שיעור חזרה

**תרגול חזרה**

בתרגיל זה נחזור על נושאים חשובים שלמדנו בסמסטר. מומלץ לתרגל יחד עם חברים. בהצלחה!

**חלק ראשון – שיחות**למוקד התמיכה של "נזק בינלאומי" מגיעות מגוון שיחות מלקוחות מבולבלים. הקשיבו לכל אחת מהשיחות וענו על השאלות שלאחר מכן.

1. **הקלטה מספר 1 - להאזנה להקלטה לחצו כאן:**

<https://drive.google.com/file/d/0B539Ut4VLSWDVml2blBrRV8yTGM/view?usp=sharing>

**לקוח:** שלום, אני צריך עזרה עם האינטרנט שלי  
**נציגה:** שלום, מה הבעיה?  
**לקוח:** אין אינטרנט.  
**נציגה:** אוקיי, בואי ננסה להבין יותר לעומק. מה הכוונה "אין אינטרנט"?  
**לקוח:** אני מנסה להיכנס לפורום מסוים ב"תפוז" ואני מקבל שגיאה  
**נציגה:** איזו שגיאה את רואה על המסך?  
**לקוח:** כתוב משהו "404"... אני לא ממש מבין

1. מה הבעיה שחווה הלקוחה?

|  |
| --- |
| הפורום אליו היא מנסה להיכנס לא קיים עוד בשרת של "תפוז" |
| תשובה |

1. הנציגה ביקשה מהלקוחה לנסות לגלוש לאתר אחר. מה המטרה בבדיקה זו? ומה תהיה התוצאה?

|  |
| --- |
| המטרה היא לבדוק אם הבעיה היא "באינטרנט" בצד של הלקוחה, או בצד של השרת – כלומר באתר הספציפי אותו היא מנסה לקבל.  התוצאה של הבדיקה תהיה שהיא מצליחה לגלוש לאתרים אחרים. כיוון ששגיאת 404 היא ספציפית עבור עמודים לא זמינים בשרת. |
| תשובה |

1. לאיזה פרוטוקול שייכת השגיאה הזו? לאיזו שכבה?

|  |
| --- |
| פרוטוקול HTTP, שכבת האפליקציה. |
| תשובה |

1. **הקלטה מספר 2 - להאזנה להקלטה לחצו כאן:**

<https://drive.google.com/file/d/0B539Ut4VLSWDRlkxR1phby1ndG8/view?usp=sharing>

**לקוחה:** שלום, יש לי בעיה חמורה

**נציג:** שלום לך, מה התקלה?

**לקוחה:** כבר שעה אני לא מצליחה לגלוש

**נציג:** לאיזה אתר את מנסה לגלוש?

**לקוחה:** אני רוצה לקנות כרטיס להופעה של ג'סטין ביבר בברלין!!

**נציג:** ואו! איזה כיף לך. אז תארי לי שלב אחרי שלב מה את עושה.

**לקוחה:** אוקיי, חברה העבירה לי את הכתובת דרכה קונים את הכרטיסים. אני מדביקה את הכתובת בשורת ה-URL בדפדפן, אבל האתר לא עולה.

**נציג:** אני מבין. ותגידי, גלשת פעם לאתר לקניית הכרטיסים לג'סטין ביבר? או שזו הפעם הראשונה שאת מנסה להיכנס לאתר?

**לקוחה:** לא, זו פעם ראשונה. רק לאחרונה נכנסתי לקטע שלו ☺

**נציג:** אה הא. ולאיזה אתר את גולשת באופן תדיר?

**לקוחה:** אני כל 5 דקות בפייס, ברור.

**נציג:** נהדר. אז נסי רגע להיכנס לפייס. את מצליחה?

**לקוחה:** אני לא מבינה איך זה קשור, אני צריכה אתר אחר....

**נציג:** פשוט תנסי, זה עשוי לעזור לי להבין מה הבעיה.

**לקוחה:** הו! כן. לפייסבוק אני מצליחה לגלוש.

**נציג:** כנסי לאתר נוסף שאת בדרך כלל מבקרת בו.

**לקוחה:** ספורט5, אני חולה על ספורט5. הנה! מצליחה גם.

**נציג:** עכשיו נסי להיכנס לאתר אחר שלא ביקרת בו לאחרונה. לדוגמה: <http://www.hop.co.il>

**לקוחה:** מנסה... לא. זה לא מראה לי את האתר הזה.

**נציג:** המממ אני חושב שהבנתי איפה הבעיה!

1. אבחנו את התקלה שיש ללקוחה. במה נראה שאין בעיה?

|  |
| --- |
| בפרוטוקול HTTP / ביציאה של הפקטות מהרשת הפנימית / בראוטר |
| תשובה |

1. מה לדעתכם הגורם לבעיה שמתוארת?

|  |
| --- |
| יש תקלה בשאילתות ה-DNS, כי כל האתרים שהלקוחה לא מצליחה לגלוש אליהם, לא נמצאים ב"קאש" ודורשים שאילתת DNS כדי לגלוש אליהם. ואילו, האתרים אליהם הלקוחה כן מצליחה להגיע, נמצאים ב"קאש" (כי היא מבקרת בהם באופן תדיר) ולכן לא דורשים שאילתת DNS. |
| תשובה |

