תשתית בסיסית - Basic infrastructure

במודול זה יסקר כל התחום של התשתית הבסיסית, ניתן אף לומר השלבים הראשונים בהליך התקפה.

Attack Cycle:

WireShark:

כלי זה הוא הכלי העוצמתי ביותר שקיים בניתוח תעבורת רשת
בעת פתיחת כלי זה ניתן לראות את כלל ה-packets מתוך כרטיס הרשת לכן אפליקציה זו נקראת SNIFFER
כלי זה הינו פסיבי משמע שללא מניפולציה לא ניתן לדעת שמישהו מאזין.
לכן כלי זה הוא בין הכלים הראשונים להפעלה במטרה לבדוק האם ישנה פריצה ואיזה מידע עובר ברשת.
ישנם עוד כלים שעושים Sniffing במערכות אחרות כמו לינוקס.

Kismet: 2 עובד עד שכבה
tcpdump:
>cd pump -i eth0 -w pcap_file.pcap - תכתוב את הקובץ במיקום מסוים

File Format:

Packet capture
Driver
libpcap
winpcap

פרמטרים להאזנה לפקטות:

pac - vpurny vfkkh ביותר להאזנה ונתמך ע"י רוב הסניפרים
pcap / packet capture -
פורמט זה מכיל פקאטות בלבד ונוצר ע"י הדרייבר של libpcap בד"כ UNIX

Pcapng -
פורמט זה מכיל כמות אדירה של מידע אקסטרה כמו סטטיסטיקה ועוד.

Wireshark usage:

הכלי wireshark משמש אנשי סייבר ל-4 דברים:

1. בחינה - בכדי לבדוק האם יש תקיפה.
2. טיפול בתקלות.
3. דיבאגינג - בדיקת מבנה של פרוטוקול מסוים.
4. למידת הרשת.

כפתור ה-capture option:

Enable promiscuous mode on all interfaces:
מצב זה הוא מצב מיוחד המגדיר ל-wireshark לא להפיל packets שלא מיועדות אלי.

בכדי להתגבר על עקרון הפרגמנטציה wireshark יודע להרכיב את הפאזל בעצמו.

Wireshark filters:

כלי זה מאפשר סינון של מידע בהתאם לרצונותיו של החוקר במטרה להציג מידע רלוונטי ככל הניתן.
הכלי wireshark מאפשר 2 סוגים של filters,

Hard filter
Soft filter

ה-HARD פילטר מגדירים בהתחלה והגדרה זו תתפוס את התעבורה בהתאם ל-Filter.
ה-soft filter זהו פילטר אשר מתייחס לתצוגה בלבד.

Filters:

Soft

Ip.src == 10.0.0.12
Ip.dst == 10.0.0.12
Ip.addr == 10.0.0.12
tcp
Dns
Tcp.port == 80
Tcp contains pass
Http.response.code == 200
Vlan.id == 1

Footprinting:

שלבי התקפה:

1. מי המטרה
2. איסוף מידע
   a. יש שאומרים ש-70% מכל תהליך הפריצה הוא איסוף מידע או reconesense, כחלק מאיסוף המידע יש תהליך של footprinting כלומר מציאת עקיבות.

סוגי footprinting:

1. משג pinpointing - מונח מקצועי המתאר צמצום מרחב תקיפה של מטרה.
2. עוד מושג של footprinting הוא Bussiness structure - מבנה הארגון יכול להוביל לחשיפת חולשות בארגון.
3. עוד מושג של footprinting הוא social information - למידת עמדות חברתיות בארגון הוא קריטי לתכנון תקיפה מאורגן.

Useful information for footprinting:

- Domain name
- Authentication details
- Routing tables
- IDS
- News - articles
- Passwords
- Users
- Groups
- Ip
- Vpn
- Websites
- Acl
- Email

Search engines:

- Google Advanced search
- Netcraft
  - https://searchdns.netcraft.com
- Shodan.io
  - התקנה של SHODAN ללינוקס:
  - Pip install shodan
  - Shodan Filters: (no space)
    - Port:##
    - Country:il
    - net:ip-SM
- Ipinfo.io
- Censys
- Pastebin.com (credit cards and more)
- Linkedin

Google Dorks:

GHDB - google hacking database

אתר שמכיל קומבינציות של שאילתות מיוחדות שגוגל יודע לעבד ולהציג תוצאות בהתאם.

Website footprinting:

- OS
- Directories
- Scripting platforms
- Version
- Whois.net - יחפש את כל המידע של בעלי האתר
- Dmitry -i - כלי חיפוש של כל המידע של בעלי אתרים ברחבי העולם
  - dmitry -i http://website.com
- Maltego - כלי חיפוש גרפי על כל המידע שיעול להיות על ארגונים, אנשים, ואתרים

Spider - Crawler:

הורדה מ-github:

>git clone blackwidow

תוכנה שתלחץ על כל הקישורים של האתר ותמפה אותו מבלי להיכנס לאתר פיזית.

