

2019

חומריעזר באבטחת מידע כיתה י"ג

תוכן

4.....	מנוחים בעולם אבטחת מידע
6.....	Malware (Malicious Software)
6.....	סוגי Malware
7.....	Worm
7.....	Trojan horse
7.....	(crypto-malware) Ransomware
8.....	Rootkits
8.....	Spyware (Spying Software)
8.....	Adware (Advertising Software)
8.....	דרכי העברת Malware
8.....	Logic bomb
9.....	Backdoor
9.....	(Robot networks) Botnet
9.....	Privilege Escalation
10.....	דרכי מניעה וטיפול בוירוסים
12.....	Confidentiality, Integrity, Availability (CIA)
12.....	(סודיות) Confidentiality
12.....	Integrity (שלמות המידע)
12.....	Availability (זמןנות)
13.....	תקיפה (הסתכלות בעניין התקוף)
13.....	תכונות של התקופים:
13.....	סוגי התקופים:
14.....	Hackers
15.....	שלבי תהליך תקיפה
17.....	Network Security Design
17.....	(DMZ) Demilitarized Zones
17.....	Subnetting
18.....	Virtual LAN (VLAN)
20.....	Tunneling protocols
21.....	(הנדסה חברתית) Social Engineering
21.....	עקרונות שמאפשרים מתקפת הנדסה חברתית
21.....	דוגמאות להנדסה חברתית:
22.....	Social Engineering Attacks
23.....	התגוננות מפני Social Engineering
24.....	סוגי התקופות

29.....	מודל AAA
32.....	Layer 2 Attacks
32.....	STP Attack
33.....	כיצד עובדת התקפת ?ARP poisoning
35.....	MAC Address Spoofing Attacks
37.....	VLAN Hopping Attack
37.....	Double Tagging attack
38.....	DHCP Spoofing Attacks
39.....	DHCP Snooping
41.....	Dynamic ARP Inspection (DAI)
41.....	הגדרת DAI
42.....	Securing Router Access
44.....	Securing Wireless Networks
44.....	IEEE 802.11 Wireless Protocols
45.....	ערוצי (Channels) רשת אלחוטית
46.....	שיטות הצפנה עבור רשתות אלחוטיות.
47.....	שיטות ההזדהות עבור רשתות אלחוטיות
50.....	סוגי התקפות אל-חלוטיות
51.....	Cryptography
51.....	סודיות (Confidentiality)
51.....	שלמות המידע (Data Integrity)
51.....	זהוי (Authentication)
52.....	(shared-key encryption) Symmetric Encryption
53.....	Symmetric key
54.....	(public-key encryption) Asymmetric Encryption
54.....	Asymmetric key -
55.....	הצפנה בזמן אמת (Real-time)
55.....	החלפת מפתחות
56.....	key escrow (נאמנות המפתח)
56.....	Hashing (גיבוב)
56.....	אלגוריתמים נפוצים לביצוע Hashing
57.....	(Hash message authentication code) HMAC
58.....	חתימה דיגיטלית (digital signature)
60.....	-IDS/IPS מבוא
65.....	Firewall Technologies
66.....	Stateless Packet Filtering Firewall

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולכם!

66.....	Stateful Inspection Packet Filtering Firewall
67.....	Application Awareness Firewall
67.....	Proxy Firewalls
68.....	IPsec Site to Site VPN גרסה מצומצמת
70.....	Virtual Private Network לכיתות הנדסאים
86.....	Virtual Private Network
86.....	יתרונות VPN
87.....	VPN Protocols
87.....	VPN Authentication Protocols
89.....	Internet Protocol Security (IPSec)
90.....	מחסנית הפורוטוקולים של IPSec
91.....	שיטת הצפנה
97.....	Site to Site VPN תרגיל:
102.....	ASA Adaptive security appliances
104.....	System Message Logging (Syslog)

מוניינים בעולם אבטחת מידע

Asset (נכס)

כל דבר בעל ערך לארגון, שיש צורך להגן עליו.
נכס מוחשי (אנשים, מחשבים, וכן הלאה).

נכס לא מוחשי (מסד נתונים, רשימות אנשי קשר, חשבונות משתמשים, תדמית החברה).
הידיעה על איזה נכסים אנו צריכים לננות להגן, ערכם, מיקומם ורמת החשיפה שלהם יכולם לעזור לנו לקבוע בצורה יעילה יותר כמה זמן וכוסף יש להשקיע כדי לאבטח את הנכסים.

Vulnerability (חולשה)

חולשה במערכת או בתכנון, פוגעת בביטחון או בפונקציונליות ומאפשרת לתקוף לעקוף את מנגנון האבטחה.

ברשת קיימן פוטנציאלי גדול לחולשות וזאת כתוצאה אחד או יותר מהסיבות הבאות:



- שגיאות בתכנון, שגיאות בהגדירות, פגמים במדיניות
- גישה פיזית לא מורשת למשאבי רשת, פגיאות בחומרה
- חולשות בפרוטוקולים ובתוכנות, אי התקנת עדכוני אבטחה.
- סימאות חולשות, הגורם האנושי

Zero-day (unpublished) vulnerabilities

בכל יום מתגלות חולשות חדשות. Zero-day vulnerability זו חולשה שלא פורסמה ברבים ולכן למערכות הגנה קשה מאוד להתמודד אתה. כדי לזהות התקפות כאלה לא ניתן להשתמש ב-signature של רשת חשודה על ידי שימוש ב-IPS/IDS או על ידי זיהוי אנושי.

Threat (איום)

איום קיים כאשר מזוהה סכנה אבטחה פוטנציאלית לנכס. לסבירה מסוימת יש או אין חולשה לאיום מסוים, זה תלוי בסוג האיום ובסוג סביבת העבודה. לדוגמה: איום יכול להיות מתקפה חדשה על Oracle database server או אם אתה משתמש ב- Microsoft SQL server אז לא קיימת לך חולשה לאיום.

Risk (סיכון)

איום מהו זה סיכון רק כאשר קיימת חולשה לאיום. רמת האיום קובעת את רמת הסיכון. ככל שרמת האיום גדולה יותר כך גם רמת הסיכון גבוהה יותר. לדוגמה: אם קיימת חולשה אך היא עדין לא התגלתה אז הסיכון לא ממש. דוגמא נוספת: אם קיימים איומים, אך קיימות הגנות ראויות אז פוטנציאלי האיום קטן ובכך קטין הסיכון.



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר ללימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

(ניסיונן) Exploit

זהו הכלי שבבעזרתו תוקף מנצל את החולשה.

כאשר Exploit משוחרר לאינטרנט, תוקפים עם מעט ידע ויכולות יכולים לנצל חולשות.

דוגמאות ל- Exploits : Scripts, Malware, Password crackers



Payload

כדי לנצל Vuln, אנו משתמשים ב- Exploit ששולח Payload לקורבן.

כלומר, Payload זה הקודшибו שיבוצע במערכת היעד כדי לנצל חולשה שקיימת במערכת היעד.



אמצעי מנע - זהו מיחסום שמפחית סיכון פוטנציאלי. מטרתו נטרול הפגיעה או לפחות הפחחת הסבירות לניצול הסיכון. ניתן להפחית את הסיכון על ידי הוצאות כסף על אמצעי אבטחה אך בדרך כלל לא נשקיע יותר כסף משוו הנכס. בכלל מקרה, לא ניתן לבטל את הסיכון לחלוtin ולכן אנו חייבים למצוא את האיזון בין האיים לבין הסיכון.

דוגמאות לאמצעי מנע:

- Administrative (מנהל): כתיבת מדיניות, נהלים, הנחיות ותקנים.
- Physical (פיזי): אבטחה פיזית עבור שרת, רשת, ציוד ותשתיות.
- Logical (לוגי): סיסמאות, חומות אש, מערכות למניעת חדירות, רשימות גישה ועוד.

Malware (Malicious Software)

הטכנית הנפוצה ביותר ב- Cyberattack היא שימוש ב- Malware. Malware זהו שם כללי לתוכנה זדונית (Malicious Software) שתוכננה במיוחד כדי לפרוץ למחשב, לגרום לו נזק או להציג מידע ללא אישור.

תוכנות Malware:

- פועלם ברקע כדי לא להתגלות (Transparent). חלקם יחשפו כמו Ransomware.
- תוכנו ננצל חולשות במערכות הפעלה או בתוכנות.
- אך עליינו לעדכן את מערכת הפעלה והתוכנות כדי לחסום את החולשות.
- אין מערכות שחסינות מפני Malware. פועלם נגד כל פלטפורמה/מערכת הפעלה.

גורמים שמקשים על זיהוי Malware:

- הסכם העצום של תוכנות זדוניות שקיימות ונוצרות על בסיס יומי הוא כמעט בלתי נתפס. בנוסף, שימוש בכלאי איתור מובסס חתימה לא מספיק יעילים.
- פעמים רבות, Malware מוטבע ביישום מהימן ונסלח בפרוטוקול שמורשה לעבר דרך ה- Firewall.
- לארגון קיימים משאים מוגבלים (אדם וטכנולוגיה) וקשה להם לעמוד בקצב הגידול של הייקף תעבורת הרשת.
- השימוש הגובר בהצפנה מנסה לזהות תעבורה זדונית בراتש.

סוגי Malware

Virus - זה קוד זדוני שמופעל על המחשב ללא ידיעת המשתמש. מטרתו העיקרית היא לשכפל את עצמו ולהעביר את המידע שלו להלאה. במקרה הטוב, וירוס לא יעשה נזק מלבד להיות נוכח במערכת הפעלה אף במקרה הגrouch יותר וירוס יכול לפגוע במידע, להרוויס את מערכת הפעלה ולהתפשט למערכות אחרות. כדי שווירוס יפעל, המשתמש צריך להפעיל את הוירוס בצורה כלשהי כמו לחיצה על קישור. בנוסף הוירוס צריך Host כדי לפעול ולהפיץ את עצמו, הוא לא יכול לעשות זאת לבד.

סוגי וירוסים:

- **Boot sector** - וירוס שמאותגן בסקטור הראשון של הדיסק קשה. כאשר מערכת הפעלה עולה, הוא נטען יחד אתה לזכרון RAM לפני שהאנטי וירוס פועל.
- **Macro** - זה קוד מזיך שבדרך כלל משולב במסמך או מייל ומופעל אוטומטית כאשר המשתמש פותח את המסמך או המייל.
- **Companion** (ווירוס נלווה) - זה קובץ הפעלה (תוכנה לגיטימית) שמצומד אליה וירוס. כאשר התוכנה הלגיטימית מופעלת, גם הוירוס מופעל.

ווירוסים מתחמכים בדרכים הבאות:

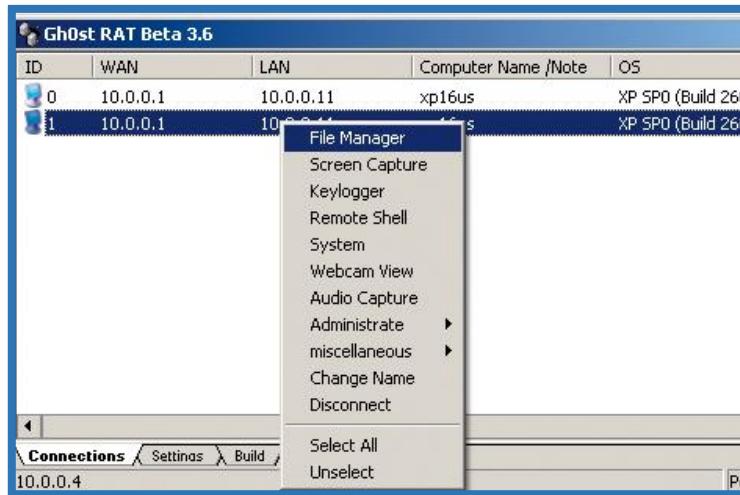
- **Polymorphic** - וירוס מוצפן שככל פעם שהוא מדבק הוא משנה את מפתח ההצפנה שלו וכך משנה את צורתו כדי לא להתגלות על ידי תוכנת אנטי וירוס.
- **Metamorphic** - דומה ל- Polymorphic, משכתב את עצמו כל פעם מחדש.
- **Armored** - מכיל קוד לא רלוונטי שמשמש כשכבות הגנה בכך להקשות על ניתוח ופיענוח הוירוס. כך לוקח זמן רב לפענה את הוירוס והוא מופץ ליוטר מערכות.
- **Stealth virus** - וירוס שמסתיר את עצמו על יד הצפנה בכך לא להתגלות.
- **Memory resident** - לאחר הפעלתו נשאר בזיכרון וմדבק כל תוכנה נוספת שנמצאת בזיכרון.

Worm

Worm שונה מווירוס בצורת הפצתו. Worm מפיץ את עצמו דרך הרשת ללא צורך בעזרה אנושית. לשם הפצתו, תולעים מנצלות פגימות במערכת היעד. תולעת שנכנסה למחשב דרך חולשה במערכת, מנצלת את הרשות כדי לנוע בכוחות עצמה למערכות עם חולשה דומה.

Trojan horse

סוס טרויאני מאפשר לתוקף לבצע פעולות zdוניות מאחוריו הקלעים על-ידי השגת גישה לא מורשת למערכת. מגע למערכת על-ידי הורדיה ללא כוונה או דרך התקנים נשלפים (disk on key). לדוגמה, Ghost Rat (Remote Administration Tool) זה סוס טרויאני שמאפשר שליטה מרוחק על מערכת הפעלה חלונות.



(crypto-malware) Ransomware

תוכנה שמצפינה את המידע האישי של המשתמש. אם המשתמש ירצה לקבל את מפתח הפענוח (המפתח הפרטני), הוא יצטרך לשלם סכום מסוים לפיקוח עינוי של התוקף. גם אם המשתמש מחליט לשלם, אין ערבות לכך שבאמת התוקף ייתן את המפתח המתאים.



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
לשונמת לבכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

Rootkits

Rootkits זו תוכנה שמשתלבת ב- BIOS/UEFI, boot loader או בלית מערכת הפעלה ומאפשרת גישת root/administrator למערכת הפעלה. קשה לאלו Rootkit בغالל שהוא נטען למערכת לפני שמערכת הפעלה נטענה במלואה וכך הוא יכול להסתיר פעילות זדונית מערכות הפעלה. לדוגמה, יכול להסתיר קבצים, חשבון משתמש, process שפועל במערכת מלהופיע ב- Task Manager או להסתיר connection שלא יופיע ב- netstat.

Spyware (Spying Software)

Spyware זו תוכנה זדונית שעוקבת אחר פעילות המשתמש (ללא ידיעת המשתמש) ומדוחה לצד שלישי. לדוגמה, keylogger שומר את לחיצות המקלטים במקלדת. Spyware לא מפייץ את עצמו בצורה אוטומטית אלה המשתמש מתקין אותה לא במודע תוך כדי התקנת תוכנה אחרת או תוך כדי ביקור באתר אינטרנט נגוע. שימוש Spyware בצורה חוקית, מאפשר מעקב אחר פעילות הילדים או העובדים.

Adware (Advertising Software)

המטרה המרכזית של Adware זה רוח כספי עלי-ידי העברת פרסומות למשתמש. נחשב לסוג מסוים של Spyware בגלל שהוא שולח למשתמש פרסומות לפי העדפות והפעולות של המשתמש. בדרך כלל הפרסומות לא מזיקות אך חלק מהמקרים הם פוגעות ביצועי המחשב. צורת הבדיקות ב- Adware, זהה לצורות הבדיקות ב- Spyware.

דרבי העברת Malware

תוכנה זדונית לא מגיעה למחשב מהוור. יש צורך להעביר אותה בדרך מסוימת למחשב. ניתן לבצע זאת במספר דרכים כאשר הדרך הקלה ביותר היא להציג פיסית למחשב לא מוגן ולבצע מקומי את הפעולה/zdונית. כאן אני מפרט את דרכי העברת Malware:

דרך תוכנה, מייל או התקן אחסון נייד

- פתיחת קובץ שנשלח במייל ומכל תוכנה זדונית.
- שירות FTP קל להעלאה והורדנה של קבצים.
- תוכנות (P2P) peer-to-peer כמו torrents..bit
- התקן אחסון נשלף כמו DVD/USB.
- רשתות חברותיות.
- אתרים שמיכלים תוכנות וסקייפטים זדוניים.

Logic bomb

זו תוכנה זדונית שמזמנת לפעול רק כאשר משהו מסוים קורה. לדוגמה:

- פועלת בתאריך מסוים או לאחר זמן מסוים מרגע הפעלה.
- פועלת כאשר המשתמש ביצה פעלת מסוימת כמו הפעלה המחשב מחדש או הפעלת תוכנה מסוימת.

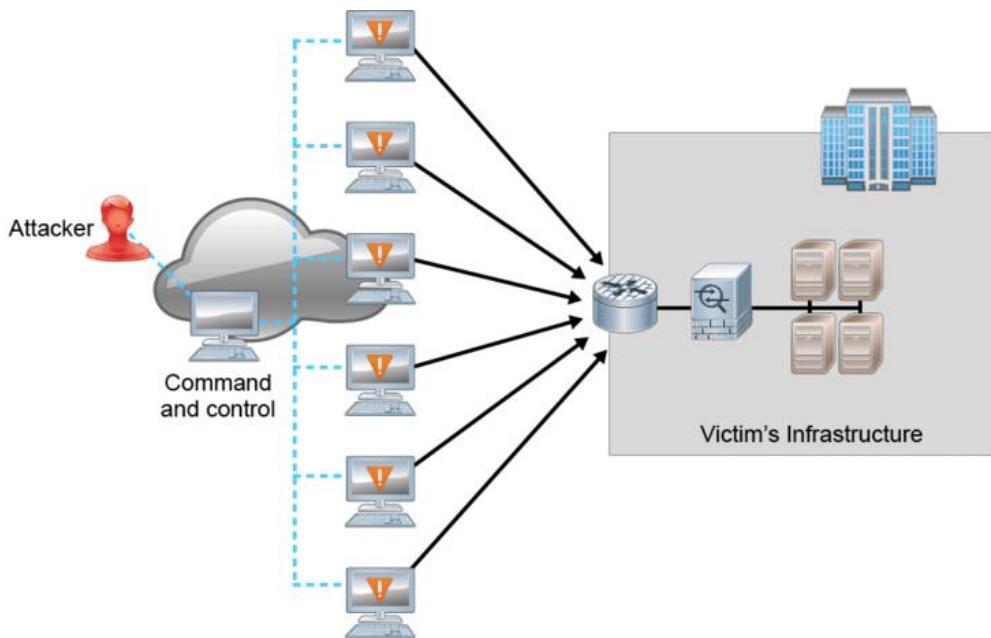
Backdoor

זו דרך לעקוף את מגנוני ההזדהות ואמצעי אבטחה נוספים כדי לאפשר גישה לא מורשת למחשב/תוכנה. תוכנות מסוימות מגיעות עם Backdoor מובנה בתוכם (במתקoon או לא) . Backdoor או Worm Trojan horse יכולים ליצור במערכת



(Robot networks) Botnet

Zombie זהו התקן שמחובר לרשות ונשלט על ידי Hacker במטרה לסרוק או לתקוף מחשבים אחרים בראשת. **Botnet** זה אוסף של Zombies שמוכנים לקבל הוראות מהתוקף. בדרך כלל, התוקף משתמש בערוצ חשי (מוזפן) כדי לנהל את המחשבים ב- Botnet .
בדרך כלל Botnet משמש להתקפות מסוג: spam | spyware ,adware ,DDos



Privilege Escalation

על-ידי ניצול באג, ליקוי בתוכנה או ב- firmware, ניתן לקבל גישה למשאבים שבדרך כלל מוגנים ולא נגישים למשתמש או לתוכנה. כתוצאה לכך, המשתמש מקבל זכויות נוספות שמאפשרות לו לדוגמה: לקבל שליטה ניהולית או לקרוא מיילים ללא אישור.

דרכי מניעה וטיפול בווירוסים

מניעה זה עניין של תחזקה ושימוש זהיר במחשב, לדוגמה, גלישה באתרים אמינים ופתיחה דוואר אלקטרוני בזהירות. המטרה היא לא לנסוט למןעו מהמערכת מלהידבק בווירוס ובמידה והמערכת נדבקה אז לנסוט למזער נזקים.

פעולות להתגוננות מפני ווירוסים:

- חובה שתוכנת אנטי-ווירוס תהיה מותקנת במחשב ושהיא מתעדכנת לפחות פעם ביום. חשוב לציין, אנטי-ווירוס לא יכול לגלוות הכל. הוא בדרך כלל לא מגלה bombs logic.rootkits ופעולות של botnet.
- חובה להתקין עדכוני אבטחה כדי שמערכת הפעלה והתוכנות יהיו עדכניות כמה שיותר. בתיכון מושחררים עדכוני אבטחה שכיסויים חורי אבטחה.
- רצוי להתקין במחשב Firewall ובנוסף לשיהה Firewall בנתב או להתקין נפרד.
- רצוי להפריד בין המערכת הפעלה לבין התוכנים החשובים באמצעות שני מחיצות נפרדות (p,c). קרקל יותר לגבות את הנתונים ובקרה הצורך להתקין מחדש את מערכת הפעלה.
- כדי להגן על הקבצים מפני שינוי או צפיה ניתן להצפין את הקבצים.
- הכרשת העובדים בנושא הבאים: כיצד ווירוסים יכולים לפגוע במערכת, איך לסרוק קבצים לפני שימושם מהתקין אחסון ניד ולא לפתח כל קובץ שמצוך למייל.
- לבטל את ההפעלה האוטומטית של התקני אחסון (dvd/usb).

סימפטומים שבדרך כלל מופיעים במערכת שנגעה בווירוס:

- התוכנות במחשב עובדות לאט יותר.
- חלונות פתאום קופצים למסך.
- קבצים לא מזוהים מופיעים או קבצים נעלמים.
- הגודל של תוכנות מסוימות משתנה.
- המחשב נכה או נדלק באופן מפתיע.
- הדיסק קשייך פעיל בဓורה קיזונית.
- המערכת הפעלה לא עולה או מראה הודעות שגיאה בזמן שהיא עולה.
- האנטי ווירוס לא פעיל או לא ניתן להתקין אנטי ווירוס.
- שחזור מערכת לא פעיל.
- הסוללה נגמרה מהר.

תהליך הסרת וירוס:

- איתור מערכת עם סימפטומים של ווירוס.
- בידוד המערכת הנגעה.
- גיבוי קבצים חשובים.
- ביטול System Restore (במערכת Windows).
- תיקון המערכת על ידי עדכון אנטי ווירוס וסריקת המערכת.
- רצוי דרך Safe mode או דרך boot כמו Knoppix.
- הפעלת System Restore (במערכת Windows).
- הדרכת המשתמשים.

לא תמיד ניתן להציג מחשב שנפגע מתוכנה זדונית. במקרה זה יש לגבות את המידע שבמחשב, ולאחר מכן להתקין מחדש את המערכת הפעלה והתוכנות. בנוסף, לעיתים כדאי גם לבצע התקינה מחדש של ה-S-UEFI/BIOS.

לטיסום התהליך יש לסרוק שוב את המחשב כדי לבדוק שלא נותרו עקבות.

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החברת מכילה חומר ללימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

רשימה עדכנית של הוירוסים העדכניים ביותר.
www.pandasecurity.com/israel/homeusers/security-info

united states computer emergency readiness team
www.us-cert.gov

Confidentiality, Integrity, Availability (CIA)

CIA זהו מודל שמאגדיר בצורה כללית את דרישות האבטחה בארגון. כל אמצעי אבטחה שאתה מיישם, אמור לתרום להשגת אחת משלשות המטרות הבאות:

- Confidentiality (סודיות)
- Integrity (שלמות המידע)
- Availability (זמןנות)

יש ליישם את שלושת העקרונות האלה כאשר מתייחסים לאבטחה של חומרה, תוכנה, תקשורת ונתונים.

(סודיות) Confidentiality

כדי להגן על סודיות המידע עליך למנוע מגורמים לא מורשים לגישות למידע. ש להגדר את רמת הרגישות של המידע ולהשיקع משאבים רבים יותר בהגנה על מידע רפואי יותר מאשר במידע רגיש פחות. כדי להגן על סודיות המידע ניתן להשתמש בהצפנה או במודול AAA:

- Authentication - בדיקת זהות.
- Authorization - מתן הרשות גישה למשאים.
- Accounting - מעקב אחר שימוש במשאים ופעולות המשתמשים. המעקב חשוב בין היתר כדי לספק הוכחה שלא ניתנת להכחשה במידע ובוצעה עבירה (non-repudiation).

(שלמות המידע) Integrity

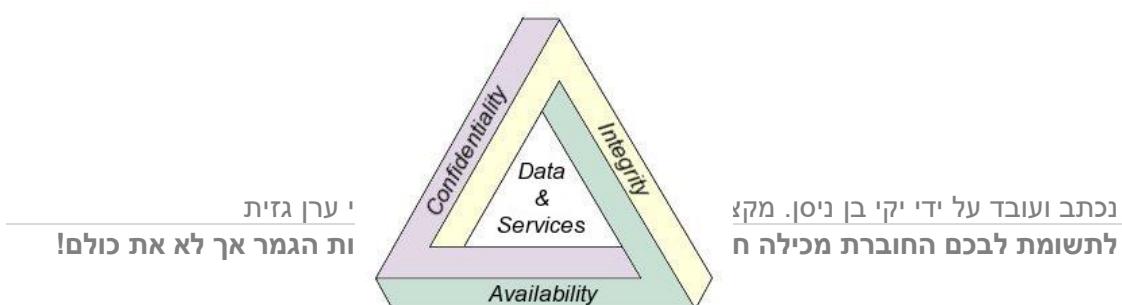
מטרת ההגנה: למנוע מגורמים לא מורשים לשנות את המידע (שמירת המידע בשלמותו). לדוגמה: לא נרצה שגורם זר יוריד את מחירי המוצרים באתר האינטרנט של החברה. אנו מאבטחים את שלמות המידע באמצעות גיבוב (Hashing).

(זמןנות) Availability

מטרת ההגנה: לשמר על זמינות שירותי המחשב, התקשרות ולגרום למציע להיות זמין למשתמשים שמורים לגשת למידע.

כדי לספק זמןנות, ניתן להשתמש בטכנולוגיות הבאות:

- Fault Tolerance - יישום מכניות עמידות בפני תקלות.
- Redundancy - יתירות.
- Virtualization - סביבה וירטואלית מקלה על יישום Availability.
- Cloud Computing - העברת חלק השירותים מהמחשב לענן.
- ביצוע עדכנים (updates) ושדרוגים (upgrades) לתוכנות ולמערכות הפעלה.
- מניעת צוואר בקוק על ידי הספקת רוחב פס נדרש.
- גיבוי המידע בכך שהמידע יהיה זמין גם במקרים חריגיים של אובדן מידע.



תקיפה (הסתכלות בעיני התקוף)

מאז שהומצא המחשב, הומצאה גם היכולת לנוטות ולנצל אותו לרעה. בעבר, התקלות במערכות מחשב הייתה קטנה ולקן המתק האפשר שנגרם על-ידי התקיפת מערכות מחשב היה מוגבל. בשנים האחרונות, קיימים הרבה מקורות מידע דרך רשותות חברותיות ואתרי אינטרנט והתקלות שלם במערכות מחשב הולכת וגוברת וכך גם התגברו המתקפות הן בכמות והן באיכות. כיום לא מספיק לדעת איזה משאבים זמינים להגנה אלא יש צורך גם לדעת מי יש להtagון.

כיום לא ניתן להסתמך רק על Firewall או פתרונות שמחזרים מתקפות מוכרות, וזאת בגלל שתוקף מתחכם יכול לעקוף את ההגנה. מאחריו כל מתקפה עומדת תוקף אונשי ולכן הדרך לפתרון מיטבי ל证实 סיבר מחייב הבנה ממשעوتית של דרכי פעולה של התקוף. כמובן, מול תוקף מימן וממקד מטרה יש להנל קרב לכל דבר וקרבות נסמכים על מודיעין והבנה של פעילות התקוף ושלבי ההתקפה.

כדי להתמודד עם האיוםים על אבטחת הרשת, יש לדעת מה המוטיבציות מאחורי התקפות רשת, מי היעד להתקפה וכייד ארגונים יכולים להגן על עצםם.

מבנה של התקופים:

- האם התקוף מגיע מתוך הארגון או מבחוץ.
- מה רמת התחכם של התקוף.
- איזה משאים ומיימן יש לתוקף.
- מה כוונתו/המוטיבציה של התקוף.

סוגי התקופים:

- **Script kiddies** - אדם חסר ידע בתחום אבטחת מידע או פריצה שימושה בכל פריצה מבלי להיות מודע למתרחש מאחורי הקלעים. בדרך כלל הגנה בסיסית חוסמת תוקפים אלה.
- **Hacktivist** - תוקף על רקע אידיאולוגי (פוליטי או סוציאלי) שרצה לשבש פעילות או למשוך צומת לב כדי להעלות על סדר היום את המטרה שלהם.
- **פשע מאורגן** - קבוצת אנשים מתחכמים שמטרתם העיקרית היא רוח כספי.
- **מדיניות (Advanced Persistent Threat)** - באמצעות משאים וכלי מתחכמים הן מסיגות מידע והשפעה פוליטית.
- **Insiders** - מישהו מitor הארגון (לא חייב להיות עובד הארגון). חלקם מסכנים את הארגון בטיעות שהם עשו וחלקם בזדון.
- **מתחרים** - ריגול תעשייתי.

המניעים מאחורי האיוםים:

- **כספי:** קיימות דרכים רבות לעשות עסקית רוחניים כספיים באמצעות פעולות זדוניות. חדירה למערכות מכירות ונבנת פרטני כרטיס אשראי. הצפתת קבצים במטרה לדוש כופר. חדירה לארגוני פיננסיים כדי להעביר כספים לחשבונות זרים.
- **шибוש:** למקרה הצער, קיימות קבוצות רבות שמטרתם גרים לשיבושים בפעולות של ארגונים ומוסדות. שיבושים אלו נוצרים מכמה סיבות:
 1. מחראה על פעולות, החלטות, או התנהגויות של הארגון.
 2. הסחה בעודו זדוני אחר קורה בתוך הרשת.
 3. קבלת פרסום תקשורת.
- **גיאופוליטי:** באופן לא מפתיע, קיימות קבוצות שמצוות עם מדינות לאות שימושה באינטרנט כדי לבצע לוחמת סייבר.

- **ריגול:** ריגול תעשייתי/פוליטי יכול להיות אידיאולוגי או מרצון להרוויח כסף.

סוגי Hackers

White Hat Hacker (Ethical Hackers)

הם עובדים בתחום אבטחת מידע (הגנה) ונחשבים חלק מן הממסד. תפקידם לבצע מבדקי חדרה שמטרתם לבדוק את יציבות מערכות המחשב ואת עוצמת המיגון שלהם.

Black Hat Hacker - אקרים שמשתמשים בידעו כדי להפיל או לחדור למערכות ללא רשות. לרוב, פעולותיו ייחסבו עבירה על החוק. כאשר האקרים של כובע שחור מוצא פרצה, סביר להניח שהוא ישמש בה לצרכיו, ובמקרים אחרים אולי אף יסחר בה.

Gray Hat Hacker - סוג זה של האקרים נמצא בתחום האפור. לעיתים קרובות, הוא יחשוף פגיעות במערכות ללא אישור של הבעלים. אם ימצא בעיות, הוא ידווח עליהן לבאים, ולפעמים יבקש תשלומים קטנים כדי לתקן את הבעיה. עם זאת, סוג זה של פריצה עדין נחשב בלתי חוקי וזאת בגלל שהאקר לא קיבל אישור לפני הניסיון לתקוף את המערכת.

Open Source Threat Intelligence (OSINT)

זהו מונח שמTARGET מידע שנאסף ממוקורות ציבוריים במטרה לקבל החלטות לגבי תקיפה.

כדי להגן על הארגון נshall את עצמנו מספר שאלות:

1. **למה** שמשיחו **יתקוף** אותנו? מה המוטיבציה של התקוף?
עלינו לדעת איזה נכסים יש לנו שתוקף ירצה לגנוב או לפגוע בהם.
2. **כמה** קשה יהיה לתקוף להסיג את המטרה שלו? הקושי לתקוף אותנו משפיע על הזמן המאמץ והכישרין שהתקוף צריך כדי להצליח בתפקידו.
3. האם אנו מודעים לסוג האיוםים, כל תקיפה וטכניקות תקיפה העדכנים בויתר?
4. האם נדע אם נותקף? האם יש לנו מערכת לזיהוי תקיפות?
5. האם אנו מוכנים להגיב לתקיפה? האם אנחנו יכולים להמשיך לתפקיד לאחר תקיפה?

שלבי תהליך התקיפה

ההכרות עם שלבי התקיפה מתחכמת מאפשר לנו לתכנן את ההגנה לפני הצעדים של היריב ולהציג מידע מודיעיני מתאים על כל שלב.

מודל Chain Cyber Kill (הוצג בשנת 2011 על ידי חברת Lockheed Martin האמריקאית).