1. נסו לחשוב על הצעות לפתרון / לאבחון עמוק יותר של התקלה

|  |
| --- |
| בדיקה מאיזה שרת DNS הלקוחה מקבלת שירות – אולי יש בו בעיה.  נבדוק האם התשובה של השרת אוטורטיבית?  נוכל לנסות להגדיר שרת DNS לבחירתנו, אליו יופנו מעתה השאילתות (כמו 8.8.8.8 של גוגל) |

1. לאיזה פרוטוקול שייכת השגיאה הזו? לאיזו שכבה?

|  |
| --- |
| פרוטוקול DNS, שכבת האפליקציה. |
| תשובה |

1. **הקלטה מספר 3 - להאזנה להקלטה לחצו כאן:**

<https://drive.google.com/file/d/0B539Ut4VLSWDMTlrN1VUcnhjdEk/view?usp=sharing>

**לקוחה:** שלום, אני חייבת עזרה דחוף דחוף דחוף

**נציג:** כן, איך אפשר לעזור?

**לקוחה:** קניתי מחשב חדש מהמם מהחנות. אני מנסה לחבר אותו לאינטרנט. יש לי פה בבית רשת, עם כמה מחשבים שכבר מחוברים והכל טוב. אני לא מבינה בנושא הזה כלום.. אני על המחשב החדש - כתוב כאן משהו "להגדיר IP ידנית" או "להגדיר IP באופן אוטומטי". אני צריכה לבחור ביניהם. במה לבחור?! אני לא יודעת מה עדיף! חשבתי יאללה נבחר באוטומטי - נשמע קל... לא נדאג לכלום... ראש שקט... אבל אולי דווקא ידני יותר כדאי כי אסור לעשות דברים בחיים "על אוטומט".

1. מה הסיטואציה ומה ההבדל בין שתי האפשרויות שניצבות בפני הלקוחה?

|  |
| --- |
| למעשה הלקוחה מנסה לחבר מחשב חדש לרשת הפנימית שבביתה. האפשרות הראשונה לעשות זאת היא ע"י שימוש בהגדרה ידנית של כתובת IP פנימית למחשב החדש שמצטרף לרשת. אפשרות נוספת היא הגדרת כתובת IP פנימית למחשב החדש באופן אוטומטי מתוך טווח של כתובות אפשריות. |
| תשובה |

1. איזה פרוטוקול קשור לפעולה זו?

|  |
| --- |
| פרוטוקול DHCP |
| תשובה |

1. איך הייתם מייעצים ללקוחה לפעול?

|  |
| --- |
| כיוון שללקוחה אין כלל ידע בתחום, אין שום סיבה שתגדיר לבד את ה-IP הפנימי של המחשב. לשם כך בדיוק נועד DHCP! לכן, נייעץ לה לבחור להגדיר IP באופן אוטומטי, והיא תוכל להירגע...  |
| תשובה |

1. **הקלטה מספר 4 - להאזנה להקלטה לחצו כאן:**

<https://drive.google.com/file/d/0B539Ut4VLSWDVjRMdGVpcHFhck0/view?usp=sharing>

**מלצר:** שלום וברוכים הבאים לארומה!

**לקוחה:** שלום. מה הוויפי כאן?

**מלצר:** הרשת נקראת aroma והסיסמה זה ilovecoffieforever.

**לקוחה**: אוקיי.... התחברתי.

**מלצר**: אחלה, אני יכולה להציע לך משהו לשתות?

**לקוחה**: אממ שנייה לפני זה, טיפה מוזר, אבל - אני רואה שיש לך כאן מחשב נייד. יש לך אולי כמה דקות שאני אציק לך עם שאלות?

**מלצר**: בטח. אבל, יש משהו שאת צריכה לדעת עליי. יש לי תסמונת בריאותית חמורה מאוד.

**לקוחה**: אוי אני מצטערת לשמוע!

**מלצר**: כן, העניין הוא שאני לפעמים אומר שקרים. אני לא שולט בזה. אני מתכוון להגיד את האמת, אבל מדי פעם פשוט יוצאת לי התשובה ההפוכה.

**לקוחה**: אין בעיה, אני אבין כבר מתי את משקרת ומתי את דוברת אמת...

**מלצר**: אוקיי, על אחריותך... אז אני מקשיב.

**לקוחה**: יופי, ואני רואה שגם את מחוברת לרשת של ארומה. אז ככה, חיפשתי באינטרנט "what’s my ip" וראיתי שה-IP החיצוני שלי הוא 3.3.3.3. את יכולה לבדוק מה ה-IP שלך?

**מלצר**: כן... איזה קטע, גם שלי 3.3.3.3

**לקוחה**: מעניין. ובואי נבדוק IP פנימי – נכתוב ב-cmd את הפקודה ipconfig. אז אני רואה שה-IP הפנימי שלי הוא 10.0.0.1. מה שלך?