Site mirroring:

יוריד את כל תוכן האתר למחשב.

>httrack https://site.com

Recon-ng:

ישנו כלי מאוד מוכר הנקרה recong-ng והוא עוזר במציאת מידע על כל מטרה באינטרנט ע"י שימוש בכל אתרי החיפוש שקיימים ומציג את כל התוצאות שלהם במקום אחד.
בכדי לפתוח פרוייקט להלן הפקודות:

>workspace add Name
>add domainד websitename
>load <module>
>show <module>
>show options - יראה את האופציות הניתנות להורדה או להרצה
>set <option> <value>
>show info
>run www.website.com

Network scan:

הסיבה לסריקת רשת היא במטרה לקבל מידע על הפגיעויות שבה, עוד סיבה לסריקת הרשת היא כדי לקבל מידע עדכני נאמן בצורה אקטיבית על מטרות פוטנציאליות ברשת.

המידע החשוב להשגה לדוגמא:

- מבנה הרשת
- טווח כתובות IP
- איזה פורטים פתוחים, שירותים שיושבים על אותם פורטים...

כל אלו יכולים לעזור לתוקף להשיג גישה למטרה.

ידיעת שירותי תקיפה שונים יסייע לתוקף למצוא Attack vector ידיעת השרתים הפעילים תועיל בסריקת פגיעויות ובחירתם.

טרמינולוגיה:

Host - מחשב ברשת
Fingerprint - כך מזהים שירותים שונים ברשת למשל שירות טלנט
Ports - פורטים לוגיים

כלים לסריקת רשת וסוגי סריקות:

בכדי לקבל מידע על המכשירים שפועלים ברשת יש לבדוק קישוריות בין המכשירים, אך רוב חומות האש חוסמות PING כברירת מחדל.
לכך קיימים כלים שונים שיכולים לבדוק קישוריות ללא חסימת הקישוריות של חומת האש.

Hping3:

הוא כלי המרכיב חבילות TCP/IP במטרה לנתח את הרשת, כלי זה מאפשר לשלוח כמה סוגי בקשות ICMP אשר יסייעו לנו בהכרת הרשת, כמו כן הוא תומך בעוד פרוטוקולים.
שליחת פינג echo רגיל:

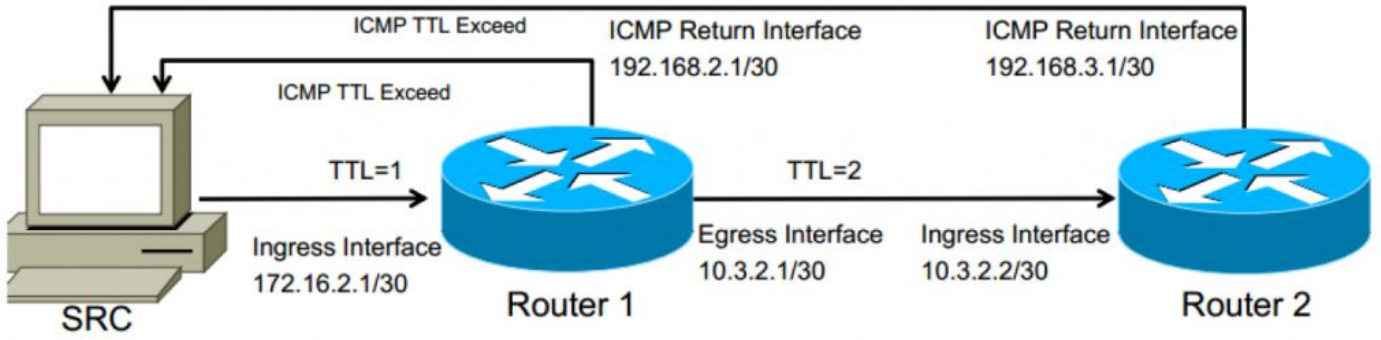
>Hping -1 IP

פקודה שתסרוק את כל הרשת ע"י שליחת PING, בצורה הזו אפשר לגלות איזו מהכתובות דולקות ברשת וכך לדעת את המחשבים הפועלים ברשת:

>hping -1 10.0.0.x --rand-dest -i eth0 --fast

>hping --traceroute -V -1 IP --tr-stop

פקודה זו עושה את פעולת Traceroute על הרכיבים שהחבילה עוברת ברשת עד שמגיעה אל היעד, הכלי יסרוק כל HOP שהחבילה עוברת ויחזיר מידע על אותו רכיב וכך ממפה את הרשת.



Nmap:

שמו של הכלי מורכב מהמילים network mapper ממפה רשת ושימושו העיקרי הוא סריקת הרשת

>nmap 10.0.0-255.0-255

בסריקה רגילה NMAP יציג את 1000 הפורטים הנפוצים ביותר הפתוחים אצל המטרה וכך לגלות נקודות חולשה על המטרה ויציג מספר פורט, הסוג שלו, מצב הפורט, וסוג השירות שמשתמש באותו פורט.
בנוסף NMAP יציג את כתובת ה-MAC של אותה מטרה.