לפי המודל קיימים 7 שלבי התקיפה מרכזים שתוקף מבצע בשלבי התקיפה:



1. סיור (Reconnaissance)

בשלב זה התוקף ממפה את אתר היעד על-ידי ביצוע מחקר וaiso ננתונים. ניתן לבצע זאת בצורה פסיבית ללא יצירת קשר עם הנתקף כמו השגת כתובות מייל, בניית תרשימים ארגוני של הארגון הנתקף, מידע של אנשי הארגון ברשותות חברותיות, השגת מידע טכני ממוצרים שפורסמו, מקורות חינימ של אנשים שעבדו בו ועוד. ניתן לבצע Reconnaissance בצורה אקטיבית כמו לטלפון או ל走访 לראיין עבודה.

2. בניית אמצעי התקיפה (Weaponization)

לדוגמה: הצמדה של סוס טרויאני לקוד שמנצל חולשה (exploit) ביחד עם אמצעי העברת שמתאים לעד הנתקף. לדוגמה, ייצור מסמך PDF שמכיל קוד שיופעל בעת פתיחת המסמך ויאפשר משיכת סוס טרויאני לאתר התקוף.

3. משלוח אמצעי התקיפה לעד (Delivery)

לדוגמה: שליחת מייל דיג (phishing) שמכיל את מסמך PDF לאחת מכותבות המייל אשר זהה בשלב הסיור.

4. ניצול החולשה בעד (Exploitation)

הפעלה של אמצעי התקיפה באופן שמאפשר את הרצת הקוד שאוטם תכנן התקוף. לדוגמה, תוכנה Acrobat Reader אצל הנתקף פותחת את מסמך PDF, מריצה את הקוד שתכנן התקוף ומאפשר לתוקף לבצע פעולות המשך.

5. התקינה (Installation)

בשלב זה מותקן הכליל על גבי מחשב בארגון הנתקף ומאפשר לתוקף תקשורת מרחוק למול הכליל המותקן על המחשב. התקינה זו נועדה לאפשר לתוקף נגישות קבואה למחשב הנתקף, וזאת ללא צורך בהרצה מחודשת של אמצעי התקיפה המקורי.

6. שליטה ובקרה (Command & Control)

בשלב זה התוקף מסיג גישה שמאפשרת תקשורת רציפה בין התקוף לבין הכלים שלו שモותקנים במחשב בראשת הנתקף. תקשורת זו הינה לרוב דע כיוונית ומאפשרת לתוקף מצד אחד להעביר פקודות לכלים שלו, ומצד שני לקבל מהם תשדרות שמקילות מידע.

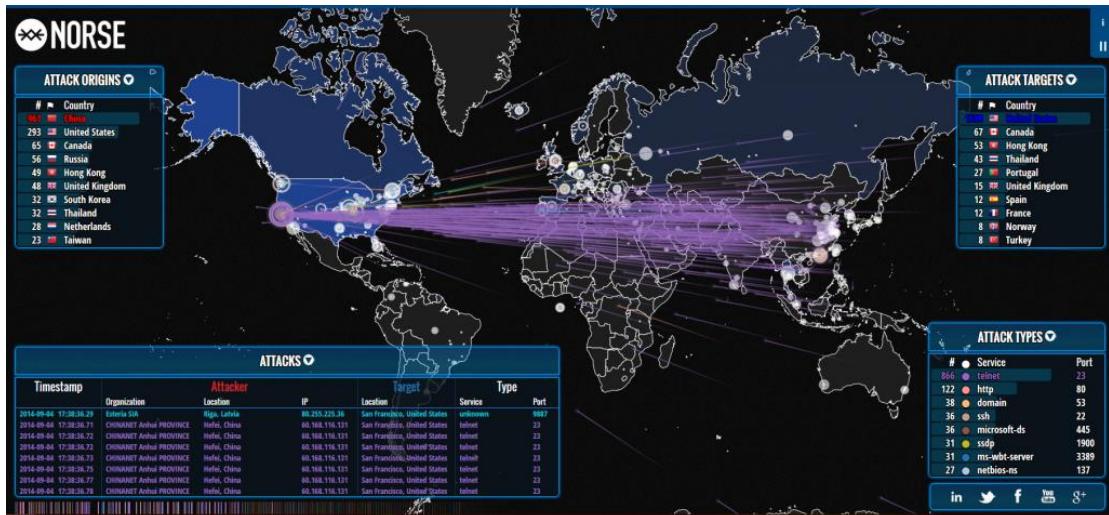
7. פעולות על גבי היעד (Action on Objectives)

לאחר שהושגה נגישות ראשונית לשרת של היעד הנתקף, יכול התקוף לבחור מה ברצונו לעשות: לחקור את רשות היעד בכך להציג גישה למקומות נוספים. לגנוב מידע. לפגוע בראשת היעד ובהתקלים בה היא תומכת.

צפיה בתקיפות בזמן אמת

קייםים מספר אתרים שמחישים לנו בצורה מרתיקת את התקיפות הסיבר בזמן אמת בעולם.

- <http://threatmap.fortiguard.com>
- www.checkpoint.com/ThreatPortal/livemap.html
- <https://cybermap.kaspersky.com>
- [/http://map.norsecorp.com](http://map.norsecorp.com)



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלום!

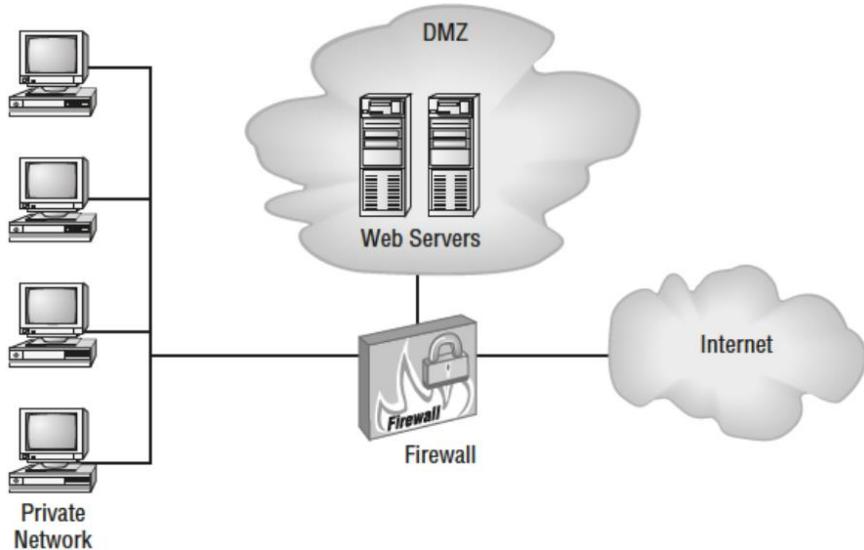
Network Security Design

(DMZ) Demilitarized Zones

אזור מפוזר הוא אזור שבו ממוקמים שירותי ציבורים במטרה לאפשר גישה דרך האינטרנט לאנשים שאינם שותפה לא יכול לסגורם אליהם. ההנחה היא שאדם שניגש למשאים ב-DMZ אינו

בכח רוח מיישו שאתה סומך עליו שייגש למידע אחר.

על ידי בידוד שרת ב-DMZ, ניתן להגביל גישה לאזרחים בראשת. השרת נגיש גם מהרשת הפנימית אך אחרים לא יכולים לגשת למשאי רשות נוספים. בדרך כלל אנו יוצרים Firewall בערצת DMZ.



Subnetting

אחד הדברים הראשונים שיש לשקול כאשר מתכוונים רשות זה החלוקה שלה לחתמי רשות. חלוקה לחתמי רשות מאפשרת:

- שימוש בכתובות בתוך עיליה יותר
- יצירת רשות בתוך יותר וקלה יותר לניהול.

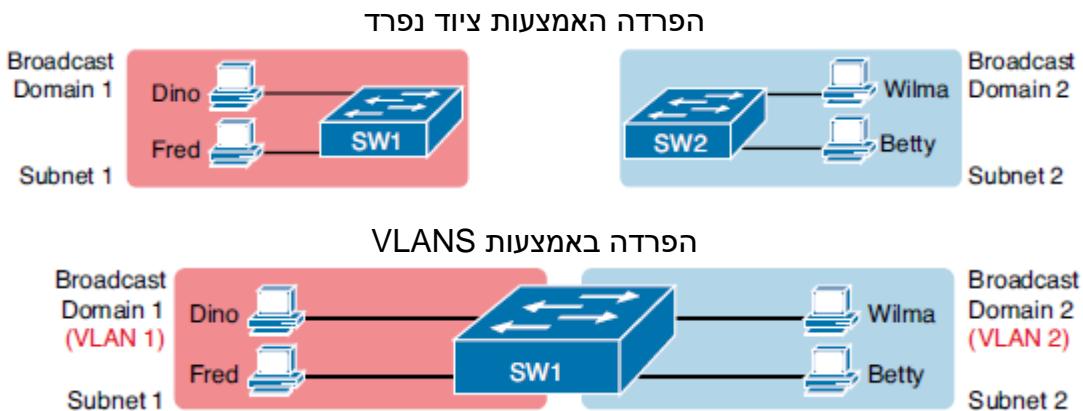
מנקודת מבט ביטחונית, Subnetting מאפשר להגביל את הגישה למשאים בראשת רק לאנשים שזקוקים לגישה לאותם משאים.

בנוסף ניתן לוודא כי חלק מסוים של הרשות בטוח יותר מאשר מקטע אחר של הרשות.

חיבור בין קטעי רשות שונים מתבצע באמצעות נתב או Firewall.

Virtual LAN (VLAN)

הטכנולוגיה מאפשרת לחלק את הרשת לשכונות וירטואליות נפרדות. בתרשים ניתן לראות כיצד ניתן להשתמש במתקן אחד לצורך הפרדה במקום לשני מתקנים.



יתרונות השימוש ב- VLAN

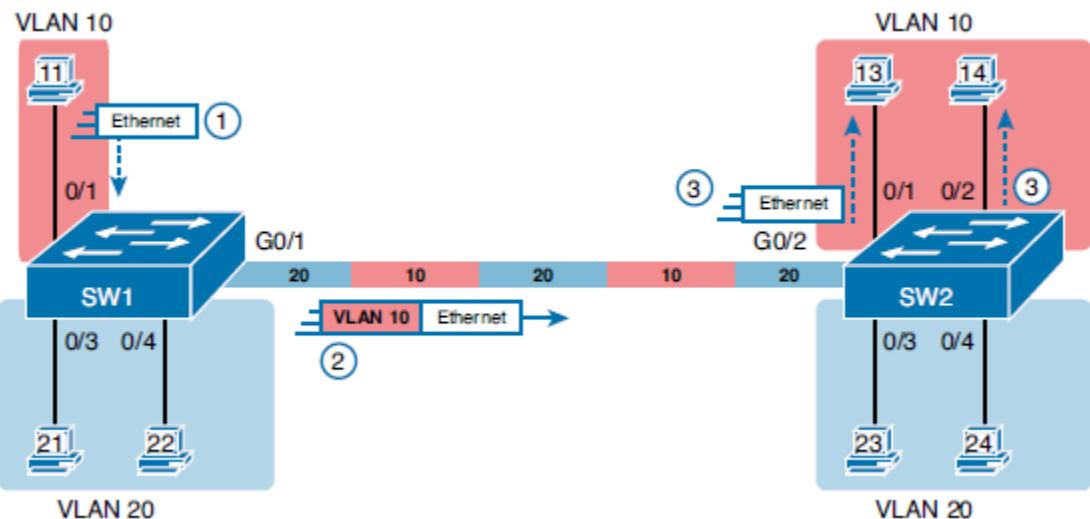
- **מידור** - הגברת האבטחה על-ידי בידוד מחשבים עם מידע רגיסטר מהרשת.
- **שיפור ביצוע הרשת** - כל VLAN יוצר Broadcasts Domain נפרד ולכן על-ידי חלוקת הרשת ל- VLANים יותר ביצוע הרשת משתפרים.

כמה עובדות לגבי VLAN

- כבירות מחדל כל הממשקים שייכים ל- VLAN1.
- VLAN ברירת מחדל נקרא Native VLAN.
- יש לתת לכל VLAN כתובת רשת שונה.
- ההגדירות נשמרות בקובץ `lan.dat` שנשמר בזיכרון flash שבמתקן.

פרישת VLAN על פני כמה Switches

ברשת שבה VLAN נפרש על פני כמה מתקנים, יש צורך בסימון כל Frame שעובר בין המתקנים, כדי שמתג היעד ידע לאיזה VLAN הוא Frame שייר. כדי לבצע זאת אנו מגדירים את ה- ports שמחברים בין המתקנים כ- Trunk.



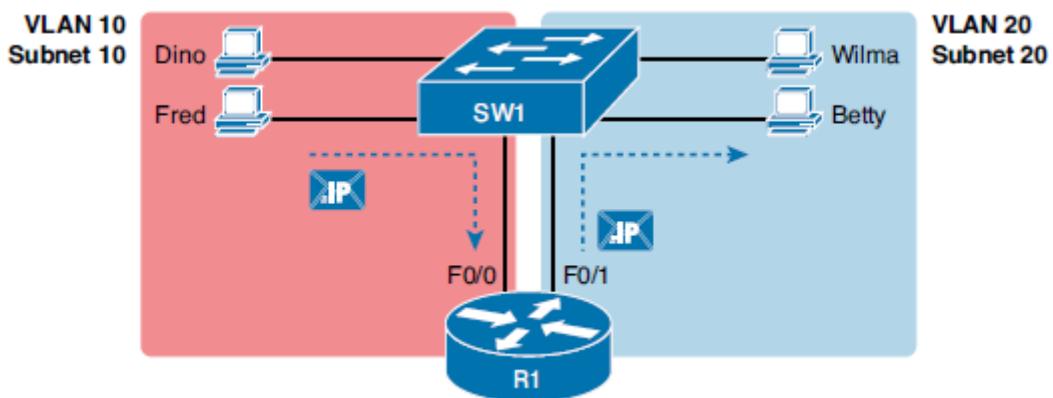
נכתב ועובד על ידי יקי בניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

חיבור בין VLANs

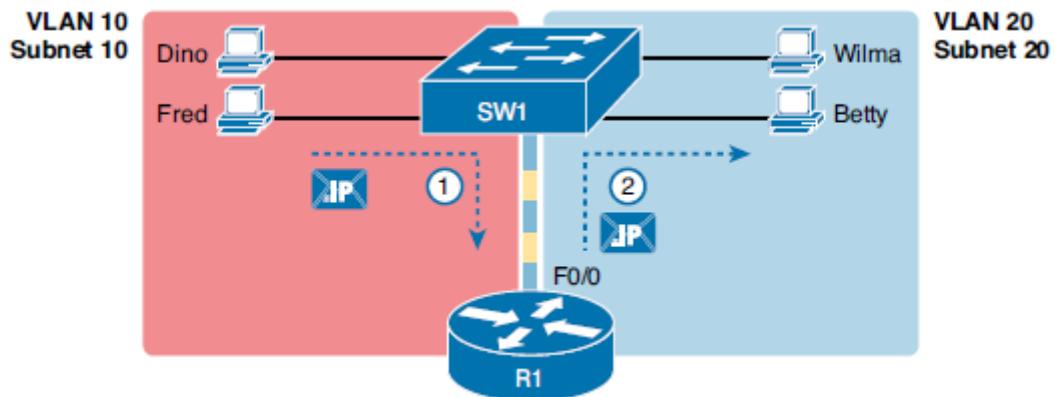
כדי לאפשר תקשורת תקינה, יש לאפשר תקשורת בין VLANs שונים.
לדוגמא לחבר בין השירותים לבין שאר המחשבים.

כדי לחבר בין VLANs יש צורך בהתקן שעבוד בשלב 3 (נתב או מתג שעבוד בשכבה 3).
בעזרת נתב ניתן לגרום לשני VLANs שונים, לתקשר אחד עם השני.

ניתוב בין שני VLANs באמצעות שני ממשקים בנתב



ניתוב בין שני VLANs באמצעות ממשק אחד בנתב (router-on-a-stick)



Tunneling protocols

יצירת tunnels יוצרת נתיב וירטואלי בין שתי מערכות או רשתות ומוסיפה אבטחה ותמייה בפרוטוקולים נוספים. הchnelia נארחת מחדש לחבילה אחרת וכאשר החבילה מגיעה לעד היא נפרקת ונשארת החבילה המקורית.

פרוטוקולי Tunneling הנפוצים ביותר:

- Point-to-Point Tunneling Protocol (**PPTP**)
זהו פרוטוקול קצר מיושן ופחות מאובטח מהפרוטוקולים האחרים.
יודע להצפין PPP packets. אחד מהחולשות של הפרוטוקול זה שתהיליך הקמת הקשר לא מוצפן. רק לאחר הקמת הקשר הפרוטוקול מצפין את המידע.
Microsoft Point-to-Point Encrypting (MPPE) משמש בפרוטוקול PPTP להצפנת המידע. עובד ב-TCP port 1723.
- Layer 2 Tunneling Protocol (**L2TP**)
יודע להצפין PPP packets. ברוב המקרים יעשה שימוש בפרוטוקול זה.
L2TP משמש בפרוטוקול Internet Protocol Security (**IPSec**) ל扞נתם המידע. עובד ב-UDP port 1701.
- Secure Shell (**SSH**)
SSH זהו פרוטוקול תקשורת מוצפן שמאפשר גישה מרוחק ל-Shell של התקן מרוחק. הprotokol עובד ב-TCP PORT 22.
- Internet Protocol Security (**IPSec**)
IPSec זה לא Tunneling Protocol אבל הוא עובד עם Tunneling Protocols IPSec זו חבילת פרוטוקולים שתפקידה לאבטחה תעבורת רשות מסוג TCP/IP וTCP/IPSEC להגן על המידע שזורם ברשת.

Social Engineering (הנדסה חברתית)

בדרך כלל משתמשים עם הרשות גישה למידוע הם החוליה הchlsha באבטחת מידע. הנדסה חברתית היא תהליך שבו התקוף מקבל גישה על ידי ניצול טבע האמון של האדם, ביצוע מניפולציה וניתול התנהגויות צפויות. לעיתים קרובות, כדי לתמן אנשים, נעשה שימוש במינימוניות חברותית, מערכות יחסים, או ניצול של נורמות תרבותיות.

התקפה זו מאפשרת לעקוף את מגגנו האבטחה והיא מתבססת על העובדה שכלי מערכות המידע נועד לספק שירותים למשתמשים, ולמשתמשים יש אמצעים לגשת אל המידע שהפורץ רוצה להשיג.

לפעמים זה מונח לחשב שלא ניתן לשחד אותנו אך האמת היא שcumut לכלי אחד יש מחיר. המחיר שלך יכול להיות כל כך גבוה כך שאף אחד לא ישלם אך האם זה נכון לגבי כל עובדי החברה? הסכנה הגדולה ביותר מכך מועלם בתוך החברה שמוון למסור מידע רגיש.

עקרונות שמאפשרים מתקפת הנדסה חברתית

קיימים מספר עקרונות שמאפשרים להתקפת הנדסה חברתית להיות יעילה. רובם מסתמכים על הרצון שלנו לעזור, באופן כללי לבתו אחרים ולכבד סמכות. הנה כמה עקרונות עליהם מבוססת התקפת הנדסה חברתית:

- **Authority** (סמכות) - אם תצליח לשכנע את הקורבן שיש לך סמכות לבקש את מה שאתה מבקש, כנראה שהוא ייתן לך מה שתבקש בלי לשאול יותר מיד' שאלות. ניתן להתחזות למנהל בכיר, תמייהה טכנית, משאבי אנוש או שוטר.
- **Intimidation** (הפחדה) - על-ידי איום, צעקות ואוליו אשםה.
- **social proof** (הוכחה חברתית) - כולנו רוצה שימורנו לנו שגם צודקים, משכילים ומוסכימים. נגרום לקורבן לקלות ראש על-ידי הקשבה בצומת לב, הסכמה אתם, על ידי כך שנתקסים אותם, נגרום להם לחשב שאין סיכוי שנגរום להם לנזק.
- **Scarcity** (מצומצם) - על-ידי שכנוע שקיים מלאי מצומצם, הקורבן יכול להתנתק בחוסר זיהירות. לדוגמא, קיימים רק חמישה חופשות וכדי להזמין חופשה יש צורך בהזמןה מידית דרך האינטרנט.
- **Urgency** (דחיפות) - על-ידי שכנוע הקורבן שגם הוא לא יבצע מיד פעולה מסוימת אז הוא יפסיד כסף, פורץ לא קיים יברוח, יגרם נזק לחברת או יגרם נזק אחר.
- **Familiarity** (הכרות מוקדמת) - כאשר אנו מתעסקים עם אנשים שאנו מכירים, הגנות מסוימות יורדות.
- **Trust** (אמון) - ניתן לזכות באמון באמצעות הדדיות. כאשר מישחו עושים משהו בשביבך, פעמים רבות קיימת תחושה שאתה חיב לו. ניתן ליצור זאת על ידי עזרה למישחו בפתרון בעיה או קניית ארוכה.

דוגמאות להנדסה חברתית:

- התקוף מטילן למשתמשים ומתחזה לעבוד בצוות IT ומשכנע את המשתמשים שהם צריכים להגיד את הסיסמות שלהם לערכיהם מסוימים וזאת חלק מטהlixir הכנה לשדרוג השרת הלילה.
- השארת DiskOnKey בשטח ציבורי. כאשר משתמש יחבר אותו למחשב, המחשב ידבק בתוכנה זדונית.
- יצירת משתמש פיקטיבי בראשות חברותticות כדי להציג מידע למשתמשים.
- שליחת דוא"ל שמספרה משתמש לוחוץ על קישור לאתר זמני (phishing).

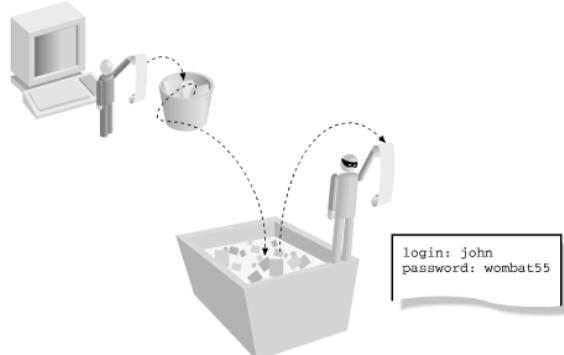
Shoulder Surfing

צפיה במשהו מכניס מידע רגיש כמו סיסמה, מספר כרטיס אשראי או מידע רגיש אחר. ההגנה הטובה ביותר היא סריקה של הסביבה בה אתה נמצא לפני חשיפת מידע רגיש. הגנה נוספת זה החלפת מנגנים המחייבים כניסה סיסמה במנגנים שקוראים כרטיס דיזיין. הקפדה על כך שמסכי מחשב לא יהיו חשופים לחילונות או עובי אורה. קיימים ציפוי מסך שאפשרים לצפות במסך רק למי שיושב ממול המסך.



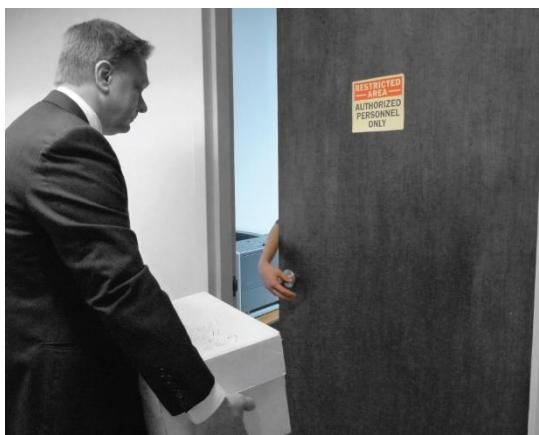
Dumpster Diving

חברות בדרך כלל מייצרות כמהות עצומה של נייר, אשר ברובו בסופו של דבר מתגלגל במכל אשפה או במחוזר. נייר זה עשוי להכיל מידע רגיש מאוד. בסביבות אבטחה גבוהה וסביבות משלטיות רגישות הנויות נקרעים או נשרפים אך רוב העסקים לא עושים זאת.



Tailgating

שיטה של כניסה למערכת נעה היא לעקוב אחר משזה שפותח דלת נעה ולהיכנס מיד אחריו. הרבה אנשים לא חושבים פעמים על אי-רווח זהה וזה קורה כל הזמן כאשר הם מחזיקים את הדלת פתוחה, וממשהו מאחוריהם נושא קופסאות לבדוק או נכה בדרך קלשה פשוט נכנס אחרים.



כתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

התחזות Impersonation

התחזות למשהו שאתה לא, כמו שליח פיצה, מבטח או דמות שתאפשר את הסגת המטרה. התחזות יכולה להתבצע גם דרך הטלפון או דרך דואר אלקטרוני.

Hoaxes

זהו איום שנראה אמיתי אבל הוא לא אמיתי.

בדרך כלל זה מיל או הודעה דרך רשות חברותית על וירוס או סכנה אחרת שלא קיימת. זו יכולה גם להיות הודעה מיל על זכיה גדולה בירושה או הגרלה במטרה לקבל עלייר פרטיים.

Phishing

מיל או אתר שמתזזה למיל או אתר אחר במטרה לגנוב סיסמה מידע או כסף.

Whaling

כמו אר הקורבן הוא מישהו מאוד חשוב.

Vishing

סוג של Phishing דרך שיחת טלפון.

Watering Hole Attack

במידה והתקוף לא מצליח להיכנס לארגון שלך אז התקוף יחבר לך במקומות שאתה יוצא אליהם. לדוגמה: באינטרנט קפה או לפגוע באתר שאתה משתמש ולשלוח לך מיל על קיום האתר חליפי.

התגוננות מפני Social Engineering

כדי לשמר על המידע מוגן, ולהימנע ממתקפת Social Engineering, ננקוט בצעדים הבאים:

- יש לתרדר את העובדים כיצד להתחמק מהתקפו כאלו, לדוח על פעילות חשודה ולגרום לעובדים להישאר במידעות גבוהה.
- פרסם את הנהלים ומדיניות החברה כולל זיהוי מתקשרים ומבקרים. תהליך דיווח על תקריות.
- סינון דואר SPAM, סינון תכנים, הגדר אבטחה בדפדפן.
- שליטה פיסית שכוללת מעקב ומצלדות.

סוגי התקפות

DoS (Denial of Service)

התקפת DoS, משכיתה שירות מסוים וכך מונעת משתמש לגיטימי לקבל גישה לשירות.

זו התקפה קלה מאוד לביצוע והנזק שהוא גורמת רב.

דוגמאות לנזק שיכל להיגרם מהתקפת DoS.

- מניעת גישה למילוי, תוכנה, מערכת או תקשורת.
- מניעת גישה לאתר אינטרנט ללא הפלת מערכת הפעלה או התקשרות.
- תקינות המערכת הפעלה.

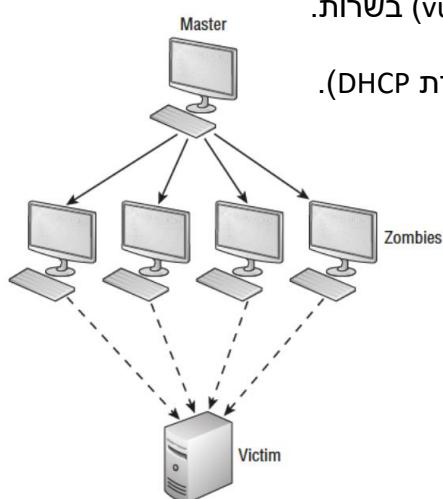
קייםות דרכים רבות לביצוע התקפת DoS אך ההתקפה לא חייבת להיות מתחכמת.

לדוגמה: מניעת הספקת חשמל מהתקנים ברשות.

הדרך השכיחה ביותר לביצוע התקפת DoS היא לגרום לבזבוז של משאבי הרשות/השרות בכי ליצור עומס (Overload) על השירות וכתוצאה לכך לגרום למניעת השירות.

דרך נוספת לביצוע התקפה זאת היא ניצול נקודת תרופה (vulnerability) בשירות. לפעמים התקפה זו משמשת כהסחה להתקפה אחרת.

לדוגמה: תקיפת DNS Server כדי להתחזות לשרת DNS (כגון לABI לשרת DHCP).



DDoS (Distributed Denial of Service)

DDoS זו מתקפה שפועלת בדומה לDoS רק על ידי מספר רב יותר של מחשבים ולכן בהיקף נרחב יותר.

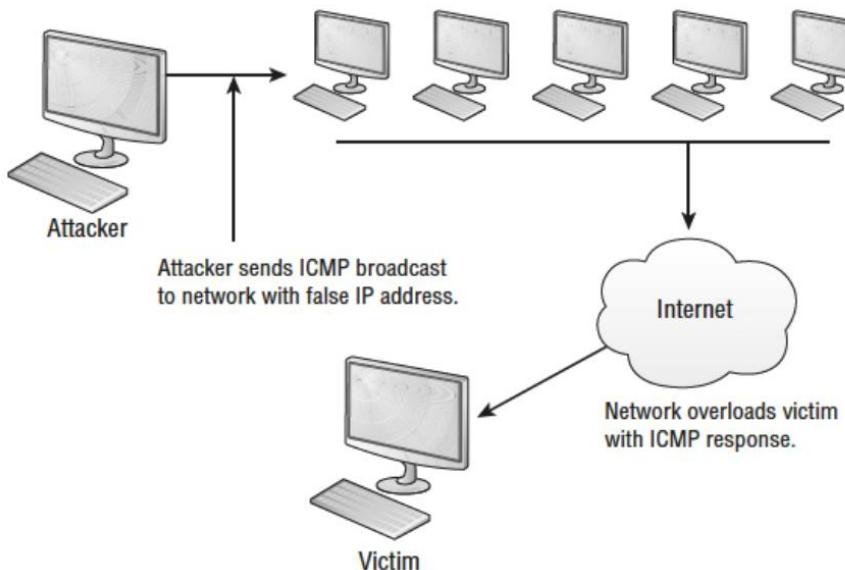
דרך ייעלה מאוד לביצוע מתקפת SDoS, היא שימוש ב-Botnets.

Smurf DDoS Attack

בהתתקפה זו, התוקף שולח ping request שמכיל:

- כתובת מקור - הכתובת של היעד להתקפה.
- כתובת היעד - כתובת broadcast של הרשת.

כך, הבקשה מגיעה לכל המחשבים ברשת. כתגובה, כל המחשבים ברשת שולחים ICMP response למקורן. התקפה זו מבלצת את רוחב הפס של הקורבן. כדי למנוע התקפה זו, אל תאפר לנתב להעברת עבורות ICMP וכן התקפות כאלה לא יכולים להגיע מחוץ לרשת.



זיווף זהות (Spoofing)

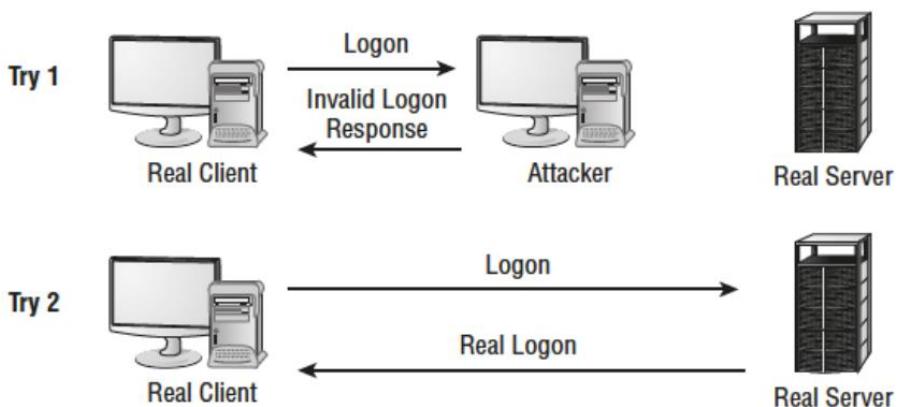
בתקפה זו התוקף מתחזה למישהו אחר (מייל, מספר טלפון, שרת web, שרת dns...).

לכן כאשר התוקף משדר מידע, זה נראה ללקוח שמקור המידע מערכתי אחר.

בדרך כלל מתקפת Spoofing משתמשת בסוגים שונים של התקפות אחרות.

קיימים סוגים שונים של התקפות Spoofing:

- **IP address spoofing** - זה הסוג הנפוץ ביותר של זיווף. לביצוע התקפה, תוקף משתמש בכתובת מקור שונה מהכתובת המקורי שלו.
- **MAC address spoofing** - כדי לבצע זיווף כתובות MAC, תוקפים משתמשים בכתובות MAC שאין להם. זיווף כתובות MAC מנצל חולשות בשכבה 2 של הרשת.
- **Application or service spoofing** - לדוגמא זיווף של שירות DHCP, זיווף של לקוחות DHCP, זיווף של שירות DNS, זיווף של מייל ועוד.



Man in the Middle

בסביבת רשת רגילה, לא ניתן לצותת לתקשורת רשת מסווג Unicast שאנו לא חלק ממנו.