**\*מלצר**: 10.11.9.8

**לקוחה**: מה?? באמת? רגע, ומה ה-subnet mask שלך? שלי 255.255.255.0

**מלצר**: כן, גם שלי.

**לקוחה**: אוקיי... ותגידי, מה ה-default gateway שלך מוגדר להיות?

**\*מלצר**: בואי נראה.... 10.0.0.1

**לקוחה**: מעניין מאוד מה שאת אומרת. אני אחשוב קצת על התשובות שלך...

**מלצר**: אחלה. ועכשיו אפשר להציע לך קפה?

**לקוחה**: כן, יש לכם חלב סויה?

**מלצר**: כן.

**לקוחה**: רגע. זה שקר או אמת?

**מלצר**: ☺

**\* = שקר**

1. עזרו ללקוחה לזהות איזה תשובות של המלצרית הן שקר.סמנו את התשובות השקריות, והסבירו מדוע הן לא נכונות.

|  |
| --- |
| תשובות לא נכונות:  מלצרית: 10.11.9.8  (חייב להיות לשתיהן אותו subnet mask, ולכן לא יכול להיות שיהיה לה IP שלא מתחיל ב-10.0.0.X כמו של הלקוחה.  מלצרית: בואי נראה.... 10.0.0.1 (ה-IP הזה תפוס ע"י הלקוחה) |

**חלק שני – נכון או לא נכון?**ינון ומיכל לומדים יחד למבחן ברשתות. בזמן הלמידה הם רשמו מסקנות, אך חלקן לא מדויקות כל כך. עזרו להם למצוא את המשפטים הלא נכונים, והסבירו מדוע.

