**-iL**

-iL IpList.txt

אפשרות זו טוענת לסריקה קובץ שהכנתם עם רשימת כתובות IP למשל

nmap -sS -iL IpList.txt

**-iR**

מאפשר לנו לבצע סריקה של כתובות IP ראנדומליות ולבדוק האם יש פורט פתוח בכתובת IP, לא משנה איזה כתובת

תוכלו להשתמש בפקודה: על מנת לחפש האם יש שרתים כלשהם ברשת שפתוח בהם פורט 80

nmap -Pn -sS -p 80 -iR 0 –open

**–exclude  \  –excludefile file.txt**

על ידי פקודה זו נוכל לבטל \ לדלג על סריקה של כתובות מסוימת, אם זה רשימה בתוך קובץ טקסט או כתובות IP מסוימים

nmap -sS 192.168.1.10  –excludefile file.txt

nmap -sS 192.168.1.10  –exclude host1 host2 …

**list scan  -sL**

בתצורה זו ה nmap לא יבצע פינג או ישלח Packet מכל סוג שהוא, בתצורה זו הוא מבצע שאילתת DNS הפוכה על מנת לגלות את שם התחנה \ הדומיין גם את השם שמאחורי כתובת ה IP

nmap -sL site.co.il

ניתן יהיה לראות את שם השרת עליו מאוחסן האתר – vultr!

**-sn**

סריקה זו אומרת לnmap, אל תבצע סריקת פורטים, אלא תציג רק אילו “מחשבים” פעילים או לא

למשל הפקודה

nmap -sn 192.168.1.1-254

בסוף, הוא יציג לכם סריקה של 254 הוסטים ,כמה מהם פעילים ואילו בדיוק מהם פעילים

ניתן להשתמש גם בפקודה

nmap -sn -n -v 192.168.10-254

-n הצג את הקפיצות ליעד ( יציג לנו בצורה אנכית את הכתובות אחת אחת)

-v קיצור של verbose , יציג את כל המידע על הסריקה

**-Pn**

בתצורה זו NMAP מדלג על סריקה האם המחשבים פעילים או לא (הוא מדלג על שלחת ה SYN), הוא פשוט מריץ על כל הטווח את בדיקת הפורטים ורק בסוף יציג תוצאה

nmap -Pn 192.168.1.1-254

**-PS**

בתצורה זו הNMAP יבצע בדיקה האם המחשב פעיל על ידי שליחה של SYN בודד אחד,אם השרת ישלח בחזרה אלינו דגל מסוג RST זה אומר שהפורט סגור, אם הפורט פתוח המטרה (השרת) ישלח לנו כעת SYN + ACK כמו שהסברתי למעלה, מאותו הרגע המכונה שלנו עם ה NMAP תחזיר למטרה \ שרת דגל מסוג RST ובכך “תשבור” את ה Threeway Handshake

nmap -PS 192.168.1.1-254

**-PA**

בתצורה זו הNMAP שולח ACK ו SYN במקום SYN בלבד ובכך בודק אם הפורט פתוח או סגור, אם סגור המטרה תשלח לנו RST אם פתוח הוא ישלח SYN ואם סגור נקבל מהמטרה RST. על ידי שליחה של גם SYN + ACK אנחנו מעלים את הסיכוי לדלג על ה FW שנאמר מבצע חסימה של SYN מתמשכים.

nmap -PA 192.168.1.1-254

**-PU**

בדיקה זו מבצעת בדיקה האם הHost פעיל או לא על ידי שליחה של UDP Ping, כאשר המטרה מחזירה שגיאה ICMP port unreachable זה אומר שהפורט סגור, אם הוא מקבל חסימה או חוסר תגובה, זה אומר שהמכונה למעלה

nmap -PU 192.168.1.10-254

**-PY**

אפשרות זו שולחת SCTP Packet במצב זה הוא שולח דגל INIT בלבד, אם הפורט בתחנה סגור הוא יקבל INIT-ABORT ואם הוא פתוח הוא יתחיל ב SCTP ובתהליך הפרוטקול שלו שהוא Fourway-HandShake

**-PE, -PP, -PM**

בתצורה זו כאשר nmap שולח בדיקה האם המטרה פעילה או לא הוא יכול לבצע זאת על ידי פינג שהוא ICMP, למעשה ברגע ששלחנו למטרה ICMP מסוג Eco Request אנחנו צריכים לקבל מהמטרה Eco Reply, לרוב ברגע שהIPS \ FW מבין שמבוצע סריקה מסוג זה הוא חוסם את הסריקה.

**-PO**

אפשרות זו בודקת אם המחשב פעיל ואת הפורטים על ידי שליחה של IP Ping זו תצורה יחסית חדשה בNMAP והוא משלב את הסריקה של TCP ו UDP ו SCTP בכך מיישם אותם בסריקה אחת.