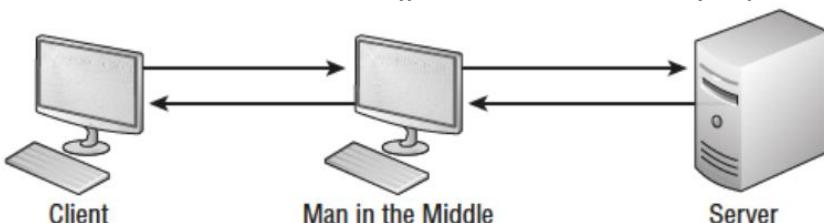
התקפת Man in the Middle מאפשרת לתוקף להיכנס בין שני התקנים שמעבירים ביניהם

מידע וכן התוקף מסוגל להאזין למידע ואף לשנותו.

ישנם כמה דרכים לבצע התקפת Man in the Middle, ARP poisoning, אחת מהם היא ARP poisoning.

ARP poisoning ?ARP poisoning

התקפה ייעלה רק אם התוקף והלקוח נמצאים באותו Broadcast Domain.Broadcast Domain. ב כדי להתחזות ליעד, התוקף שולח ללקוח ARP Replay ובו מצינית הכתובת IP של היעד ואליו משוויכת הכתובת הפיסית של התוקף. על ידי כך התוקף מזייף רשומה בטבלת ARP cache של הלקוח וגורם לו לחשב שהtokף הוא היעד.



Phishing

מייל או אתר שמתזזה למייל או אתר אחר במטרה לגנוב סיסמה מידע או כסף.

נאכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החברת מכילה חומרוי לימוד הנדרשים לצורך בחינות הגמר אך לא את כלום!

Vishing

סוג של Phishing דרך שיחת טלפון.

(DNS poisoning) Pharming

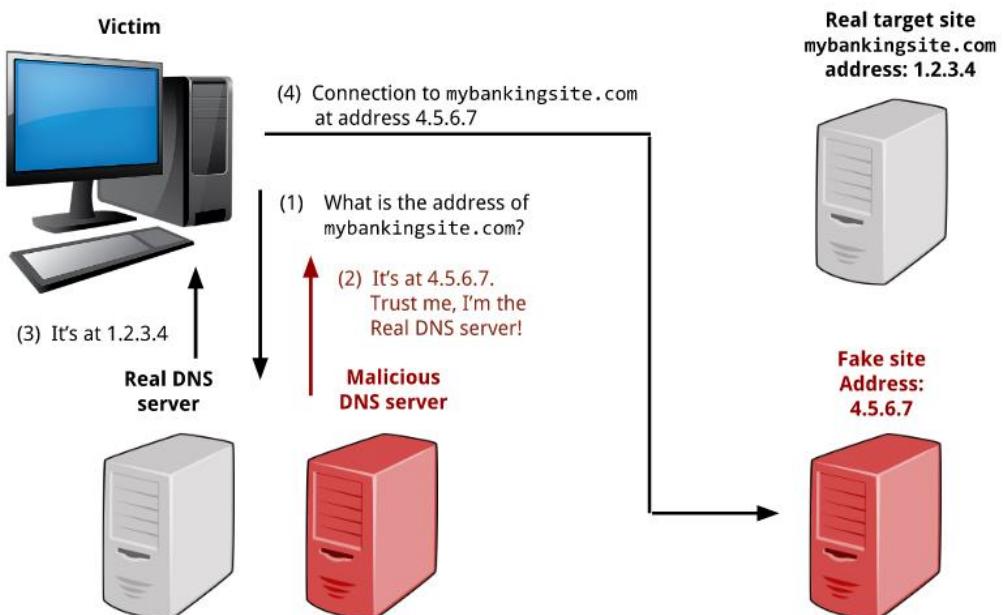
זה כל דרך בה ניתן לזייף את תרגום השמות במחשב הלקוח.
לדוגמא: הוספת רשומות בקובץ hosts או ביצוע DNS Spoofing.

DNS poisoning/DNS Spoofing

בהתקפה זו התקוף מתחזה לשרת DNS ולכן כל הבקשות לתרגום שמות מגיעות אליו. זה מאפשר לתקוף לבצע מניפולציה על הבקשות שהוא מקבל על-ידי שליחת תגובה DNS משלו. זהה אחת ההתקפות המסוכנות יותר כי מאוד קשה לגלוות אותה.

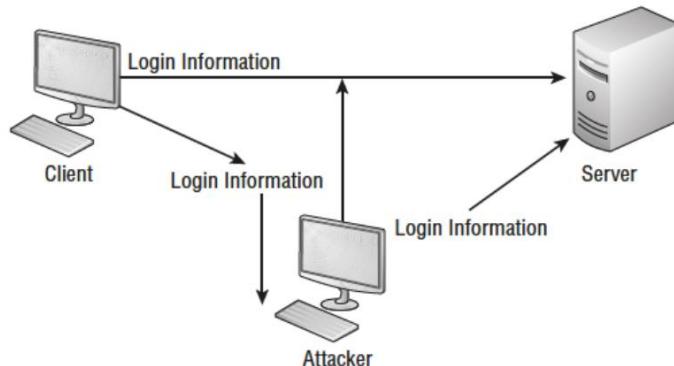
ניתן לבצע התקפה זאת ברשת המקומית בשני צורות:

- התחזות לשרת DHCP
- man-in-the-middle attack



Replay Attack

במהלך Replay Attack, התקוף מאיין לטעבורת הרשות של הקורבן ווגונב את המידע המוצפן של הקורבן. על-ידי שליחת המידע המוצפן לשרת, התקוף מקבל גישה לשרת בשם הקורבן.



נכתב ועובד על ידי יגאל זרנוק – מדריך לתוכנה ותוכנה – מדריך לתוכנה ותוכנה
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

Password Attacks

- קיימים סוגים שונים של התקפות לגניבת סיסמה:
- **ניחוש** - תוקף יכול להציג סיסמות באופן ידני או להשתמש בכל תוכנה לאוטומציה של התהילה. סיסמות רעות במיוחד מאפשרות לתקוף בודד לבצע ניחוש מושכל.
 - **Brute force** - ההתקפה מבוצעת על ידי תוכנות בשם "password crackers". התוכנה מנסה באופן שיטתי כל סיסמא אפשרית עד ניחוש הסיסמה הנכונה. הניסיון יכול להתחל בניחוש כל האופציות שקיים ב吐ו אחד ולאחר מכן לעבור לסיסמות באורך שני תוויות, וכן להלאה מנסה את כל היצירופים האפשריים, עד שאחד מהם עובד. שיטה זו מאד איטית. הגנה טובה היא נעילת החשבון לאחר מספר ניסיונות כשלים.
 - **Dictionary attacks** - התקפה זו משתמשת במילון שמכיל מיליוני מילים וצירופי תוויות וזהת כדי לנחש את הסיסמה. התקפות כאלה לא תמיד מצליחות. לעיתים קרובות מנסים התקפת Dictionary לפני התקפת Brute force.
 - **Hybrid** - שילוב של Dictionary ו- Brute force.
 - **Rainbow tables** - זה טבלה שמתרגמת ערכיו hash לסיסמות ומאפשרת התקפה מהירה שניתנת לביצוע Offline. אם יש לנו סיסמא צורת hash, טבלה זו מאפשרת לגלות את הסיסמה המתאימה לו.

Time to brute force password space, assuming 10,000 attempts per second			
	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
Length = 5 characters	19 minutes	1 day	8 days
Length = 6 characters	8 hours	65 days	2 years
Length = 7 characters	9 days	11 years	200 years
Length = 8 characters	241 days	692 years	19,000 years
Length = 9 characters	17 years	42,000 years	1.8 million years

Malicious Insider Threats

אחד הסכנות הגדולות לארגון זהעובד של החברה עם כוונות רעות. זה שהעובד נימצא בתוך החברה ויש לו גישה למשאבי החברה, מאפשר לו לעبور את קוו ההגנה הראשון של החברה. אך יש להישמר גם מסכנות שmaguit מפנים.

Privilege Escalation

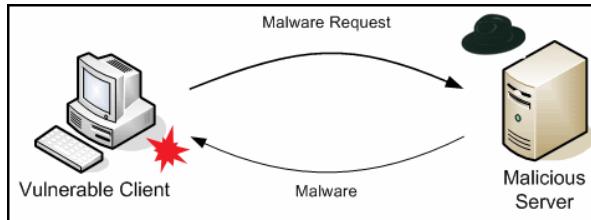
משתמש מצליח להציג יותר הרשות ממזה שצריך להיות לו וכך הוא יכול לבצע דברים שהוא לא אמר לעשות (לדוגמא: למחוק קבצים או לראות מידע). בדרך כלל בזמן פיתוח תוכנה, המפתח משאיר דרך להיכנס לתוכנה כמנהל ולפni שהתוכנה משוחררת לקהל המתכונת מסיר את הכניסה הזרת. אם המתכונת שכח להסיר את הכניסה הזרת אז ניתן להשתמש בה כדי לקבל הרשות מנהל.

(Christmas Tree attack) Xmas Attack

זו סיריקה מותחנת (לדוגמא עם תוכנת nmap) שמצוילה להתחמק מי Firewalls במטרה לגלוות Ports פתוחים במחשב של הקורבן.

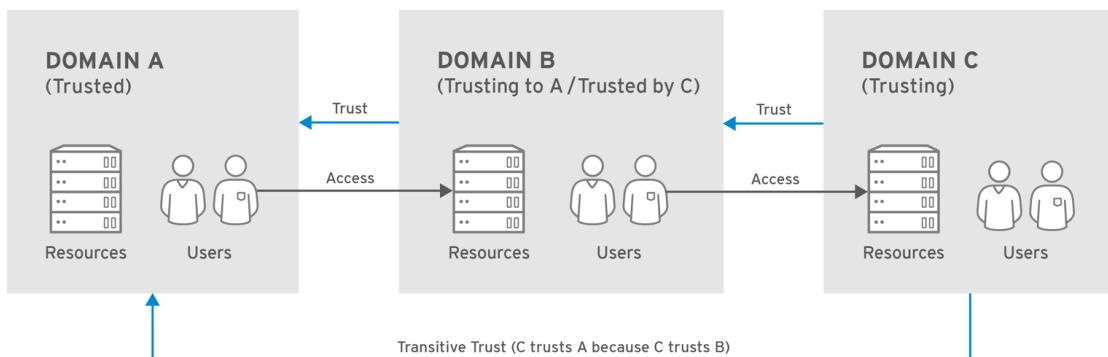
Client-side Attack

זו מתקפה שמטרה תוכנות במחשב הלקוח (לדוגמא: דפסן, ftp client). כאשר התוכנות יוצרות קשר עם שרת זדוני הם מorigdot קוד זדוני ללא ידיעת המשתמש. בדרך כלל, לאחר התקפה מוצחת, מחשב הלקוח משמש ככלי לתקיפת השירותים בתוך הארגון וכן ההתקפה על השירותים מגיע מבפנים.



Transitive Attacks

כאשר משתמש/Area A יכול לפנות למשאים באזורי B ומשמש/Area C יכול לפנות למשאים באזורי B, אך אם משתמש/Area C מצליח לחדר לשרת באזורי B, זה מאפשר לו גישה לאזורי A. לדוגמא: משתמש מהאינטרנט שמצילich לפોર્ચુન લશરેટ Web - DMZ, מצליח לחדר LAN.



URL Hijacking

התקפה זו גורמת למשתמש לחשב שהוא נכנס לאתר מסוים אבל בפועל הוא נכנס לאתר אחר. בדרך כלל השימוש הוא בכתובות URL שנראית דומה או בקישור למקום שונה מהשכתב בתיאור הלינק.

לדוגמא: במקום bankpoalim.co.il להשתמש ב- bankhapoalim.co.il

Watering Hole Attack

במידה והתקף לא הצליח להיכנס לארגון שלך אך התקף ייכה לך במקומות שאתה יוצא אליהם. לדוגמא: באינטרנט קפה או לפגוע באתר שאתה משתמש ולשלוח לךמייל על קיים האתר חליפי.

מודל AAA

המודל מייצג:

- **Authentication** - בדיקת זהות (מי יכול להתחבר?).
 - **Authorization** - מתן הרשות גישה למשאים (מה המשתמש יכול לעשות?).
 - **Accounting** - מעקב אחר שימוש במשאבים ופעולות המשתמשים.
- המעקב חשוב בין היתר כדי לספק הוכחה ניתנת להכחשה במידע ובוצעה עבירה (non-repudiation).

Authentication

אנו רוצים שרק לאנשי IT מורשים תהיה גישה ניהולית להתקני הרשות (נתבים ומוגדים). בراتת קטנה עד בינונית, אימות באמצעות משתמשים מקומיים מספיק אך אם קיימים בراتת מאות מכשירים, ניהול המכשירים יהיה כמעט בלתי אפשרי. שינוי של סיסמה אחת ידרש שעות כדי לעדכן את כל ההתקנים בراتת.

הזהות באמצעות שרת

ברשת בה קיימים הרבה נתבים ומוגדים, עדיף להשתמש בשרת חיצוני כדי לנצל את כל המשתמשים עבור רשות מלאה. חשבונות המשתמשים קיימים בשרת ואשר משתמש רוצה להתחבר לנטב, הנטב בודק מול שרת האם מותר להשתמש להתחבר.

סוגי שירותי ההזהות

שרת ההזהות יכול להשתמש באחד מהפרוטוקולים הבאים:

- **TACACS+** (Terminal Access Controller Access-Control System Plus) זהו פרוטוקול שפותח על ידי Cisco. שיטה זו בדרך כלל מיושמת בעזרת ACS (Cisco Secure Access Control Server).
- **RADIUS** (Remote Authentication Dial in User Service) זהו פרוטוקול פתוח (Open Standard).

הבדלים בין הפרוטוקולים:

- **תקשרות** - TACACS+ משתמש ב- TCP port 49. לאומת זאת, RADIUS משתמש ב- UDP port 1812 Accounting UDP port 1813 Authentication UDP port 1813 לצורך.
- **הפרדת תהליכי** - TACACS+ מפheid בין פונקציות AAA זהה מאפשר שימוש בפונקציה אחד בנפרד או שילוב+ TACACS עם שיטה אחרת. לדוגמה: ההזהות עם Kerberos ושימוש ב- TACACS+ לזרבי Authentication.
- **האישור (Authorization)** זהה מבקשת להפעיל רק תהליך אחד מתוך השניים. RADIUS משלב את תהליך ההזהות (Authentication) עם תהליך האישור (Authorization).
- **הצפנה** - TACACS+ מצפין את כל התקשרות, RADIUS מצפין רק את הסיסמה בזמן הקמת הקשר עם הרשות.
- **תאמיות** - אם משתמשים בצד של יצירנים שונים, RADIUS יכול לא לעבוד במקרה תקינה או לא לעבוד בכלל.

- (Authorization) RADIUS לא יכול לשלוט בرمת האישור •
שימוש מוקלד על ציוד של Cisco TACACS+ יכול.

סוגי התשובה שיכול שירות TACACS+ להחזיר לנוטב:

- Accept - מאשר את המשתמש.
- Reject - פוטר את המשתמש.
- Continue - השרת מבקש עוד מידע על המשתמש.
- Error - במהלך תהליך ההזדהות התביצה שגיאת תקשורת.

ישום AAA-Authentication

לפני שימוש ב- AAA, רצוי ליצור משתמש מקומי.
המשתמש יאפשר חיבור במקרה של תקלה בשרת האימונים.

```
Router(config)#username {admin} privilege {15} secret {123}
```

כדי שהמערכת תבקש הזדהות עם המשתמש המקומי, נשתמש בפקודה login local.

```
Router(config)#line console 0
Router(config-line)#login local
```

```
Router(config)#line vty 0 4
Router(config-line)#login local
```

אפשר AAA

כדי לאגרום להתקן לתמוך במודל AAA, יש לאפשר זאת בהתקן.
מיד לאחר הפקודה, החיבור מרוחק (telnet/ssh) ידרוש שימוש במסתמש מקומי.

```
Router(config)#aaa new-model
```

הגדר באיזה שיטה הזדהות לשימוש

יש ליצור/לשימוש ברשימה שבה יציינו השיטות לפייהם תיבדק זהות המשתמש.
רשימה בשם default משפיע על כל צורות ההתחברות.

לאחר מכן יש להגדיר כיצד ההתקן יבודק את המשתמש. בדוגמה, הנטב ינסה לתקשר עם שירות+tacacs+, אם השירות לא זמין אז נעשה שימוש בהזדהות מקומית.

```
Router(config)#aaa authentication login {default} {local}
```

```
Router(config)#aaa authentication login {c1} {enable}
```

```
Router(config)#aaa authentication login {default} group {tacacs+} {local} {enable}
```

האופציה **enable** משתמש בסיסמה של **enable password** כדי להיכנס.
האופציה **local** משתמש במשתמש מקומי.

כדי שהרשימה תשפייע על צורת ההתחברות:

```
Router(config)#line console 0  
Router(config-line)#login authentication {default}
```

הגדרת מקום השירותים ובאייזה פרוטוקול להשתמש
.shared encryption key TACACS+ או RADIUS והגדרת מקום שרת

```
Router(config)#tacacs-server host {172.16.0.1}  
Router(config)#radius-server host {172.16.0.2} auth-port {1812} acct-port {1813}
```

הגדרת סיסמה

```
Router(config)#tacacs-server key {password}  
Router(config)#radius-server key {password}
```

כדי לבדוק תפקוד נתן להשתמש בפקודה {radius/tacacs+}

Layer 2 Attacks

כדי להתגונן מפני התקפות עליר להבין את התקפות.
התקפות שפועלות בשכבה 2 של מודל OSI, משתמשות בכתובות פיזיות (mac address) או
שההתקפות מכונות לפרוטוקולים שפועלים בשכבה זו.

סוגי ההתקפות שנלמד:

- STP Attack
- ARP Poisoning Attacks
- MAC Address Spoofing Attacks
- MAC Address Flooding – CAM Overflow Attacks
- VLAN Hopping Attack
- DHCP Spoofing Attacks

STP Attack

מה זה (Spanning Tree Protocol (STP))

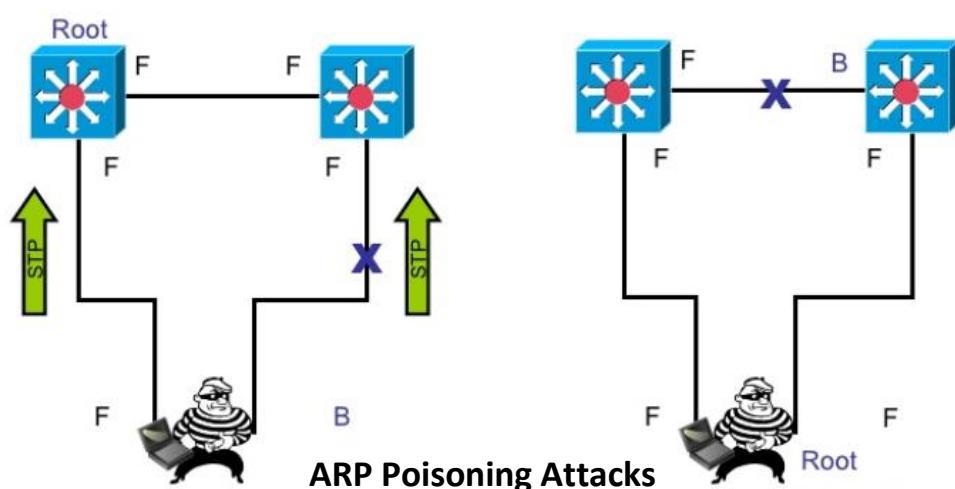
STP הוא פרוטוקול רשת שמאפשר טופולוגיה לוגית ללא לולאות.
המתגים משתמשים ב- BPDU Packets כדי לשփר בניהם את פרטי המתג (BridgeID) וכך
לקבוע מי המתג שייהי ה- Root Bridge (הנמור מנצח).
לאחר בחירת המתג שישמש כ- Root Bridge, כל המתגים ישמרו את המסלול הייעיל ביותר
להגיע ל- Root Bridge פתוח וכל מסלול נוסף ייחסם.

התקפה

בהתקפה זו התוקף מתחזק ל- Root Bridge במטרה:

- לחסום את העברת המידע (DoS Attack).
- לשבש את זרימת המידע ולאפשר לתוקף לצותת מידע (Man-in-the-middle)

הזרקת BPDU Packets מזויפים עם RID נמוך מאוד (נקרא גם STP) משפייע על
הטופולוגיה על ידי בחירת המחשב של התוקף לשמש כ- Root Bridge.



כיצד עובד ARP?

כאשר שני מחשבים שנמצאים באותו מתחם שידור מתקשרים ביניהם, הם משתמשים בכתובות הפיזיות שלהם. לכן על מחשב המקור לדעת את הכתובת הפיסית של מחשב השני.

ARP מתרגם כתובת IP לכתובת פיסית על-ידי שידור arp requestarp request ב- broadcast. מחשב היעד ישלח ב- unicast כתגובה arp reply ובא מופיעה הכתובת הפיסית שלו.

כדי להפחית את כמות ה- arp request (broadcast), מערכת הפעלה מתחזקת בזיכרון RAM טבלאות ARP Cache לכל כרטיס רשת. בטבלה כתובות IP מתרגמות ל- כתובות פיסיות.

הרשומות נכנסות לטבלה בזורה דינמית, אך ניתן להכניס לטבלה רשומות בזורה סטטית. כל רשומה נשארת בטבלה בין 2 ל- 10 דקות (תלוי במערכת הפעלה).

C:\Users\yaki>arp -a			
Interface:	10.37.34.35 --- 0x4	Internet Address	Physical Address
		Type	
		dynamic	bc-f6-85-c7-fc-cb
	10.37.34.254	dynamic	00-26-88-39-08-4c
	10.37.34.255	static	ff-ff-ff-ff-ff-ff
	224.0.0.22	static	01-00-5e-00-00-16

דוגמה (Wireshark):
כתוצאה מבקשת ping, 10.37.34.35 מבקש לגלוות את הכתובת פיסית של 10.37.34.10.

ping 10.37.34.10

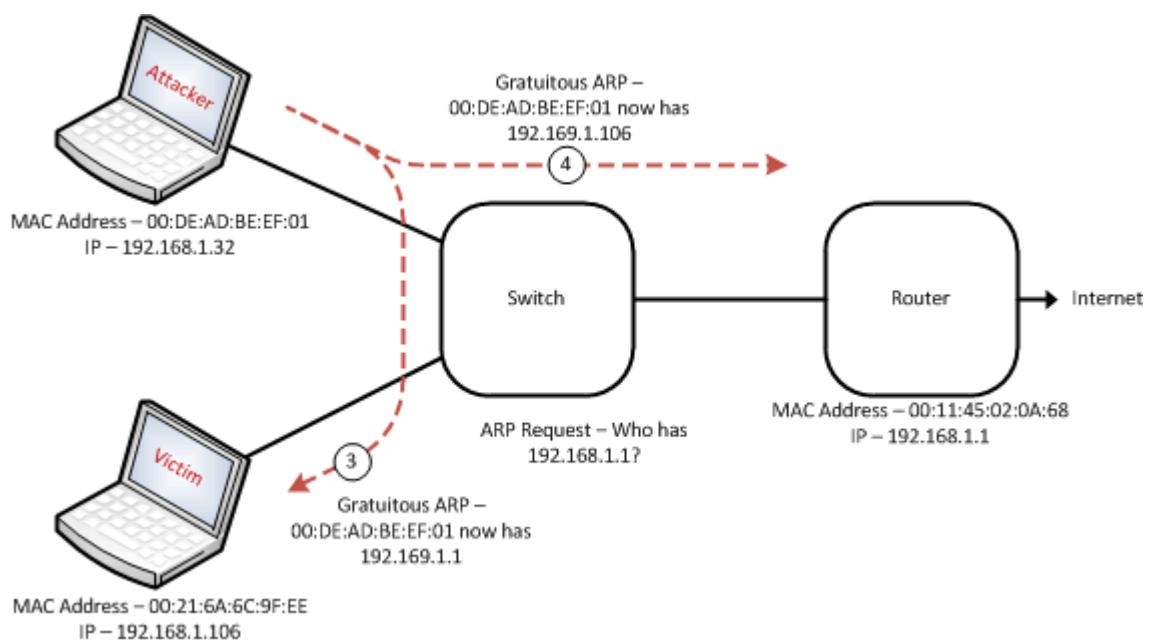
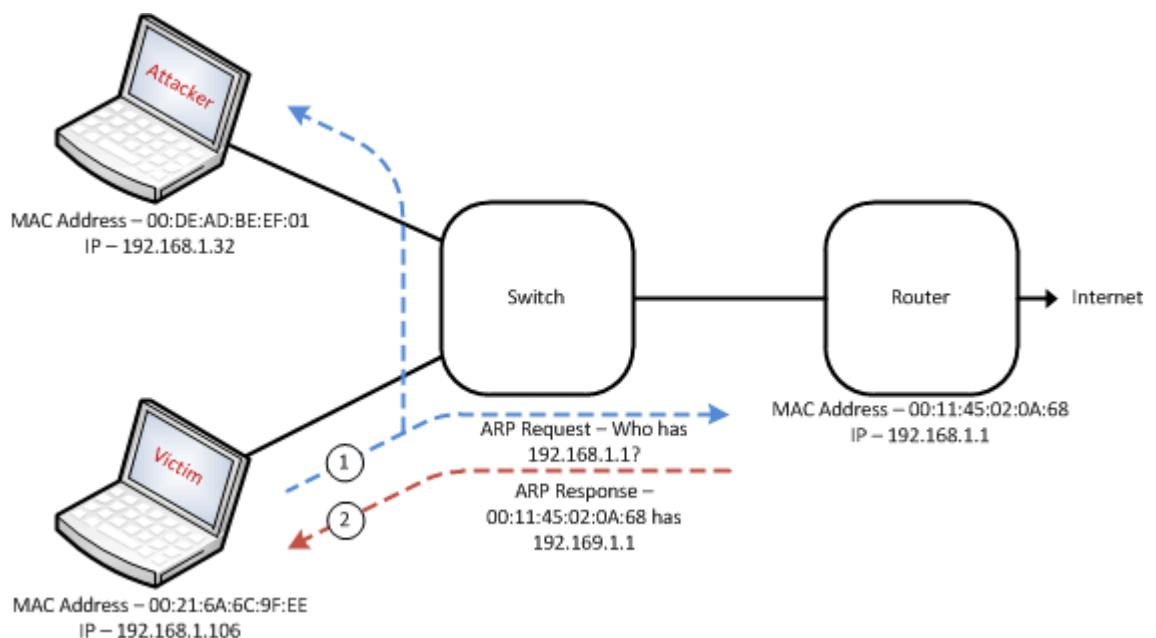
Source	Destination	Protocol	Length	Info
48:5a:b6:da:cb:a3	Broadcast	ARP	42	who has 10.37.34.10? tell 10.37.34.35
bc:f6:85:c7:fc:cb	48:5a:b6:da:cb:a3	ARP	60	10.37.34.10 is at bc:f6:85:c7:fc:cb

כיצד עובדת התקפת ARP poisoning?

התקפה יعلיה רק אם התוקף והקורבן נמצאים באותו Broadcast Domain. בסביבה רשת עם מתגים, לא ניתן לצותת לטעבורת Unicast שאמנו לא חלק ממנו. התקפת זו מאפשרת לתוקף להתחזות ל- Default Gateway או ליעד אותו הקורבן רוצה לתקשורת.

כך התוקף מצליח להאזין ואף לשנות את המידע שעובר בין שני התקנים.

ב כדי להתחזות ליעד, התוקף שולח לקורבן ARP Replay (נקרא גם ARP Gratuitous) ובו מצינית הכתובת IP של היעד והכתובת הפיסית של התוקף. כך התוקף מזייף רשומה בטבלה ARP cache של הקורבן וגורם לו לחשב שהትוקף הוא היעד.



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

MAC Address Spoofing Attacks

שלא כמו רצחות, מתגים מעבירים נתונים רק דרך היציאה שאליה משוויכת הכתובת הפיסית של היעד.

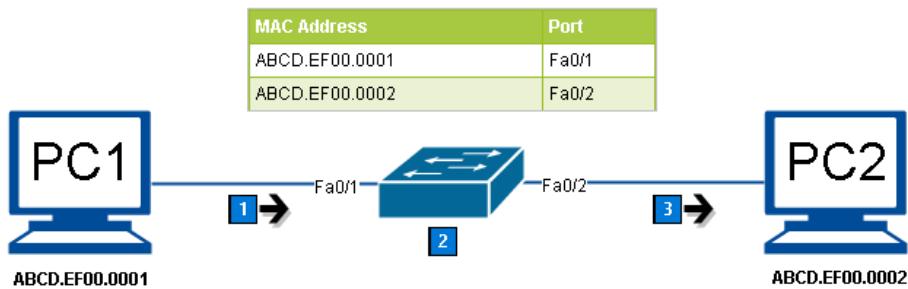
מתגים שומרים את הכתובות שימושיות למשקעים בטבלאות content-addressable memory (CAM).

טבלאות חיפוש אלה מאפשרות על ידי תהיליך של לימוד כתובות במתג.

התקפה זו מתרחשת כאשר תוקף משנה את הכתובת הפיסית שלו כך שהתקן שלו מתחזה להתקן אחר.

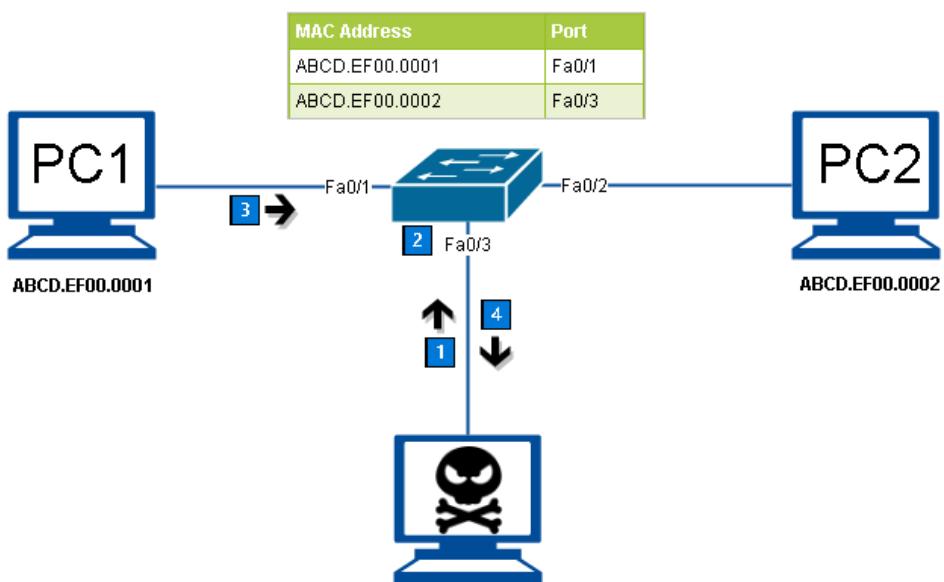
מטרת ההתקפה:

- לחסום את העברת המידע (DoS Attack).
- לאפשר לתוקף לצותת למידע (Man-in-the-middle).
- לאפשר לתוקף לעקוף מנגן הגנה מסווג מבואו Access controls.



כאשר התוקף שולח Frame עם כתובת מקור של PC2, אז המתג מסיר את הכתובת מי fa0/1 ורושם אותה ב-fa0/3 שזיה המקומם שהתקף נמצא. עכשו התקף קיבל את המידע שמיועד ל-PC2.

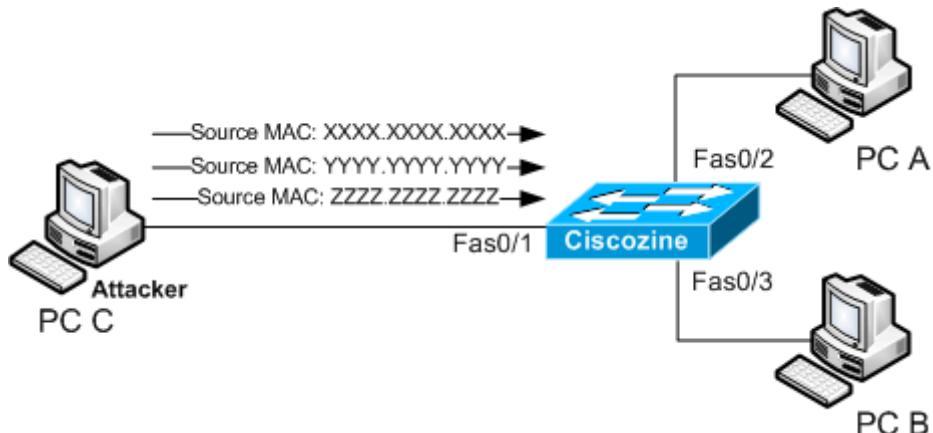
על התקף לשולח Frame עם כתובת מקור של PC2 ללא הפסקה, אחרת כאשר PC2 ישלח Frame, המתג ילמד את מקומו (fa0/2).