1. כל פרוטוקול שעובר מעל שכבת הרשת (IP), כלומר ש-IP עוטף אותו, הוא בוודאות בשכבת התעבורה. לא נכון - ICMP
2. כתובת MAC של מחשב אף פעם לא יכולה להשתנות, גם במקרה של החלפת חומרה. לא נכון - החלפת כרטיס רשת
3. אם לראוטר הביתי שלנו לא היתה פונקציה של NAT, לא היינו יכולים לתקשר עם שרתים באינטרנט. נכון, כי אי אפשר להשתמש ב-IP הפרטי שלנו כדי לדבר עם ישויות באינטרנט. חייבת להתבצע החלפה של כתובת ה-IP שלנו.
4. ניתן להשתמש בפרוטוקול ARP רק במידה ויש לי את כתובת ה-IP של היעד. נכון – המטרה של ARP היא לבדוק MAC של מישהו שנמצא איתי בתת רשת לפי **הIP שלו**
5. לחיבור בשכבת האפליקציה (סוקט) יש 4 מאפיינים: IP מקור, IP יעד, MAC מקור ו-MAC יעד. לא נכון, במקום MACים, PORTים
6. המידע כאשר הוא עובר בכבל או באוויר, עובר בבסיס ספירה הקסאדצימלי. לא נכון, הוא עובר בבסיס בינארי, מתח גבוה\נמוך או ספינים בכבלים אופטיים.
7. פרוטוקול Stateless לעולם לא יכול לאפשר מנגנון אותנטיקציה (לוגאין). לא נכון – cookies HTTP כדוגמא, אבל חשוב להבין שאלו לא פתרונות שהם ממש חלק מובנה בפרוטוקול
8. ע"י הסנפה, ניתן לגלות את ה-MAC של כל ראוטר הנמצא ביני ובין מחשב היעד. אם הכוונה להסנפה מנק' בודדת, ולא בוצעו שאילתות ייחודיות שמכילות את המידע הזה, אז לא. ניתן לראות רק MACים של ישויות בתת רשת שלנו.
9. זכרון מטמון נועד כדי לשפר ביצועים ומהירות. נכון מאוד. וכדי להקל על האקרים – כתגובה הומצא הevil bit בשכבת הIP.
10. שכבות שונות במודל השכבות כלל לא מודעות אחת לשניה ולא יודעות מה התפקיד של שכבות אחרות. לא ממש – השכבות כן מודעות לתפקיד אחת של השניה ונעזרות אחת בשניה. הן פשוט לא מתעניינות איך כל שכבה מממשת את הפתרונות שלה אלא רק סומכות על זה שזה יקרה.
11. ב-TCP, מספרי ה-SEQ מייצגים את מספר החתיכה (ראשונה, שניה וכו'). כמעט, הם מייצגים את מספר הבית הראשון בחתיכה, וכך עוזרים לי להרכיב את ההודעה בצד השני.
12. בלחיצת היד המשולשת ב-TCP, מתקבלת החלטה האם התקשורת תהיה חד-כיוונית או דופלקס. לא נכון, אפשר להתחיל בכל שלב דופלקס
13. אין דרך אמיתית למנוע מתקפת DDoS לחלוטין. נכון. למעט חקיקה, חינוך וחברה אידיאלית.
14. פרוטוקולים אשר מעבירים מעט מידע תמיד ישתמשו ב-TCP, מכיוון שכאשר המידע קצר, התקורה פחות משמעותית ולא נורא "לשלם" אותה. לא נכון, למשל ב-DHCP לצרכי broadcast.
15. כאשר אנו רוצים להעביר מספר פורט בהודעת פרוטוקול, לא יהיה הבדל בגודל השדה בין אם נכתוב אותו בשיטה טקסטואלית או בינארית. לא נכון. כאשר אנו מעבירים מספרים קידוד בינארי יהיה חסכוני בהרבה. כאשר אנו מעבירים טקסט, אין הבדל.
16. בפרוטוקול UDP המידע של שכבת האפליקציה מתחלק להרבה חבילות קטנות, ואם אחד נאבדת המידע עשוי להגיע פגום. ה-UDP לא מחלק בעצמו את המידע, אבל מידע אכן עלול להאבד ואז המידע אכן יגיע פגום.
17. לפי שיטת Next Hop, אף מחשב לא יודע מהו המסלול המלא שתעשה חבילה. נכון מאוד אלא אם ה-NEXT HOP הוא היעד והשולח הוא המקור.
18. Tracert מציג מסלול שלא בהכרח קיים במציאות. נכון מאוד. יכול להיות שיש, אבל זה לא בטוח.
19. תוכנות P2P לא אוהבות NAT מכיוון שהוא מגביל את מספר החיבורים שהן יכולות לבצע עם משתמשים (עמיתים) אחרים ברשת. נכון חלקית, NAT מגביל ומסבך את היכולת שלי לפתוח שרת שמאזין בתוך הרשת. עם זאת, יש מספר דרכים להתגבר על כך!
20. כאשר אני רוצה להעביר חבילה למחשב הנמצא בתוך הסאבנט שלי, אני יכול להיעזר בשירותיו של ה-Default Gateway. אני לא זקוק ל-Default Gateway כדי להעביר חבילה למישהו בתוך הסאבנט שלי. אני יכול לעשות פשוט ARP ולרשום את ה-DST MAC ו-DST IP שלו בחבילה שלי.
21. אם כרטיס הרשת שלי מקבל חבילה אשר בשדה ה-Dst IP נמצא ה-IP שלי, הוא "יקח" אותה. נכון אם ורק אם יש עליה גם את הMAC שלי.
22. Wifi היא טכנולוגיה כל כך פופולרית כי היא מאפשרת מהירות גבוהה יותר מרשת קווית. לא נכון! היא איטית בסדר גודל!
23. ניתן להתחבר לרשת בלי להגדיר Default Gateway. לא נכון, ניתן להגדיר אותו ידנית או לקבל אותו דרך DHCP אבל הוא חייב להיות מוגדר!
24. ללא שרת DHCP, ירבו המקרים של התנגשויות IP ברשת. סביר להניח שכן, אלא אם זו רשת מצומצמת שהוגדרה ידנית.
25. חבילה אשר נעה ברשת לא משתנה בכלל בדרך, מלבד שדה ה-TTL. לא נכון! ה-MAC משתנה בכל מעבר בין תת רשת.
26. מפתח הצפנה הוא קוד העובר בעת ההתחברות לרשת אלחוטית. נכון חלקית, תלוי איזה סוג של מפתח יש מפתחות אישיים, ויש מפתחות משותפים. ב-WPA המפתח לא עובר בצורה מלאה וגלויה אף פעם כדי שלא יהיה אפשר להסניף אותו. עוברים רק נגזרות מתמטיות כלשהן שלו.
27. פרוטוקול UDP לא מבצע כלל בדיקה של נכונות המידע. לא נכון – יש checksum
28. CIDR Notation הוא שיטה חדשה שהחליפה את ה-Subnet Mask. לא נכון, היא שיטה מקבילה להצגת אותו מידע.
29. כל פרוטוקול במודל השכבות כולל חלק של הדרים וחלק של מידע. נכון, הוכחה: בלי המידע לא היה טעם להעביר הדרים, בלי ההדרים לא היה טעם להשתמש בפרוטוקול.
30. ניתן להתחבר לרשת Wifi בלי שאני רואה אותה ברשימת הרשתות הזמינות ב-Windows. נכון! לעיתים מטעמי אבטחה נהפוך את הרשת לנסתרת
31. ללא Multiplexing לא נוכל להריץ כמה תוכנות המשתמשות ברשת על המחשב שלנו. נכון! עד כדי שימוש במספר כרטיסי רשת שונים.
32. אם אני גולש ברשת Wifi פתוחה (ללא ססמא), גם אם אני גולש ב-HTTPS כולם יכולים להסניף ולקרוא את ההודעות שאני שולח. נכון! יוכלו לראות מה ששלחנו, אבל לא יוכלו להבין כלום מזה. מזל שיש הצפנות!
33. ב-UDP יש מנגנון מסוג Retransmission (שליחה מחדש). פשוט לא נכון.
34. הפעולה בה ראוטר מקבל חבילה ובודק מה היעד הבא שלה בטבלת הניתוב נקרא Routing. לא, זה נקרא Forwarding. Routing מתאר את תהליך הניתוב בצורה רחבה יותר.
35. אם אנחנו שולחים חבילה גדולה של 5 מ"ב בעזרת פרוטוקול UDP, היא לא תחולק לחבילות קטנות יותר. לא מדויק, UDP רוכב על פרוטוקול IP אשר יבצע חלוקה לחבילות קטנות יותר כאשר ההודעה גדולה כל כך.
36. Wifi (802.11( הוא פרוטוקול בשכבת הקו. נכון, שזה קצת מצחיק... כי אין פה קו...
37. כל הרשתות שיש להן Subnet Mask של 255.255.255.0 מתחילות ב-10.0.0.X. ממש לא.
38. חלק המידע של פרוטוקול SMTP הוא בשפת HTML. לא נכון! הוא MIME! בתוך ה-MIME עשוי להופיע HTML.
39. בכל חבילה אשר נעה ברשת תמיד יהיו את כל השכבות (קו-רשת-תעבורה-אפליקציה). לא נכון. למשל DHCP
40. יש שרתי TLD כמספר הסיומות שקיימות בעולם. לא נכון, יש הרבה יותר! (יש גיבויים)
41. MITM היא סכנה אשר קיימת בפרוטוקול ARP בלבד. לא נכון. בכל סוג תקשורת כמעט.
42. ה-Default Gateway שלי לא יכול להיות Switch לעולם. נכון, ל-DEFAULT GATEWAY חייבת להיות כתובת IP ולכן לא הגיוני שהוא יהיה Switch. עם זאת, הראוטר הביתי שלנו יכול לתפקד גם כSWITCH בין המחשבים בבית, שמחוברים אליו ישירות בכבל!

