התקפת תקשורת DoS DDoS

CYBER SCHOOL

מטרות

לימוד התקפות רשת, ועל יכולתן לבצע מניפולציות על התקני רשת ותשתיות ואף לפגוע בהן. להכיר את סוגי תקיפות הרשת והכלים. בשיעור זה נתמקד בהתקפת DoS/DDoS.

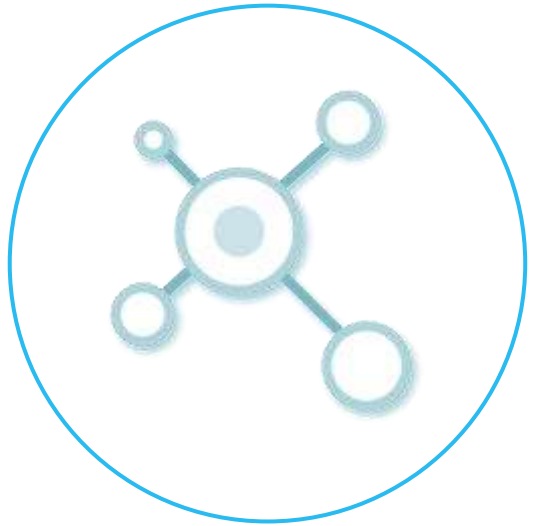
- מונחים ומושגים
- DoS/DDoS

CYBER SCHOOL

CYBER SCHOOL

מונחים ומושגים

מתקפות רשת - סקירה כללית



המטרה היא לבצע מניפולציה על תשתיות הרשת או לפגוע בה.

- יירוט של מידע רגיש (On-Path)
- מניעת שירות (DoS)