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

MAC Address Flooding – CAM Overflow Attacks

כידוע, כאשר עוברים frames דרך המתג, המתג לומד את כתובת המקור של התקן ומעדכן את טבלת MAC שלו. כמוות זה' כירון שמקצת לטבלה ב-ram היא מוגבלת. בהתקפה זו, התוקף מציף את המתג ב-frames עם כתובות מקור הקרהיות. בשלב מסוים הטבלה מלאה ולא יכולה להכיל כתובות נוספות. כתובות שנלמדו לפני ההתקפה עדין נשארות בטבלה אבל כתובות חדשות לא נלמדות וכך. בשלב זה המתג מתפרק כרצת וזה מאפשר לתוקף לצותת לטעורות הרשות.

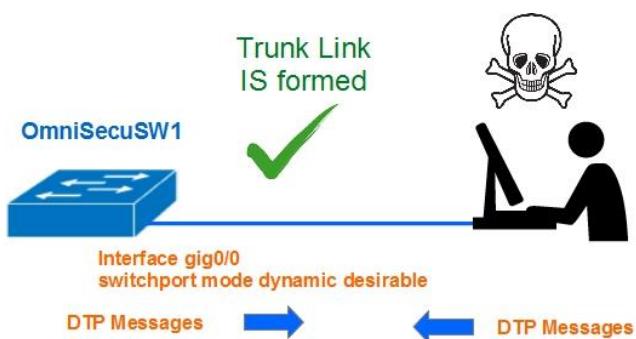


VLAN Hopping Attack

כברית מחדל משק במתג מוגדר כ- Access port, כלומר הוא יכול להיות שייר ל- VLAN אחד בלבד. לאומת זאת ממשקים שמודרים כ- Trunk port מעבירים מידע מ- VLANים רבים. התקפה זו מאפשרת לתוקף לקבל גישה לתקשורת רשת מרשות VLAN אחרת מאשר ה- VLAN אליו התקוף שייר. ניתן לשים VLAN Hopping Attack בשני צורות:

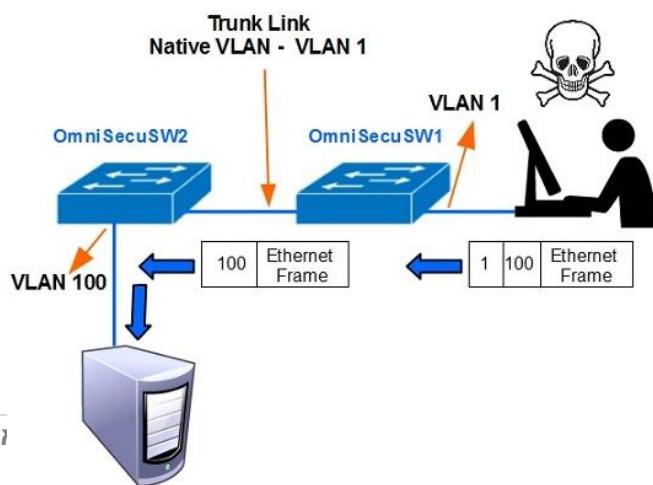
Switch Spoofing attack

(DTP) Dynamic Trunk Protocol משמש ליצור Trunk בצורה אוטומטית בין שני מתגים. משק במתג שמחובר למיכיר קצה (מחשב או מדפסת) נמצא בדרך כלל ב- access mode ומיכיר הקצה יקבל גישה רק ל- VLAN אליו הוא שייר. תבעורה מ- VLANים אחרים אינם מעבירים דרך משק זה. אם התקוף מחובר למשק במתג אשר מוגדר כ- "dynamic auto" או "trunk" והתקוף שלוח מהמחשב שלו הודיעת (DTP), נוצר link בין המחשב לבין המתג. כך התקוף יכול לזכות במידע מכל VLAN. הערה: במקרה שהתקוף יכול לחבר מתג.



Double Tagging attack

התקפה זו תעבור רק אם התקוף מחובר למשק שייר ל- Native VLAN. התקוף משנה את ה- Frame המקורי כדי להוסיף שני טגים. הטג החיצוני של ה- VLAN שלו וTAG מוסתר פנימי של VLAN של הקורבן. כאשר ה- Frame מגיע למתג, המתג יכול לראות רק את הטג החיצוני של VLAN אליו המשק באמת שייר. המתג מסיר את TAG החיצוני. כאשר ה- Frame מגיעה למתג הבא, הוא יפתח את ה- Frame ויראה את TAG השני ויעביר את המידע ל- VLAN השני.



DHCP Spoofing Attacks

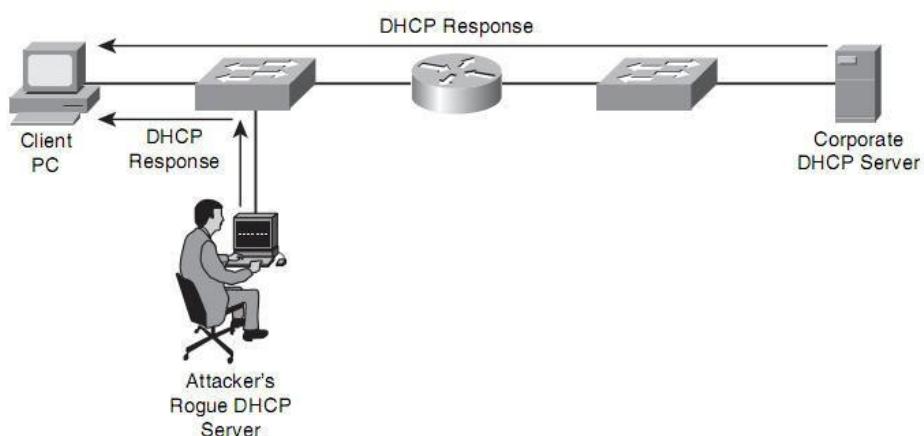
ברשת שתומכת בחלוקת כתובות بصورة אוטומטית, התקנים בעליים ללא הגדרות רשות ושלוחים ב- Broadcast הודיעו DHCP Server מזהה את הפינה ועונה למחשב הפונה בהודעה שמכילה את הגדרות הרצויות. הבעה היא שמאוד קל לחבר לרשת שרת DHCP לא מורשה (Rogue DHCP server).

בהתקפת DHCP spoofing גורם למחשב הנתקף לחשב שהוא שרת DHCP לגיטימי. כדי שלא תהיה תחרות עם שרת DHCP המקורי, רצוי לנטרל את השרת המקורי באמצעות **DHCP Starvation Broadcast**. ההתקפה עיליה רק אם התקף והקרבן נמצאים באותו Domain.

על ידי חלוקת כתובות IP ללוקחות ברשת, התקף מצליח להתזות ל- Default Gateway ולשרת DNS וכן כל תעבורת הרשות היוצאת עוברת דרך התקף. התחזות לשרת DNS מאפשרת לזהיף את תהליך תרגום השמות וכך לבצע Phishing.

התקפת DHCP Chosphing חושפת את הליקות סכנות הבאות:

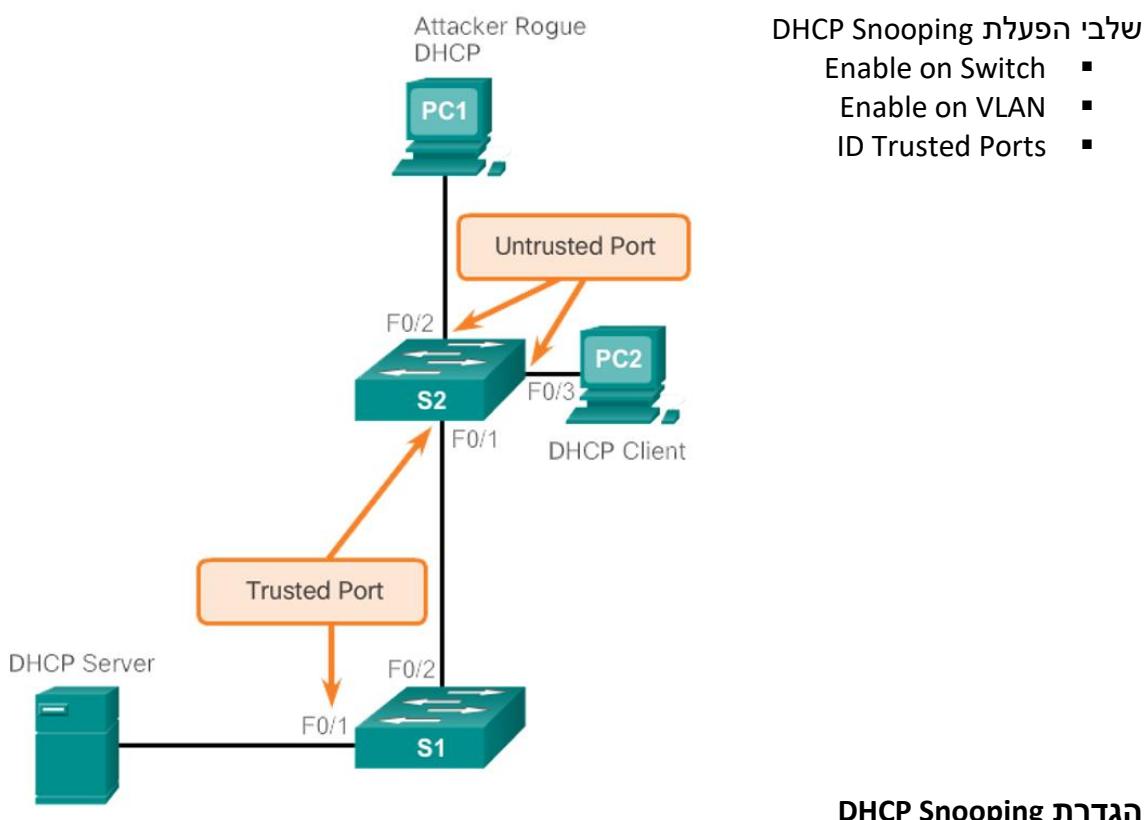
- denial-of-service
- man-in-the-middle
- Phishing



DHCP Snooping

כאשר DHCP Snooping פועל במתג, הוא מונעה התקפת DHCP Spoofing. כלומר, שרת DHCP לא מושהה (Rogue DHCP) לא יכול לחלק כתובות ברשת. בנוסף ניתן להגדיר ש-DHCP Starvation ימנע התקפת DHCP Snooping.

- .Untrusted DHCP Snooping מאפשר לנו להגדיר את הממשקים של המתג כ-Trusted או Untrusted. כאשר אנו מפעילים DHCP Snooping, כל הממשקים במתג מוגדרים כ-Untrusted. שרת DHCP שמחובר דרך Untrusted port לא יכול לחלק כתובות בגין שהמתג מסנן הודעות DHCP offer שנכנסות דרך Untrusted port.
- .Trusted port להגדיר מתג לא מסנן הודעות שmag'iyot משרת DHCP Server דרך Trusted port.



Switch(config)#ip dhcp snooping הגדרת DHCP Snooping במתג.

Switch(config)#ip dhcp snooping vlan {10},{20-25} הפעלת DHCP Snooping ב-VLANS.

Switch(config)#ip dhcp snooping trust אוטומטיות, כל הממשקים ששוכנים ל-VLANS יփכו ל-Untrusted.

Switch(config-if)#ip dhcp snooping trust

מניעת DHCP Starvation

ניתן להגביל את כמות ה- DHCP requests שיכולים להיכנס דרך Untrusted Ports על-ידי הגדרת Rate Limit (הכמות לשנייה). אפשרות זו מגינה על השירות מפני כמות מוגזמת של בקשות לטיפול (התקפת DHCP Starvation). ניתן להשתמש גם ב- Port Security.

```
Switch(config-if)#ip dhcp snooping limit rate {packets per second}
```

בדיקות ההגדרות

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface      Trusted    Rate limit (pps)
-----
FastEthernet0/1   yes        unlimited
FastEthernet0/2   yes        unlimited
```

כאשר ל Kohort מתקשרים בראשת, המתג בונה "bindings table", מסד נתונים שמאפשר את:

- כתובות MAC של הלוקו.
- הכתובת IP שהוקצתה ללוקו.
- לאיזה משק במתג ולאיזה VLAN הלוקו מחובר.
- כמה זמן נשאר לחכירת הכתובת IP (DHCP lease time).

הפרות יכולות להתרחש עקב חוסר התאמה בין כתובות MAC או ניסיונות לספק שירות DHCP דרך ports untrusted. כאשר DHCP snooping מגלת הפרה, המנות המפזרות נזרקות ונוצרת רשומה ב- log שמכלילה את הטקסט DHCP_SNOOPING.

הגדרות מתקדמות

הבסיס נתונים של DHCP Snooping נשמר מקומית ואותה המתג מוחק אותו.

ניתן לשמר אותו במקומות אחרים (לדוגמה: בזיכרון flash או שרת tftp).

```
Switch(config)#ip dhcp snooping database {flash:/snoopy.db}
```

```
Switch(config)#ip dhcp snooping database {tftp://10.1.1.1/directory/file}
```

כדי לראות את הבסיס נתונים השתמש בפקודה:

```
Switch#show ip dhcp snooping binding
```

```
Switch#show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type        VLAN  Interface
-----          -----          -----       -----      -----  -----
00:01:C9:54:AE:D0  10.0.0.10     86400      dhcp-snooping  1     FastEthernet0/1
Total number of bindings: 1
```

כדי לראות סטטיסטיקה של הבסיס נתונים השתמש בפקודה:

```
Switch#show ip dhcp snooping binding database
```

Dynamic ARP Inspection (DAI)

DAI מספק הגנה מפני ARP Poisoning/Spoofing Attacks על ידי בדיקה שיש התאמה בין כתובת הפיסית לכתובת IP. כדי להשתמש בו- Dynamic ARP Inspection יש צורך בהפעלת DHCP Snooping DHCP וזאת כי משתמש בו- DHCP Snooping database בצד בדוק כל_packet שנכנס דרך Untrusted port.



לחلك מההתקנים מוגדרת כתובות קו קבוע וכאן הכתובת שליהם לא מופיע DHCP Snooping database. את כתובות אלה עליינו להכניס בצורה ידנית ל- ARP ACL שנוצר במיוחד למטרה זו ובתוכו יש מיפוי של כתובות קו לכתובות פיסיות.

חיבור בין מתגים (Trunk) יהיה port Trust. DAI לא מבצע בדיקה על port Untrusted.

בנוסף, DAI מפעיל מגבלה של עד 15 בקשות ARP לשניה דרך port err-disable אם יהיה יותר, ה-port יכנס במצב של.

הגדרת DAI

הפעלת DAI בכל VLAN במתג:

```
Switch(config)#ip arp inspection vlan {1}
```

בדיקה:

```
Switch#show ip arp inspection vlan {1}
```

הגדרת משקדים שמחברים בין מתגים כ- Trust port

```
Switch(config-if)#ip arp inspection trust
```

:ARP ACL

```
Switch(config)#arp arp access-list {V1}
```

```
Switch(config-arp-acl)# permit ip host {10.1.1.1} mac host {aaaa.bbbb.cccc}
```

```
Switch(config)#ip arp inspection filter {V1} vlan {1}
```

נקتب ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ווערכו על ידי ערן גזית
لتשומת לבכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

Securing Router Access

הגדרת תמייה ב- (SSH)

בניגוד ל- Telnet שלא מצפין את המידע, SSH מאפשר ניהול מרוחק בצורה מוצפנת (RSA) של מתגים, נתבים ושרותים. כדי להגדיר SSH בנתב, יש ליצור RSA public/private keys לצורך הצפנה המידע.

השלבים הם:

1. הלקוח מתחבר לשרת והשרת שולח ללקוח את ה- public key.
2. הלקוח והשרת דנים בניהם לגבי ההגדרות בהם ישתמשו, זה כולל את סוג ההצפנה הסימטרית.
3. הלקוח יוצר מפתח סימטרי ומצפין אותו עם ה- public key של השירות.
4. הלקוח שולח את המפתח הסימטרי לשרת, השירות מסיר את ההצפנה של המפתח הסימטרי עם המפתח הפרטני שלו.
5. בעזרת המפתח הפרטני הם מצפינים ומפענחים את המידע כולל תהליך הזיהוי.

כדי ליצור את המפתחות יש צורך לתת לנtab:

```
Host Name ▪  
Domain Name ▪  
Router(config)#hostname R1  
R1(config)#ip domain-name yaki.local
```

ביצירת המפתחות רצוי שאורך המפתחות יהיה לפחות bit 1024 (תתבקש להכניס את אורך המפתחות).

במקרה של דוגמא זו, שם המפתחות יהיה R1.yaki.local
R1(config)#crypto key generate rsa
R1(config)#ip ssh version 2

ניצור חשבון משתמש מקומי כדי להתחבר מרוחק ב- SSH.
R1(config)#username admin secret 123

לבסוף, נגדיר שינוי תמייה מי Telnet ל- SSH ונגדיר אימות באמצעות משתמש מקומי.

```
R1(config-line)#transport input ssh  
R1(config-line)#login local
```

כדי לנהל את הנtab מרוחק, נרשם במחשב את הפקודה הבאה:
ssh -l {user name} {IP}

```
C:\>ssh -l admin 10.1.1.254  
Password:  
  
R1
```

ניתן לעבוד על ידי יקי בן ניסן.
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

Privilege levels in IOS CLI Shell

אפשר לנו לשער מספר פקודות ל- Privilege level מסויים.

ב- IOS Cisco יש 16 רמות של הרשות (0-15):

- רמת הרשות 0 – מאפשר כניסה ל- user mode ללא אפשרות לפקודות.
- רמת הרשות 1 - User mode.
- רמת הרשות 15 - Privileged mode.
- רמת הרשות 14-2 - זמינים עבור התאמת אישית.

כאשר משתמש נכנס ל- User mode הוא משתמש ברמת הרשות של "1".

במצב זה המשתמש לא יכול לשנות הגדרות או לראות את ה- running configuration . המשתמש יכול להציג את מצב הממשקים או את טבלת הניתוב.

על-ידי כניסה ל- Privileged mode המשתמש משתמש ברמת הרשות של "15".

Securing Wireless Networks

רשתות אל-חוטיות חשובות לאוֹתן התקפות כמו רשתות חוטיות אָרְבָּן גַּדְעָן לרשות חוטית שבסה התקן מחובר פיסית לרשות, ברשת אל-חוטית האות משודר לכל כיוון באמצעות גלי רדיו. בהתאם לסוג הziוד ומיקומו, טווח השידור יכול לצאת מחוץ לתחום השליטה שלך ולכן, בנוסף לכל התקפות אליה חשופה רשות חוטית, רשות אל-חוטית חשופה להתקפות נוספות.

ברשת אל-חוטיות קיימות שני סכנות עיקריות:

- **גישה של גורם לא מושה לרשות**

ניתן למנוע סכנה זו על-ידי חיבור המשתמש להזדהות בהתחברות לרשות. לדוגמה, ההזדהות באמצעות שירות RADIUS.

- **ציטוט למידע**

באמצעות Sniffer ניתן ללכוד packets שעוברים בין התקנים ל-Access Point. התקפה כזו לא ניתנת לגילוי ומסכנת את סודיות המידע שימושו ברשת. כדי להתגונן מפני התקפה כזו, יש להציג מידע שימושו בזרה אל-חוטית.

IEEE 802.11 Wireless Protocols

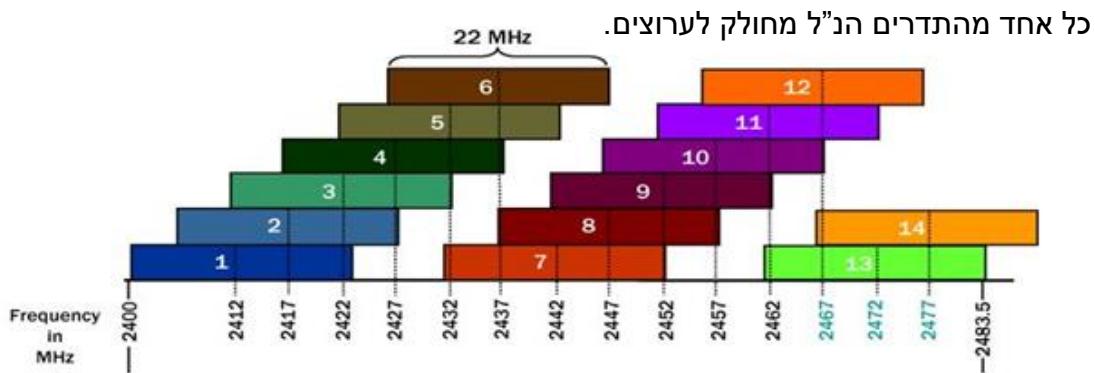
IEEE 802.11 זהו שם כולל למשפחה של תקנים ברשות WIFI מקומיות (WLAN). 802.11 הם פרוטוקולים שמאפשרים תקשורת אל-חוטית תוך שימוש בגלוי רדיו. בשנת 1999, הוציא אט הסטנדרט הראשון בקבוצה. רוב נקודות הגישה האל-חוטיות תומכות ביותר מתקן אחד. בתקנים g ו- 802.11n ניתן לעבוד ב- mixed mode שמאפשר תמייהה בתקנים שתומכים בתקן איטי יותר.

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g

ערוצי (Channels) רשת אלחוטית

רשתות WIFI יפעלו בד"כ באחד משני תדרים:

- 2.4 GHz(802.11b/g/n)
- 5.2 GHz (802.11a/ac)



ישנם ערוצים אשר חופפים זה זהה. הערוצים שאינם חופפים, מצויים במרחב של חמישה ערוצים זה מזה. בין הערוצים 1, 6 ו 11 אין חפיפה.
אם קיימת לנו שני רשתות בבית, יהיה עדיף להגדיר אחת על ערוץ 9 ואת השנייה על ערוץ 5+ח כדי להימנע מהפרעות וסיכוי גבוה של איבוד חבילות.

קיימות תוכנות רבות שמאפשרות לגלוות פרטיים על Access Points, לדוגמה **NetSpot**.

	SSID	BSSID	Alias	Graph	Signal	%	Min.	Max.	Average	Level	Band	Channel	Width	Vendor	Security	Mode	Last seen
□	yudgimel	00:6CBC:EF:97:A8			-43	62	-46	-39	-43		2.4	11	20	Cisco	WPA2 Personal		now
✓	yudaled	00:6C:BC:EE:44:1E			-65	36	-67	-65	-65		2.4	11	20	Cisco	WPA2 Personal		now
□	elchi	C0:AC:54:F8:66:BC			-77	22	-81	-75	-78		2.4	9 + 1	40	Sagemcom	WPA2 Personal		now
□	idan	14:AE:DB:47:7D:B5			-84	14	-92	-84	-88		2.4	1	20	VTech	WPA2 Personal		now
□	BezeqFree	06:AE:DB:47:7D:B5			-84	14	-92	-84	-88		2.4	1	20	-	WPA2 Personal		now

שיטות הצפנה עבור רשתות אלחוטיות

Wired Equivalent Protection (WEP)

WEP משתמש ב- RC4 אלגוריתם ההצפנה ומאפשר שימוש במפתח הצפנה של 64/128 bit. ככל שהמפתח ארוך ומורכב יותר, כך רמת האבטחה גבוהה. צורת השימוש ב- RC4 חושפת בו חולשה. לתוכף שמאזין לרשות ואוסף חבילות מידע (IV) תהיה יכולה לגלו את המפתח יחסית בקלות מכיוון שהצפנה היא סטטית ולא משתנה ולכן WEP ניתן לפרקתו תוך דקוק. עדיף לא להשתמש ב- WEP אם התקנים תומכים בהצפנה חזקה יותר.

Wi-Fi Protected Access (WPA/WPA2)

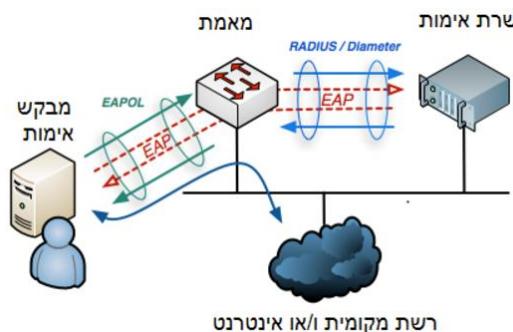
WPA ו-WPA2 פותחו בעקבות חולשות שנמצאו ב- WEP ותוך יישום תקן האבטחה 802.11i. בכך לתרמו בהתקנים יישנים יותר, WPA לא מיישם את תקן 802.11i במלואו. WPA משתמש באלגוריתם ההצפנה RC4 יחד עם TKIP (Temporal Key Integrity Protocol). TKIP פותח כדי לחזק את ההצפנה של WEP תוך תאינות לאחר התקנים יישנים שתומכים ב- WEP בלבד. TKIP מייצר לכל חבילת מידע מפתח חדש. כיוון TKIP לא משמש עוזר כי גם הוא פריז.

WPA2 משתמש ב프וטוקול CCMP במקום TKIP על מנת להשיג אבטחה נוספת. CCMP משתמש בהצפנה באלגוריתם AES 128/192/256bit שזו הצפנה חזקה מאוד.

שיטות היזדהות עבורי רשותות אלחוטיות

(Pre-shared key) PSK IEEE 802.1X Authentication
 ב כדי להתחבר לרשת ניתן להזדהות באמצעות Shared Key Authentication. שיטה זו לא כל כך בטוחה בגלל שכל התקנים משתמשים באותו secret key. גליי הסיסמה בהתקן אחד מסכנת את הרשת כולה. החלפת secret key זו מושימה לא קלה מכיוון שיש להחליף את secret key גם בכל תחנות העבודה.

(Extensible Authentication Protocol) EAP IEEE 802.1X Authentication
 ביצוע ההיזדהות מול שרת RADIUS. שרת RADIUS מאפשר ניהול מרכזי ומקבב אחר המשתמשים שמתמחברים לרשת אל-חווטית. שיטה זו עדיפה ובוטיחה כאשר יש צורך בניהול מחשבים רבים. שיטה זו ידועה בשם Enterprise Authentication.



Extensible Authentication Protocol
 EAP מספק מסגרת לאימוטים משתמשים ברשותות אלחוטיות. בין חמשת סוגי EAP שאומצו על ידי תקן WPA/WPA2 הם:

- EAP-TLS
- EAP-PSK
- EAP-MD5
- LEAP - צריך לדעת ל מבחן
- PEAP - צריך לדעת ל מבחן

(Lightweight Extensible Authentication Protocol) LEAP
 LEAP נוצר על ידי סיסקו (פרוטוקול קנייני) כתוסף ל-EAP וرك כפتروן מהיר לביעות של WEP. אחד הסיבות שהוא נקרא משקל קל, היא שנעשה בו שימוש רק בסיסמא ללא שימוש בתעודות דיגיטליות, כולל וPKI לא מעורב. הפרוטוקול מבוסס על MS-CHAP של Microsoft, כולל המידע שנשלח בין התקנים מכיל חסכנות אבטחה, כולל כמות גדולה של המידע לא מוצפן וכן ניתן לראות את המידע.

(Protected Extensible Authentication Protocol) PEAP
 Microsoft, Cisco ו-Rsa security פועלו יחד לייצור PEAP. מחליף את LEAP ותומך בכל הגרסאות הנוכחיות של Windows. PEAP יוצר מנירה בעזרת פרוטוקול TLS וכן מצין את כל התעבורה בתקשות. יש צורך בתעודה דיגיטלית רק בשרת האימוט. על ידי הוספה PEAP, Tunnelling מוסיף שכבה אבטחה נגד התקפות man in the middle והאזורות.

ממשק ניהול

צעד ראשון של אבטחה. שנה את סיסמת ניהול של ה- Access point לסיסמה מורכבת והגדיר שלא ניתן יהיה לנוהל אותה מרוחק.

ביטול SSID broadcast

SSID (Service Set Identifier) זהו שם הרשות האלקטרונית.

השם יכול להכיל עד 32 תווים של אותיות ומספרים והוא רגיש לאטיות קטנות או גדולות. כבירות מחדל, Access Point משדר את ה- SSID שלו ב- Broadcast וכך כל אחד יכול לגלו את ה- Access Point. ביטול SSID Broadcast לא מאפשר לגלו את ה- Access Point. הגנה זו נחשבת חלשה כי בדרכים מסוימות ניתן לגלו את נוכחות ה- Access Point.

Wireless Network Mode:	Mixed
Wireless Network Name (SSID):	Teddy-Bear
Wireless Channel:	11 - 2.462 GHz
Wireless SSID Broadcast:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

MAC Address Filtering

רוב נקודות הגישה מציעות את היכולות של סינון MAC, אך הוא כבוי כבררת מחדל. כתובת ה- MAC היא המזהה הייחודי שקיים עבור כל כרטיס רשות. סינון על פי כתובת פיזית של התקן זו דרך הגבלת חיבור התקנים לרשות אל-חוטית. מכון שכתובת זאת לא משתנה אף פעם, ניתן ליצור רשימה שבה מופיעו למי יש גישה ולמי אין גישה.

ID	MAC Address	Status	Description	Modify
1	16-CC-20-CE-14-93	Enabled	PC	Modify Delete

Add New... [Enable All](#) [Disable All](#) [Delete All](#)

موقع וסוג האנטנה

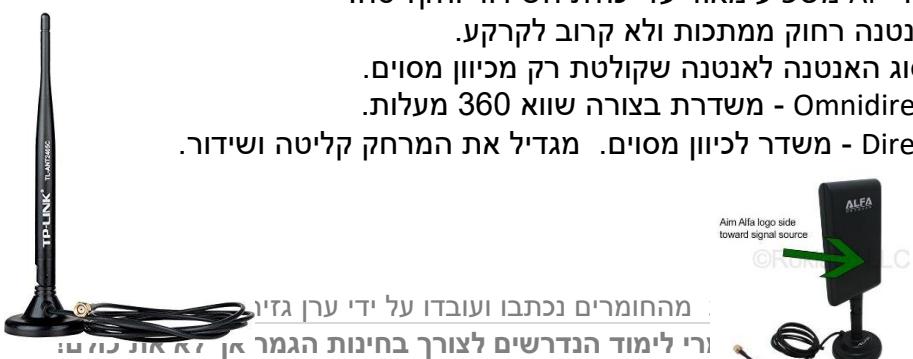
موقع האנטנה וה- AP משפייע מאוד על יכולת השידור והקליטה.

יש למקם את האנטנה רחוק ממתכוות ולא קרוב לקרקע.

ניתן לשנות את סוג האנטנה לאנטנה שקולטת רק מכיוון מסוים.

ישר Omnidirectional antenna - משדרת בצורה שווה 360 מעלות.

Directional antenna - משדר לכיוון מסוים. מגדיל את המרחק קליטה ושידור.



נכתב ועובד על יד
لتשומת לבכם ה

עוצמת השידור

ככל שעוצמת השידור חזקה יותר, כך ניתן לקלוט ממרחק גדול יותר. כדי למנוע מהאות לצאת מחוץ למתחם, ניתן להנמיך את עוצמת השידור ב- AP, להציג את ה- AP למיקום אחר או להחליף את סוג האנטנה. קיימות תוכנות שמאפשרות לגלוות את עוצמת האות, לדוגמה NetSpot. ייחדות המידה של עוצמת השידור נמדדות ב- dB. אנטנה ממוצעת משדרת בעוצמה של 20dB והעוצמת השידור מוכפלת כל dB.

Site Surveys (ביצוע סקרים באתר)

קיימות תוכנות רבות שמאפשרות לגלוות את עוצמת האות ומידע נוסף על הרשות האל-חותית. לדוגמה, NetStumbler או AirMagnet Survey. על-ידי התקנת תוכנה על הסולולרי והיליכה ברחבי האתר ניתן לגלוות נקודות שבהם יש בעיית קליטה ונקודות שבהם יש קליטה חזקה מדי שייצאת מחוץ למתחם. בנוסף ניתן לגלוות AP שלא בשליטהך.

Captive Portals

זו דרך אחרת ניתן לדרש מהמשתמשים להזדהות לפני שנוטנים להם גישה לרשות האל-חותית. הרשות הגישה היא לפרק זמן מסוים.



VPN Over Open Wireless Networks

קיימות סכנות רבות ברשות אל-חותיות פתוחות:

- אין הצפנה וכן ניתן לצותת למידע.
- לא ניתן לשמור על מי שמחובר לרשות זו.

אם יש צורך בחיבור לרשות כזאת, רצוי להשתמש ב- VPN שמצפין את כל המידע וכן מקטין את רמת הסיכון.

Wi-Fi Protected Setup (WPS)

זו טכנולוגיה שנוצרה כדי לאפשר לך לחבר בקלות ל- wireless access point. הבעה בטכנולוגיה זו היא הקוד של 8 ספרות שנייה לפרוץ תוך כמה שניות באמצעות无线 access point brute-force. لكن חובה לבטל את WPS בכל point.

AP isolation

טכנולוגיה זו לא מאפשרת תקשורת בין הלקוחות שמחוברים ל- WAP.

סוגי התקפות אל-חוטיות

Rogue Access Points (נקודות גישה סוררת)

זו נקודת גישה שהתווסףה לרשת ללא ידיעת מנהל הרשת. התקוף מחבר לרשת החוטית AP שמאפשרת לו להתחבר לרשת בצורה אל-חוטית. גם אם אחד העובדים הוסיף אותה, ניתן שהיא לא עומדת בסטנדרט האבטחה של החברה ולכן היא מסוכנת. כדי לגלוות Rogue Access Points יש צורך בשימוש בתוכנות סריקה.

Evil Twins

זה AP שמתמחה להיות AP אחר עם אותו SSID. לדוגמה ב��תי קפה או מקום אחר. בדרך כלל המטרה להתקפה זה ביצוע phishing. בדרך כלל ה- AP ממוקם במקום שעוצמת היקליטה שלו תהיה גבוהה יותר מה- AP המקורי במטרה שימושים יתחברו לנקודה הגישה המזויפת. (WLC) Wireless LAN Controller זהו פתרון מצין להתקפה זו. בשיטה זו, קיימים כמה AP שימושיים למכשור הקשור בהם ומדוחים לו שהם מחוברים. כל פעם שמת לחבר AP זה, WLC מזיה אותו על ידי ביצוע security scan (סריקה שמתרבצת מיד פעם).

Jammin/Interference

זו התקפת DOS על AP. זו יכולה להיות הינה להתקפת Evil Twins. על-ידי שידור רעשים בעוצמה גבוהה באותו תדר שידור של ה- AP התקוף תופס את מרחב השידור של אותו AP. ניתן לאתר את מקור הרעש באמצעות תוכנה כמו NetStumbler.

Wi-Fi deauthentication attack

התקוף משדר אות ניתוק ל- WAP כדי לנתק משתמש שמחובר לרשת האל חוטית. כך התקוף מצליח לילכוד packets שקשורים להתחברות מחדש של המשתמש. מידע זה מאפשר לתקוף לגלוות את ה- SSID ואת ה- WPA/WPA2 handshake. מידע זה יכול לשמש להתקפת dictionary attack ואפשרר את גילוי הסיסמה. כדי למנוע התקפה זו, השתמש בסיסמא מורכב ואורך, כזו שלא נמצאת במיילון.

בנוסף התקפה זו יכולה לבצע DOS על המשתמשים על ידי ניתוקם מהרשת.

Bluesnarfing

גניבת מידע דרך חיבור Bluetooth.

Bluejacking

שליחת מידע לא מורשה להתקן Bluetooth, כמו הודעת טקסט.

Cryptography

криיפטוגרפיה נוצרה כדי לאבטח מידע.

מידע יכול להיות במצבים הבאים:

- מידע בתנועה (לדוגמה: מידע שזורם בין שרת ללקוח).
- מידע במנוחה (לדוגמה: סיסמאות שמואחסנות בשרת).
- מידע בשימוש (לדוגמה: מידע שנמצא בזכרון RAM)

криיפטוגרפיה מספקת אבטחה בדרכים הבאות:

- סודיות (Confidentiality) - הצפנה
- שלמות המידע (Integrity) - גיבוב (Hashing)
- אבטחה (digital certificate) אבטחה (Authentication)
- ראיות (digital signatures) לא-ראיות (Non-repudiation)

סודיות (Confidentiality)

כדי להגן על המידע שזורם ברשת (מידע בתנועה) אנו משתמשים בהצפנה. בסופו עליינו לשולט בגישה למידע מאוחסן (מידע במנוחה). אנו עושים זאת באמצעות הרשאות גישה ולפעמים נוסיף לכך גם הצפנה. כדי לספק הגנה יعلاה, עליינו לסמן את המידע לפי רמת הסודיות שלו. לדוגמה: סודי, סודי ביותר ומסוג.

הצפנה המידע מאפשרת רק למורשים להבין תוכן המידע. כמובן, אדם לא מרשה ש杂志社 תראה מידע שאינו מובן (cipher text) בגלל שאין לו את היכולת לפענוח את הנתונים. אלגוריתם ההצפנה ואורך המפתח משפיעים על חזק ההצפנה. ככל שההצפנה חזקה יותר צריך יותר זמן ומשאבים כדי לפענוח cipher text ללא מפתח.

כך נראה תוכן של מידע מוצפן (Caesar cipher)