**חלק שלישי – שאלות פתוחות**

1. **סבא בצרה**

סבא שלכם מתקשר אליכם ואומר שהוא ניסה הכל, אבל הוא לא מצליח לגלוש לפייסבוק ולעשות לייק ו-share לתמונה שסבתא העלתה שלכם כשהייתם תינוקות. אחרי לבטים קשים, הגעתם למסקנה המוסרית שלמרות הפגיעה הברורה במעמד החברתי שלכם בעקבות הפעולות העתידיות של סבא, אתם עדיין תעזרו לו להתחבר לאינטרנט.

1. ביקשתם ממנו לפתוח את ה-CMD ולרשום ipconfig. כעבור רבע שעה הוא מעדכן שהוא עשה את זה, וכתובת ה-IP שכתובה לו שם לא נמצאת בכלל בסאבנט של הראוטר שלו! איפה כנראה שהייתה הבעיה?
2. סבא שינה את כתובת ה-IP שלו ידנית ועכשיו היא נמצאת בסאבנט הנכון, אבל הוא עדיין לא מצליח לגלוש לפייסבוק ולהראות לכם את החיבה הדיגיטלית שלו. ביקשתם ממנו להסניף על התעבורה שלו ולפלטר על HTTP ולהגיד לכם אילו הודעות שגיאה מופיעות שם. אחרי שעה סבא אומר שהוא הצליח לפלטר על HTTP, אבל אין בכלל חבילות של HTTP בהסנפה! מה יכולה להיות הבעיה? איך ניתן לפתור אותה? (רמז – היזכרו בכל תהליך הגלישה לאתר)
3. לבסוף סבא שלכם רואה בהסנפה שהוא מצליח לשלוח הודעת TCP לפורט 80 של השרת של פייסבוק, אבל אין תשובה... כשאתם מנסים לגלוש לאתר הוא עובד, וכשסבא שולח PING ל-IP של השרת אז השרת עונה, אז מה יכולה להיות הבעיה האחרונה?

|  |
| --- |
| 1. נראה שה-IP של המחשב שלו לא תואם לרשת. הקצאת כתובות IP נעשית ע"י שרת ה-DHCP, ולכן סביר שהבעיה הייתה בהגדרות של שרת ה-DHCP שלו (לרוב מדובר בראוטר עצמו ברשתות ביתיות). 2. עכשיו שה-IP שלו תקני, תהליך הגלישה לאינטרנט מתחיל בבקשת DNS שמטרתה להפוך את הדומיין של Facebook לכתובת IP מתאימה, ורק אז הדפדפן יכול להוציא את בקשת ה-HTTP הרלוונטית. אם סבא לא רואה בכלל פקטות HTTP בתעבורה, אז סימן שהבעיה היא עוד לפני שמגיעים לשלב הזה – לכן הבעיה היא כנראה ב-DNS. במקרה כזה, אפשר לבדוק מה שרת ה-DNS שמוגדר למחשב (ipconfig /all), ובכל מקרה ניתן להגדיר את השרת DNS של גוגל (8.8.8.8) בתור שרת אפשרי. יכול להיות שהבעיה ב-DNS היא לא בהגדרות, אלא בחסימה של Firewall, אבל עם בעיה כזאת אנחנו מתמודדים בסעיף הבא... 3. כאן אנחנו רואים שהאתר תקין (אנחנו מצליחים לגלוש אליו וה-PING עובד), אבל סבא ספציפית לא מצליח להרים קישור בפורט 80 מול השרת. במקרה הזה סביר מאוד שהבעיה היא חסימה רשתית כלשהי, וסבא צריך לבדוק את החוקים של ה-Firewall של הראוטר שלו ולוודא שהוא יכול לגשת בפורט הזה החוצה (ושאין חסימה על כתובת ה-IP של Facebook). |
| תשובה |

1. **שומרים על ריכוז במקום העבודה**

מחקרים רבים מראים ששליחת מיילים בזמן העבודה מורידה את הפרודוקטיביות משמעותית ויוצרת קטיעה של חוט המחשבה. חואניטה, מנכ"לית של חברת סטארט-אפ בתחום הראייה הממוחשבת, החליטה למנוע מהעובדים שלה את האפשרות לשלוח מיילים כדי להגביר את הפרודוקטיביות של החברה.

1. אילו פרוטוקולים מאפשרים שליחת מייל (במייל ארגוני, לא ג'ימייל)? כיצד ניתן לחסום את האופציה הזאת מבחינת תקשורת?
2. האם בוודאות חסימה זאת תפעל על כל השרתים של שליחת המיילים?
3. האם ניתן לחסום מהעובדים קריאה או שליחה של מייל בג'ימייל?

|  |
| --- |
| 1. הפרוטוקול עליו למדנו הוא SMTP בפורט 25. ניתן לחסום את התעבורה היוצאת בפורט 25. 2. פורט 25 הוא פורט מוכר, אבל אין זה אומר שכל השרתים מאזינים בפורט הזה. ניתן לפתוח שרת SMTP בפורט אחר. 3. קריאת ושליחת מיילים בתיבת Webmail מתבצעת ע"י שימוש בפרוטוקול HTTP, ולכן אם נחסום את הפורט 80 או 443 (HTTPS) נחסום את כל הגלישה של המשתמשים, וזה יהיה רעיון לא כל כך מוצלח. |
| תשובה |

1. **To Be Or NAT To Be**

חיים, תלמיד בניצני מגשימים, פנה אליכם כדי לקבל עזרה. הם למדו על NAT וכל הסיפור הזה של IPים משתנים מבלבל אותו מאוד... תוכלו לעזור לו?