TCP Flags:

URG - Urgent - דגל זה מורה לצד המקבל כי החבילה היא דחופה וחייבת להיות מעובדת מיידית
PSH - דגל זה מורה לצד המקבל להכניס את המידע שאבד בדרך בפקטה במיקום ספציפי
SYN - דגל זה מורה על התחלת תקשורת/הקמת חיבור
ACK - שדגל זה דולק הוא מהווה אישור לקבלת המידע
RST - דגל זה מודיע על reset של כל השיחה

סריקת NMAP הדיפולטיבית נקראת גם TCP SCAN מבצעת three way handshake מלא ומשתמשת בדגלים

- SYN
- ACK
- FIN

>nmap ip/24 -sS

דגל זה מורה ל-NMAP לבצע סריקה שקטה כדי להתחמק מ-Firewall:

>nmap ip -sU

יסרוק שירותי UDP:

>nmap ip -O

האות O מסמן את ה-OS ומזהה fingerprints על מנת לזהות את מערכת ההפעלה.

הכלי NMAP לפני שהוא סורק את המטרה הוא בודק באמצעות PING אם המטרה דולקת, אך אם מלמטרה יש חומת אש דלוקה הפינג לא יעבוד לכן ניתן לבצע סריקה ללא פינג:

>nmap ip -Pn

ישנן 3 סריקות שעוזרות להתחמק מאנטי וירוס וחומת אש:

Fin scan - -sF ip
Null scan - -sN ip
Xmas scan - -sX

בימינו ישנם מערכות הגנה המגינות מפני מערכות סריקה, רוב מערכות ה-IDS מחפשות דגלי SYN על מנת לזהות סריקה בסריקות האלו לא היה SYN דולק וכך ניתן לעקוף מערכות הגנה אלו:

Fin scan -

תשלח דגל FIN דולק, במידה והפורט פתוח מכונת היעד מחזירה RST

Null scan -

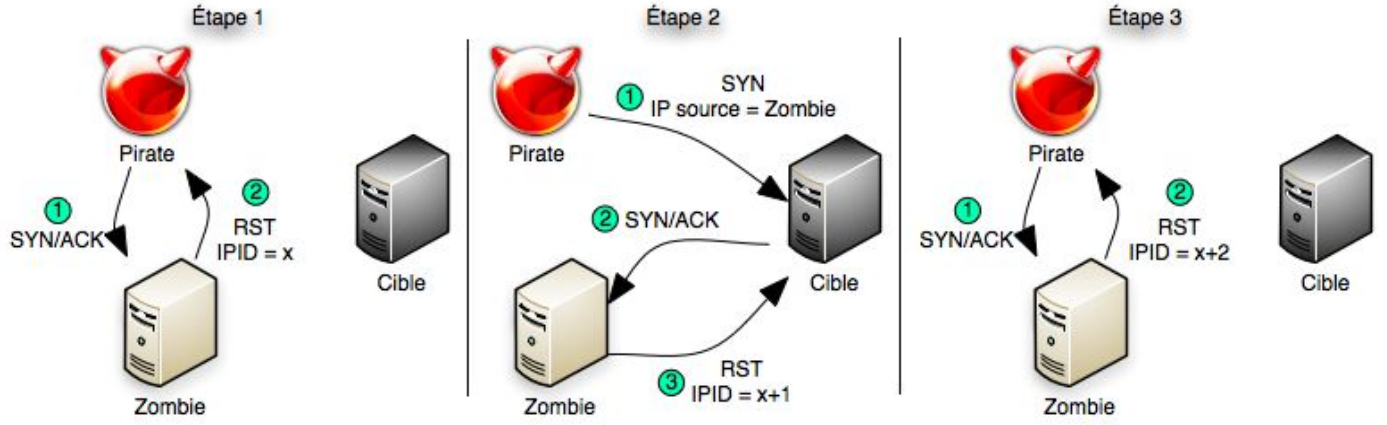
כל הדגלים בחבילה מאופסים במידה והפורט פתוח אני לא אמור לקבל תשובה, במידה והפורט סגור יתקבל RST.

XMAS scan -

הדגלים URG, FIN, ו-PUSH יהיו דלוקים ביחד במידה והפורט פתוח הוא יחזיר RST ובמידה והפורט filter filtered אני לא אקבל תשובה, ובמידה והפורט סגור אני אקבל FIN.

idle scan:

סריקה זו מאפשרת לסרוק מחשב באמצעות מחשב אחר באותה הרשת, המטרה היא לדעת אם הפורט במחשב שאותו נרצה לתקוף דלוק.