```
Tp uijt jt uif tfdsfu nfttbhf. Ju jt fbtz up ef-fodszqu jg zpv lopx uif lfz.
```

```
"So this is the secret message. It is easy to de-encrypt if you know the key."
```

שלמות המידע (Data Integrity)

על-ידי ביצוע גיבוב (Hashing) ניתן לבדוק בוודאות שהמידע לא שונה או הושחת תוך כדי העברתו לידי וכן לא ניתן לזייף את המידע. כמובן, אם יבוצע שינוי במידע, זה יתגלה.

זיהוי (Authentication)

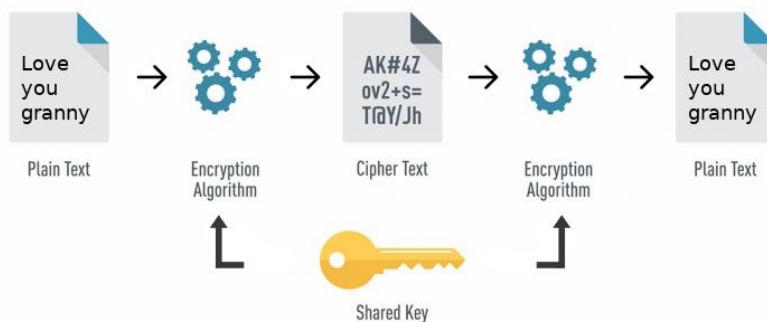
זיהוי הדדי של שני הצדדים לפני ותוך כדי שידור הנתונים.

זיהוי הנתונים כתובים שהגינו מההתקפה ולא נתונים שנשלחו על-ידי מתחזה.

(shared-key encryption) Symmetric Encryption

זהו אלגוריתם מתמטי דו כיווני שמשתמש במפתח אחד לצורך הצפנה/פיענוח של מידע. שני הצדדים משתמשים באותו מפתח (Session key). בדרך כלל האלגוריתם ידוע לכל והסודות נשמרת כל עוד המפתח נשמר.

Symmetric Encryption



תרגיל:

פענה את הטקסט המוצפן.
שיטת ההצפנה היא צופן קיסר והמפתח הוא 1 - (לדוגמא, כדי לפענה נבצע $c + 1 \rightarrow b$)

קייםים שני סוגי אלגוריתמים סימטריים:

- מצפן מודע זורם, bit אחר bit - **Stream cipher**

XOR operation	
1+1=0, 0+0=0, 1+0=1, 0+1=1	
Input	10011100101010
Keystream	<u>00011010001110</u>
Output	10000110100100

- מצפן בכל פעם מקטע נתונים אחד. **Block cipher**

Type	Method	Algorithms
Stream Cipher	Works with one bit at a time	RC4
Block Cipher	Works with blocks of data	DES, 3DEC, AES, Blowfish, Twofish, IDEA

Block cipher יכול לעבוד במספר מצבים:

- Electronic Code Book (ECB) Mode - כל בלוק עצמאי. מתאים להודעות קצרות.

- Cipher Block Chaining (CBC) Mode - יש קשר בין הבלוקים כדי לטעטש את התבנית הצפנה. מתאים להודעות ארוכות.
 - Stream cipher (CTR) Mode - הופך עיל כי יודע לעבד את המידע במקביל.
 - Counter (CTR) Mode - מואוד עיל כי יודע לעבד את המידע במקביל.
 - Galois/Counter (GCM) Mode - גודל בלוק 128bit.

אלגוריתמים שימושים ב- Symmetric key

חזק ההצפנה תלוי בסוג האלגוריתם ואורך המפתח.

(Data Encryption Standard) DES

בשנות השבעים DES נבחר על ידי ממשל ארצות הברית כסטנדרט ההצפנה. כיוון שהשיטות הידועות באותה תקופה לא עשו שימוש באלגוריתם DES, היה קשה לשבור אתDES. בשנת 1999 הוחלף על ידי 3DES.

(Triple DES) 3DES

אם אלגוריתם זה עובד בשיטת block cipher של 64bits. בשנת 2001 הוחלף על-ידי AES. DES 3DES זהה לו- מלבד העובדה שהוא יוצר שלושה מפתחות ומצפין את הבלוק שלוש פעמים וכך אורך המפתח 168bits (56^3). הוא עמיד יותר מפני brute-force אך כיוון שהוא נחשב כחלש.

(Advanced Encryption Standard) AES

בשנת 2002 נבחר AES כסטנדרט ההצפנה על ידי ממשל ארצות הברית. ממשלת ארצות הברית מסווגת את סוג ההצפנה של AES-256 כ- סודי ביותר. AES משתמש ב מפתח באורך 128/192/256 ועובד בשיטת block cipher block של 128bits AES מהיר, משתמש כמעט מושלמים וכי יכול לעבוד בפלטפורמות רבות. לדוגמה, WPA2 מצפין מידע בתנועה בתקשורת אל-חוטית. BitLocker | Encrypting File System (EFS) ונעשה בו שימוש להצפנה מידע במנוחה ב- ישנים דרכי לתקן את המנגנון שמשתמש ב- AES אך לא את האלגוריתם עצמו ולכן AES נחשב כיום לאלגוריתם הסימטרי החזק ביותר.

(Ron's Cipher) RC

RC4 זהו streaming cipher פופולרי בהצפנה אלחוטית WEP/WPA. RC5 משתמש במפתח באורך 128bit, משמש גם ב-TLS, SSL ו- BitTorrent ועוד. RC6 עובד בשיטת block cipher, משמש במפתח באורך 128bit ו- 256bit וחשב כמערכת חזקה.

Twofish | Blowfish

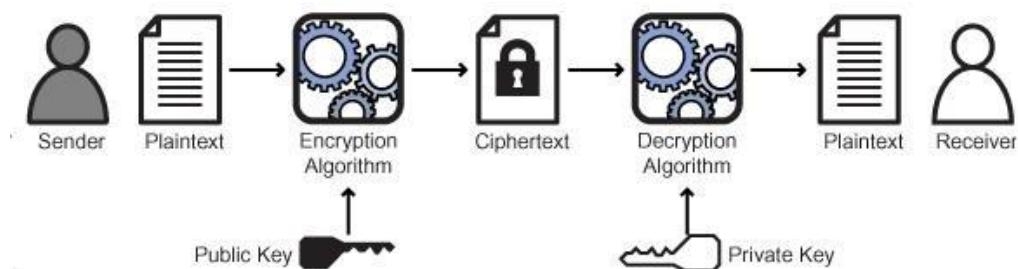
המ מהירים מאוד ולא מוגנים באמצעות זכויות יוצרים ולכן כל אחד יכול להשתמש בהם. Blowfish נוצר בשנת 1993, 64-bit block cipher, משתמש במפתח באורך 32-448 bits. Twofish הוא היורש של Blowfish, משתמש במפתח באורך עד 256 bits, Threefish עם מפתח באורך עד 1024bit. קיימ גם 128-bit block cipher.

(public-key encryption) Asymmetric Encryption

בשיטתה זו, ההצפנה והפענוח מתבצעים באמצעות זוג מפתחות שונים אך קשורים במבנה בקשר מתמטי.

מפתח ציבורי (Public-key) - בדרך כלל משמש להצפנה ומופץ בצורה חופשית לכל מי שהוא רוצה שילוח לנו מידע מסווגן. מפתח זה לא מסוגל לפענח מידע שהוא מצפן.

מפתח פרטי (Private-key) - בדרך כלל משמש לפונCTION. מידע שהוצפן באמצעות המפתח הציבורי, מופיע רק באמצעות המפתח פרטי.



למשימות קצירות כמו חתימה דיגיטלית או הצנת מפתח סימטרי. אסימטרית לא-חזקקה יותר מהצפנה סימטרית ולכן, בדרך כלל הצפנה אסימטרית משמשת למטרות שאורך המפתח ארוך יותר בהצפנה אסימטרית מהצפנה סימטרית, הצפנה אסימטרית מודרנית מושפעת מאוד על המעבד. אורך המפתח בין 512-32768bits.

אלגוריתמים שימושיים ב-

RSA (Rivest–Shamir–Adleman) – שיטהryptographic פומבית. מושם להצפנה מידע ולחתימה דיגיטלית. מפתח באורך 512/1024 או יותר. משמש ב-SSH, SSL, TLS ועוד. יכול לשמש להחלפת מפתחות.

באורך 3072bit יכול להיות מוחלף בפתח ECC באורך 256bit. כנראה ECC מושמע ככryptography על מנת לאפשר אבטחה גבוהה RSA אך עם מפתח קצר יותר. לדוגמה: מפתח RSA משיג את אותה רמת אבטחה כמו ב- RSA אך עם מפתח קצר יותר.

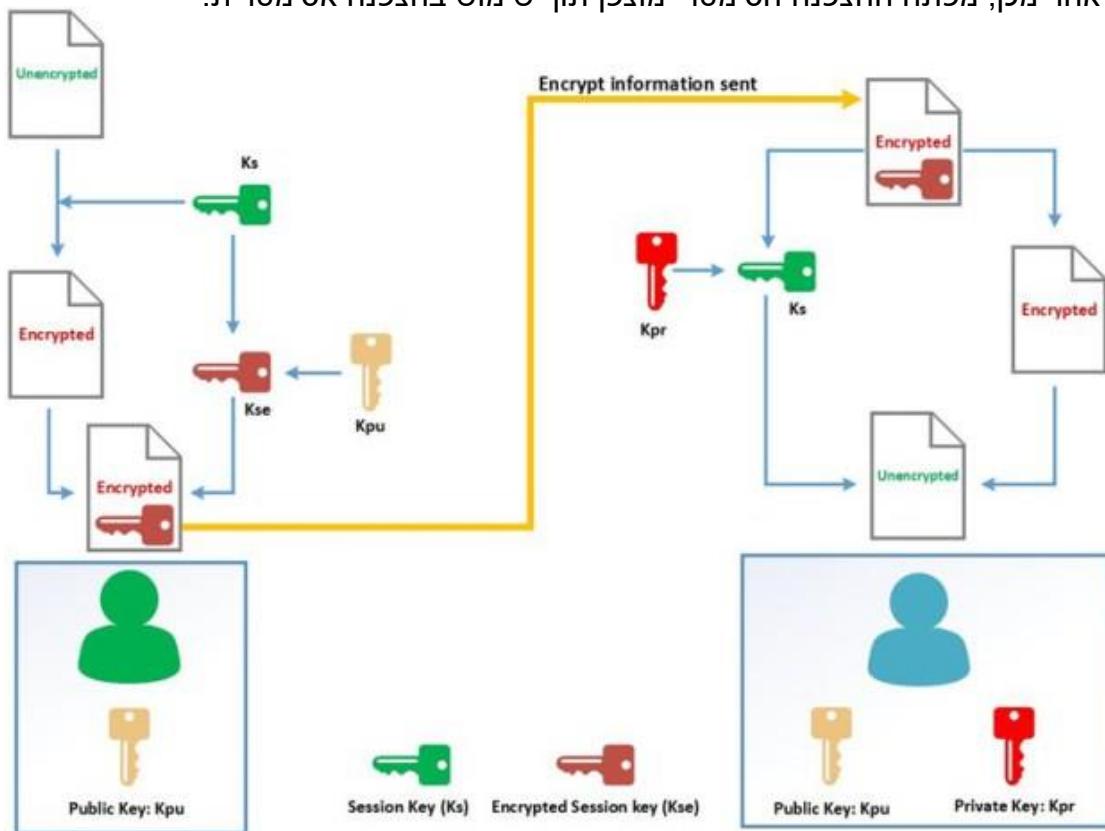
Group 1	768 bit modulus
Group 2	1024-bit modulus
Group 5	1536-bit modulus
Group 14	2048-bit modulus
Group 19	256-bit elliptic curve
Group 20	384-bit elliptic curve
Group 21	521-bit elliptic curve

נוצר בשנת 1993 ומשמש בעיקר ליצירת key Symmetric key exchange (Diffie–Hellman) DH key exchange לצורך הצפנה סימטרית דרך רשת ציבורית. אורור וועג המפתח נקבע לפי Diffie-Hellman Groups.

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי יקי בן ניסן.

הצפנה בזמן אמת (Real-time)

כאשר נדרש הצפנה בזמן אמת, ההצפנה צריכה להיות מהירה ומאובטחת. שילוב בין ההצפנה סימטרית להצפנה אסימטרית מסיג מטרה זו. תחילה, המידע מוצפן באמצעות ההצפנה סימטרית (session key) וילכ בлок נתונים נוצר מפתח סימטרי חדש. לאחר מכן, מפתח ההצפנה הסימטרי מוצפן תוך שימוש בהצפנה אסימטרית.



החלפת מפתחות

החלפת מפתחות זה נושא חשוב במיוחד בתחום לקריפטוגרפיה סימטרית. קיימות שתי גישות לחילופי מפתחות:

- **in-band key exchange** – החלפת המפתח בתוך ערוץ תקשורת המוצפן (https משמש בשיטה זו). הרבה פעמים מפתח סימטרי מגן באמצעות הצפנה אסימטרית.
- **out-of-band key exchange** – המפתח מוחלף בערוץ תקשורת שונה מהערוץ המרכזי שיוצפן או שהמפתח יועבר דרך דואר אלקטרוני, טלפון, או דרך אחרת שלא קשורה לתקשורת.

נאמנות המפתח (key escrow)

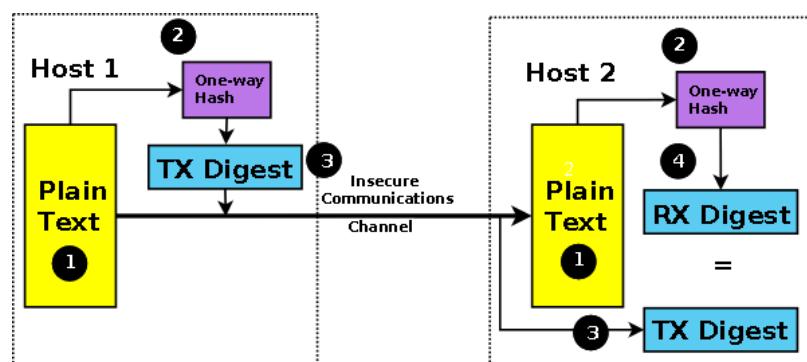
נאמנות המפתח זהה הסדר שבו המפתחות הפרטיים מוחזקים בנאמנות אצל גורם צד שלישי, כך שבנסיבות מסוימות, צד שלישי יוכל לקבל גישה למפתחות אלה. לדוגמה: עסקים שרצו גישה אל התקשרות הפרטית של העובדים או ממשלות שרצו להציג את התוכן של תקשורת מוצפנת.

(גיבוב) Hashing

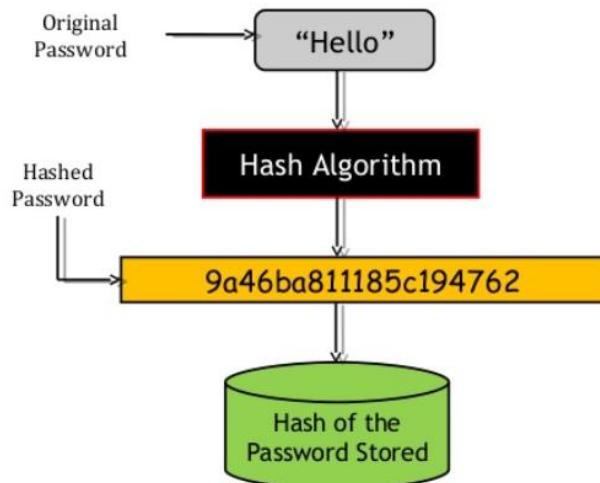
אלגוריתם מתמטי חד כיווני שמאיר קלט באורך משתנה לפולט באורך קבוע (קצר בהרבה). לא ניתן לתרגם Hash חוזרת - data כמו שלא ניתן להחזיר מיש תפוזים להיות תפוזים.

Hash מספק:

- **שלמות המידע (Integrity).** הוכחה שהמידע לא שונה תוך כדי העברה.



- אחסון סיסמאות.



אחת הביעות של Hashing זה Collision. לשני נתונים שונים יש Hash זהה. ככל שה-Hash אරוך יותר כך התופעה תהיה פחות נפוצה. התקפת Collision attack מנצלת חולשה זו.

אלגוריתמים נפוצים לביצוע Hashing:

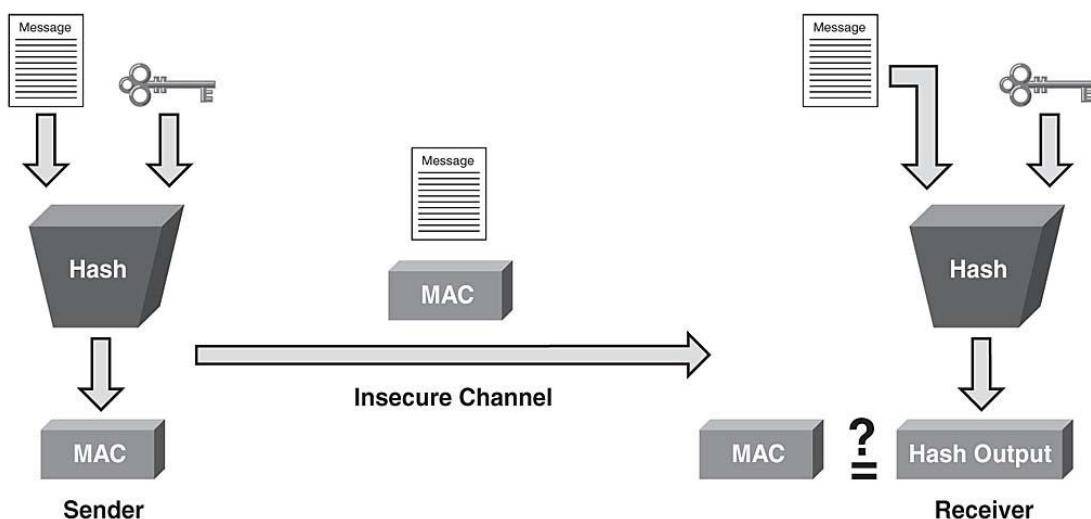
- **MD5** (Message Digest Algorithm) - נוצר בשנת 1992. מפתח באורך bits 128. ב-1996 התגלה באלגוריתם בעיות התנגדויות ולכן מומלץ להשתמש בו- SHA.

- .160 bits (Secure Hash Algorithm) **SHA-1** •
קיים נחשב לא בטוח בגל בעיות התנגשות.
- .256/384/512 bits (Secure Hash Algorithm) **SHA-2** •
(RACE Integrity Primitives Evaluation Message Digest) **RIPEMD** •
זהו 128/160/256/320 bits Open standard אלגוריתם פחות נפוץ, מפתח באורך s.

www.freeformatter.com/message-digest.html

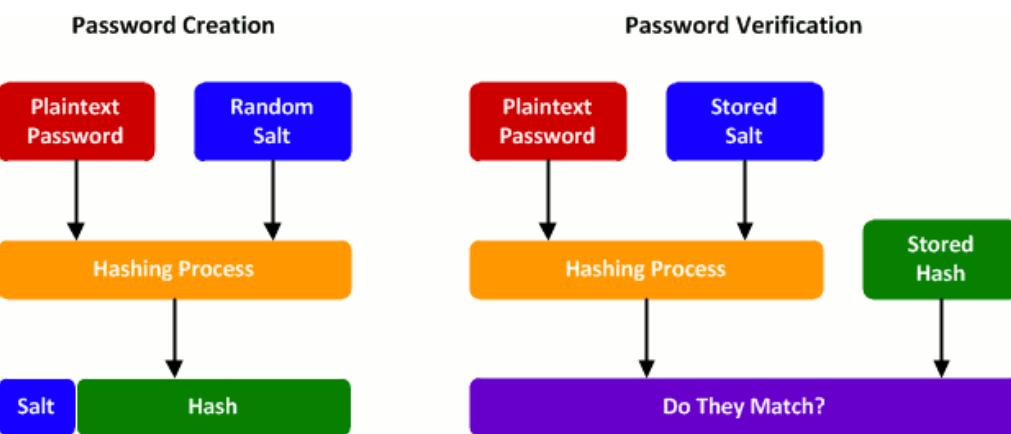
(Hash message authentication code) HMAC

התקפת Man in the Middle מאפשרת לצותת למידע בתנועה ולזייף אותו ואת ה- Hash כך לא ניתן לגלוות שהמידע שונה. HMAC פותר בעיה זו על ידי הוספה סיסמה (secret key) שידועה רק לשני הצדדים. ללא ידיעת הסיסמה ה- Hash לא ניתן לזיוף. HMAC זו שיטה שעובדת עם רוב האלגוריתמים.



זו טבלה מוכנה מראש שמתרגמת סיסמות לערכי hash. Rainbow tables. אם יש לנו hash של סיסמה, טבלה זו מאפשרת התקפה מהירה שנייה לביצוע Offline. באמצעות התקפה מוצלחת ניתן לגלוות את הסיסמה המתאימה להash. Ophcrack זה כלי תקיפה open source שמאפשר התקפה זו.

זו שיטה דומה מאד ל- HMAC במטרה להגן על hash של סיסמה. Salting



תרגיל: הכנס לאתר - <http://www.xorbin.com/tools/sha256-hash-calculator>
הכנס טקסט וצור Hash.

GnuPG – תוכנה חינמית לחתימה והצפונה.

www.freeformatter.com/hmac-generator.html

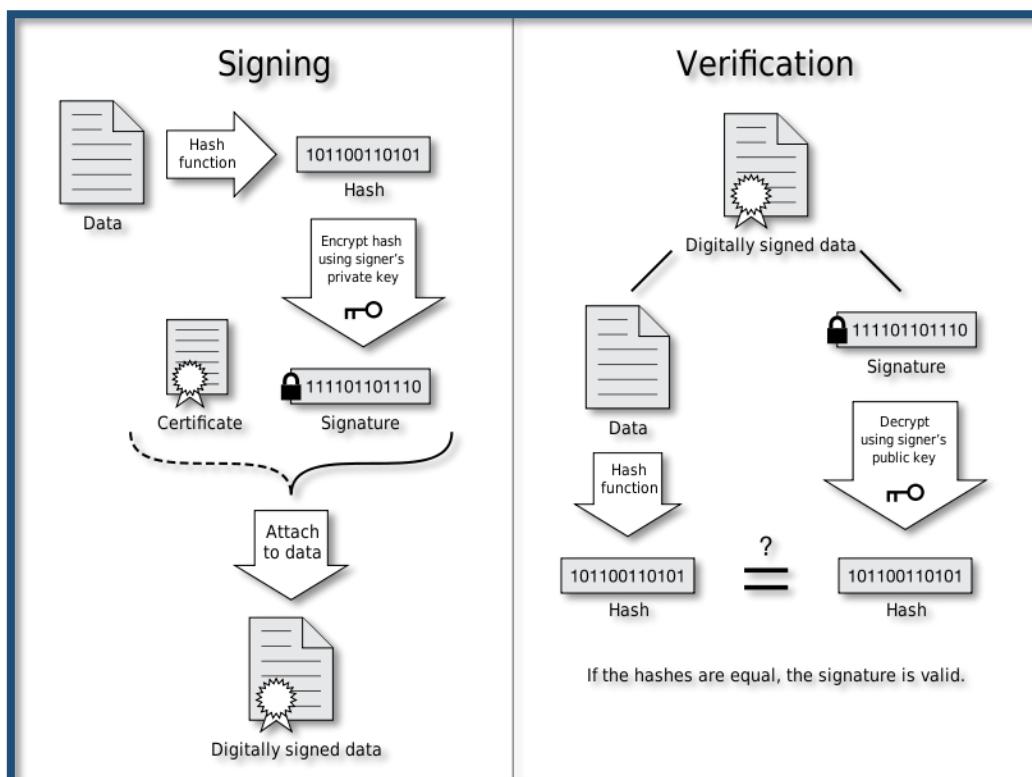
חתימה דיגיטלית (digital signature)

חתימה דיגיטלית זה Hash שהוצפן באמצעות Private-key. מטרת חתימה דיגיטלית להוכיח שהמידע לא שונה (integrity) ולהוכיח ממי הגיע המידע (non-repudiation).

שימוש בחתימה דיגיטלית כולל את התהליך הבא:

- ייצור Hash ממידע שהוא רצים לשולח.
- הצפתה ה- Hash באמצעות המפתח הפרטני ושליחתו ליעד.
- היעד מקבל את המידע, את ה- Hash המוצפן ואת המפתח הציבורי.
- היעד מסיר את הצפונה של ה- Hash באמצעות המפתח הציבורי וכך הוא יודע שהוא שלח לו את המפתח הציבורי מחזיק גם במפתח הפרטני (non-repudiation).
- היעד יוצר Hash מהמידע ומשווה אותו ל- Hash שנשלח לו. כך הוא מאמת שהמידע לא שונה בדרך (integrity).

רצוי שה- Public key יהיה משוויר ל certificate ב כדי שנitin יהיה לזרות את מחזיק ה- Public key. אם נשלחת גם ה- certificate, אז נבדקת זהותו של השולח מול שרת CA.



חשיבותה של חתימה דיגיטלית לא מוצפינה את הקובץ עצמו ולכון הקובץ חשוב

- קיימים שני אלגוריתמים לייצור חתימה דיגיטלית:
- RSA - מאוד נפוץ ומשמש סטנדרט מסחרי.
 - Digital Signature Algorithm (DSA) - משמש סטנדרט בamodel ארצות הברית.

Cryptanalysis

עם הזמן אנו לומדים אנשים עושים דברים שבבר נחשבו כבלתי אפשריים. בכל פעם שהוא מפתח אלגוריתם שנחשב כבלתי פריז, מישהו אחר מצליח לפזר אותו. Cryptanalysis זה אדם שתפקידו לחפש חולשות באלגוריתם שאנו משתמשים בכך לאפשר הסרת הצפנה ללא מפתח.

הנה כמה טכניקות לפריצת אלגוריתמים:

Exploiting Human Error

טעויות אנוש הם הסיבה העיקרית לנתקודות תורפה בהצפנה. לדוגמה: מייל שנשלח מוצפן וגם נשלח בטיעות לא מוצפן. אם לא-Cryptanalysis יש את שני המילים, הוא יוכל יהסית בקלות לפענה הצפנה של מיילים מוצפנים נוספים. דוגמא נוספת: המפתח מגיע בטיעות לידיים הלא נכונות.

Brute-Force Attacks

התקפה מבוצעת על ידי תוכנות בשם "password crackers". התוכנה מנסה באופן שיטתי כל סיסמה אפשרית עד ניחוש הסיסמה הנכונה. הניסיון יכול להתחיל בניחוש כל האופציות שקיימות בתו אחד ולאחר מכן לעבור לסיסמאות באורך שני תוים וכך מנסים את כל הצירופים האפשריים עד שאחד מהם עבד.

Frequency Analysis

בשיטת זו, בוחנים בלוק של מידע מוצפן במטרה למצוא מקטע מוצפן שחזור על עצמו. באנגלית המילים the, that, and, is very מוצאות. האותיות a ו-z גם מאוד נפוצות. עם הזמן, מציאת קטעים שחוזרים על עצמם מאפשרת לפענה את שיטת ההצפנה. שיטה זו לא עובדת על אלגוריתמים של ימינו.

Chosen Plaintext

זו התקפה שבה התקוף משווה בלוק של מידע מוצפן לטקסט לא מוצפן (לפי בחירת התקוף). המטרה לנסות לגלו את מפתח ההצפנה כדי לפענה הודעות נוספות.

Related Key Attack

התקפה זו דומה להתקפת Chosen Plaintext אלא שהיא שהפעם יש לתקוף את הטקסט המוצפן עם שני מפתחות שונים. התקפה זו מאוד גבוהה אם יש לתקוף את הטקסט הלא מוצפן בהתאם.

מבוא ל- IDS/IPS

נושאים עיקריים

היום נסקור את המושגים מאחוריו גליי והגנה בפני פריצה. אנו נבחן את ההבדל בין מערכת גליי פריצה (IDS) לבין מערכת למניעת חדירה (IPS), וכן להשוות בין IPS מבוסס רשות לבין IPS מבוסס מארח. נדונ גם בפרישות הרשות השונות הזרמיות עבור חיישני IPS. לבסוף, נגדיר כמה מהמנוחים הנפוצים הקשורים לטכנולוגיות IPS.

IDS לעומת IPS

מערכות איתור חדירות (Intrusion detection) ומערכות חיישני מניעה (prevention)
הן המתארות פעילות העוללה לפגוע בסודיות, באמינות ובזמןיות של משאבי
מידע, עיבוד ומערכות מחשב. החדרות יכולות לבוא לצורךות רבות ובהתקם פותחו
טכנולוגיות שונותiae לאיתור חדירות. לטכנולוגיה הראשונה שפותחה, IDS, היי יכולות חישה,
אבל יכולת קטנה לפעול על סמך מה שהוא זיהתה. באופן מסורתי, מערכות IDS יושמו כדי
לפקח באופן פסיבי על תבעורה ברשת. חיישןאפשר IDS מקבל עותקים של זרם
התבעורה ומנתח את תבעורה זו ולא את מנות המעברות בפועל. במצב לא מקוון, הוא
משווה את זרם התבעורה שנתרפס עם חתימות זדוניות ידועות, באופן הדומה לתוכנה
שבוחנת וירוסים. למרות שהתבעורה מנוטרת ואולי אפילו יופיע יוזה, לא נעשית פעולה על
מנות על ידי IDS. מצב זה של יישום IDS נקרא מצב מופקר או פסיבי - *promiscuous or passive* -
mode.

IPS פועל בטור זרם הנטונים כדי לספק הגנה מפני התקפות זדוניות בזמן אמת. מצב זה נקרא מצב מותם – **Inline mode**. שלא כמו IDS, IPS אינו מאפשר למנוע מעורר לצד האמין של הרשות אם הן חריגות. ל-IPS יש את יכולת לנתח את התעבורה משכבה קו הנטונים (שכבה 2) עד לשכבה היישום. לדוגמה, IPS יכול:

- לנתח את התעבורה השולטת במיפוי הקשר בין שכבה 2 לשכבה 3, כגון ARP ו-

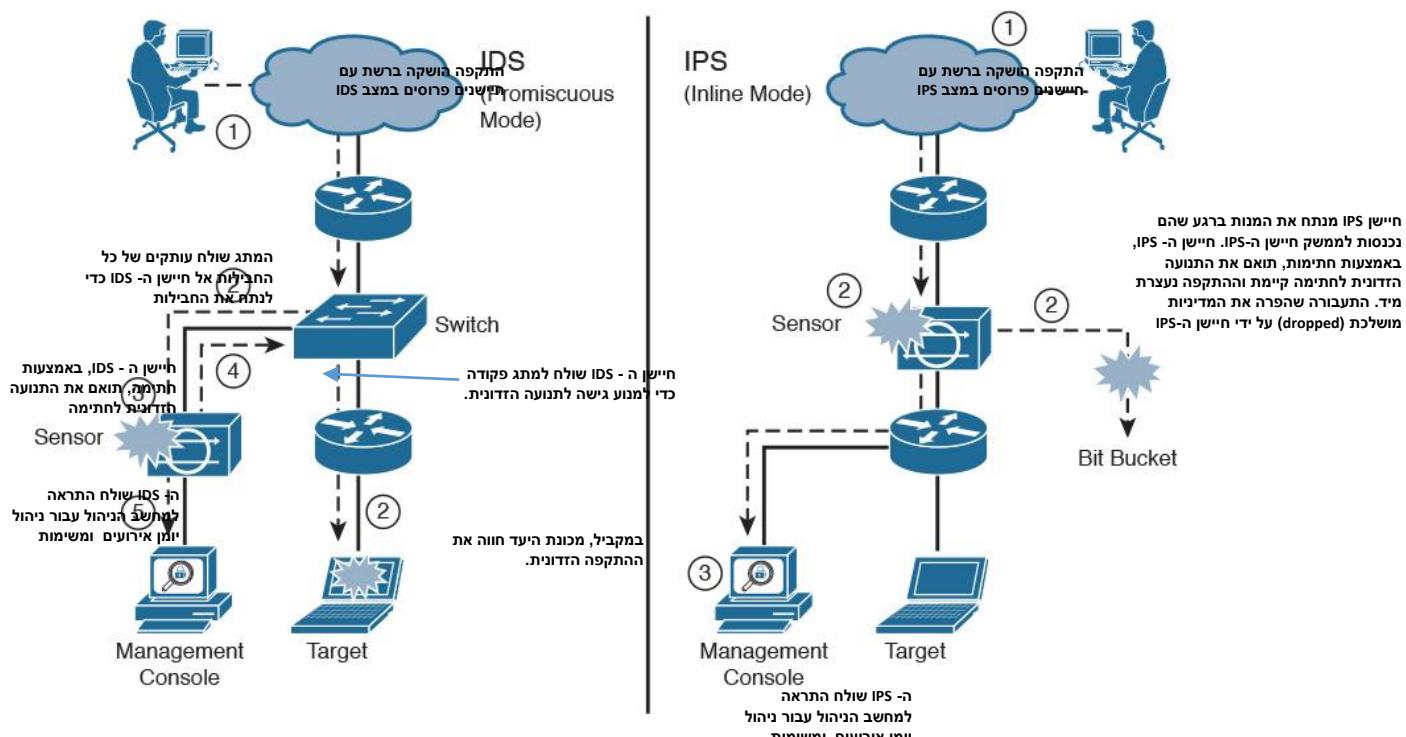
.DHCP

- לוודא שכללים של פרוטוקולי רשות כגון UDP, TCP, ICMP ועוד ממלאים על פי התקן.

- לנתח את ה"מטרען" של תעבורת המידע שיוצרים הישומים כדי לזהות דברים כגון

התקפות רשות, נוכחות של תוכנות זדוניות ותכונות שגויות של שירותי.

חישון נפרס במצב IDS וחישון נפרס במצב IPS



להלן השלבים המתרחשים כאשר התקפה הושקה בסביבה המפוקחת על ידי IDS:

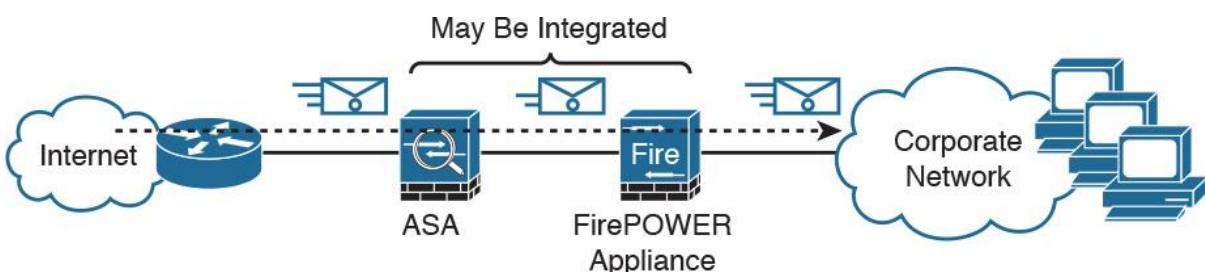
1. התקפה הושקה ברשות עם חישנים פרויסים במצב IDS

2. המתג שולח עותקים של כל החבילות אל חישון ה- IDS (מוגדר במצב מופקר, שמוסבר בהמשך בסעיף זה) כדי לנתח את החבילות. במקביל, מכונת היעד חווה את ההתקפה הזרדונית.
3. חישון ה - IDS, באמצעות חתימה, תואם את התנועה הזרדונית לחתימה.
4. חישון ה - IDS שולח למתג פקודה כדי למנוע גישה לתנועה הזרדונית.
5. ה- IDS שולח התראה למחשב הנהול עבור ניהול יומן אירועים ומשימות ניהול אחרות.

להלן השלבים המתרחשים בעת הפיגוע בהתקפה על סביבה שבוצעת IPS:

1. התקפה הושקה ברשות עם חישנים פרויסים במצב IPS (מוגדר במצב מוטבע Online), אשר מוסבר בהמשך בסעיף זה).