CYBER SCHOOL

יעדים של
מתקפות רשת

מכשירי קצה

ציוד בניית
רשתות

התקני
אבטחה

שרתים

CYBER SCHOOL

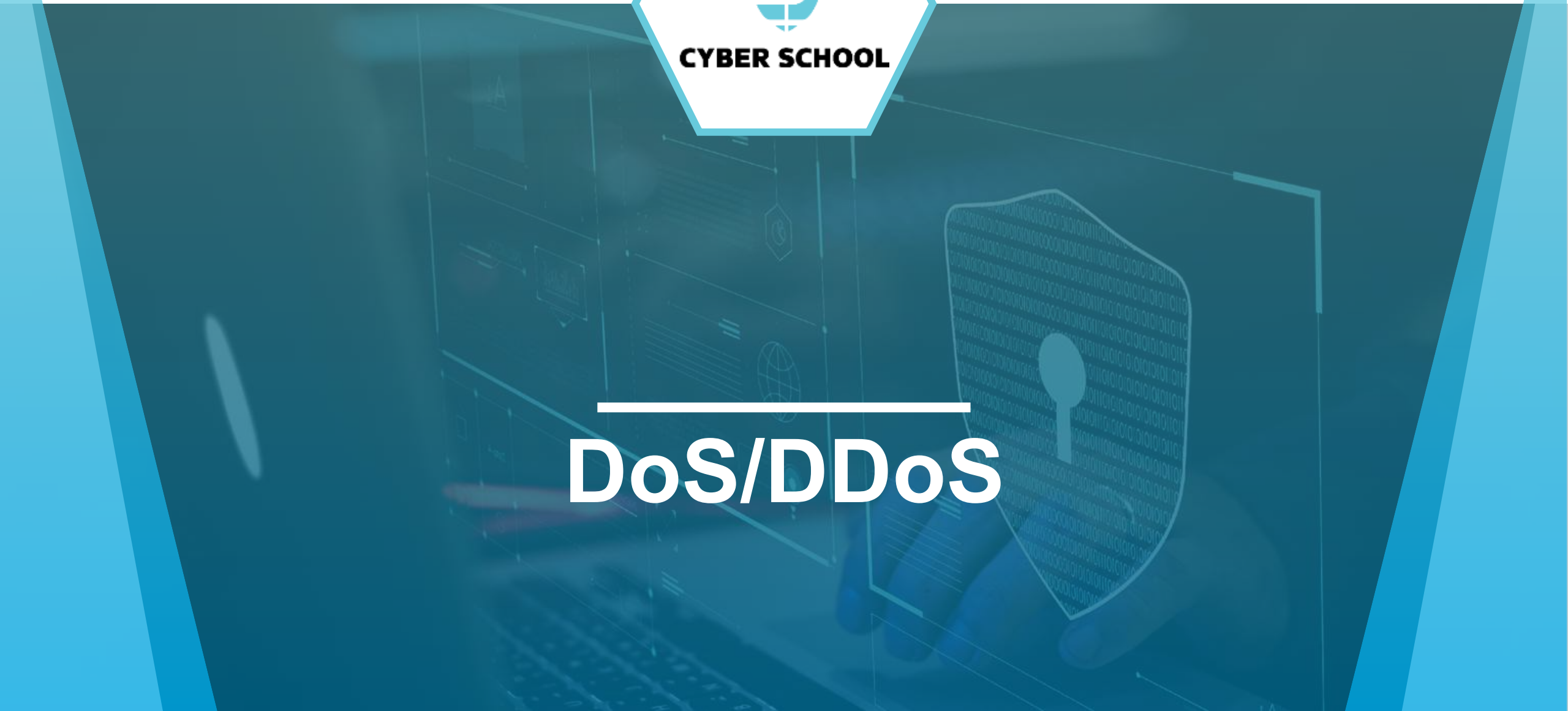
מתקפות רשת נפוצות

- לפניכם כמה סוגים ידועים של התקפות רשת שניתן להפעיל כנגד שירותים שונים.

Sniffing	יירוט תעבורת רשת באופן אקטיבי או פסיבי
IP Spoofing (זיוף כתובות IP)	התחזות לכתובת IP אחרת
MAC Spoofing (זיוף MAC)	התחזות לכתובת MAC אחרת
הרעלת DNS	מניפולציה על המידע ברשומות ה-DNS
הרעלת פירוק שמות (Name Resolution Poisoning)	מתמקדת בפרטי ההתחברות של משתמשים באמצעות דומיינים מזויפים

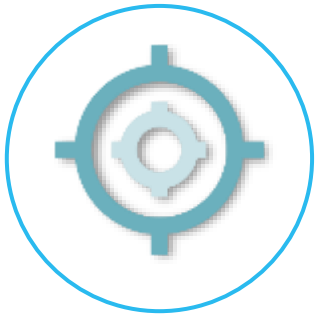
CYBER SCHOOL

CYBER SCHOOL



DoS/DDoS

התקפות מניעת שירות (DoS)