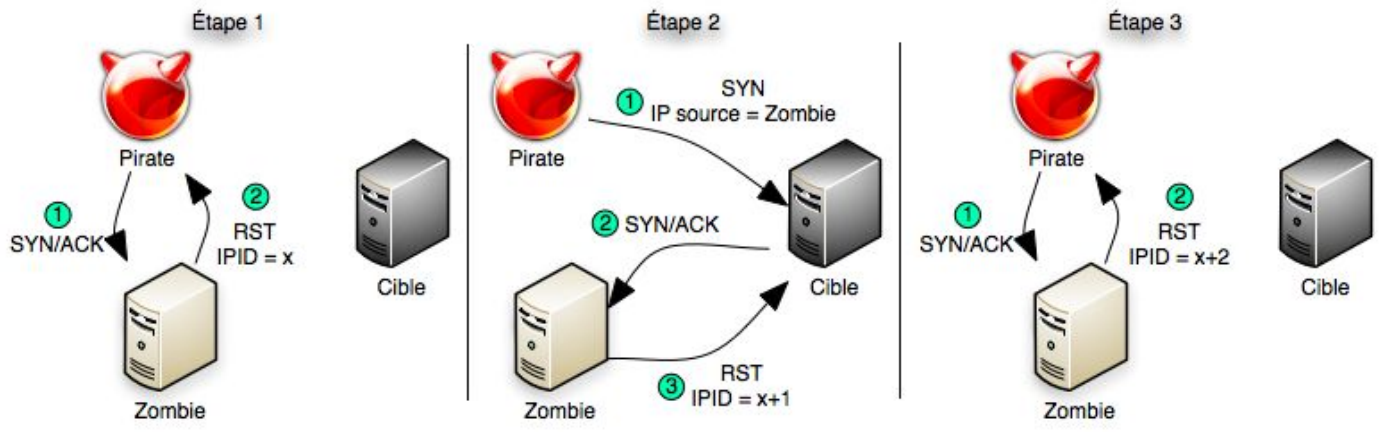


בציור שלפנינו יש את התוקף שהוא ה-"Pirate", המחשב שנעזר באמצעותו לסרוק את המטרה ה-"Zombie", ולסוף יש לנו את המטרה (Cible) .

שלבי הסריקה:

1. PIRATE שולח חבילה ל-ZOMBIE בפורט מסוים.
2. ZOMBIE מחזיר ל-PIRATE תשובה FIN ואת ה- IPID.
   a. בשכבת ה-IP ישנו מספר IP-ID למשל 6000.
3. ברגע ש-PIRATE קיבל FIN הוא מתעד את ה-IP-ID שהוא 6001
4. PIRATE שולח חזרה SYN ל-CIBLE בשם ZOMBIE הנמצאים באותה הרשת.
5. אם מחשב CIBLE שלח SYN-ACK למחשב ZOMBIE ברשת, ה-IPID ישתנה ויעלה בעוד 2 ל-6002 משמע שנוצרה תקשורת בין CIBLE ל-ZOMBIE, ולכן זה מעיד שהפורט של CIBLE פתוח.
   אם ה-IPID לא עלה ב-2 מספרים אלא רק ב1 זה אומר שהיתה תקשורת רק עם ה-ZOMBIE ולכן נניח שהפורט של CIBLE סגור.

מערכות WINDOWS מקפיצות את ה-IP-ID באופן רנדומלי.



1. SYN to Z
2. Fin from Z (get the IP-ID) 6000
3. Sending SYN to Target to think its from Z
    a. If the port is open target sends Syn-ack to Z and Z sends back RST (ipid +1)
    b. If the port is closed the target doesn't send syn-ack to Z and Z doesn't send back RST (ipid 0)
4. Syn to Z
5. Fin from Z (get IP-ID)
6. If IPID- 2=old IP-ID the port is Open
7. If IPID -1=old IP-ID the port is closed

>nmap -sI <zombie ip> <target ip>

>nmap --script ipidseq target-ip -p #

NSE:

ראשי תיבות של nmap script engine זהו מושג המתאר סקריפטים הניתנים להרצת סריקות ספציפיות ובמציאת שירותים שונים ע"י Nmap.

ניתן להשתמש ב-NSE באמצעות הפקודה:

--script <script name>

ה-NSE מתחלקים למספר קטגוריות:
סקריפטים מסוג auth משתמשים לאונטתיקציה
סקריפטים מסוג broadcast -
סקריפטים מסוג brute - ברוט פורס
סקריפטים מסוג default -
סקריפטים מסוג discovery - אחראים על מציאת מידע
סקריפטים מסוג DOS אחראים על קריסת המטרה
סקריפטים מסוג exploit פריצה למטרה
סקריפטים מסוג malware בודק אם המטרה נדבקה בmalware
סקריפטים מסוג external - משתמש בשירותים חיצוניים
סקריפטים מסוג vuln בודק אם המטרה פגיעה

>--script *

הרצת כל הסקריפטים.

>--script *vuln*

הרצת כל הסקריפטים מסוג מסוים.

>locate *.nse

יסרוק את כל הסקריפטים של NSE במערכת.

Firewall bypass (full):

ניתן להשתמש בדגל T- על מנת ליצור timing לסריקה חוזרת.

>nmap ip -D

ה-D אומר Decoy מלכודת או פיתיון.