**-PR**

נפוץ מאוד בסריקה של רשת LAN שבה אתם נמצאים, שכן המחשב שלכם מקבל ARP מכל המחשבים המחוברים ברשת, בתצורה זו הוא שולח ARP Request על מנת לקבל תשובות משאר המחשבים ברשת וכל מחשב שפעיל אמור לשלוח חזרה הודעה וברגע שהוא מצא את המחשבים הפעילים הוא יבצע עליהם סריקת פורטים

**–disable-arp-ping**

על מנת לבטל לחלוטין סריקה של ARP על ידי NMAP יש להקיש את הפקודה הזו

**–traceroute**

על מנת לראות מה הקפיצות ליעד ניתן להשתמש בפקודה זו

**-n**

יבטל את בדיקת ה DNS לכל Host ו Host

**-r**

יבצע בדיקת DNS לכל ההוסטים

**–system-dns**

יבצע בדיקה של ה Hosts שאנחנו סורקים מול שרת הDNS של המחשב

**חיפוש פורטים פתוחים**

ל NMAP קיימים 6 קטגוריות של פורטים

**Open**

התוכנה \ אפליקציה מקבל חיבורי TCP \ UDP או SCTP וזו המטרה הראשית בחיפוש פורטים פתוחים וסריקתם ואילו המטרה הנגדית היא של פיירוואל שמטרתו היא לחסום את הפורטים האלו למי שאינו מורשה

**Closed**

הפורט פתוח אך אין שום שירות שמאזין לו, כדאי לבדוק לאחר זמן מה אם אותו השירות שמשתמש בפורט הזה עלה, שכן פתחו את הפורט הזה לשימוש אבל אין שום אפליקציה פעילה.

זהה למצב בו פותחים פורט בפיירוואל אבל אין שום אפליקציה שמשתמשת בפורט הזה ולכן הוא פתוח אבל סגור.

**Filtered**

פורטים אלו חסומים ב FW או על ידי כלים אחרים ויוצגו כ Filtered

**Unfiltered**

הוא מייצג שהפורט לא זמין, זאת אומרת שהוא אינו מצליח לקבוע אם הפורט פתוח או לא ורק סריקת ACK (סריקה מסוג -sA שנדבר עליה בהמשך) יכולה להציג פורטים בתצורה הזו ורק סריקה “שקטה” כמו SYN שהוא sS או FIN יכולים לגלות אם הפורט הזה פתוח או לא

**Open|Filtered**

כאשר NMAP לא מצליח לקבוע אם הפורט ה Filtered או פתוח הוא מציג את זה בתצוגה הזו, זאת אומרת שהפורט פתוח אבל הוא לא יודע אם יש שירות מאחוריו או לא.

**Closed|Filtered**

NMAP לא מצליח לקבוע האם הפורט סגור או Filtered ועל כן יש להשתמש בסריקה שקטה

**סריקת פורטים**

**-sS**

זה סריקה מסוג Syn והוא הנפוץ ביותר, הוא מהיר ביותר ויכול לסרוק אלפי פורטים בכמה שניות ובכל זאת להישאר “מוסתר” מפני מערכות IPS אשר נמצאות ב Firewall וזאת על ידי כך שהוא אינו מסיים את פעולת ה TCP במלואה ולא שולח דגל Fin  
והסריקה לרוב נקראת “חצי סריקה” בגלל שהוא לא פותח תקשורת TCP מלאה ונעצר ב SYC+ACK

**-sT**

כאשר לא ניתן להשתמש ב-sS בסריקת SYN ניתן להשתמש בסריקה פחות טובה שהיא סריקת TCP Connect, על ידי סריקה זו ה NMAP שולח בקשת TCP בתצורה בה הNMAP מבקש מהשרת עצמו ליצור איתו קשר במה שנקרא System Call לרוב עדיף להשתמש בSYN Scan

**-sU**

סריקה זו למעשה סורקת את הרשת בפורטים של UDP, יש הרבה שמוותרים על סריקה זו, אך זו טעות שכן אפליקציות כמו SNMP פועלות בטווח זה (161) ולרוב משלבים את הסריקה יחד כך:

nmap -sU -Ss 192.168.1.1-254

**-sV**

יבצע סריקה לגירסה של הפורט אותו הוא מחפש

**-sY**

סריקה זו היא מסוג SCTP והוא פרוטוקול יחסית חדש לTCP ו UDP ויש אפליקציות מסוימות שמשתמשות בפרוטוקול זה שמשלב בין TCP לUDP ובכך יעיל יותר.