1. למה בכלל צריך להחליף את כתובת ה-IP הפנימית בכתובת חיצונית? מה הבעיה בלפנות לשרת באינטרנט עם הכתובת הפנימית שלי?
2. אם ה-NAT מחליף את כתובות ה-IP של כל המחשבים ברשת לאותה בכתובת החיצונית, איך הוא יודע להחזיר את התשובות למחשבים הנכונים? (נניח ששני מחשבים מדברים דרך ה-NAT באותו הזמן)
3. אמרו משהו בשיעור של חיים על זה ש-NAT גם עוזר לאבטח את הרשת הפנימית – מה היתרון ב-NAT שעוזר להגן על המחשבים ברשת?

|  |
| --- |
| 1. כמו שלמדנו בשיעור, יש יותר מחשבים מכתובות IP ולכן יצרו טווחי IP פרטיים, ככה שלהרבה מחשבים בעולם יכולה להיות אותה כתובת ה-IP (כל עוד הם לא נמצאים באותה רשת פנימית). ככה, כאשר כל אחד מאיתנו נמצא ברשת הביתית שלו, יכולה להיות לכולנו אותה כתובת ה-IP ואנחנו עדיין נהיה מסוגלים לתקשר עם האינטרנט ואחד עם השני (בעזרת הכתובות החיצוניות של הראוטר הביתי שלנו).   אם הראוטר לא יחליף את הכתובת שלנו לכתובת חיצונית ייחודית, אז שרת שאנחנו פונים אליו עם כתובת פנימית ינסה לענות לנו, אבל הראוטרים לא ידעו איפה הכתובת נמצאת (כי הכתובת קיימת בהמון רשתות בעולם). יותר גרוע מזה, הראוטר של השרת שאליו אנחנו פונים אולי יחשוב שהכתובת היא כתובת מקומית בתת הרשת שלו... לכן חייבים שכתובות שמתקשרות באינטרנט יהיו ייחודיות (ולא כתובות פנימיות).   1. מזל שיש גם פורטים ולא רק כתובות IP... ה-NAT פשוט דואג שבטבלה הפנימית שלו תהיה הצמדה בין כל שיחה של מחשב ברשת הפנימית (כתובות ופורטים של שני הצדדים) לבין השיחות שהוא מנהל (בהם הוא החליף את הכתובת והפורט של המחשב ברשת שלו). כל עוד הוא לא ממחזר את הפורטים ודואג שלא יהיה מצב שלשתי שיחות יהיו אותם הפורטים וה-IP של השרת בצד השני, הוא יידע למי להעביר את החבילות לפי הפורטים וה-IP, וכך הוא יכול לשרת כמות גדולה של מחשבים שנמצאים באותה רשת. 2. בגלל שכל המחשבים ברשת מיוצגים ע"י אותה כתובת IP (הכתובת של ה-NAT), אז למחשב מחוץ לרשת אין יכולת לפנות ישירות למחשב ברשת הפנימית – הוא יכול לפנות רק ל-NAT. במצב כזה, מחשבים ברשת יכולים רק ליזום תקשורת מול האינטרנט, והאקרים לא יכולים לפנות ישירות אליהם, מה שמגביר את האבטחה על המחשבים. זה כמובן לא מגן על המחשבים באופן מוחלט כמו שראינו בקורס, אבל זה בהחלט משפר את המצב. |
| תשובה |

1. **היררכיית DNS**
2. היררכיות DNS זה דבר מסובך... מה הבעייתיות בפשוט לאפשר לשרת ה-ROOT לשמור את כתובות ה-IP של כל הדומיינים, ושכולם יפנו אליו?
3. הסבירו את היררכיית שרתי ה-DNS – אילו סוגי שרתים יש ואיך מתנהלת בקשה איטרטיבית של DNS?
4. מה היתרון של מנגנון ה-caching בשרתי DNS לוקאליים? מה החיסרון?