>nmap ip -f

ה-f מייצג fragmentation כלומר מחלק את המידע לפריימים קטנים כך של-Firewall יהיה קשה למצוא את המידע.

>nmap ip -A

פריצה אגרסיבית ל-firewall ע"י שמפעיל את כל הרשת.

>nmap ip -sV

כלומר Service Verbose, הכלי מתחבר לפרוטוקול אחר כדי לסרוק את הרשת ולדעת איזה פרוטוקול ושירות פעילים ברשת.

כלים נוספים לסריקת רשת:

Zenmap - nmap GUI
Netdiscover - סורק את כל המחשבים שיש ברשת
Netdiscover -r 10.0.0.0/16
P0f - מאזין ואוסף את כל המידע שיכול לאסוף
Masscan - הכלי הזה סורק את כל האינטרנט לפורט בודד ב8 דקות
לא מדויק.

Password Cracking:

סיסמה מוגדרת כרצף של תווים אשר מצפינה/מגינה ובודקת מידע.

Hash:

פונקציה חד חד כיוונית חד חד ערכית המייצגת fingerprint לשלימותו של המידע

Strong password:

סיסמה חזקה מוגדרת כסיסמה בעלת אורך של 8 תווים לפחות, מורכבת מאותיות גדולות, אותיות קטנות, מספרים, ותווים מיוחדים.
הסיבה לכך היא שככל שהסיסמה מורכבת יותר היא קשה יותר לפיצוח.

ישנן ארבע דרכים שונות לפריצת סיסמאות:

1) דרך ראשונה Guessing - ניחוש הסיסמה ע"י איסוף מידע על מנת להבין מידע מסוים על הסיסמה.
2) דרך שניה phishing - מונח מקצועי המתאר מצב של התחזות על מנת לגנוב את הסיסמה.
3) דרך שלישית מילון ניסוי וטעייה של הסיסמאות הנפוצות ביותר.
4) דרך רביעית Cracking - ביצוע bruteforce מלא ומנסים את כל האופציות האפשריות עד שמצליחים.

Weaknesses in Passwords & Hash:

לכל אחד מהמונחים סיסמה או גיבוב עם הזמן הם הופכים להיות חלשים יותר.

Cryptography:

זהו מונח מקצועי המתאר את תורת הצפנים,
צופן = הוא אלגוריתם שנועד להסתיר מידע.

Types of HASH:

- MD5 = 16** 32
- SHA1 = 16**40
- SHA256 = 16**64
- NTLM = Windows hash
- NetNTLM = windows's hash with salting
- Blowfish = Linux's Hash

Rainbow Tables:
https://Hahskiller.co.uk
https://Korelogic.com

נתונים כלליים:
המעבד מחשב את כל הנתונים המתמטיים.

i7 - 1000000 passwords per second
GPU - is eq to about 300 CPUs about 30-80 Billion passwords per second.
Web bruteforce is eq to about 20-40 pp/s

המונח של קבוצה של כרטיסי מסך המאוגדים יחדיו נקרא - Rig.

כלים:

Cat /etc/shadow - מיקום הסיסמאות בלינוקס
John:
> Unshadow /etc/passwd /etc/shadow > crackme
>john crackme

כלי john מבצע bruteforce ב-HASH

> john crackme --wordlist= <filepass location>

יש מילון דיפולטיבי בלינוקס שנקרא rockyou הנמצא:

> usr/share/wordlist/rockyou.txt

קבצי סיסמאות:

Google - most common passwords
Github - most common passwords

פריצת RAR:

> rar2john file.rar >crackme
> john crackme

GPU Tools:

ישנו כלי שדומה ל-john אך משתמש ב-GPU ונקרא Jumbojohn
ניתן להוריד אותו מ-github

> git clone <download link>
Hashcut:

כלי פיצוח HASH ל-windows.

> hashcut -a [hash mode] -m [setting] [hashfile] [dictionary]
> hashcut -I - יציג אם יש GPU

Crunch:

כלי ליצירת קובץ סיסמאות בלינוקס.

> crunch 10 10 0123456789 -t 05%%%%%

יוצר template ל-crunch.

Cewl:

כלי זה אוסף מאתרים

>cewl http://hackeru.co.il -w [location to keep]

CUPP:

כלי זה מציג שאלון על המטרה עם כל מיני שאלות הקשורות למטרה שיכולות לאסוף מידע אישי עליו בכדי למצוא סיסמא אפשרית.

HYDRA:

> hydra -l username -P passfile https://facebook.com/login.php (or website IP) http-post-form “login.php: email=^USER^&pass=^PASS^:error”

HYDRA WIZARD:

הוא הכלי HYDRA ב-wizard.

Ncrack:

> ncrack -p ssh -u root -P passfile -T5 127.0.0.1 -f

Social Engineer

הנדסה חברתית מונח היא מקצועי המתאר ביצוע מניפולציות באופן פסיכולוגי על אינדיבידואלים במטרה לקבל מידע ו/או גישה ביתר קלות.