מניעת שירות (DoS)
מתקפה שגורמת לשירות לקרוס על ידי ניצול תכונה פגיעה

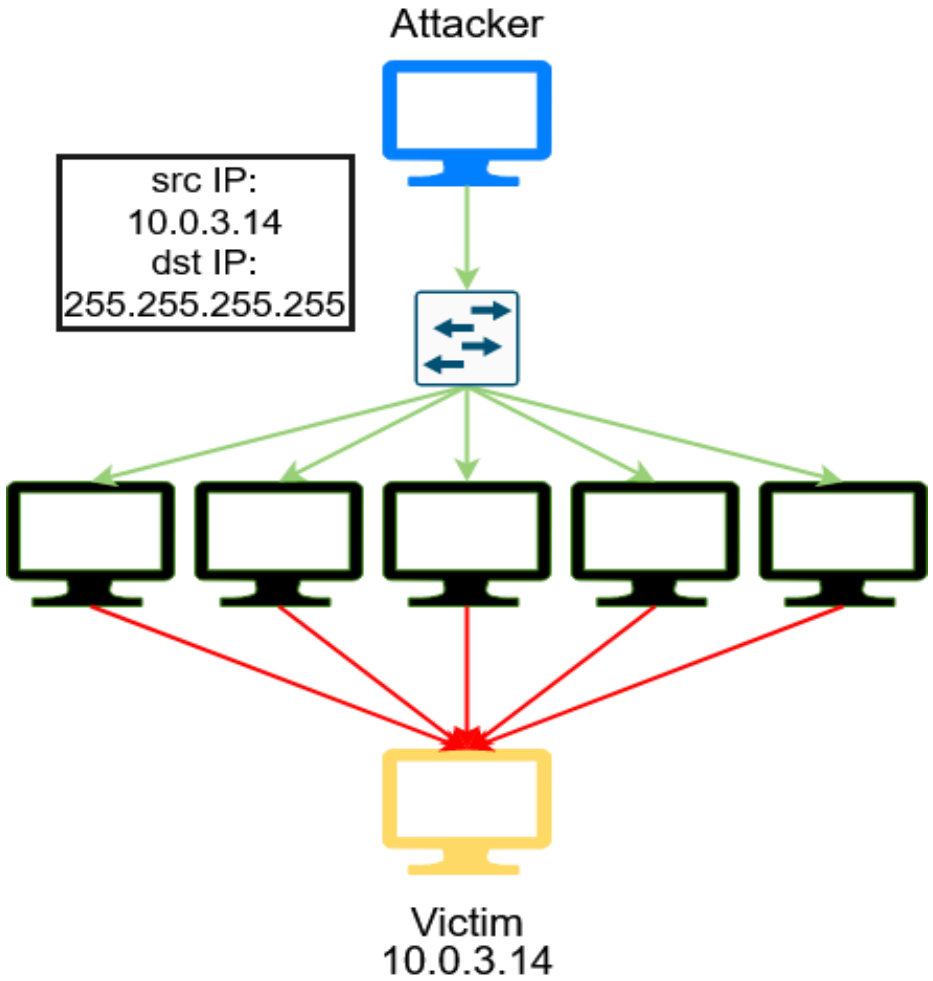
מניעת שירות מבוזרת (DoS)
התקפת DoS המופצת בין מקורות מרובים ליצירת כמות גדולה יותר של תעבורה

- התקפות DDoS הן בעצם התקפות Dos בקנה מידה גדול יותר.

CYBER SCHOOL

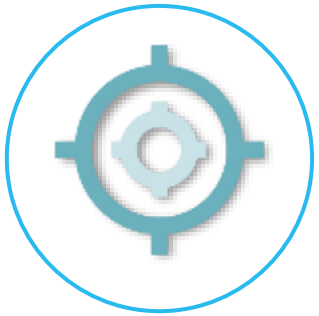
מתקפת Smurf

- מתקפת DDoS שמשתמשת בפרוטוקול ICMP
- משתמשים בכתובת IP מזויפת כמקור לשידור פינג.
- המחשבים מגיבים אל כתובת המקור.



CYBER SCHOOL

קטגוריות של מתקפת DDoS



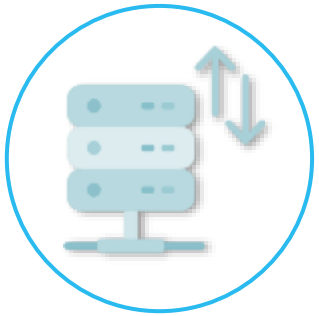
Dos יישומים
מתקפה שגורמת לשירות לקרוס על ידי ניצול תכונה פגיעה של האפליקציה

DDoS נפח (Volumetric)
מתקפות שמשתמשות בכמויות מסיביות של תעבורה כדי להפיל שירותים

- השימוש במילה "נפח" (Volumetric) מצביע על כך שהמתקפה כוללת נפח גדול של תעבורה.