|  |
| --- |
| 1. לא משנה כמה שרת ה-ROOT יהיה חזק ומגובה, הוא לא יהיה מסוגל לעמוד בעומסים של פניות מכל מי שגולש לאינטרנט בכל העולם... בנוסף, שמירה של כל ההצמדות בין הדומיינים לכתובות IP בטבלה אחת תיקח המון מקום והחיפוש בטבלה יהיה איטי (מה שעוד יותר יאט את זמן התגובה של שרת ה-ROOT). בגדול, אם כולם היו פונים רק אליו אז כל האינטרנט היה מאט עד לכדי עצירה. 2. כדי למנוע מצב של עומס כל כך גדול על שרת ה-ROOT, מערכת ה-DNS היא מערכת מבוזרת. שרת ה-ROOT אחראי להגיד מיהו שרת ה-TLD שאחראי על הדומיין המבוקש (com/org/gov וכו'). שרת ה-TLD אחראי להגיד מיהו השרת האוטורטיבי שאחראי על הדומיין המבוקש (google/facebook וכו') והשרת האוטורטיבי כבר יודע מה כתובת ה-IP של הדומיין השלם (www.google.com למשל). שאילתה איטרטיבית מתנהלת בסדר הנ"ל – השרת הלוקאלי פונה אל שרת ה-ROOT, שמחזיר לו את כתובת ה-IP של שרת ה-TLD המתאים. לאחר מכן הוא פונה אל שרת ה-TLD, שמחזיר לו את כתובת ה-IP של השרת האוטורטיבי. לבסוף הוא פונה לשרת האוטורטיבי שנותן לו את כתובת ה-IP הרצויה, אותה הוא מחזיר למחשב שפנה אליו במקור. 3. התהליך שמתואר בסעיף הקודם אינו קצר ודורש פנייה למספר שרתים. כדי לאפשר חוויית משתמש טובה יותר (וכדי להקל על העומס ששרת ה-ROOT ושרתי ה-TLD חווים), שרתי ה-DNS הלוקאליים שומרים ב-Cache שלהם את הדומיינים שלקוחותיהם חיפשו. באופן הזה, אם אנחנו מחפשים כתובת שחיפשנו בעבר, שרת ה-DNS הלוקאלי יוכל לענות לנו ישירות מבלי להצטרך להטריד את השרתים הגלובליים.   החיסרון בשיטת ה-Caching הוא אבטחתי. כמו שלמדנו, העובדה ששרת לוקאלי שומר את כתובת ה-IP של דומיין מסוים, אומר שניתן לגרום לו לשמור כתובת לא נכונה, כך שכל הלקוחות שלו כעת יקבלו כתובת IP שקרית שיכולה להכיל אתר זדוני עבור גניבת סיסמאות. |
| תשובה |

1. **טווחי IP**

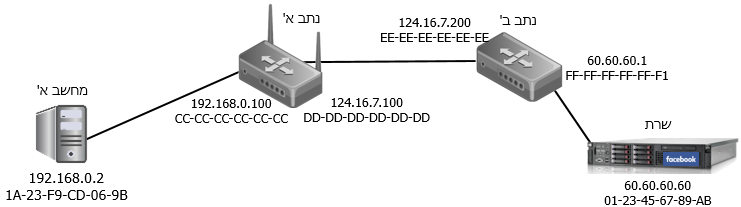
דני (שם בדוי), שאל את המדריך שלו בהפסקה כמה שאלות שהמדריך קצת הסתבך איתן... נסו לעזור למדריך להסביר לדני איך שכבת הרשת עובדת.

1. החשיבות של כתובת ה-IP ברורה לי – כל מחשב צריך כתובת כדי שנוכל לדבר איתו. אבל למה צריך שכל הכתובות IP שנמצאות באותה תת רשת יהיו באותו הטווח? מה הבעיה עם זה ששני מחשבים שנמצאים באותה תת הרשת יהיו בעלי IPים שונים לחלוטין?
2. עשיתי tracert אתמול לגוגל מהמחשב שלי בבית וקיבלתי רשימת נתבים שדרכם ההודעות שלי נשלחו. הבוקר ביצעתי שוב tracert מאותו המחשב וקיבלתי רשימת ראוטרים שונה! למה שמשהו כזה יקרה?

|  |
| --- |
| 1. למחשב שנמצא בתת הרשת אין באמת בעיה עם זה שהכתובות יהיו כלליות ולא בטווח ספציפי, אבל לנתב זה חשוב מאוד. אם הכתובות לא היו מחולקות לפי טווחים, הנתב היה צריך לזכור עבור כל כתובת IP לאיזה רגל צריך להעביר את החבילה, והטבלה הזאת היא ענקית ומהירות התפקוד של הנתב הייתה יורדת משמעותית. העובדה שהכתובות ממויינות לפי טווחים מאפשרת לנתב להתייחס רק לחלק הרלוונטי בכתובת כשהוא רוצה להבין לאן לנתב את החבילות, והוא יכול להכניס כמות גדולה מאוד של כתובות תחת אותו כלל ניתוב בטבלת הניתוב שלו, ובכך לתפקד הרבה יותר מהר... 2. כמו שלמדנו בשיעור, תפקידה של שכבת הרשת היא לדאוג שהמידע עובר במסלול הכי יעיל שאפשר. זה נעשה ע"י מגוון אלגוריתמים שאיתם הנתבים מדברים אחד עם השני כדי לעדכן אחד את השני בעומסים שלהם, כך שטבלאות הניתוב של הנתבים תמיד תהיינה כמה שיותר עדכניות ומתאימות, ובאמת ייצגו את המסלולים המהירים ביותר להעברת החבילות. יכול להיות שאתמול הרשת עבדה באופן תקין, אך הבוקר כשדני ניסה לשלוח את ה-tracert הרשת השתנתה (למשל, נוצר עומס גדול מאוד על אחד הנתבים) ולכן טבלאות הניתוב של הנתבים השתנו כך שכעת המסלול המהיר ביותר של החבילות מהמחשב של דני לגוגל הוא אחר, ולכן הנתבים שהוא עובר דרכם שונים ותוצאת ה-tracert גם כן שונה בהתאם. |
| תשובה |

1. **כתובות IP ו-MAC**

ניזכר ברשת שראינו בשיעור שכבת הקו:



מחשב א' שולח בקשת HTTP לשרת שבתמונה. נעקוב אחרי הבקשה ונראה מיהם הכתובות בכל שלב בשיחה.