2. חישון IPS מנתח את המנות ברגע שהם נכנסות למסך חישון ה-IPS. חישון ה-IPS, באמצעות חתימות, תואם את התנועה הזרדונית לחתימה קיימת והתקפה נעצרת מיד. התעבורה שהפירה את המדיניות מושלכת (dropped) על ידי חישון ה-IPS.
3. חישון ה - IPS יכול לשולח התראה לתוכנת הנהול לצורך עבור ניהול יומן אירועים ומשימות ניהול אחרות.

האיור הבא מציג פריסת של IPS, שבו ה- Cisco ASA שולט בגישה בין הרשות הארגונית לבין האינטרנט, בהתאם על כתובות IP ויציאות (ports) של המקור והיעד, ואילו מכשיר ה- FirePOWER IPS שולט בגישה המבוססת על תוכן מנות.



טכנולוגיית IPS נפרשת על ידי חישנים, אשר ניתן לתאר אותן דרך אחת מהפעולות הבאות:

- מכשיר אשר תוכנן במיוחד כדי לספק שירותי IPS יעודיים (כפי שניתן לראות בתרשימים מעל).



- מודול המותקן בהתקן רשות אחר,

כגון ASA מתג או נתב.

X-5506 עם FirePOWER הוא

דוגמה לסוג זה של פריסת

כאשר טכנולוגיית איתור חדיות נולדה לראשונה, נעשה שימוש בשתי אסטרטגיות שונות במהותן:

- זיהוי אנומליה (משהו לא נורמלי): סוג זה של טכנולוגיה לומד בדרך כלל דפוסים של פעילות רשות רגילה, עם הזמן, מייצר פרופיל בסיס עבור רשות נתונה. שינויים מזהים פעילות חשודה על ידי הurecta דפוסי הפעולות החורגים מן הבסיס הזה.
- זיהוי מבוסס-כללי: תוקפים משתמשים בטכניקות שונות כדי לפולש ולפגוע במערכות. טכניקות שונות של מעקב מרחוק משמשות לפולישה לעיתים קרובות. כמו שיטות מעקב ותקיפה דפוסים ידועים שבאמצעותם ניתן לזהות את המעקב או התקיפה. גלאי פעילות זדונית בדרך כלל מנתחים תנווה ברשות בזמן אמת באמצעות מסד נתונים של כלליים, כדי לקבוע אם מתרחשת פעילות חשודה.

מערכות IPS מודרניות משלבות זיהוי אנומליה וגילוי המבוסס על כלליים, כמו גם טכנולוגיות חדשות ומתקדמות אחרות, כגון מוניטין, הקשרים, מתאמים אירופים ושירותים מבוססי ענן, כדי להבטיח הגנה על הרשות.

IPS מבוסס מארח ו-IPS מבוססי רשות

<u>IPS מבוססי רשות</u>	<u>IPS מבוסס מארח</u>
'תרונות:'	
ארכיטקטורה זו ניתנת להרחבה בצורה הרבה יותר גבוהה	מסתמך על "SOCNIM/CHIYSHNIIM" שהוצבו על מערכות קרייטיות בארגון
אינו יכול בדרך כלל "לראות" זרמי תעבורת מוצפנים	יכול לזהות חדיות המבוצעות באמצעות תקשורת מוצפנת
	יכול לנתח פעילותית בתוך מערכת הפעלה המארחת לאחר קבלת התעבורה והפענוח שלה לפניהם הצפנה התעבורה והשליחה של הלאה

	מתאים היטב לדיהוי של פעילות שאינה מייצרת תעבורת רשת
	יכל בקלהות לזהות שינויים בשלמות של קבצים חיוניים על ידי השוואת קובץ hashes קיימ לקובץ hashes הידוע כקובץ אמיתי.
	חסרונות:
	הוא דורש כי סוכנים יהיו מותקנים על כל מכונה שיש לפקח עליה
	ניהול מרוחק של סוכנים אלה יכולים להיות אתגר
	нетל עיבוד נוספת נסוף
	נדרשת לאינטראקטיבית אינטראקטיבית עם תוכנת הלוקה

ישנו שני סוגי IPS : IPS מבוסס רשת ו-IPS מבוסס מארח. באופן מסורתי IPS, מבוסס מארח הסתמך על "סוכנים" שהוצבו על מערכות קריטיות בארגון. הסוכנים עיקבו אחר היבטים שונים של הפעולה של המארח, בחיפוש אחר סימניים לעבירות חשודה. הסוכנים ידווו על גילוי למסוף ניהול מרכזי או יכתבו דוח פעילות על האירועים במערכת. גישה מודרנית יותר היא למקם את העבודה של ה-IPS בענן ולמקם חיבור פשוט על המארח כדי לגשת להגנה מבוססת הענן. ארכיטקטורה זו ניתנת להרחבה בצורה הרבה יותר גבוהה, המאפשרת את ההגנה על כל המערכות ברשת.

IPS מבוסס מארח יכול לזהות חדירות גם אם הן מתבצעות באמצעות תקשורת מוצפנת. **IPS** מבוסס רשת אינו יכול בדרך כלל "לראות" זרמי תעבורת מוצפנים, אך IPS מבוסס מארח יכול לנתח פעילותות בתחום המערכת המארחת לאחר קבלת התעבורת והפענו שלה **לפני** הצפנה התעבורת והשליחה של הלאה. מארח מבוסס IPS מתאים היטב לדיהוי של פעילות שאינה מייצרת תעבורת רשת. לדוגמה IPS מבוסס מארח עשוי לזהות פעילות כגון הפרת מדיניות או חדירה פיזית למערכת, כגון משתמשים לא מורשים המנסים לגשת לנתונים מקומיים. מארח מבוסס IPS יכול בקלהות לזהות שינויים בשלמות של קבצים חיוניים על ידי השוואת קובץ hashes קיימ לקובץ hashes הידוע כקובץ אמיתי.

-IPS מבוסס מארח יש כמה חסרונות, עם זאת. לדוגמה, הוא דורש כי סוכנים יהיו מותקנים על כל מכונה שיש לפקח עליה. במקרה, ניהול מרוחק של סוכנים אלה יכולים להיות אתגר. כמו כן, מנהלי מערכת עשויים להיות מודאגים עם הצבת נתל עיבוד נוספת על מערכות שכבר מונצחות בכבדות או

מכשירים ניידים פשוטים. לבסוף, סוכני IPS מסויימים מבודדים מארח יכול להציג למשתמש הודעות קופצות, ולאלץ את המשתמש לאינטראקטיבית אינטראקטיבית עם תוכנת הלקוח. הדבר עלול לגרום מחוויות המשתמש הכלולות, וכתוצאה לכך משתמשים משכיתים את הסוכן (אם יש להם זכויות ניהול) או מתקשרים לתמיכה טכנית.

אפשרויות פרישה של IPS

קיימות מספר אפשרויות לפרישת חישון רשות במצב מופקר או פסיבי. אחת השיטות הנפוצות ביותר היא להגיד את התוכנה (SPAN) במתג מסווג Cisco Catalyst Switched Port Analyzer (SPAN) במתג מסוג IDS ולחבר את חישון ה-IPS לפורט שהגדכנו. חישון ה-IPS יראה עותקים של כל המסגרות התואמות את תצורת הלכידה של קונפיגורציה ה-SPAN כפי שהוגדרה על הפורט במתג. בתרחיש ה-IDS באירור הבא. מגבלה אחת של פתרון SPAN היא שיציאת היעד של SPAN עשויה להיות מוגזמת. פתרון הוא להשתמש ברצף רשות. הרצת מוכנס ישרות בין שני התקנים. הוא מספק קישוריות דו-כיוונית מלאה בין שני המכנים, ומאפשר לIDS להקיש ממש על זרימת התנועה. איור 3-6 מראה היכן תבוצע פרישת רשות.

Firewall Technologies

Firewall משמש כאחד מקווי ההגנה הראשונים. מטרתו הבסיסית, לבדוק רשות אחת (trusted zone) מרשת אחרת (untrusted zone). הוא מבצע זאת על-ידי החלטה איזה תובורה רשאית לעבור ולאיזה כיוון וזואת לפי המדיניות שנקבעה. Firewall מסתמך על סידרת חוקים שמתייחסים לתובורה יווצרם את מדיניות ה-Firewall. Firewalls יכולים להיות תוספת תוכנה עבור שירותי ותchnות עבודה או שהם יכולים להיות מערכות עצמאיות כחומרה בלבד (Appliances) כלומר התקנים עצמאיים שפועלם באופן עצמאי במידה רבה ודורים פחות תחזקה ותמיכה מאשר מוצר מבוסס שרף.

קיימות שיטות שונות באמצעות Firewall יכול לסנן מידע שעובר ברשות.

• Stateless Packet Filtering

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו וועבדו על ידי ערן גזית
لتשומת לכם החוברת מכילה חומרה לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

- Stateful Inspection
- Application Awareness
- Proxy Firewalls

Stateless Packet Filtering Firewall

סינון packets שעוברים דרך firewall על בסיס:

- Source/Destination Address
- Source/Destination Port

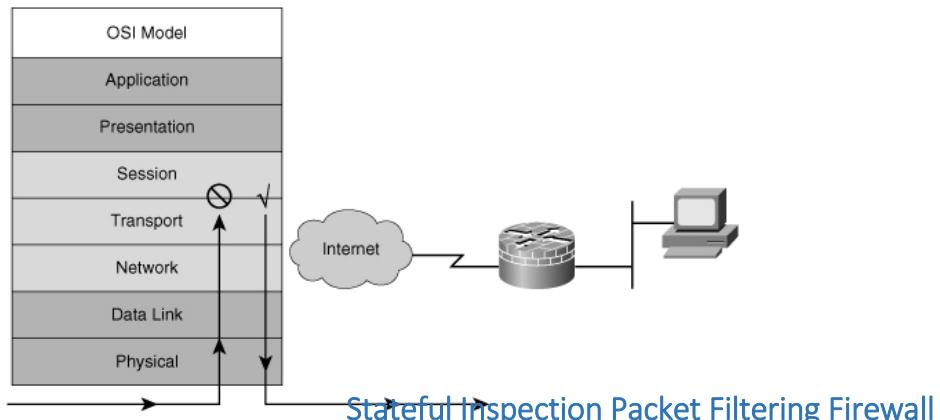
הבדיקה מתבצעת בשכבה הרכשת (IP), שכבת העברת (Port) כאשר כל packet עומד בפני עצמו ואין התייחסות לטעורה שעוברת בעבר או טעורה שעוברת עכשו. שיטה זו לא מזהה התקפות רבות ולכן זר טכנולוגיה לא כל כך בטוחה ונחשבת כסינון ראשוני.

יתרונות

- הבדיקה השטחית מאפשרת ביצועים מהירים.
- לא בודק את תוכן ה- Packet Filtering ולא בעיות תאימות עם תוכנות.

חסרונות

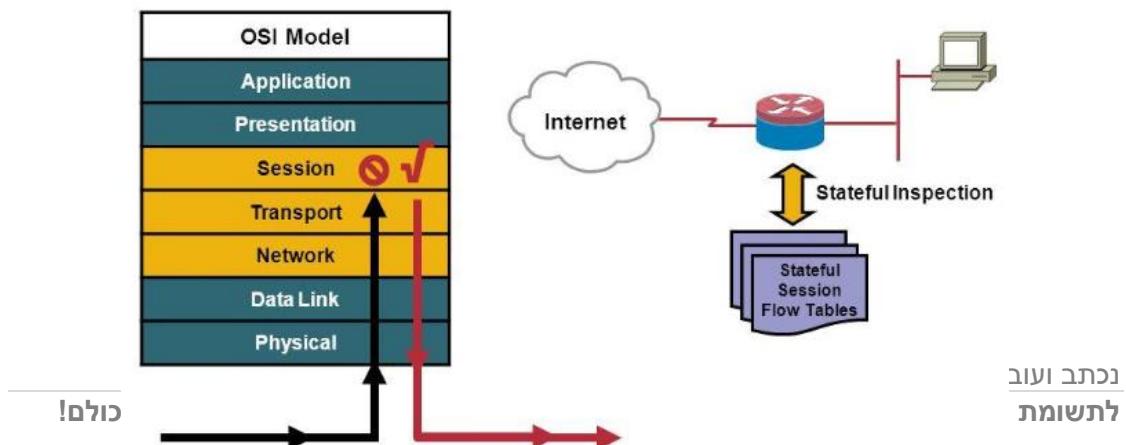
- בגלל שאין בדיקה של תוכן החביליה, רמת אבטחה נמוכה ולכן תוקף יכול להשתמש ב- port פותח למטרות שונות ממה שהוא מיועד.
- לא מסתמן על מידע שעבר בעבר (logs) ולכן לא ניתן לעצור התקפות מתחככות.



Stateful Inspection Packet Filtering Firewall

ה- Firewall עוקב אחר כל connection שעובר דרכו ושומר את המידע הזה בטבלאות מעקב.

כך ה- Firewall יודע איזה packets יוצאו ועל בסיס זהאפשר למידע לחזור. ה- Firewall זוכר את המידע על החבילות שעברו בעבר ולכן יש לו תומנת מצב ברורה יותר לגבי תקינות החביליה ויש לו יכולת גבואה יותר לזיהות ולהסום התקפות.



נכחד ועובד
لتשומות

Application Awareness Firewall

הדור האחרון של התקפות מכוון ישירות כלפי תוכנות ולכון שכבת האפליקציה סובלת מכמות ההתקפות הגדולה ביותר. הסיבות הן:

- שכבה זו כוללת את כמות פרוטוקולים הגדולה ביותר.
- שכבת האפליקציה זו השכבה המורכבת ביותר ולכון קשה להגן עליה.

כדי להגן על Application Layer צריכים לפעול בכמה מישורים:

1. בדיקה האםpacket עומד בסטנדרטים של הפרוטוקול שלו הוא ש"יר

לדוגמה: לפני הסטנדרט אין בheader שלpacket מידע HTTP מידע ביןארי.

על ידי הכנסת מידע ביןארי לheader ניתן להתקיף את השירות.

בדיקות שלא קיימים מידע ביןארי ב- header מונעת התקפה מסווג זה.

2. וידוי התאמנה בין סוג הפרוטוקול לשימוש שנעשה בו.

יתכן שהדריך בה משתמשים בפרוטוקול לא תואמת לציפיות מאותו פרוטוקול.

דוגמא: תקשורת מסוג peer-to-peer משמשת להעברת הודעות/קבצים מסוות פנים

דרך הרשת. למרות שיש הרבה פרוטוקולים שימושיים לתקשורת כזו, ניתן להקים

תקשורת כזו על בסיס HTTP (80). במקרה שבדרכו כלל 80 port פתוח רצוי לחסום

אותו לצורכי peer-to-peer.

3. חסימת data מזין. גם אם תקשורת עומדת בסטנדרטים ומתאימה לצורה בה

משתמשים בפרוטוקול, עדין יכול להיות שהמידע שבתווך הpacket מזין למערכת.

דוגמא: משתמשים יכולים לפתח script מזין שמוחבא בתוך email או מוסווה ב

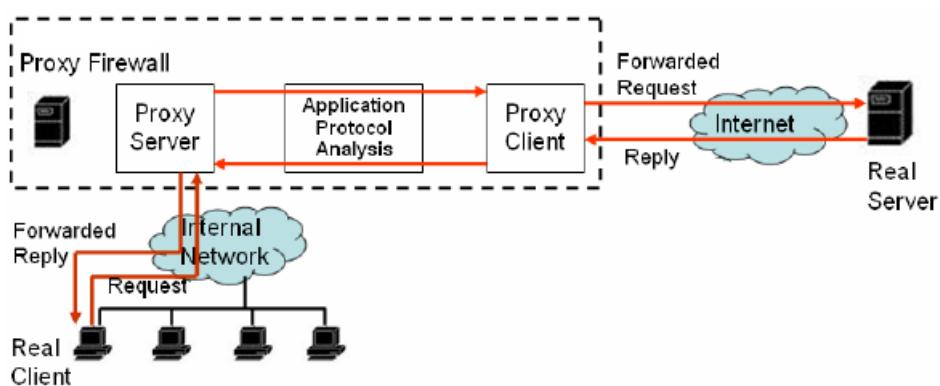
.link

Proxy Firewalls

זהו Firewall שמשמש כמיטווח ונמצא בין כל connection, אך אין קשר ישיר בין המחשבים בתוך הארגון למחשבים מחוץ לארגון.

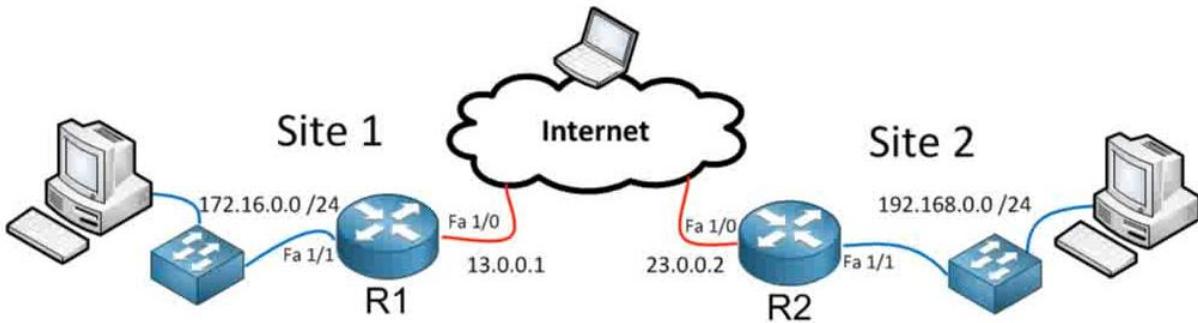
Proxy Firewalls יכולים לעבוד בשני עמקים:

- (Session layer) – עובד בשכבה חממה (Circuit-level proxies)
- (application layer) - עובד בשכבה שבע (Kernel proxy Firewall)



גרסה מצומצמת IPsec Site to Site VPN

מטרת VPN IPsec, יצירת קשר ישיר ומאובטח בין שני סניפים.



מגן על המידע בדרכים הבאות:

- **סודיות** (Confidentiality) באמצעות הצפנה. פרוטוקול ברירות המחדל הוא IPsec HMAC Hashing.
- **שלמות המידע** (Data Integrity) באמצעות HMAC Hashing.
- **זיהוי** (Authentication) באמצעות Pre-Shared secret key (PSK) או באמצעות RSA signature.
- **הסימת שידור חוזר שלpacket** (Anti-Replay) (packet).

IKE (Internet Key Exchange) protocol

לפרוטוקול IKE יש כמה תפקידים:

- **Automatic key generation** - מושתמש ב- Diffie-Hellman algorithm כדי ליצור מפתחות.
- **Automatic key refresh** - החלפת מפתח לפי זמן או לפי כמות מידע.
- **Negotiation of the security association (SA)** - ביצוע אימות אוטומטי בין הצדדים.

IKE phase 1

IKE Phase 1 Tunnel היא ערך תקשורת מאובטח שמאפשר החלפת מידע בצורה פרטית בין שני VPN Peers. הקמת IKE Phase 1 Tunnel כוללת שלושה שלבים.

שלב ראשון

ביצוע בינה לבין נושאים (policy sets):

- Hashing
- Authentication (קובע האם בהזדהות הם משתמשו בסיסמה או בתעודת).
- Diffie-Hellman Groups (קובע את חזק המפתח).
- קובע כמה זמן IKE phase 1 יהיה פתוח, כברירת מחדל זה יום אחד.
- (קובע את סוג ההצפנה הסימטרית).

שלב שני

ניהול מפתחות (Key Management)

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

הגדרת מפתחות סימטריים והצפנתם באמצעות אלגוריתם אסימטרי (Diffie-Hellman).
Asymmetric Algorithm Diffie-Hellman key exchange algorithm
הו שיצר בזורה.
דינמיות Symmetric keys המשמשים להצפנה המיידע.
בנוסף האלגוריתם משמש להעברה מאובטחת של המפתחות.

שלב שלישי:

ביצוע הזרחות בין הצדדים והקמת ערך תקשורת מאובטח.

IKE יכול לעבוד בשני מצבים:

Main Mode

בשיטת זו נשלחים יותר packets וזהות הצדדים לא נשפטת, لكن שיטה זו יותר מאובטחת.
הקמת IKE Phase 1 Tunnel מורכבת משלושה שלבים:

Aggressive Mode

בשיטת זו נשלחים פחות packets אך זהות הצדדים חשופה, لكن שיטה זו פחות מאובטחת.

(IPSec tunnel) IKE phase 2

נעשה שימוש ב- IKE phase 2 כדי להקים את tunnelトンNEL דרכו זורמים בצורה מאובטחת הנתונים של המשתמשים.

IKE phase 2 מבצע Negotiation לגבי ארבע נושאים:

- Hashing
- Diffie-Hellman Groups (phase 1).
- Life Time - קובע כל כמה זמן צריך ליצור מפתח חדש. לפי זמן או לפי כמות הנתונים שעברה.
- Encryption (קובע את סוג ההצפנה הסימטרית).

בין שני הצדדים חייבת להיות התאמה בכל הפרמטרים מלבד ה- Life Time שיכל להיות שונה.



לכיהות הנדסאים Virtual Private Network

מנחרות Site to Site מסוג IPSec משמשות כדי לאפשר העברת מאובטחת של נתונים, כולל וידאו בין שני אתרים (למשל משרדים או סניפים). מנהרת VPN נוצרת ברשות הציבורית באינטרנט ומודפנת באמצעות מספר אלגוריתמים מתקדמים להצפנה על מנת לספק את סודיות הנתונים המועברים בין שני האתרים.

מסמך זה יציג כיצד להציג שני נתבי סיסקו כדי ליצור מנהרה קבועה מאובטחת של VPN דרך האינטרנט, באמצעות פרוטוקול (IP) Security (IPSec). אנו מניחים שתwo נתבי סיסקו יש כתובת IP ציבורית סטטית.

מנהרת VPN יכול גם להיות מוגדרת באמצעות GRE (Generic Routing Encapsulation) עם GRE מנהרות עם GRE הן מנהרות המפשtot מאד את התצורה והניהול של מנהרות VPN. לבסוף, מנהרות מסוג DMVPNs - מגמת VPN חדשה מספקת גמישות רבה וכמעט ללא תקורה ניהולית.

מנהרת IPSec(IP Security Association and Key Management Protocol) ISAKMP (Internet Security Association and Key Management Protocol) ISAKMP לבנייה והצפנה של מנהרת VPN. IKE (Internet Key Exchange), המכונה גם VPN, הוא פרוטוקול המשא ומתן המאפשר לשני המארחים להסכים על איך לבנות את החיבור המאובטח על ידי IPsec. המשא ומתן של ISAKMP מורכב משני שלבים: שלב 1 ושלב 2.

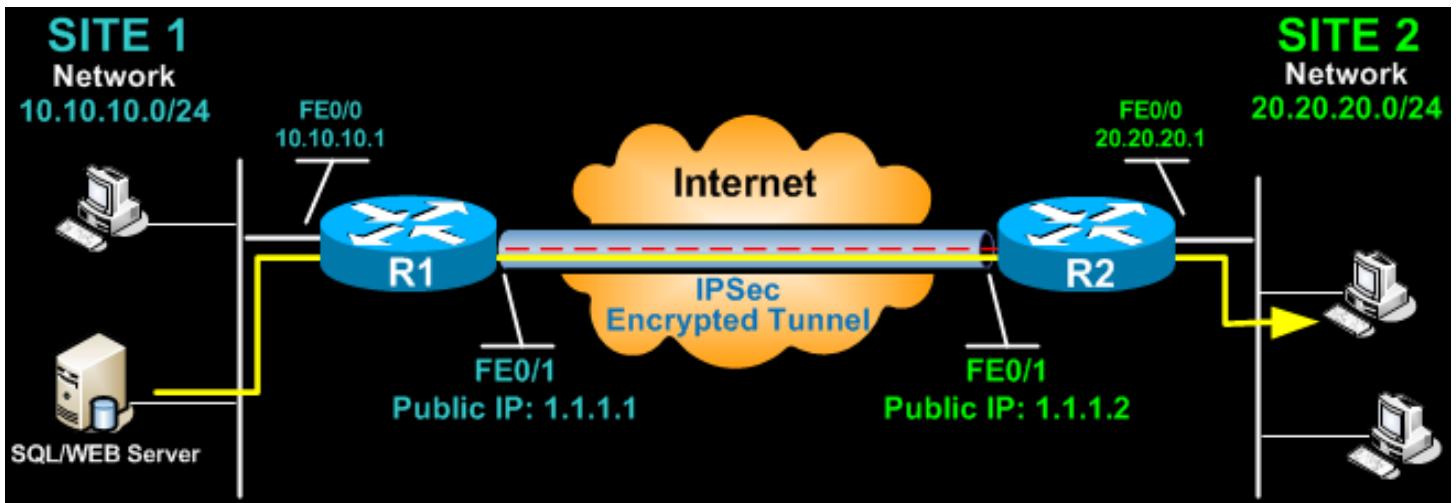
שלב 1 יוצר את המנהרה הראשונה, אשר מגינה מאוחר יותר על הودעות משא ומתן של ISAKMP. שלב 2 יוצר את המנהרה ש מגינה על הנתונים. לאחר מכן נכנס לפעולת IPSec כדי להצפין את הנתונים באמצעות אלגוריתמים של הצפנה ועל מנת לספק איזמות, הצפנה ושירותי Anti-replay.

כדי לעזר לנו להפוך את ההסביר לקל למשך, אנחנו נפצל אותו לשני שלבים הנדרשים כדי לאפשר למנהרת VPN IPSec לעבוד.

השלבים הבאים הם:

- (1) הגדרת ISAKMP (שלב 1)
- (2) הגדרת IPSec (שלב 2, ACLs, Crypto MAP)

לדוגמה, בין שני סניפים של חברת קטנה, (אתר 1 ואתר 2). שני נטבי הסניפים מתחברים לאינטרנט ויש להם כתובת IP סטטית שהוקצתה על ידי ספק שירותי האינטרנט שלהם, כפי שמצוג בתרשימים:



.20.20.20.0/24 עם רשת פנימית של 10.10.10.0/24, ואילו אתר 2 מוגדר עם רשת 20.20.20.0/24. המטרה היא לחבר את רשתות ה-LAN בצורה ולאפשר תקשורת מלאה ביניהם, ללא כל הגבלות.

הגדרת (ISAKMP - (שלב 1 ISAKMP (IKE

IKE קיים רק כדי להקים (IPsec) SAs (Security Association). לפני זה קורה, IKE חיב לנהל משא ומתן על (ISAKMP SA) היחסים עם העמיתים. כדי להתחיל, נתחל ל לעבוד על הנטב של אתר 1 (R1).

הצעד הראשון הוא קביעת מדיניות ISAKMP שלב 1:

1

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)# encr 3des
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# lifetime 86400
```

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומתיכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

הפקודות מגדירות את המאפיינים הבאים:

3DES - שיטת הצפנה שתשתמש עבור שלב 1.