**-sN -sF -Sx**

סריקת XMAS, או בשמה השני סריקת “עץ חג המולד” משתמש בחולשה בTCP שאם שולחים את שלושת הדגליםFIN PSH ו URG ומקבלים חזרה RST זה אומר שהפורט סגור ואילו אם לא נקבל תשובה כלל, הפורט למעשה פתוח

**-sA**

בדיקה מסוג ACK ששולח דגל מסוג ACK ובכך בודק אם הכתובת שהיא כתובת של FW היא Stateful או Stateless

Stateless- אומר שהפיירוואל לא פותח את הPacket כולה וקורא רק את ה Heder

Stateless – אומר שהפיירוואל פותח את כל ה Packet ובדוק את התוכן וכך קשה יותר לעקוף אותו

הוא שולח רק ACK ובכך מחכה לקבל RST על כל פורט שמחזיר RST הוא מבין שהפורט פתוח אך אינו יודע אם יש שירות מאחוריו.

**-sW**

הוא דומה מאוד ל-sA הוא שולח דגל ACK אבל בהודעת ה RST שמגיעה חזרה הוא בודק את ה Windows Size שם בחלק מהאפליקציות אם חוזר 0 זה אומר שהפורט סגור ואם חוזר 1 זה אומר שהפורט פתוח

**-sM**

הM מייצגת מימון, כן כן ישראלי בשם אוריאל מימון שעל שמו נקרא אופציה זו והוא זה שגילה אותה

הוא גילה שמערכות מסוג BSD (יוניקס) כאשר נשלח FIN\ACK והפורט פתוח, הן פשוט מפילות את החבילה ולא שולחות RST ובכך כל חבילה שNAMP יפיל בתצורה זו יהיה פורט למעשה פתוח.

**–scanflags**

יהיה סריקה עצמאית למשל

–scanflags ackfin

ישלח ACK ו FIN

למשל

–scanflags syn

יבצע את אותה הפעולה כמו -Ss

**-sI**

סריקה מתקדמת בה ניתן להזין כתובת IP של מכונה אחרת לה יש לנו גישה והסריקה תבוצע מהמכונה הזו ותוחזר אלינו

**טווחים**

**-p**

חיפוש של טווח פורטים מסוים למשל

nmap -sS -p1-1000 192.168.1.10

יבצע סריקה של הפורטים מ 1 עד 1000

**–exclude-ports**

על ידי פקודה זו נוכל להגדיר לו אילו פורטים לא לסרוק

**-F**

ברירת המחדל של סריקת NMAP (של כמות הפורטים שהוא סורק) זה 1000 על ידי התוספת -F הוא יבצע סריקה של 100 הפורטים הנפוצים ביותר ולא 1000 ובכך הסריקה תיהיה מהירה יותר

**-r**

יבצע את הסריקה והתוצאה לפי סדר נומרי מ 1 עד 1000 אם הגדרתם סריקה רגילה

**גילוי שירותים \ שמות וגרסאות \ מערכות הפעלה**

**-Sv**

מבצע סריקה של השירות, את השם שלו ואת הגירסה שלו אם הוא מצליח לקבל מהפורט הפתוח והאפליקציה אשר משתמשת בפורט זה

**–allports**

יבצע בדיקה לכל הפורטים וינסה לברר את שמם וגרסתם

**-O**

מנסה לגלות את גרסת מערכת ההפעלה שאותה אנו סורקים

**NSE – Nmap Scripting Engine**

הוא למעשה סקריפט סריקה של NMAP ניתן להוריד או להשתמש בסקריפטים קיימים של סריקה

-sC

מבצע סריקה של הסקריפט ברירת המחדל

–script

בחירת סקריפת סריקה

nmap –script “http-\*”

יבצע סריקה בעזרת כל סקריפט שמתחיל ב http

nmap –script “not intrusive”

יפעיל את כל הסקריפטים של הסריקה חוץ מאלו הנחשבים כ”מוגזמים”

**פקודות נוספות**

**-v**

יציג את כל פעולות הסריקה

**-d**

יציג תקלות או בעיות אם קיימות בזמן הסריקה

**–reason**

יציג מה קבע שהפורט \ המטרה הזו פתוחה או פעילה, אם זה SYN קבע זאת? האם זה ACK קבע זאת?

**–open**

הצג רק פורטים פתוחים שבהם נוכל להשתמש

**-oX**

-oX tal.xml

ייצא את המידע לקובץ XML שאותו ניתן למשל לטעון ל Metasploit או להשתמש בו באפליקציות אחרות של איסוף מידע.

**–stylesheet**

–stylesheet tal.xml

בתצורה זו גם כאן המידע מיוצא לקובץ XML שאותו ניתן לפתוח ב Firefox בתצוגה נוחה.

