dynamic Host Configuration Protocol)

מה זה DHCP?

הוא פרוטוקול רשת המאפשר ניהול אוטומטי של הגדרת פרמטרי רשת במכשירים. באמצעותו, ניתן להקצות כתובות IP, שער ברירת מחדל (Gateway), כתובות DNS ועוד, בצורה אוטומטית וללא צורך בהתערבות ידנית.

מטרת DHCP:

לספק דרך יעילה ואוטומטית לניהול כתובות IP ברשתות, ובכך למנוע התנגשויות IP ולפשט את תהליך ההגדרה של מכשירים חדשים ברשת.

שימושים של DHCP:

1. **הקצאת כתובות IP דינמיות**: מייעל את השימוש בכתובות IP ומונע התנגשויות.
2. **ניהול רשת פשוט**: מאפשר חיבור מכשירים חדשים לרשת ללא צורך בהגדרות ידניות.
3. **עדכון פרמטרים באופן אוטומטי**: כשנדרש לשנות כתובות שרתי DNS או שער ברירת מחדל, ניתן לעדכן זאת דרך ה-DHCP.
4. **שירותי רשת גדולים**: חיוני ברשתות ארגוניות, רשתות Wi-Fi, וסביבות דינמיות אחרות.

איך DHCP עובד?

1. **Discover**:
   - מכשיר חדש שמתחבר לרשת שולח הודעת שידור (Broadcast) כדי למצוא שרת DHCP.
2. **Offer**:
   - שרת DHCP מגיב עם הצעה (Offer) לכתובת IP זמינה ופרמטרים נוספים.

3. **Request**:
   - המכשיר מבקש רשמית את כתובת ה-IP המוצעת.
4. **Acknowledge**:
   - השרת מאשר את הבקשה (ACK) והכתובת מוקצית למכשיר למשך זמן מסוים (Lease Time).

פרמטרים שמוקצים על ידי DHCP:

1. **כתובת IP**: כתובת ייחודית למכשיר ברשת.
2. **Subnet Mask**: מגדירה את טווח הכתובות ברשת המקומית.
3. **Default Gateway**: הכתובת של הנתב או שער ברירת המחדל.
4. **DNS Server**: כתובות שרתי ה-DNS המשמשים לתרגום שמות דומיין.
5. **כתובות נוספות או אפשרויות מותאמות אישית**: כמו כתובת WINS, שרת Proxy וכו'.

סוגי הקצאות DHCP:

1. **הקצאה דינמית**:
   - כתובות IP מוקצות זמנית ומשתנות בהתאם לזמינות ברשת.
   - ברירת המחדל והשימוש הנפוץ ביותר.
2. **הקצאה ידנית (Manual)**:
   - האדמיניסטרטור קובע כתובות IP מסוימות למכשירים ספציפיים על פי כתובת MAC.
   - משמש בעיקר עבור שרתים, מדפסות או מכשירים קריטיים אחרים.
3. **הקצאה סטטית (Static)**:
   - כתובת IP קבועה שמוגדרת ישירות במכשיר ולא באמצעות DHCP.

שיפורי אבטחה עבור DHCP:

1. **הפעלת DHCP Snooping**:
   - טכנולוגיה ברמת מתגי רשת שמאפשרת סינון של הודעות DHCP לא חוקיות.
2. **שימוש ב-VLANs**: בידוד רשתות כדי למנוע גישה לא מורשית.
3. **הגבלת כתובות MAC**: מונע ממכשירים לא מזוהים לקבל כתובת IP.
4. **הצפנה והגנה ברשתות ציבוריות**: יש להשתמש באמצעי אבטחה נוספים ברשתות Wi-Fi כדי למנוע התקפות.

יתרונות DHCP:

1. **ניהול אוטומטי**: מפשט את תהליך ההגדרה של מכשירים ברשת.
2. **מניעת טעויות ידניות**: אין צורך בהגדרת כתובות IP באופן ידני.
3. **חסכון במשאבים**: שימוש יעיל בכתובות IP בטווח מוגבל.
4. **גמישות**: מאפשר שינוי פרמטרים בצורה דינמית.

חסרונות DHCP:

1. **תלות בשרת DHCP**: אם השרת אינו פעיל, מכשירים לא יוכלו לקבל כתובות IP.

2. **אבטחה מוגבלת**: פרוטוקול DHCP אינו כולל אמצעי אבטחה מובנים, מה שעלול לאפשר התקפות כמו:
   - **DHCP Spoofing**: תוקף מתחזה לשרת DHCP ומספק כתובות מזויפות.
   - **IP Starvation**: תוקף מבקש כתובות IP רבות כדי למנוע ממכשירים לגיטימיים לקבל כתובות.
3. **חוסר שליטה בכתובות IP קבועות**: במקרים מסוימים, מכשירים עשויים לקבל כתובות שונות לאחר חידוש ה-Lease.