MD5 – אלגוריתם הגיבוב

Pre-share – השתמש בפתח משותף מראש כשיטת האימוט

group 2 - קבוצה 2 - **קבוצת דיפי-הילמן (Diffie-Hellman)** לשימוש

86400 – זמן החיים של מפתח השיחה. מבוטא ערך של קילובייט (לאחר כמות X של תנועה, לשנות את המפתח) או שניות.

יש לציין כי מדיניות ISAKMP שלב 1 מוגדרת באופן גלובלי. שימושות הדבר היא שאם יש לנו חמשה אתרים מרוחקים שונים והגדנו חמישה גדרות שונות של 1 ISAKMP Phase (אחד עבור כל נתב מרוחק), כאשר הנתב שלנו מנשה לניהל משא ומתן עבור VPN בכל אתר שהוא, הוא ישלח את כל חמישה ההגדרות וيشתמש בהתקדמות הראשונה המתקבלת בשני הקצוות.

כעת אנחנו הולכים להגדיר את מפתח המשותף מראש **למטרת אימוט עם העמית שלנו** (נתב R2) באמצעות הפקודה הבאה:

```
R1(config)# crypto isakmp key firewallcx address 1.1.1.2
```

ה מפתח המשותף מראש (Pre Shared Key) של העמית מוגדר כ- "firewallcx" כתובות IP הציבורית שלו היא 1.1.1.2. בכל פעם ש-R1 ינסה להקים מנהרת VPN עם R2 זהו המפתח המשותף מראש שהוא ישתמש בו (1.1.1.2).

הגדרת IPSec

כדי להגדיר את IPSec علينا להגדיר את הפרטים הבאים לפי הסדר:

- יצירת IPSec Transform
- יצירת ACL מורחב
- יצירת מפתח Crypto
- החלט מפתח crypto למסמך

2

יצירת המירה (Transform) של IPSec ISAKMP מדיניות שלב (2)

השלב הבא הוא ליצור סט המירה המשמש להגנה על הנתונים שלנו. אנחנו קוראים לסט זה בשם TS:

```
R1(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

הפקודה הנ"ל מגדירה את הדברים הבאים:

ESP-3DES - שיטת הצפנה

MD5 - אלגוריתם גיבוב

3

יצירת ACL מורחב

השלב הבא הוא ליצור רשימה גישה ולהגדיר את התעבורה שהיא רצים לנtab לעבר דרך מנהרה ה-VPN. בדוגמה זו, זה תהיה תעבורה מרשת 10.10.10.0/24 ל-20.20.20.0. רשימת גישה שמנגד'רים לתעבורת VPN נקראות לפעמים **.crypto access-list**

```
R1(config)# ip access-list extended VPN-TRAFFIC
```

```
R1(config-ext-nacl)# permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255
```

הערה: ניתן גם להגדיר את רשימת הגישה באמצעות רשימת גישה נוספת שמיית!

ראה דוגמא:

```
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
```

4

יצירת מפתח crypto

מפתח Crypto היא שלב האחרון של ההגדרה שלנו ומחבר את תצורת IPSec, תצורת ACL-ISAQMP, שהוגדרה ו-IPSec שהוגדרו לפני כן.

Crypto map =

1 + 2 + 3

```
R1(config)#crypto map CMAP 10 ipsec-isakmp
```

```
R1(config-crypto-map)# set peer 1.1.1.2
```

```
R1(config-crypto-map)# set transform-set TS
```

```
R1(config-crypto-map)# match address VPN-TRAFFIC
```

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

73

קראונו למפת ה- CMAP שלנו.-tag `crypto ipsec isakmp` אומר לנodb שMapView זו היאMapView הצפינה של IPsec. למרות שיש רק עמידת אחד שהוצאה בMapView הצפינה זו (1.1.1.2), ניתן לקבל מספר רב של עמידות בתחוםMapView הצפינה נתונה.

החלתMapView למשק הציבורי

השלב האחרון הוא להחיל אתMapView crypto על המשק היוצא של הנodb. כאן, המשק היוצא הוא .FastEthernet 0/1

```
R1(config)#interface FastEthernet0/1
R1(config-if)#crypto map CMAP
```

שים לב שאתה יכול להקצות רקMapView אחת למשק.

ברגע שאתה מימוש mapView במשק, אתה מקבלים הודעה מהנodb המאשר כי `isakmp` פועל: ."ISAKMP is ON"

בשלב זה, השלכנו את הגדרת ה- IPSec VPN בנodb 1.

עתה אתה עברים לנodb 2 כדי להשלים את הגדרת ה- VPN. ההגדרות עבור הנodb 2 זהות, כאשר ההבדל היחיד הוא כתובות IP של עמידות ורשימות הגישה:

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)# encr 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 86400

R2(config)# crypto isakmp key firewallcx address 1.1.1.1
R2(config)# ip access-list extended VPN-TRAFFIC
R2(config-ext-nacl)# permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255

R2(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

```

R2(config)# crypto map CMAP 10 ipsec-isakmp
R2(config-crypto-map)# set peer 1.1.1.1
R2(config-crypto-map)# set transform-set TS
R2(config-crypto-map)# match address VPN-TRAFFIC

R2(config)# interface FastEthernet0/1
R2(config-if)# crypto map CMAP

```

תרגום כתובות (NAT) ומנהרות VPN של IPSec

תרגום כתובת רשת (NAT) **חייב** להיות מוגדר כדי לספק גישה לאינטרנט לマארחים פנימיים. בעת קביעת ההגדרות של מנהרת VPN מסווג Site-to-site, חובה להנחות את הנטב לא לבצע NAT על מנת המיועדות לרשת VPN המרוחקת.

זה נעשה בקלות על ידי הוספת הצהרת Deny בתחילת רשימת הגישה NAT כפי שמצוג להלן:

:1 עברו הנטב של אתר

```

R1(config)#ip nat inside source list 100 interface fastethernet0/1 overload
R1(config)#access-list 100 remark --[Define NAT Service]--
R1(config)#access-list 100 deny ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255
R1(config)#access-list 100 permit ip 10.10.10.0 0.0.0.255 any
R1(config)#access-list 100 remark

```

עבור הנטב של אתר 2:

```
R2(config)# ip nat inside source list 100 interface fastethernet0/1 overload  
R2(config)# access-list 100 remark =[Define NAT Service]=  
  
R2(config)# access-list 100 deny ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255  
  
R2(config)# access-list 100 permit ip 20.20.20.0 0.0.0.255 any  
  
R2(config)# access-list 100 remark
```

הפעלת אינומת מנהרת ה- VPN

בשלב זה, סימנו את ההגדרות שלנו, ומנהרת ה- VPN מוכנה להפעלה. כדי להפעיל את המנהרה, אנחנו צריכים לכפות כי מנה אחת תחצה את ה-VPN וזה יכול להיות מושג על ידי פינג מנטב אחד למשנהו:

```
R1#ping 20.20.20.1 source fastethernet0/0  
Type escape sequence to abort.  
  
Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:  
  
Packet sent with a source address of 10.10.10.1  
  
.!!!!  
  
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/47/48 ms
```

הפינג הראשון קיבל `out time`, אבל השאר קיבלו תשובה, צפוי. הזמן הדרוש כדי להעלות את המנהרת VPN הוא לפחות יותר מ 2 שניות, מה שגורם לפינג הראשון לקבל `out time`.

כדי לאמת את מנהרת ה- VPN, נשתמש בפקודה `show crypto session`:

```
R1#show crypto session  
Crypto session current status  
  
Interface: FastEthernet0/1  
  
Session status: UP-ACTIVE  
  
Peer: 1.1.1.2 port 500
```

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומתיכם החוברת מכילה חומר ללימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

IKE SA: local 1.1.1.1/500 remote 1.1.1.2/500 Active

IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 20.20.20.0/255.255.255.0

Active SAs: 2, origin: crypto map

ולסיכום

1. קביעת מדיניות ISAKMP שלב 1
2. יצירת המרה (Transform) של IPsec (ISAKMP) מדיניות שלב 2
3. יצירת ACL מורחב
4. יצירת מפת crypto
5. החלטת מפת Crypto למשק הציבורי

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 2
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.226
Branch(config)#
Branch(config)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
Branch(cfg-crypto-trans)# exit
Branch(config)#
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Branch(config)#
Branch(config)# crypto map HQ-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Branch(config-crypto-map)# set transform-set HQ-VPN
Branch(config-crypto-map)# set peer 209.165.200.226
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# int s0/0/1
Branch(config-if)# crypto map HQ-MAP
Branch(config-if)# ^z
Branch#
```

① **ISAKMP Policy**
Specifies the initial VPN security details

② **IPsec Details**
Specifies how the IPsec packet will be encapsulated

③ **Crypto ACL**
Specifies the traffic that will trigger the VPN to activate

④ **VPN Tunnel Information**
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL

⑤ **Apply the Crypto Map**
Identifies which interface is actively looking to create a VPN

- .4. בחר מ בין ההיגדים הבאים את היגד הנכון לגבי פרוטוקול Diffie-Hellman .
1. פרוטוקול Diffie-Hellman משתמש בהצפנה סימטרית כדי להצפין נתונים בערך תקשורת לא מאובטח
 2. במהלך שלב 1 IKE Phase 1 נעשה שימוש בפרוטוקול Diffie-Hellman כדי לבצע אימוחת לנתב העמית
 3. פרוטוקול Diffie-Hellman הוא אלגוריתם המבצע בדיקה של שלמות הנתונים
 4. פרוטוקול Diffie-Hellman מספק דרך שבה שני נתבים עמייתים יוצרים מפתח סודי משותף הידוע רק להם

התשובה הנכונה 4.

קבוצות פרוטוקול Diffie-Helman

הוא **פרוטוקול שיתוף מפתח אסימטרי** הראשון שהוצע על ידי ויטפילד דיפי ומרטין הלמן ב-1976 כדי לפתרור את בעיית הפצת המפתחות. הפרוטוקול מאפשר לשני צדדים שלא נפגשו מעולם ואינם חולקים ביניהם מפתח הצפנה משותף כלשהו מראש, להעביר אחד לשני מעל גבי ערוץ פתוח (שאינו מאובטח) מפתח הצפנה ח כלשהו כך שאיש מלבדם אינו יודע מהו.

להלן רשימה של הקבוצות השונות

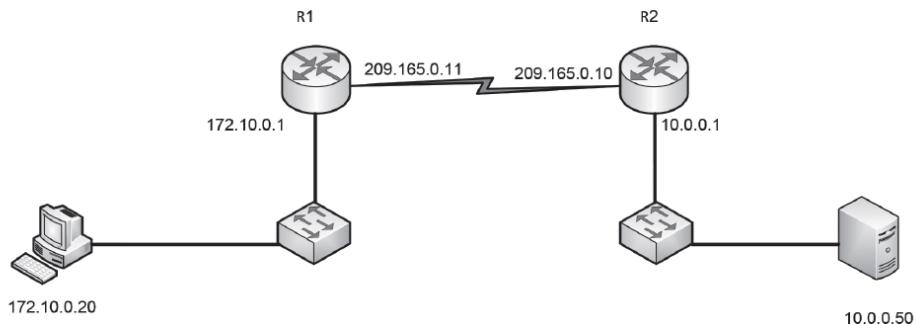
Parameter	IKE Phase 1 (IKE SA)	IKE Phase 2 (IPSec SA)
Diffie Hellman Groups	<ul style="list-style-type: none"> ▪ Group2 (1024 bits) (default) ▪ Group1 (768 bits) ▪ Group5 (1536 bits) ▪ Group14 (2048 bits) ▪ Group19 (256-bit ECP) ▪ Group20 (384-bit ECP) 	<ul style="list-style-type: none"> ▪ Group2 (1024 bits) (default) ▪ Group1 (768 bits) ▪ Group5 (1536 bits) ▪ Group14 (2048 bits) ▪ Group19 (256-bit ECP) ▪ Group20 (384-bit ECP)

ה. איזו הגדרה נדרשת לשם שימוש ב프וטוקול IKE עבור IPsec ?

- crypto map map1 100 ipsec-manual .1
- crypto map map1 100 ike-dynamic .2
- crypto map map1 100 ipsec-isakmp .3
- crypto map map1 100 isakmp-key .4

התשובה הנכונה 3

א. התבונן באיוור שלפניך:



איור א' לשאלת 6

קבע איזו מבין הגדרות הבאות תגדיר PSK על שני הנתבים שבאיור.

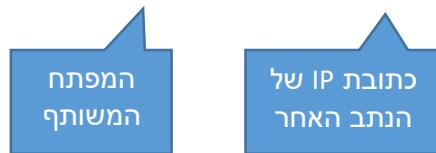
- .1
R1(config)# crypto isakmp key tikshuv address 209.165.0.11
R2(config)# crypto isakmp key cisco address 209.165.0.10
- .2
R1(config)# crypto isakmp key tikshuv address 209.165.0.10
R2(config)# crypto isakmp key tikshuv address 209.165.0.11
- .3
R1(config)# crypto isakmp key tikshuv hostname R1
R2(config)# crypto isakmp key tikshuv hostname R2
- .4
R1(config)# crypto isakmp key tikshuv address 209.165.0.11
R2(config)# crypto isakmp key tikshuv address 209.165.0.10

התשובה הנכונה 2.

הסביר:

הפקודה הנכונה להגדרת המפתח המשותף היא :

R2(config)# crypto isakmp key firewallcx address 1.1.1.1



ת. איזה מבין האלגוריתמים שלහן משמש להצפנה ב-VPN ?

- | | |
|----------|----|
| RSA | .1 |
| DH-1 | .2 |
| DH-2 | .3 |
| HMAC-MD5 | .4 |

התשובה הנכונה ? .

ראה לפי הטעלה הבאה: RSA הוא שיטת אימות לא הצפנה, DH הוא אלגוריתם להחלפת מפתחות לא להצפנה, HMAC הוא אלגוריתם גיבוב לא הצפנה. אין לשאלת זו תשובה נכונה.

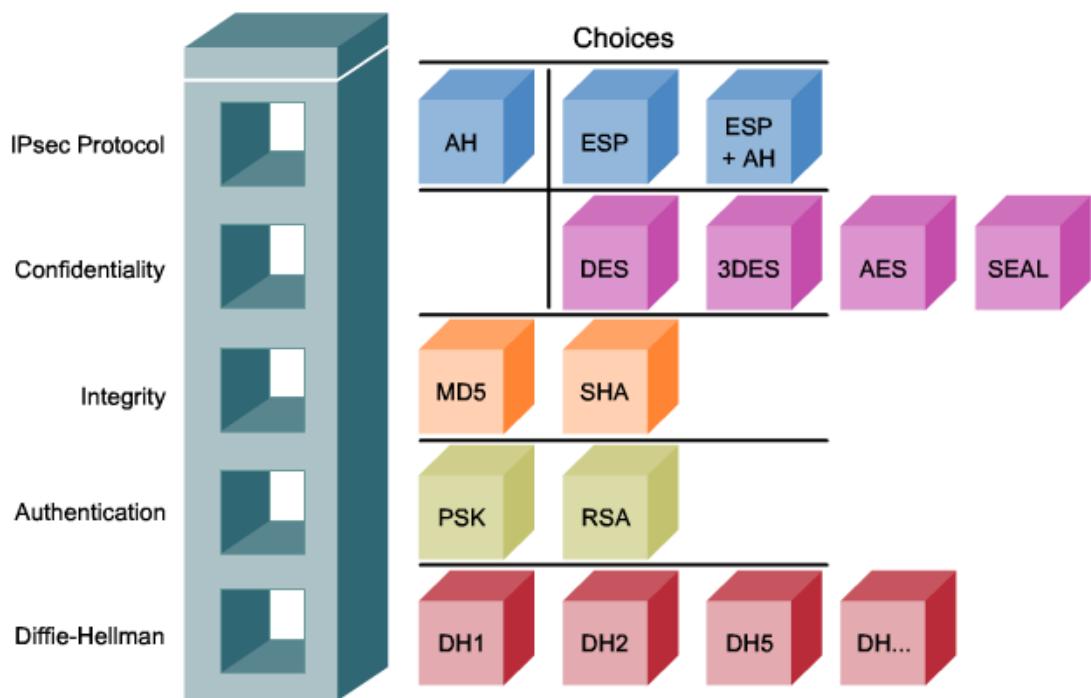
פרמטר	חזק יותר	חזק
אלגוריתם הצפנה	3-DES	DES
אלגוריתם גיבוב	SHA-1	MD5
שיטת אימות	הצפנה RSA חתימת RSA	Pre-shared
שיטת החלפת מפתחות	DH-2	DH-1
IKE SA	זמן חיים של SA	86400 שניות
86400 שניות	קטן מ-00	86400 שניות

פרוטוקול IPsec

IPsec הוא תקן (RFC 2401-2412) המגדיר כיצד ניתן להציג VPN באמצעות פרוטוקול כתובות IP.

:IPsec

- זהה מסגרת של סטנדרטים פתוחים אשר אינם תלויים באלגוריתמים חיצוניים (עצמאי ולא תלוי אחרים)
- הוא מספק סודיות נתונים, שלמות הנתונים, ואמות המקור.
- עובד על שכבה הרשת, מספק הגנה ובطיחת מנות IP בין התקני IPsec המשתתפים (עמייתים), להגן כמעט על כל תנועה היישום כי ההגנה יכולה להיות מיושמת מתוך שכבה 4 דרך שכבה 7, יש כוורת כוורת שכבה 3, וכך אין בעיות עם ניתוב.
- עובד על כל פרוטוקולי שכבה 2, כגון Ethernet, PPP, מסגרת מסמר, סינכרוני קישור קישור נתונים (SDLC), וכן רמה גבוהה קישור קישור נתונים (HDLC) ..
- זהה מסגרת של סטנדרטים פתוחים אשר עצמאית אלגוריתם.
- הוא מספק סודיות נתונים, שלמות הנתונים, ואמות המקור.
- עובד על שכבה הרשת, הגנה ובטיחת מנות IP בין התקני IPsec המשתתפים (עמייתים), מסוגל להגן כמעט על כל תבעורה מישומים מכיוון שההגנה יכולה להיות מיושמת מתוך שכבה 4 דרך שכבה 7.
- מכיל Header שכבה 3, וכך אין בעיות עם ניתוב.
- .עoped על כל פרוטוקולי שכבה 2, כגון ATM, Ethernet, Frame Relay, PPP, SDLC, HDLC, ...



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

פרוטוקול IPSec

שני פרוטוקולי ה- IPsec העיקריים הם AH ו- ESP.

- **AH (Authentication Header)** (שהוא פרוטוקול 51 IP) מספק את היכולות הבאות: כל הנתונים בטקסט לא מוצפן, אימות ואמינות.
- **ESP (Encapsulating Security Payload)** (שהוא פרוטוקול 50 IP) מספק את היכולות הבאות: הצפנה (כל הנתונים מוצפנים), אימות ואמינות.

את ESP ו- AH ניתן להחיל על מנויות IP בשני מצבים שונים, מצב transport ומצב tunnel:

- **מצב התעבורה - Transport**, אבטחה נוספת רק עבור שכבה התעבורה של מודל OSI ומעלה. מצב התעבורה מגן על המטען של המנה אך משאיר את כתובת ה- IP המקורי לא מוצפנת.
- **מצב המנהרה – Tunnel**, מספק אבטחה עבור חבילת ה- IP המקורי המלאה. מנויות ה- IP המקוריות מוצפנות ולאחר מכן מאוחסנות בחבילת IP אחרת. תופעה זו נקראת הצפנה IP בתוך IP (IP-in-IP encryption).

סודיות (הצפנה)

- DES - משתמש מפתח באורך של 56 סיביות, מאפשר הצפנה ביעילות גבוהה. DES היא מערכת הצפנה סימטרית. פחות מאובטחת. ערך ברירת המחדל של מדיניות IKE להצפנה הוא DES.
- 3DES - גרסה של DES 56-bit. DES 3DES משתמש בשלושה מפתחות הצפנה עצמאיים של 56 סיביות לכל בלוק של 64 סיביות, ומספק כוח הצפנה חזק יותר מאשר DES. משתמש במפתח סימטרי.
- AES - מספק אבטחה חזקה יותר מאשר DES והוא בעל יותר מבחינה "חישובית" מאשר DES. AES מציעה שלושה אורך מפתח שונים: 128 סיביות, 192 סיביות ו- 256 סיביות. AES היא מערכת הצפנה המשמשת במפתח סימטרי.
- SEAL - צופן שפותח בשנת 1993 על ידי פיליפ רוגאנו ודון קופרשמי, המשתמש במפתח של 160 סיביות. SEAL היא מערכת הצפנה סימטרית. הći בטוחה.

שלמות (אמינות)

שלמות ההודעה באמצעות ערך hash. ישנן שני אלגוריתמים נפוצים של HMAC: HMAC

- **HMAC-MD5 (HMAC-MD5)** - משתמש במפתח סודי משותף של 128 סיביות. ההודעה באורך משתנה ומפתח סודי משותף של 128 סיביות משולבים ומופעלים באמצעות אלגוריתם ה- HHAC-MD5 hash. הפלט הוא hash של 128 סיביות

- HMAC-SHA-1 - משתמש במפתח סודי של 160 סיביות. ההודעה באורך משתנה ומפתח הסוד המשותף של 160 סיביות משולבים ומוספעלים באמצעות אלגוריתם ה- Hash של HMAC-SHA-1. הפלט הוא 160-bit hash.
- HMAC-SHA-1 נחשב חזק יותר מ- MD5-HMAC. זה מומלץ כאשר נדרשת אבטחה מעט יותר חזקה.

אימות

קיימות שתי שיטות עיקריות להגדלת אימות בין עמיות.

- **PSK (מפתחות משותפים מראש)** - ערך מפתח סודי משותף מראש מוזן לתוך כל עמיות באופן ידי ומשמש לאימות עמיות. בכל צד, PSK משולב עם מידע אחר כדי ליצור את מפתח האימות. כל עמיות צריך לאמת את עמיתו המנוגד לפני שהמנהרה נחשבת בטוחה. מפתחות משותפים מראש קל להגדיר ידנית אבל לא בקנה מידה טוב, כי כל עמית IPsec חייב להיות מוגדר עם המפתח המשותף מראש של כל עמית אחר שבו הוא מתקשר.
- **חתימות RSA** - חילופי אישורים דיגיטליים ממשותיים את עמיותיהם. המכשיר המקומי מציר גיבוב ומצפין אותו במפתח הפרטי שלו. הגיבוב המוצפן מצורף להודעה ומועבר לקצה המרוחק ופועל כחותימה. בקצה המרוחק, ה- hash המוצפן מופיענה באמצעות המפתח הציבורי של הקצה המקומי. אם ה- hash המופיענה תואם את הגיבוב החדש, החותימה היא אמיתי. כל עמיות צריכה לאמת את עמיתו המנוגד לפני שהמנהרה נחשבת בטוחה.

החלפת מפתחות מאובטחת - Secure Key Exchange

אלגוריתמים של הצפנה כגון DES, 3DES ו- AES וכן האלגוריתם MD5 ו- SHA-1 hashing דורשים מפתח סודי סמטרי משותף לביצוע הצפנה ופענוח.

(DH) **Diffie-Hellman** הוא שיטת חיליפין של מפתח ציבורי המספק דרך לשני עמיות ליצור מפתח סודי משותף שרק הם יודעים, למרות שהם מתקשרים מעל ערך לא מאובטח.

קיימות מספר קבוצות DH:

- DH קבוצות 1, 2 ו- 5 עם גודל מפתח של 768 סיביות, 1024 סיביות, ו 1536 סיביות, בהתאם.
 - DH קבוצות אלו אין מומלצות לשימוש לאחר 2012.
 - DH קבוצות 14, 15 ו- 16 משתמשים בגודלי מפתח גדולים יותר עם 2048 סיביות, 3072 סיביות ו- 4096 סיביות בהתאם, ומומלצים לשימוש עד 2030.
 - DH קבוצות 19, 20 ו- 24 משתמשות (ECC) Elliptical Curve Cryptography, אשר מקטין את הזמן נדרש כדי ליצור מפתחות. עם גודל המפתח בהתאם 256 סיביות, 384 סיביות, ו 2048 סיביות. קבוצה 24 DH היא המועדף לשימוש לטווח ארוך.
- גרסאות חדשות יותר של IOS Cisco תומכות בקבוצות DH מתקדמות יותר.

א. 3DES הוא:

1. אלגוריתם גיבוב
2. אלגוריתם הצפנה
3. שיטת אימות
4. שיטה להחלפת מפתחות

התשובה הנכונה **2**.

ג. התבונן בהגדרות היפותית בנתבים של שני הסיניפים שלහן:

סיניף 1

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash rsh
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)# exit
```

סיניף 2

```
R2(config)#crypto isakmp policy 20
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#hash sha
R2(config-isakmp)#encryption 3des
R2(config-isakmp)#group 5
R2(config-isakmp)#lifetime 7200
R2(config-isakmp)# exit
```

מינהל הרשות אינו מצליח לחבר בין שני הסיניפים באמצעות פרוטוקול VPN.

על סמך ההגדרות שלעיל, מהו הגורם לתקלה?

1. אלגוריתם הצפנה בשני הנתבים זהה
2. מספר ה-*policy* בשני הנתבים שונה
3. ערך ה-*life time* בשני הנתבים שונה
4. אלגוריתם הגיבוב (*hash*) בשני הנתבים שונה

התשובה הנכונה 4.



Virtual Private Network

חיבור בין רשתות מרוחקות באמצעות האינטרנט יוצר שני בעיות:

- משאבי הרשת המרוחקת לא זמינים. לא ניתן לפנות לכתובות פרטיות מרוחקות.
- האינטרנט הוא מקום ציבורי ולכן מידע שנשלח דרכו חשוף לציטוט (Sniffing).

VPN יודע לתת מענה לשני הבעיה:

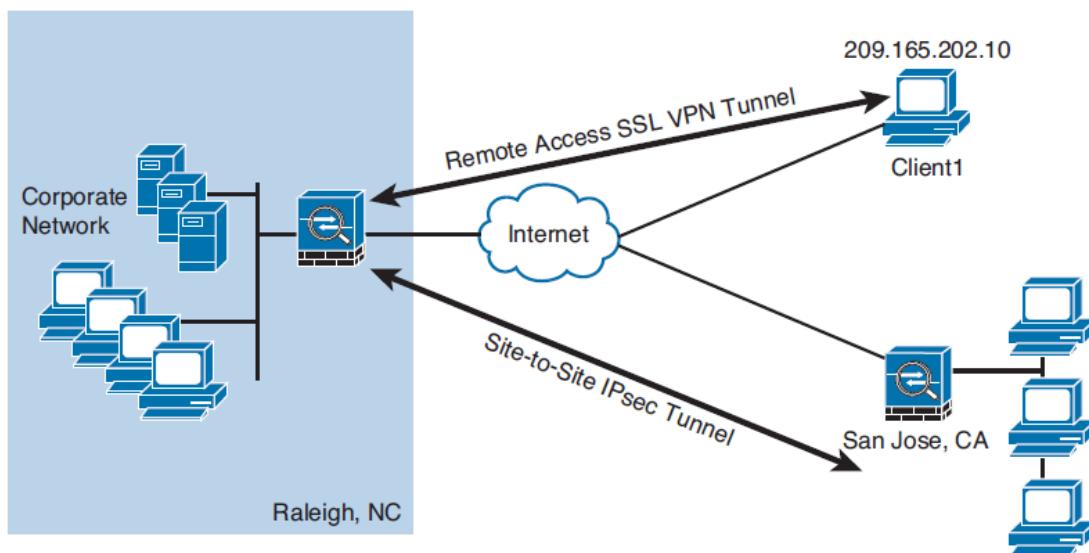
- VPN מ לחבר את המחשב לרשת המרוחקת אליו הוא מחובר ישירות לרשת LAN.
- VPN מ笪ין את המידע ורק מי שמורשה יכול לפענן את המידע.

יתרונות VPN

- **אבטחה** - המידע שמועבר באמצעות VPN מאובטח על-ידי IPSec או SSL.
- **חסכון כספי** - השימוש ב-VPN מונע את העלויות הגבוהה של קוים מושכרים (WAN) ולכן זו דרך חסכונית לחבר בין סניפים או בין עובד מרוחק למקום עבודתו.
- **יכולת גידול** - בקלות ו מהירות ניתן לחבר סניפים ומשתמשים מרוחקים נוספים.

קיימים שני סוגי עיקריים של VPN:

- **Remote Access VPN** - מאפשר לך לחבר למרוחק לתוכהן לתוכהן הארגון. כך הלקוח יכול לגשת בצורה מאובטחת למשתמשים בתוך הארגון.
- **Site-to-Site VPN** - חיבור בין סניפים. יצרת קשר ישיר ומאובטח בין שני סניפי החברה. ההצפנה מתבצעת רק ביציאת ה-packets לאינטרנט.



נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוכרת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

VPN Protocols

שלושת הפרווטוקולים (tunneling protocols) בעזרתם ניתן ליצור קשר מאובטח הם:

Point-to-Point Tunneling Protocol (PPTP)

- זהו פרוטוקול קצר מיושן ופחות מאובטח מഫוטוקולים האחרים.
יודע להצפין PPP packets. אחד מהחולשות של הפרווטוקול זה שתהיליך הקמת הקשר לא מוצפן. רק לאחר הקמת הקשר הפרווטוקול מוצפן את המידע.

PPTP משתמש בפרווטוקול (MPPE) Microsoft Point-to-Point EncryptingTCP port 1723 להצפנה המידע. עובד ב-

Layer 2 Tunneling Protocol (L2TP)

- יודע להצפין PPP packets. ברוב המקרים יעשה שימוש בפרווטוקול זה.
L2TP משתמש בפרווטוקול Internet Protocol Security (IPSec) להצפנה המידע. עובד ב- UDP port 1701.

Secure Socket Tunneling Protocol (SSTP)

- SSTP משתמש בפרווטוקול Secure Sockets Layer (SSL) להצפנה המידע.
השימוש בHTTPS מאפשר לעבר Firewalls בצורה פשוטה הרבה יותר מאשר שימוש בWindows Vista או Windows Server 2008 L2TP PPTP או SSTP. השרת חייב תעודה דיגיטלית SP1.

שלושת הפרווטוקולים משתמשים ב- (PPP) Point-to-Point Protocol לביוץ user.authentication

VPN Authentication Protocols

- כאשר מישמים VPN, יש לבחור אחד מפרווטוקולים אלה לצורך אימות שם משתמש וסיסמה של ה- Client. תהליך ההזדהות תחיליה מנסה להשתמש בפרווטוקול המאובטח ביותר המאפשר אצל ה- Client.

Password Authentication Protocol (PAP)

- לא מוצפן את הסיסמה (plaintext) ולכך עדיף לא להשתמש בו.

Shiva Password Authentication Protocol (SPAP)

- משתמש בהצפנה חלשה מסוג reversible encryption (לא נחשב להצפנה טובה).
הפרווטוקול לא מוצפן את DATA.

Challenge Handshake Authentication Protocol (CHAP)

- משתמש באlgorigitם הצפנה מסוג Message Digest 5 (MD5). CHAP לא מוצפן את DATA. DATA רק נתומם דיגיטלי (hash) ולכך פרוטוקול זה לא נחשב כפרווטוקול הצפנה.

Microsoft CHAP (MS-CHAP)

- משתמש בהצפנה מסוג MPPE ומאפשר להצפין את DATA. חזק ההצפנה כמורכבות הסיסמה.

MS-CHAP version 2 •

רמת אבטחה גבוהה יותר מ- MS-CHAP (תוקן בו בעיות אבטחה).
חזק ההצפנה לא קשור למורכבות הסיסמה.

Extensible Authentication Protocol-Transport Level Security •
.USB Key - smart cards המשמש ב- certificates (EAP-TLS)

IPSec

Internet Protocol Security (IPSec)

IPSec זו חבילת פרוטוקולים שפעלה בשכבה שלישית של מודל ISO ונפוץ מאוד בשימוש ב-VPN. IPSec מאבטח תעבורת רשת מסוג IP/TCP וכן להגן על המידע שזורם ברשות.

כיצד IPSec מאבטח את זרימת הנתונים ברשת?

זהות (Authentication)

זהוי הדדי של שני הצדדים לפני וטור כדי שידור הנתונים. ניתן לבצע אימות במספר דרכי שונות:

- Pre-Shared secret key - שימוש בסיסמא לצורך זהוי.
- Public Key Infrastructure - בשיטה זו ההזדהות מתבצעת בעזרת תעודה דיגיטלית וזוג מפתחות (key). (Public and private key).
- Remote Access VPN – משמש ב- VPN – User authentication

(Confidentiality)

רק הצדדים שמתקשרים דרך VPN, יכולים להבין את הנתונים שנשלחו. אם מישחו מצותה למידע, הוא יוכל לראות את החבילות אבל זה חסר משמעות כי תוכן של הchipila לא מובן (cipher text) כי אין לו את יכולת לפענוח את הנתונים.

כך נראה תוכן של מידע מוצפן

```
Tp uijt jt uif tfdsfu nfttbhf. Ju jt fbtz up ef-fodszqu jg zpv lopx uif lfz.
```

האלגוריתמים והנוסחאות להצפנה נתונים זמינים בפורמבית וידועות לכלם. החלק שגורם להודיע להיות סודית זה המפתח שמשמש להצפנה הנתונים.