#### חיפוש פורטים פתוחים ברשת כולה

nmap 192.168.1.0/24

nmap = הפעלת התוכנה

192.168.1.0 סריקה של כל הרשת הוא יחפש את כל הHosts ברשת

24 = מסמל את ה Perfix של השרת (255.255.255.0)

#### חיפוש Alive Hosts

nmap -sP 192.168.1.\*

-sP = פקודה לביצוע פינג לבדיקה של איזה Host פעיל (מתקשר עם הרשת)

192.168.1.\* = עם הכוכבית בסוף מציין שיבצע סריקה על כל הרשת ב Perfix 24

#### חיפוש על פי זמנים

הפקודה:

nmap -T5 192.168.1.0/24

-T5 זמן החיפוש (T5 מסמל את המהיר)

192.168.1.0/24 כתובת הרשת

T5 = המהיר ביותר

T4 = מהיר

T3 = נורמל

T2 = פחות מנורמלי

T1 סריקה איטית

T0 = האיטית ביותר – והיא שולחת Packet אחת כל 5 דקות על מנת שמערכות IPS לא יעלו על הסריקה ויחסמו אותנו על ההתחלה

#### חיפוש על פי 50 הפורטים הנפוצים ביותר

החיפוש הבא יבצע חיפוש של הרשת על פי 50 הפורטים הנפוצים ביותר במקום שהחיפוש יבצע על כמעט 1000 הפורטים הנפוצים ביותר ויחסוך גם מזמן החיפוש

הפקודה:

nmap –top -ports 50 192.168.1.0/24

–top-ports 50 = אומר לו לסקור 50 פורטים נפוצים ביותר

(את שאר הפקודה אתם מכירים)

#### בדיקת פורט מסוים אם פתוח או לא

פקודה זו מבצעת בדיקה אם פורט פתוח או סגור, לקחתי את הפורט 80 לבדיקה על כל הרשת

הפקודה

nmap -sT -p80 192.168.1.0/24

-sT = סריקה פשוטה של TCP (סריקה של לינוקס Connect)

p80 = הפורט אותו בחרתם פורט 80

ניתן לראות ששרת 192.168.1.102 פורט 80 כרגע פתוח

#### ביצוע סריקה של מחשב\שרת ברשת שאינו עונה לפינג

NMAP מבצע סריקה של הרשת קודם כל על ידי פינג על מנת לבדוק איזה מהכתובות מחזיר תשובה ולאחר מכן מבצע עליו סריקה של פורטים, סוג המערכת, שרותים שרתים וכו’ הפקודה -Pn מבצעת סריקה שנקראת No Ping זאת אומרת שה NMAP מדלג על הPING ומבצע סריקה ישירה על כל כתובת IP

דוגמא:

nmap -Pn 192.168.1.105

#### חיפוש שקט בביצוע SYN אל השרת

הסבר לפני, כאשר מבוצע התחברות TCP בין שני מערכות מבוצע “לחיצת ידיים משולשת” או באנגלית three way handshake ופה מעורבים 3 פקטים הנשלחים על מנת למנוע תיקון שגיאות וברור אם הפקטה שנשלחה שלמה  
הפקטה נשלחת עם דגל , דגל אומר לצד המקבל את סוג הפקטה, קיימים 4 דגלים

SYN – Synchronise

ACK – Acknowledge

FIN – Finished

RST – Reset

וזה עובד בשיטה הזו, צד אחד שולח את הפקטה ומקבל  Synchronise וצד שני מקבל את הפקטה וגם שולח Synchronise, מודיע לצד השני שהוא קיבל Acknowledge וכך ממשיכים עד לסיום השליחה של כל החבילה, בסיום הצד השני מודיע על Finished והתהליך נסגר Reset  
הפקודה -sS עובד בצורה הבאה:

הוא שולח SYN ומחכה לתגובה ברגע שהוא מקבל תגובה SYN\ACK הוא יודע שהפורט פתוח ואז NMAP שולח ישיר פקודת RST על מנת לסגור את ההתקשרות ביניהם לפני שיתבסס התחברות מלאה וכך Firewalls לא רושמים בלוגים שלהם את המצב הזה כי לא התבסס חיבור מעולם

#### הטעייה Decoy של NMAP

Decoy היא אפשרות נוספת ב NMAP המגדירה כאילו הבדיקה נעשת מכמה כתובות IP, כך כל Firewall Logs יקבל כאילו הבקשה הגיע מכמה כתובות IP עד שיקח זמן לאיש אבטחת המידע לאתר מי בצע את הבדיקה ואולי פרת או נכנס למערכת

nmap -sS 192.168.1.105 -D 192.168.1.50,192.168.1.55

-Ss= כתוב עליו נושא הקודם , (“חשאי”)

-D שהוא קיצור ל Decoy

192.168.1.50 192.168.1.55 כתובות ה IP שהם לא “באמת” אבל ה Firewall יחשוב שכן