1. ברגע שהמחשב מוציא את הבקשה, מהם כתובות ה-IP וה-MAC של היעד ושל המקור?
2. ברגע שנתב א' מעביר את החבילה לנתב ב', מהם הכתובות?
3. ומה קורה כשנתב ב' מעביר את החבילה לשרת?
4. לבסוף, מהן הכתובות כשהנתב שולח את התגובה דרך נתב ב'?

|  |
| --- |
| 1. כתובת ה-IP של המקור ושל היעד לא ישתנו עד שהחבילה תגיע לשרת – הם מאפשרים לנתבים להבין לאילו רגליים צריך להעביר את החבילה. כתובת המקור תהיה 192.168.0.2 וכתובת היעד תהיה 60.60.60.60. כתובות ה-MAC הן הכתובות הפיזיות של הרכיבים שמתקשרים אחד עם השני ברגע הנתון, והן משמשות כדי שכל רכיב ידע שפונים אליו בתוך תת הרשת שבו הוא נמצא. כתובת המקור תהיה 1A-23-F9-CD-06-9B, בעוד שכתובת היעד תהיה CC-CC-CC-CC-CC-CC. 2. כאמור, כתובות ה-IP לא ישתנו. כתובת המקור של ה-MAC תהיה DD-DD-DD-DD-DD-DD וכתובת היעד תהיה EE-EE-EE-EE-EE-EE. 3. שוב, כתובות ה-IP יישארו כמו שהן. כתובת המקור של ה-MAC תהיה FF-FF-FF-FF-FF-F1 וכתובת היעד תהיה 01-23-45-67-89-AB. 4. כעת השרת עונה ולכן כתובות ה-IP תתחלפנה. כעת כתובת המקור היא 60.60.60.60 וכתובת היעד תהיה 192.168.0.2. כתובות ה-MAC תתחלפנה גם כן ביחס לסעיף הקודם – כתובת המקור תהיה 01-23-45-67-89-AB וכתובת היעד תהיה FF-FF-FF-FF-FF-F1. |
| תשובה |

1. **עוצרים ARP-Poisoning**

למדנו בשיעור שכבת הקו על פרוטוקול ARP, שמאפשר לקבל כתובת MAC של רכיב כלשהו, בהינתן כתובת ה-IP שלו. למדנו גם שהפרוטוקול הזה לא מאובטח, וניתן להתחזות לכתובות IP אחרות ברשת (כמו הראוטר) ולראות את כל התעבורה של מחשב ברשת.

חורחה, מנהל הרשת של בנק אוצר החייל (שלא היה בתוכנית מגשימים), הציע למנכ"ל הבנק שיטה להגן מפני תקיפות ARP Poisoning – נשים על הראוטרים ברשת של הבנק תוכנה שמסניפה את התעבורה ומזהה כאשר רכיב שאינו הראוטר מזדהה בתור כתובת ה-IP של הראוטר (דבר שרק אמור לקרות במקרה של תקיפה, כי חורחה דואג שלא יהיו כתובות IP חופפות ברשת). כאשר הראוטר מזהה מקרה כזה, מייל יישלח לחורחה והוא יידע לפעול בנושא!

1. מה בעייתי בפיתרון של חורחה?
2. הציעו פיתרון טוב יותר. (רמז – לאיזה תעבורה אתם צריכים להיות נגישים כדי לזהות תקיפות כאלה?)

|  |
| --- |
| 1. חורחה מניח שהראוטר בכלל יקבל את התעבורה של רכיבים שמתחזים אליו, אבל הוא לא מבין ש-ARP לא עובד ככה... הראוטר אכן יקבל את כל בקשות ה-ARP שמחפשות אותו (שנשלחות ב-Broadcast), אבל את התשובות הוא לא יוכל לקבל, כי הן הרי עוברות ישירות בין המתחזה למבקש (ב-Unicast). לכן, הרעיון לא יעבוד... 2. מהבעיתיות של הרעיון של לשים את התוכנה על הראוטר, אנחנו מבינים שאנחנו צריכים לרדת שכבה כדי לזהות את התקיפות הללו. כדי להיות נגישים לתעבורת Unicast שכזו, אנחנו צריכים שהתוכנה שלנו תרוץ על הסוויצ'ים ברשת של הבנק. הם יוכלו לדעת לזהות מקרים בהם כתובת IP פתאום מגיעה מכתובת MAC חדשה (או מרגל שונה בסוויץ').   אבל יכול להיות שבאמת החלפנו ראוטר ואנחנו לא רוצים שכל מקרה כזה יקפיץ את חורחה... לכן התוכנה שלנו יכולה להתריע רק במקרה בו שתי כתובות MAC שונות עונות על בקשת ARP (אחת מהן היא האמיתית והשנייה היא של התוקף).  רעיון נוסף הוא לשים את התוכנה על כל המחשבים ברשת. |
| תשובה |

1. דני הגיע ליום הראשון של שיעור רשתות במגשימים. לאחר ההפסקה התבקש לפתוח את מחשבו האישי, להתחבר לרשת האינטרנט ולשלוח מייל למדריך (ב outlook). פרט את התהליך שעובר המחשב של דני, החל מההתחברות לרשת ועד לסיום שליחת המייל.המשך: במה היה שונה התהליך אילו היה שולח מייל באמצעות Gmail?