מהות: היא לקבל מספר דברים

1. איסוף מידע Information Gathering - לשקר למטרה או להתחזות למישהו אחר במטרה לקבל מידע רלוונטי.
    a. ראוי לציין כי התחזות למישהו אחר לא אישור מהווה עבירה פלילית.
2. הונאה - לבצע מניפולציה על קבוצות במטרה לגנוב כסף.
3. גישה למערכות System Access - ניתן לתשאל בן אדם ולקבל מידע שיכול לשמש כסיסמה.

להנדסה חברתית יש מספר וקטורי תקיפה:

1. Computer based SE:
    a. מדובר על מתקפה כאשר אני תוקף מחשב או ציוד רשת, פרוטוקולים ועוד.
2. Phone based SE:
    a. מדובר על תקיפה כאשר אני מירט טלפון של בן אדם.
3. Physical Based SE:
    a. קבלת מידע מאדם פיזי.

המונח של SE מתייחס לאמנות הפריצה ללא מחשב.

טרמינולוגיה:

Spear phishing -

מונח מקצועי המתאר תרגוט מטרה באופן ספציפי ע"י פרמטרים ידועים מראש

Vishing -

כל מה שקשור ל- Phone Based.

Baiting -

להשאיר פיתיון לאדם באופן פיזי כמו דיסק און קי על הרצפה.

certificate

תעודת certificat זהו קובץ שמוודא 2 דברים:

1. שהאתר הוא באמת מי שהוא טוען שהוא.
2. התעבורה בין לבין מוצפנת.

SE Toolkit:

כלי זה מהווה סביבה מלאה לניהול התקפות י"ע עזר בהנדסה חברתית.

Social Fish:

Pip3 install -r <file.txt>

evilginx2:

> config ip <ip>

phishing protection:

1. להתחיל לחשוד בכל מיני קבתים
2. תמיד לוודא חיבור מאובטח ב-HTTPS
   a. לראות את ה- certificate ולוודא שהיא אינה מזויפת.
3. לבדוק תוקף ל-certificate.

Web Anonymity:

ישנם מספר דרכים אשר מהווים דרך להסוואת הזהות שלנו:

Proxy:

אלו הם שרתים המאפשרים להעביר דרכם תעבורה ברשת מאשר לגשת לאתר ישירות וכך מהווה אנונימיות.
לפרוקסי מספר מטרות שימוש:

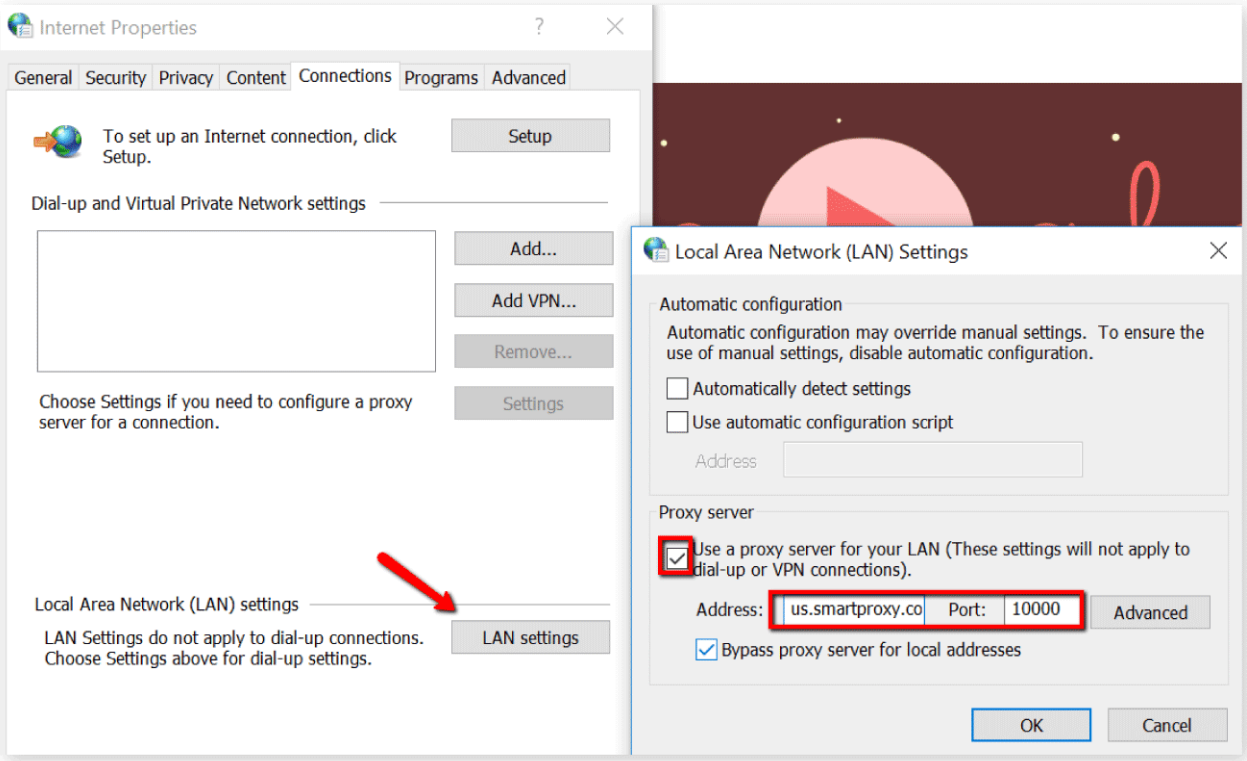
1. שמירת מידע.
2. אנונימיות ברשת בזכות פרוטוקול NAT.
   a. פרוטוקול NAT יחליף את כתובת ה-IP.
3. ביצוע פילטרים.
4. תפיסת המידע - intercept מה שיעיל יותר מלוג במקרים מסוימים.