CYBER SCHOOL

התקפות Dos ברמת היישום



משאבי שרת
כל שרת צורך חלק מהמשאבים שלו כדי לבצע הוראה. המשאבים אינם בלתי מוגבלים.

הצפת משאבי יישום
מנצלת תכונות בגון *Forgot password*, התחברויות ויצירת חשבונות

CYBER SCHOOL

התקפות Dos נפחיות

מתמקדות בפרוטוקולים של תקשורת

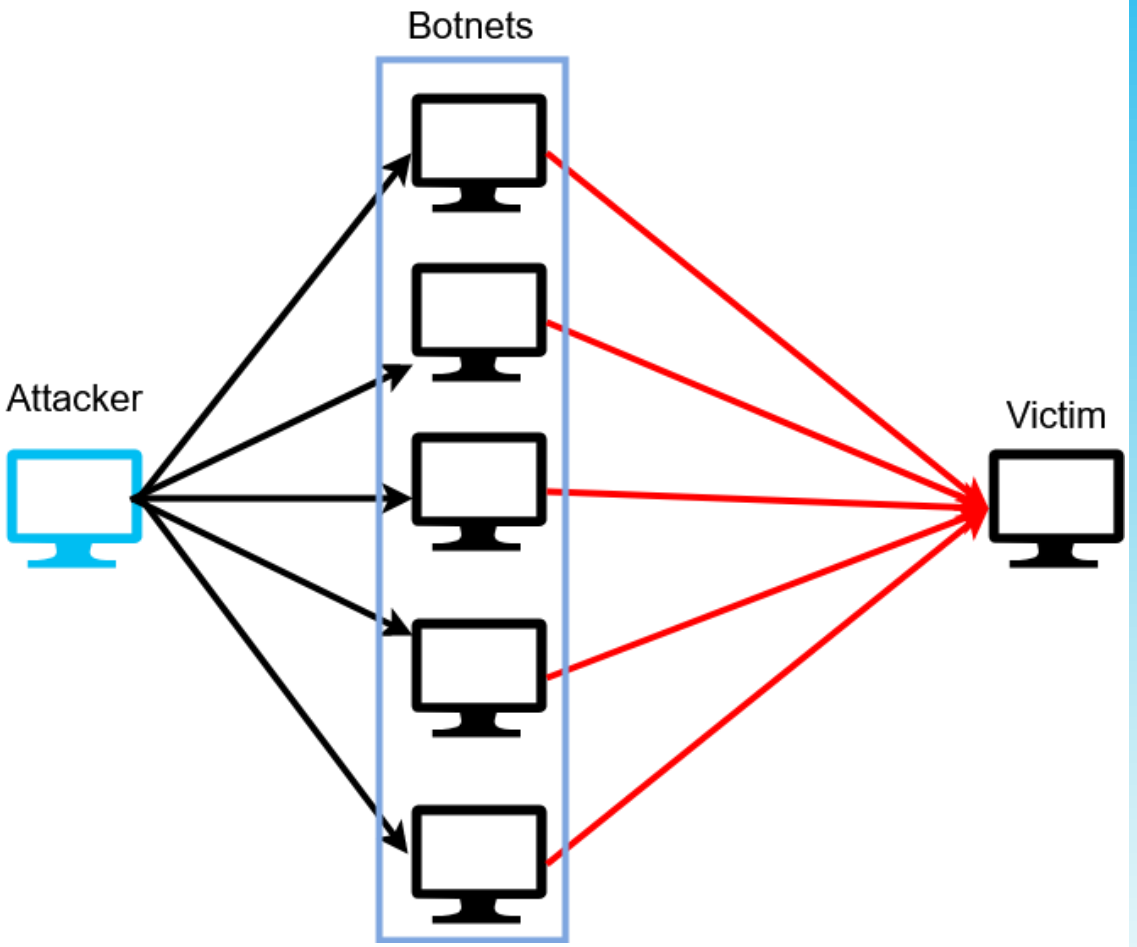
מציפות את השרתים בבקשות

צורכות את משאבי הרשת

CYBER SCHOOL

Botnets

- רשת של מחשבים הנשלטים מרחוק
- המחשבים נגועים בקוד זדוני ומגיבים לפקודות התוקף.
- ניתן להשתמש ב-Botnets (בוטנטים) להתקפות DDoS המבוצעות ממחשב מרכזי.