```
"So this is the secret message. It is easy to de-encrypt if you know the key."
```

(Data Integrity)

חותמת המידע (Data signing) לא מאפשרת את זיוף המידע.

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים כתבו ועובדו על ידי ערן גזית לתשומת לכם החברת מכילה חומר ללימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

כלומר, אם יבוצע שינוי במידע, זה יתגלה.

(Anti-Replay) packet

כל חבילה ממוספרת באמצעות Sequence Number. בדיקת ה- Sequence Number מאפשרת לתוקף ללכוד חבילה שמודרעה ולנסות לשדר אותה שוב במטרה לפתח session או לקבל גישה למשאים ברשות.

מחסנית ה프וטווקולים של IPSec

מחסנית הפרוטוקולים IPSec, מורכבת מפרוטוקולים רבים שמתעדכנים עם הזמן.

כך IPSec יהיה רלוונטי גם בעתיד כי המחסנית שלו ניתנת לעדכן ורמת אבטחת המידע יכולה להשתנות בהתאם לצרכים של המשתמש.

Negotiation Protocol

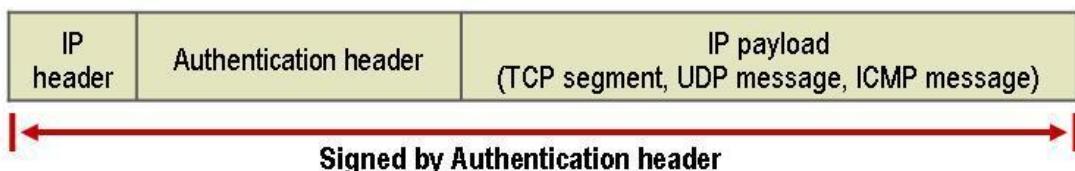
ניתן להשתמש בכל אחד מהפרוטוקולים בנפרד או עם שניים ביחד.

Authentication Header (AH) protocol

פרוטוקול זה מספק:

- **זהות**
- **שלמות המידע**
- **חסימת שידור חוזר של packet**
- **לא תומך ב NAT**

הפרוטוקול לא מבצע הצפנה ولكن המידע ניתן לקריאה אך לא ניתן לשינוי.

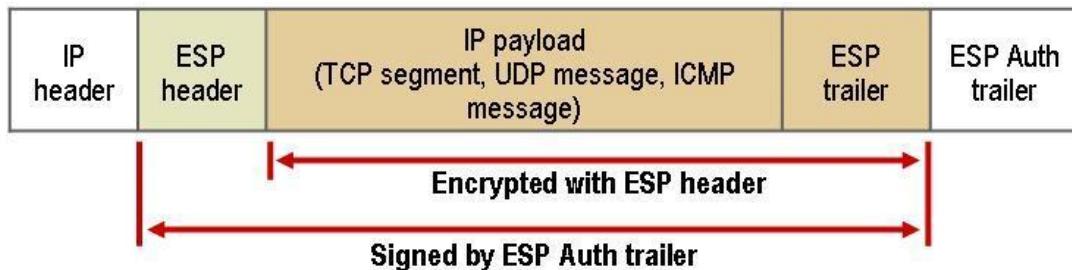


Encapsulated Security Payload (ESP) protocol

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

פרוטוקול זה מספק:

- **דיארי**
- **שלמות המידע** – שלמות המידע חלה רק על המידע כתוצאה מהצפנה, ip header יי' חשוף.
- **חסימת שידור חוזר של packet**
- **הצפנה** – הצפנה של המידע בלבד ללא הצנת ip header.

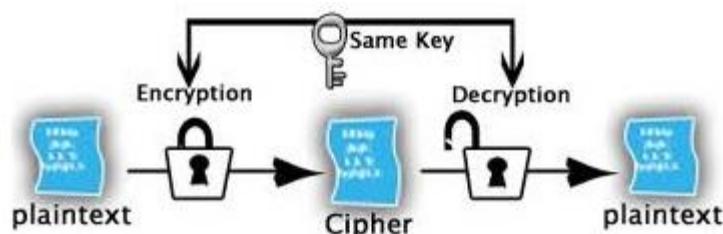


שיטות הצפנה

קיימות שני שיטות הצפנה:

Symmetric

בשיטת זו, קיימן מפתח אחד והוא משמש להצפנה ולפיענוח. שני הצדדים משתמשים באותו מפתח (Shared Secret). הצפנה סימטרית מהירה יותר מהצפנה אסימטרית ולא פחות חזקה ממנה.



הצפנה סימטריות משתמשת באחת משתי השיטות הבאות:

- מצפין block cipher – מצפין בכל פעם מקטע נתונים אחר.
- מצפין stream cipher – מצפין מידע זורם, byte אחר byte

אלגוריתמים שימושיים בו-**Symmetric key**:

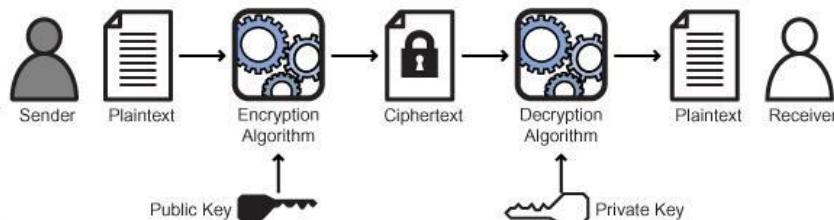
משמשים בעיקר להצפנה מידע מאוחסן (סטטי).

- DES (Data Encryption Standard) – נוצר על ידי IBM (מפתח באורך 56 bits). בשימוש החל מאמצע שנות השבעים. כיום הוא חשב ללא מאובטח בגלל המפתח הקצר שלו.
- 3DES (Triple DES) – נוצר על ידי IBM (מפתח באורך 168 bits = 3 * 56). יוצר שלושה מפתחות לכל בלוק נתונים ומצפין את הבלוק שלושה פעמים (כל פעם עם מפתח אחר). DES 3DES בשימוש גם כיום.
- AES (Advanced Encryption Standard) – מפתח באורך 128/192/256 bits. ממשלת ארצות הברית מסמינה את סוג ההצפנה של AES-256 כ- סוד' ביותר.

Asymmetric

בשיטת זו, ההצפנה והפענוח מתבצעים באמצעות מפתחות שונים. מפתח ציבורי (Public-key) משמש להצפנה ומפתח פרטי (Private-key) משמש לפענוח. המפתח הציבורי מופץ בצורה חופשית לכל מי שאנו רוצים שיישלח לנו מידע מסווג. כאשר המידע מגיע למחשב שלנו, המידע מופיע באמצעות המפתח הפרטי. בצורה זו המידע מוגן כי רק מי שיש לו את המפתח הפרטי יכול לפענוח את המידע.

Public Key Encryption



הצפנה Asymmetric מאוד חזקה אך מעמיסה מאד על המעבד ולכן IPSec משלב בהצפנה את שניהם. בשלב הראשון השולח מצפין את המידע באמצעות הצפנה סימטרית. בשלב השני השולח מצפין את מפתח ההצפנה הסימטרי תוך שימוש בהצפנה אסימטרית. חשוב לציין – לכל קובץ נוצר מפתח סימטרי חדש.

אלגוריתמים שימושיים ב- Asymmetric key

- משמשים בעיקר להצפנה מידע זורם או להצפתה תעליך היזדהות.
- RSA – מפתח באורך 512/1024 או יותר. משמש בעיקר ב- SSH. המפתח מסוג Asymmetric-key.
 - DH (Diffie-Hellman) – מפתח באורך 512/1024 או יותר. משמש בעיקר ב- NVP. המפתח מסוג Asymmetric-key.

Data Integrity Protocol (Hashing)

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לבכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

- MD - מפתח באורך 128 bits
- SHA-1 – מפתח באורך 160 bits

סוגי Authentication

קביעת סוג Authentication תלוי בטופולוגיה המחשבים וברמת האבטחה הנדרשת.

- **Kerberos V5**

פרוטוקול בירית המחלל שימושו ל Authentication בסביבת Active Directory. ניתן לשימוש בין מחשבים שנמצאים באותו trusted domains. שימוש ב프וטוקול זה לא דורש הגדרות נוספות כאשר מטבחה תקשורת בין מחשבים שמחורפים ל Domain.
- **Public Key Infrastructure**

בשיטת זו ההזדהות מטבחה באמצעות תעודה דיגיטלית. השתמש בשיטה זו במידה וברצוננו לקיים תקשורת בין מחשבים שלא נמצאים באותו trusted domains (דרך האינטרנט, שותפים עסקיים וכו'). כדי לישם שיטה זו יש צורך לפחות certification authority אחד.
- **Pre-Shared secret key**

שימוש בסיסמא לצורך זהה. שיטה זו מספקת הci פחות אבטחה ובנוסף הסיסמא מאוחסנת בצורה לא מוצפנת במחשב או ב Active Directory. **יש להשתמש בשיטה זו רק בסביבת ניטוי.**

השלבים בתקשורת בין שני מחשבים המשתמשים ב- IPSec:

1. על המחשבים מיושמת מדיניות מקומית (local policy) או מדיניות דרך GPO. המדיניות מגדרה באמצעות Filter על איזה סוג של תובורת רשות המדיניות תחול, ובעזרת Filter Actions נקבע באיזו צורה תוגן תובורת הרשות.
2. ה프וטוקול Internet Key Exchange (IKE) מחליט באיזה שיטה להשתמש בכך שהמחשבים יזהו אחד את השני. (certificate, Kerberos, preshared key).
3. מידע מוצפן או נתחתם לפני שיידרו ברשות.

הגדירות ב- firewall

בשימוש בפרוטוקולים הבאים, יש לפתח את ה- ports.

- TCP 51 – AH
- TCP 50 - ESP
- UDP 500 – IKE

Transport Mode

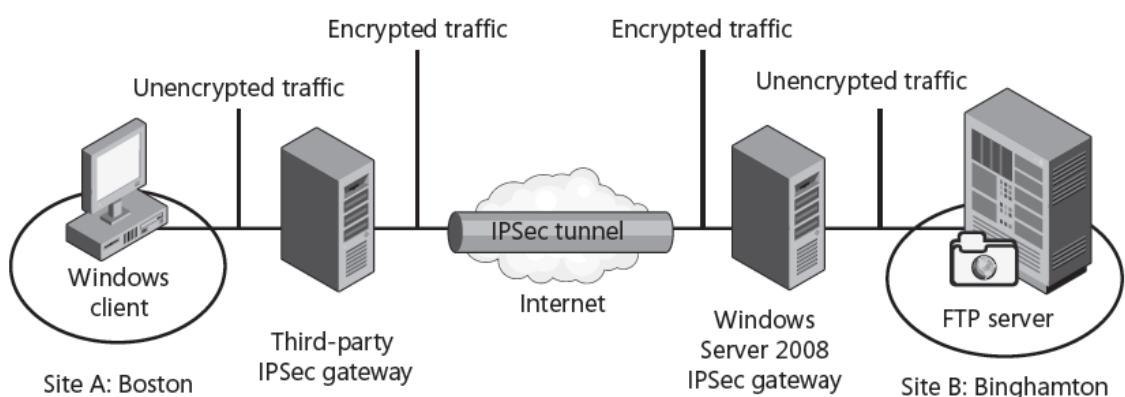
כברית מחדר IPsec עובד ב mode transport, כלומר אבטחה מקצה לקצה.

שיטת זו משמשת מחשבים בתוך LAN כדי לאבטח את התקשרות ביניהם.

Tunnel Mode

ב Tunnel Mode האבטחה היא לא עד תחנת הקצה.

בדרך כלל נשתמש בו site to site vpn במקום בשיטה זו.



IPSec Security Policy

זו סידרת חוקים שקובעים לאיזה סוג של תעבורת רשות להתייחס (filters) ואיזה סוג של הגנה לישם (block, permit, negotiate security). ניתן לישם רק מדיניות אחת למחשב ולן כל החוקים צריכים להיות באוטה מדיניות. לא ניתן לקבוע את סדר החוקים. החוקים היותר ספציפיים הראשונים ולאחר מכן החוקים הכלליים יותר.

IPsec Policy		
	IP Filter Lists	דוגמא: Filter Actions
Policy Rule #1	Filter #1: Telnet Traffic from 192.168.3.32 Filter #2: POP3 Traffic from 192.168.3.200	Negotiate Security (Require Encryption)
Policy Rule #2	Filter #1: All Telnet Traffic Filter #2: All POP3 Traffic	Block
Policy Rule #3	Filter #1: All Traffic	Negotiate Security (Request Authentication)

מדיניות ברירת המחדל Default IPSec Policies

- **(Client (Respond Only))** - שימוש ב- IPSec רק אם מחשב היעד דורש זאת. בדרך כלל נשתמש ב Policy זה על Clients.
- **(Server (Request Security))** - המחשב ידרש שימוש ב- IPSec אך יתקשר גם אם אין למחשב היעד אפשרות להשתמש ב- IPSec.
- **(Secure Server (Require Security))** - המחשב ידרש שימוש ב- IPSec ולא יצור קשר עם מחשב שלא מסוגל להשתמש ב- IPSec. כל תעבורת הרשות היוצאת תהיה מוצפנת.

The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the policy structure under 'IPSec Policy [DEN-DC1.contoso.msft] Policy'. The 'IP Security Policies on Active Directory' node is highlighted with a black rectangle. On the right, the main pane shows a table of three default policies:

Name	Description	Policy Assigned
Server (Request Security)	For all IP...	No
Client (Respond Only)	Commun...	No
Secure Server (Require Security)	For all IP...	No

יצירת חוק בעזרת Wizard

פרוט חמשת השלבים ביצירת חוק חדש:

1. **Tunnel endpoint** – אם נעשה שימוש ב- Tunneling, יש צור לczyן לubahora יוצאה את הכתובת IP של השירות הקרוב לעד שמבצע את ה- Tunneling.
2. **Connection type** – הגדרה זו מושמת להגבלת סוג החיבור (Remote access, LAN, LAN, LAN).
3. **IP Filter list** – הגדרה זו קובעת לאיזה סוג תעבורת רשות החוק יתיחס. כבירית מחדל קיימים שני סוגי Filters (All IP Traffic | All ICMP Traffic) על-ידי לחיצה על הכפתור Add, ניתן ליצור Filters נוספים.
4. **Filter action** – איזה פעולה יש לבצע על תעבורת הרשות (Request Security , Request Security (Optional) , Permit)
5. **Authentication methods** – באיזה שיטה יש להשתמש לצורך (certificate from a specified certification authority , Kerberos, preshared key)

תרגיל: Site to Site VPN

תרגיל VPN IPSec לחיבור בין שני אתרים بصورة מאובטחת על פני רשת האינטרנט.

תרחיש:

חברת **com.sheba** פתחה סניף נוסף באילת. מטה החברה נמצא בתל-אביב ויש צורך לחבר בין שני אתרים.

לחברה אין כרגע משאבים רבים ולכן הוחלט למשוך את החיבור באמצעות רשת האינטרנט. (במקום לחוכר קו ייודי או להשתמש בטכנולוגיית WAN כגון Frame Relay) כיוון שההעברה מידעת על פני רשת ציבורית חשופה לעיני כל, יש להציג את התעבורה. הפתרון יהיה שימוש ב – VPN בין שני האתרים ובתוספת הפרוטוקולים IPSec.

הערות:

לנתבי הקצה בארגונים כבר הוגדרו כתובות IP ציבוריות וכן הוגדר נתיב ברירת מחדל המוביל לאינטרנט. תרגיל זה לא עוסק בנושאים אלו.

הוראות:

בדיקות קישוריות לאינטרנט.

גשו למחשב PC0 ושגרו פינג לשרת ה – DNS בכתובת 8.8.8.8

PC>**ping 8.8.8.8**

מדוע הפינג נכשל?

לפני שניגש להגדרות ה – VPN עצמו יש להגדיר NAT כדי לאפשר גלישה באינטרנט באמצעות הכתובת הציבורית של הנתבים.

שים לב: איננו רוצים לבצע NAT לturnstile שנוודה לרשות הפרטית באתר השני. כיוון שכן נשתמש ברשימת גישה מורחבת.

הגדרות NAT כדי לאפשר גלישה באינטרנט לנtab TLV

יצירת ACL

```
TLV-RTR(config-ext-nacl)#ip access-list extended NAT  
TLV-RTR(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 192.168.1.0 0.0.0.255  
TLV-RTR(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 any
```

סימון מושגים C – I outside – I inside

```
TLV-RTR(config)#interface Serial0/0/0  
TLV-RTR(config-if)#ip nat outside  
TLV-RTR(config-if)#exit  
TLV-RTR(config)#interface FastEthernet0/0
```

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כולם!

```
TLV-RTR(config-if)#ip nat inside
```

הפעלת NAT

```
TLV-RTR(config)#ip nat inside source list NAT interface Serial0/0/0 overload
```

בדיקת קישוריות לאינטרנט.
גשו למחשב PC0 ושגרו פינג לשרת ה – 8.8.8.8 בכתובת DNS

```
PC>ping 8.8.8.8
```

האם הפינג הצליח?

פתחו דפדפן במחשב PC0 וגלשו לאתר www.facebook.com
יש אינטרנט?

הגדרות NAT כדי לאפשר גלישה באינטרנט לנtb ELAT

```
ELAT-RTR(config)#ip access-list extended NAT
```

```
ELAT-RTR(config)#deny ip 192.168.1.0 0.0.0.255 10.0.0.0 0.255.255.255
```

```
ELAT-RTR(config)#permit ip 192.168.1.0 0.0.0.255 any
```

סימון מושגים C – I inside – outside – I inside

```
ELAT-RTR(config)#interface Serial0/0/0
```

```
ELAT-RTR(config-if)#ip nat outside
```

```
ELAT-RTR(config-if)#exit
```

```
ELAT-RTR(config)#interface FastEthernet0/0
```

```
ELAT-RTR(config-if)#ip nat inside
```

הפעלת NAT

```
ELAT-RTR(config)#ip nat inside source list NAT interface Serial0/0/0 overload
```

בדיקת קישוריות לאינטרנט.

פתחו דפדפן במחשב PC1 וגלשו לאתר www.facebook.com
יש אינטרנט?

הגדרות VPN

IKE phase 1 tunnel

השלב הראשון בהגדרת ה – VPN – יצירת מנהרת 1 IKE phase 1 המשמשת כعروץ פרטי ומأבטח בין הנתבים המאפשר להם לסכם את אופן יצירת מנהרת 2 IKE phase 2 שבו יעבור המידע עצמו.

יש שני דרכים לבצע זהה של הצד השני, מפתחות משותפים וחתיומות דיגיטליות.
אנו נשתמש ב מפתח משותף.

הערה: יש עוד הגדרות רבות ל – 1 IKE אבל נשתמש בברירת המחדל.

בדיקה קישוריות – האם נתבTLAT יכול לדבר עם נתב ELAT?

שגרו פינג מנתבTLAT לכתובת הציבורית של נתב ELAT.

```
TLV-RTR#ping 90.0.0.1
```

אם הפינג הצליח, אפשר להתקדם.

על נתבTLAT

הגדרת מדיניות של 1 IKE phase 1

ניתן להגדיר יותר מי מדיניות אחת והנתב ישתמש עם המדיניות עם המספר הנמוך ביותר

בלומר יש עדיפות למединיות עם מספר נמוך

מדוע תכונה זו קיימת: יכול להיות שנתב יכול להקים קשר עם כמה סניפים שונים וחלוקת תומכים בPKI
וחלקם יודעים לעבוד רק עם סיסמא (psk - key).

```
TLV-RTR(config)#crypto isakmp policy 1
```

```
TLV-RTR(config-isakmp)#authentication pre-share
```

```
TLV-RTR(config-isakmp)#exit
```

יש לבצע את אותן הגדרות גם על נתב ELAT!

```
ELAT-RTR(config)#crypto isakmp policy 1
```

```
ELAT-RTR(config-isakmp)#authentication pre-share
```

```
ELAT-RTR(config-isakmp)#exit
```

השלב הבא בהגדרת ה – VPN יצירת מנהרת 1 IKE phase 1 הוא להגדיר את המפתח המשותף ואת כתובת הנתב המשמש כצד השני של החיבור.

על נתבTLAT

```
TLV-RTR(config)#crypto isakmp key bubu address 90.0.0.1
```

כאשר סבב הוא המפתח המשותף (בעולם האמיתי רצוי לשימוש ב מפתח חזק יותר)

יש לבצע את אותן הגדרות גם על נתב ELAT (עם כתובות ה – IP הציבורית של נתב TLV)

```
ELAT-RTR(config)#crypto isakmp key bubu address 80.0.0.1
```

בשלב האימוח בין שני הנתבים (IKE phase 1) DH הוא אלגוריתם אסימטרי שמשמש רק להחלפת מפתחות | הגנה על תעבורת שלב 1

סימון תעבורת המורשת לעבר ב – VPN.

עכשו עליינו לזרז את התעבורת אותה אנו רוצים להעביר מאתר לאתר באמצעות חיבור ה – VPN. דיהו זה מתבצע באמצעות רשימת גישה (access list) על נתב TLV

- TLV-RTR(config)#ip access-list extended VPN
- TLV-RTR(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 192.168.1.0 0.0.0.255

על נתב ELAT

- ELAT-RTR(config)#ip access-list extended VPN
- ELAT-RTR(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.255.255.255

הגדירות IKE phase 2 tunnel - VPN

השלב השני בהגדרת ה – VPN – יצירת מנהרת 2 IKE phase המשתמשת ב – IPSec כדי להעביר מידע באופן מאובטח מאתר על פני רשת האינטרנט.

הגדירות כולן זה נקבעות **transform set**.

כאן יגדרו דברים כגון אלגוריתמים להצפנה ולגבוב.

על נתב TLV

- TLV-RTR(config)#crypto ipsec transform-set ELAT esp-aes esp-sha-hmac

ELAT הוא שמו של ה – transform set על נתב TLV

על נתב ELAT

- ELAT-RTR(config)#crypto ipsec transform-set TLV esp-aes esp-sha-hmac

TLV הוא שמו של ה – transform set על נתב ELAT

הגדירות VPN – הפעלה ושימוש בכל מה שהוגדר עד כה.

דבר מה שהוגדר עד כה עדין אינו בשימוש.

בשלב זה נאחד את הכל ייחדיו ונגדיר לנתחים להפעיל את ה – VPN.

יצור crypto – רשימה המכילה את כל ההגדירות שביצעו עד כה ואז נציג את ה – crypto map – מapse.

map למשך.

על נתב TLV

- TLV-RTR(config)#crypto map MY-MAP 1 ipsec-isakmp
- TLV-RTR(config-crypto-map)#set transform-set ELAT
- TLV-RTR(config-crypto-map)#set peer 90.0.0.1
- TLV-RTR(config-crypto-map)#match address VPN

נכתב ועובד על ידי יקי בן ניסן. מקצת מהחומרים נכתבו ועובדו על ידי ערן גזית
لتשומת לכם החוברת מכילה חומר לימוד הנדרשים לצורך בחינות הגמר אך לא את כלם!

על נתב ELAT

- ELAT-RTR(config)#**crypto map MY-MAP 1 ipsec-isakmp**
- ELAT-RTR(config-crypto-map)#**set transform-set TLV**
- ELAT-RTR(config-crypto-map)#**set peer 80.0.0.1**
- ELAT-RTR(config-crypto-map)#**match address VPN**

יצרנו crypto map עכשו נקשר אותו למשק היחיה לאינטרנט כדי להפעיל את ה – VPN.

על נתב TLV

- TLV-RTR(config)#**interface serial 0/0/0**
- TLV-RTR(config-if)#**crypto map MY-MAP**

על נתב ELAT

- ELAT-RTR(config)#**interface serial 0/0/0**
- ELAT-RTR(config-if)#**crypto map MY-MAP**

בדיקות קשריות.

שגרו פינג ממחשב 0 PC למחשב 1 PC1
פתחו דפדפן על מחשב 0 PC וגלישו לאתר החברה בכתובת 192.168.1.100
הכל אמרור להצלחה.

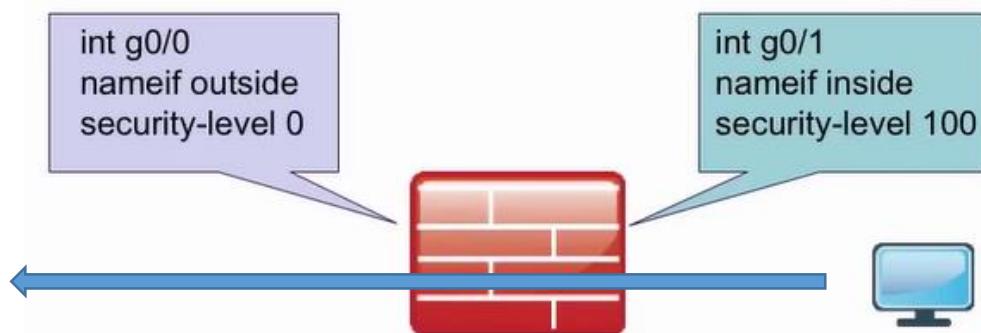
קצת פקודות show למקורה שדברים לא עובדים

- TLV-RTR#**show crypto map**
- TLV-RTR#**show crypto ipsec sa**
- TLV-RTR#**show crypto ipsec transform-set**

ASA Adaptive security appliances

- ל-ASA מערכת הפעלה משלו שאינה זהה למערכת הפעלה של מניבים והמתגים של סיסקו. היא דומה להן.
- לחומרת האש מסוג ASA יש אפשרות לעבוד במצב Stateless או Stateful
- על מנת שמיידע יזרום דרך ה-PACKET-ים חייבים להתאים לכללים המוגדרים על ה-ASA
- על כל ממשק יש להגדיר על ידי הפקודה **nameif** את רמת האבטחה של אותו ממשק.
- רמת האבטחה יכולה להיות בין 0 – הכי פחות בטוח עד ל-100 הכי בטוח.
- **כלל זהב** – מידע הזורם מאחור בטוח לאחור בטוח פחות לא לבדוק על ידי רישימת גישה מידע הזורם מאחור אבטחה נמוך לאחור אבטחה גבוהה חייב להיבדק על ידי רישימת גישה ממשקים בעלי רמת אבטחה זהה לא מחובבים במעבר דרך ACL אם הפקודה **same-security-traffic permit inter-interface deny all** בסוף כל רישימת גישה יהיה all

ASA Operation – 2 interfaces



תעבורה העוברת בין האזור הפנימי עוברת ללא בדיקה ולא הפרעה (כלל הזהב) בהיות ה-ASA מכשיר מסוג **Stateful** גם תעבורה חוזרת **תאפשר** ללא בדיקה. כל תעבורה שמקורה בחוץ נדרש בדיקה על ידי רישימת גישה ואפשרית גם בדיקה על ידי NAT.

Sample ASA Configuration – 3 interfaces

```
interface GigabitEthernet0/0
    nameif outside
    security-level 0
    ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
    nameif inside
    security-level 100
    ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
    nameif dmz
    security-level 50
    ip address 172.16.1.1 255.255.255.0
```

המידע זורם ללא בדיקה :

- מה-outside-לinside
- מה-DMZ-לinside
- מה-outside-ל-DMZ

המידע זורם וחיב בבדיקה:

- מה-inside-לoutside
- מה-DMZ-ל-outside
- מה-inside-ל-DMZ

```
ASA1(config)# interface gi0/1
ASA1(config-if)# no shutdown
ASA1(config-if)# nameif inside
ASA1(config-if)# security-level 100
ASA1(config-if)# ip address 10.10.10.100 255.255.255.0
ASA1(config-if)# interface gi0/0
ASA1(config-if)# no shutdown
ASA1(config-if)# nameif outside
ASA1(config-if)# security-level 0
ASA1(config-if)# ip address 192.168.1.100 255.255.255.0
ASA1(config-if)#

```

דוגמה להגדירה :

System Message Logging (Syslog)

להתקנים ברשת קיימן מנגנון שמאפשר להם להודיע כאשר מתרחשים אירועים מסוימים וזאת באמצעות שליחת הודעות מערכת. קריית הודעות מערכת מאפשרת לבדוק את מצב התקן ועזרת באיתור תקלות. תפקיך פרוטוקול syslog לשЛОוח הודעות מערכת.

כברירת מחדל, נתבים ומוגדים של Cisco שלוחים את כל ההודעות ל- console ובחלק מגרסאות IOS, המכשיר גם אוגר הודעות יומן ב- .buffer

עדים עבור הודעות syslog כוללים:

- Logging buffer (זיכרון RAM בתוך התקן) - פעיל כברירת מחדל
- Console line
- Terminal line
- Syslog server

כדי לראות את ההגדרות של syslog ואת ההודעות ששמורות ב- .buffer, השתמש בפקודה:
R1# **show logging**

כדי לאפשר שליחת הודעות ל- buffered/console, השתמש בפקודות:

```
R1(config)# logging console  
R1(config)# logging buffered
```

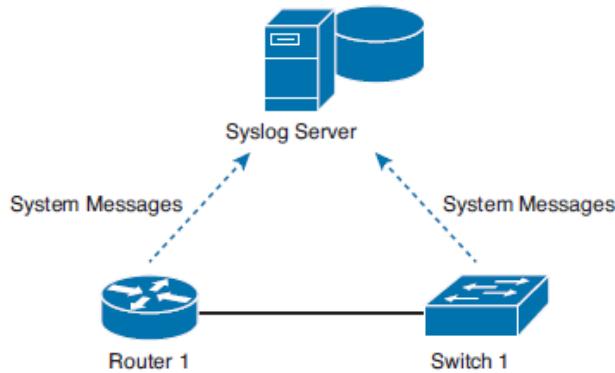
Severity Level

אחד המרכיבים החשובים בהודעת מערכת זה חומרת ההודעה. Severity Level מאפשר לנו לשלוט בסוגי ההודעות שנשלחות ל- .Syslog server ככל שהמספר נמוך יותר, כך ההודעה קריטית יותר. רמות 0-4 מייצגים אירועים שעולים להשפיע על התקן ברצינות, ואילו רמות 5-7 מייצגים אירועים פחות חשובים.

Level	Level Name	Explanation
0	Emergency	The system may be unusable.
1	Alert	Immediate action may be required.
2	Critical	A critical event took place.
3	Error	The router experienced an error.
4	Warning	A condition might warrant attention.
5	Notification	A normal but significant condition occurred.
6	Informational	A normal event occurred.
7	Debugging	The output is a result of a debug command.

כדי להגדיר איזה הודעות תישלח (Severity Level).
לדוגמה, כדי להגביל את ההודעות לרמות 0-4, השתמש באחד משתי הפקודות:
R1(config)# **logging trap {4}**
R1(config)# **logging trap {warning}**

מאפשר Syslog server להודעות מערכת ללא צורך בגישה פיסית להתקן.
זו השיטה הנוחה והנפוצה ביותר לגישה להודעות מערכת.



כדי לשלוח הודעות ל-Syslog server, יש להגדיר את הכתובת של Syslog server:

```
R1(config)# logging host {IP address of the syslog server}
```

Time-stamp

כברית מחדל, חותמת הזמן שמופיע בהודעה היא משך הזמן שההתקן פועל.
יעיל יותר שבהודעות תופיע חותמת זמן ולכן השעון בהתקן צריך להיות מעודכן.

```
R1(config)#service timestamps log datetime msec
```

ניתן לקבוע שבסמוך לחותמת הזמן, הרשומות יהיו ממוספרות.

```
R1(config)#no service timestamps
R1(config)#service sequence-numbers
```

קיימות כמה גרסאות של תוכנות חופשיות ושיתופיות שמאפשרות הקמת שרת Syslog
לדוגמה: .kiwi syslog server
Splunk Light