שירותים ל-proxy:

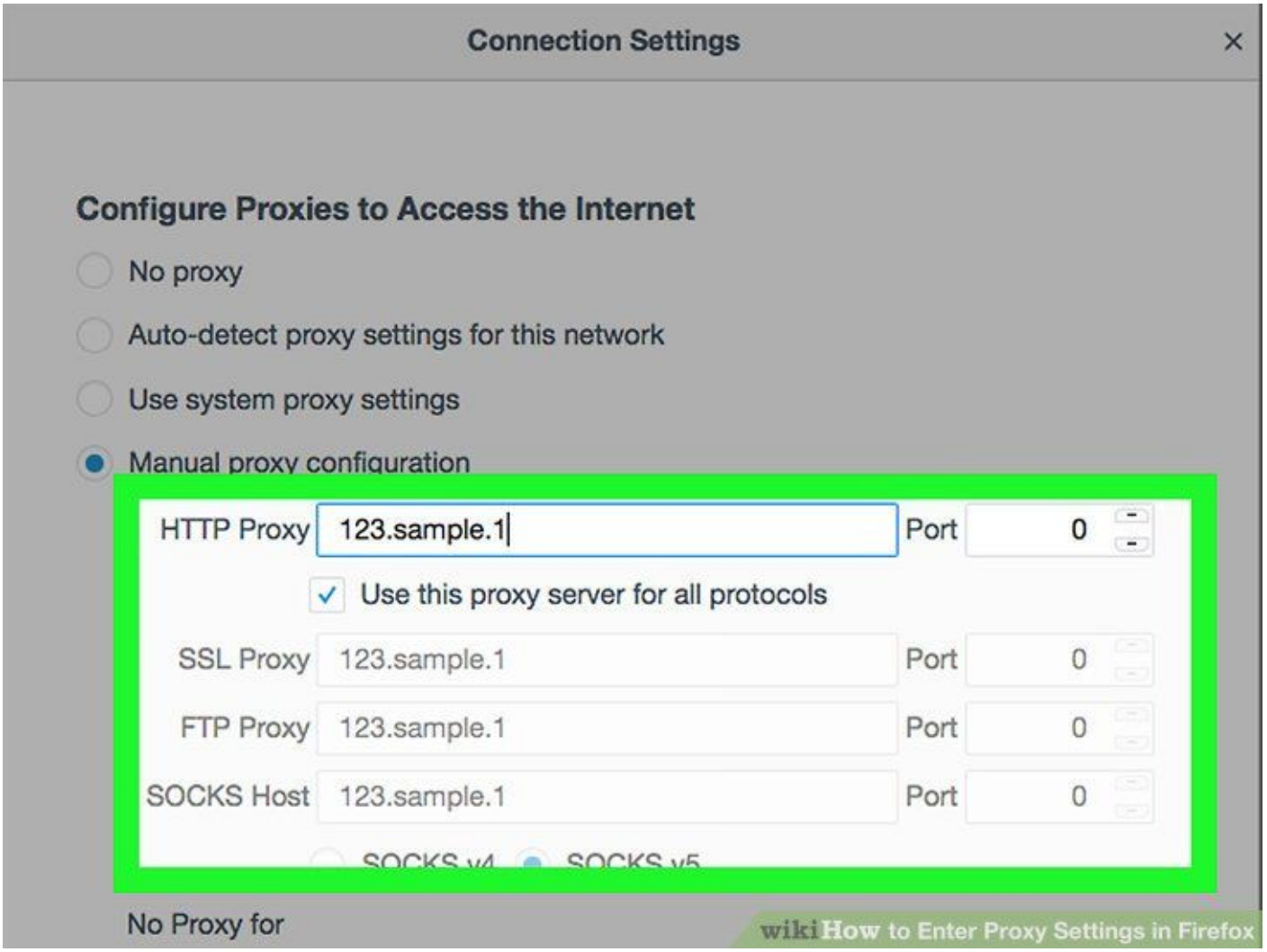
1. Proxysite.com
2. Hide.me - VPN
3. Hidester.com

העברת התעבורה ל-proxy:

ב-Chrome



ב-Firefox



VPN - Virtual Private Network:

זהו שירות של יצירת tunnel אל תוך רשת פנימית מסוימת.