CYBER SCHOOL

DDoS בשירות

שיטה פשוטה לתקיפת DDoS

מבוצעת על ידי שירותים מקוונים בתשלום

משמשת הן לצורך עריכת בדיקות אבטחה והן למטרות זדוניות

כוללת שירותים חוקיים ולא חוקיים כאחד

CYBER SCHOOL

XYZ Booter

- שירות DDoS חוקי לבדיקת כתובות IP, אתרים ושרתים.

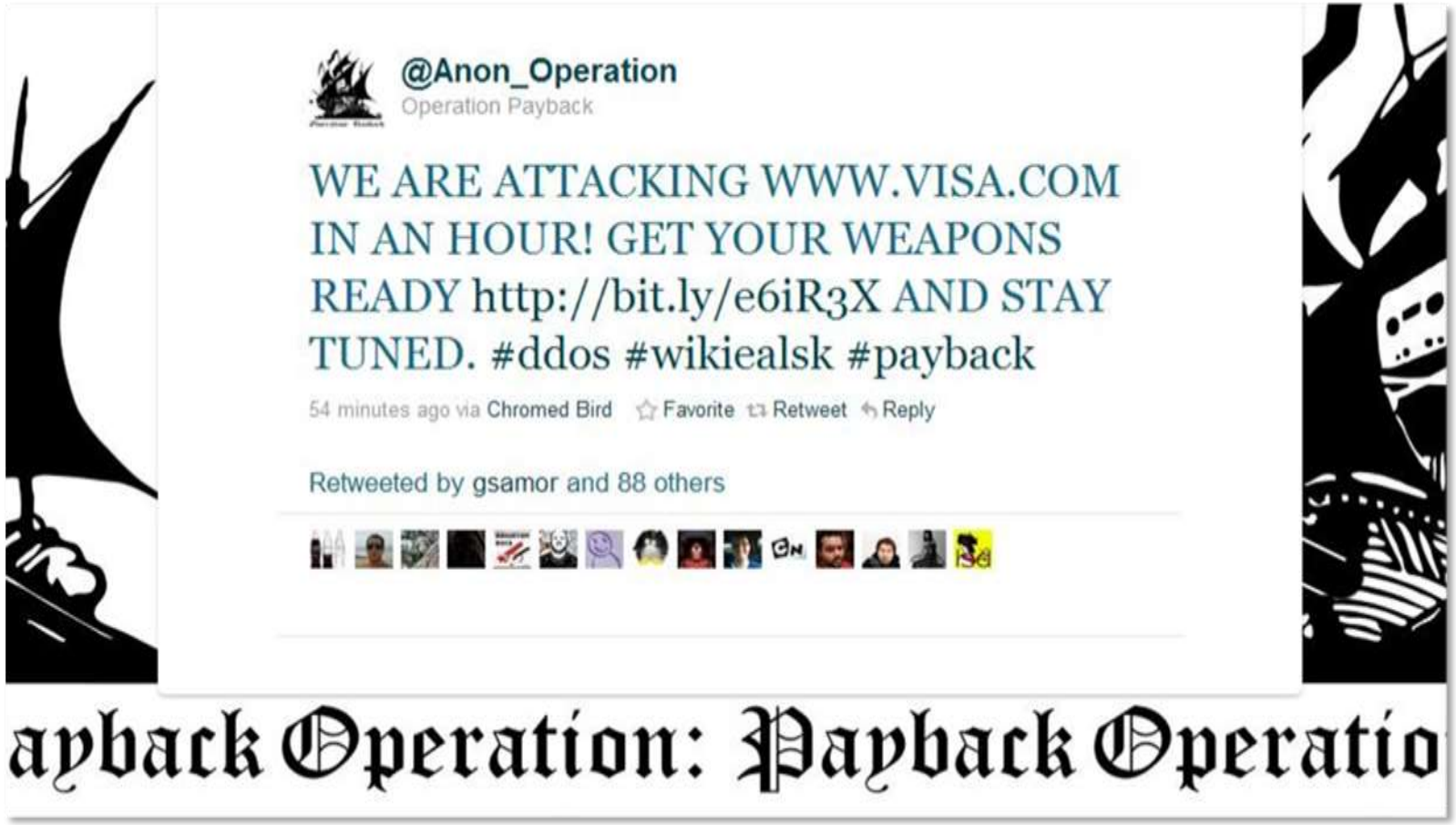
CYBER SCHOOL

Low Orbit Ion Cannon (LOIC)

- כלי DoS קל להורדה ולשימוש
- מצריך רק כתובת IP או כתובת URL כדי לעבוד
- קיימת גם גרסה מקוונת

CYBER SCHOOL

מבצע Payback



- אנונימוס השתמש ב-LOIC לביצוע מתקפת DDoS מאסיבית במהלך מבצע Payback.

CYBER SCHOOL

3hping

כלי Linux המיועד לבדיקת אבטחה
מספק את היכולת להציף את המטרה עם מנות ICMP
בעל יכולות ליצור מנות רשת

```
root@kali:~# hpingh-3
usage: hping3 host [options]
-  h  --help      show this help
-  v  --version   show version
-  c  --count     packet count
-  i  --interval  wait (uX for X microseconds, for example -i u(1000
--      fast      alias for -i u10 )10000 packets for second)
--      faster    alias for -i u100 )1000 packets for second)
--      flood      sent packets as fast as possible. Don't show
replies.
-  n  --numeric   numeric output
-  q  --quiet     quiet
-  I  --interface interface name (otherwise default routing
interface)
-  V  --verbose   verbose mode
-  D  --debug     debugging info
-  z  --bind      bind ctrl+z to ttl           (default to dst port)
-  Z  --unbind    unbind ctrl+z
--      beep      beep for every matching packet received
```

CYBER SCHOOL

צמצום התקפות DoS/DDoS

זיהוי
תחילה יש לזהות שימוש בנפח גבוה כתקיפת DDoS, ולא בהתרחשות טבעית ברשת.

Response (תגובה)
כאשר מזהים אותם, ניתן לחסום כתובות IP ויציאות, והמנות יימחקו.

CYBER SCHOOL

תרגול קצר:
הפרעה לתעבורה ברשת

10-15 דקות

המשימה

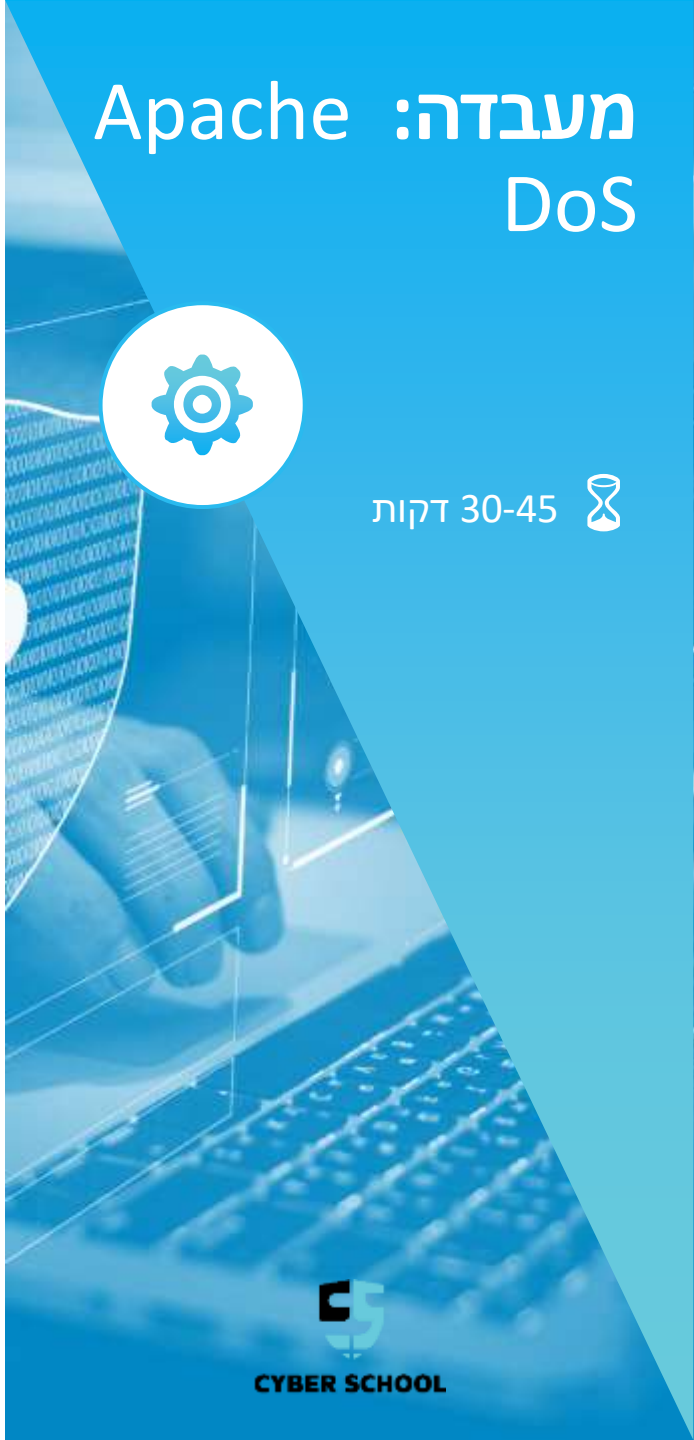
יש להציף מחשב במנות ICMP כדי לקטוע את רוחב הפס של הרשת.

השלבים

- יש להשבית את חומת האש במכונה הווירטואלית Windows VM.
- יש לפתוח את חלון הביצועים של מנהל המשימות.
- יש לשלוח פינג ל-Windows מתוך Kali.
- האם פקודת ה-ping הצליחה לקבל תשובות?
- במערכת ההפעלה Kali, יש לפתוח מסוף נוסף והריצו את הפקודה:
  doolf-- [sserdda PI swodniw]1 -3 hping
- האם פקודת ה-ping עדיין מצליחה לקבל תשובות?

CYBER SCHOOL

מעבדה: Apache DoS



30-45 דקות

המשימה

יש לבצע מתקפת מניעת שירות בעזרת הפקודה ***3hping*** נגד שרת Apache ולהקפיא את האתר.

השלבים

יש להתקין XAAMP ב-10Windows.

יש לקבוע קונפיגורציית שירותי XAAMP.

יש להריץ את הפקודה ***3hping***.

שרת רשת DoS Apache

כלים

VirtualBox
Kali Linux
10Windows

קבצים קשורים

מסמך מעבדה
XAMPP

CYBER SCHOOL

מעבדה:
הרצת Dos

20-30 דקות

המשימה

יש לבצע מתקפת מניעת שירות ברשת.

השלבים

יש לוודא שיש לכם גישה לאינטרנט.
יש להרעיל את טבלת ה-ARP של Windows10.
יש לחסום העברת תעבורה.
יש לבדוק את חיבור האינטרנט.

כלים

VirtualBox
Kali Linux
Windows 10

קבצים קשורים

מסמך מעבדה

שאלות?