Tunnel:

תעבורה דו כיוונית אשר מוצפנת בהצפנה גבוהה ומאפשרת לשייך מחשב מרשת אחת לרשת פנימית אחרת.
בדר"כ ניתן להעביר כל סוגי התעבורה באמצעות ה-tunnel.

הבדלים בין proxy ל-VPN:

1. ב-PROXY התעבורה עוברת plane text וב-vpn התעבורה מוצפנת.
2. ב-PROXY האתר אינו מודע מי פונה אליו בעוד ספקית התקשורת יכולה לדעת אך ב-VPN בגלל שהתעבורה מוצפנת הספקית אינה יכולה לדעת.
3. פרוקסי עובד בשכבת האפליקציה בלבד בעוד VPN יכול להצפין את כל השכבות.
4. פרוקסי לרוב הוא בחינם מה שא"כ ב-VPN.

שירותים ל-proxy:

1. Tunnelbear.com
2. Cyberghostvpn.com
3. Nordvpn.com

Open VPN:

זהו CLIENT לרוב שרתי ה-VPN המוכרים היום, CLIENT זה דורש קובץ קונפיגורציה באמצעותו ניתן לגשת לכל שרת VPN בעולם.

Tor:

זהו דפדפן המספק אנונימיות הצפנה ומספר קפיצות בלתי מוגבל אשר יכול לגשת לכלל האינטרנט כולל הרשת האפלה.

Dark Net:

אתרי אינטרנט שניתן לגשת אליהם אך ורק אם יודעים את כתובת האינטרנט (גם היא מוצפנת), אך ורק אם אתם עומדים בסטנדרט הצפנה מסוים וכמה קפיצות VPN עברתם.

Tor in linux:

```
>proxychains
>nano /etc/proxychains.conf
```

קבצי הקונפיגורציה ל- proxychains

```
>apt install tor
>service tor start
>curl ipinfo.io/ip
> proxychains curl ipinfo.io/ip
```

במידה ונרצה שכל התעבורה של לינוקס תעבור בTOR:
ישנו כלי בשם lazyscript סקריפט זה יכיל בתוכו anonsurf בפנים וכלי זה יעביר את כל תעבורת הרשת של מערכת ההפעלה דרך Tor.

הקמת שרת Tor:

```
>service tor stop
>python -m SimpleHTTPServer <port#>
>nano /etc/lib/tor/torrc.orgin
```

להוסיף לקובץ:

```
>HiddenServiceDir /var/lib/tor/hostname
>HiddenServicePort <port (80)> <ip:port# (8080)>
>service tor restart
>cat /var/lib/tor/hostname/hostname
```

Wireless:

WiFi:

מדובר על טכנולוגיה של העברת מידע על גבי רדיו מנקודה אחת לנקודה אחרת
תהליך הלבשת המידע על גל רדיו נקרא "אפנון" ותקשורת של WIFI עובדת על פרוטוקול IEEE 802.11 ומוכר גם בשם WLAN.

מושגים:

תדר - מדובר על גודל הגל בדר"כ מעיד גודל התדר מעיד על כמות מידע שהגל יכול לשאת והאורך לאן שהגל יכול לקלוט אותו.

Frequency:
2.4 GHz
5.0 GHz

Channel :

ערוץ - כינוי מספרי לטווח מדוייק של תדרים במטרה להימנע מהפרעות ו-collisions בגלי רדיו.

Encryption:

גלי רדיו מכילים מידע בינארי 1010, מידע זה יכול להיות מוצפן באלגוריתם מכך יוצא שאם WIFI מוגן בסיסמה המחשב מפענח את המידע הבינארי באמצעות הסיסמה.
סוגי הצפנות:

None - clear text
WEP -
זהו פרוטוקול הצפה ישן ובין הפגומים שקיימים כיון שהסיסמה נשלחת באוויר כל הזמן.
WPA 1, WPA 2, WPA 3 -
נחשב ליותר מוגן ומשתמש באלגוריתם של AES ומכיל גרסאות עם 2 מפתחות כלומר הצפנה אסימטרית.

חומרה דרושה:
במקרה של פריצת רשתות WIFI יש צורך בכרטיס רשת אשר תומך במצב שנקרא Monitor Mode, מצב זה מאפשר לקלוט רשתות גם כשלא התחברנו אליהם.

כלי פריצה לקאלי:

על מנת לגלות רשתות ניתן להשתמש במספר כלים.
1. גלאי רשתות של מערכת ההפעלה הדיפולטיבי.
    a. ניצן לגלות רשתות אלו כיון שישנה פקטה שהיא כל הזמן clear Text ומכילה את שם הרשת.
2. Wifite
3. Kismet
4. Airmon
5. Aireplay
6. Airodump
7. aircrack

WEP:

בהצפנה זו אותו מפתח משמש הן להצפנה והן לפענוח, בהצפנה זו משתמשים באלגוריתם RC4 בגודל של 64bit.
בנוסף למידע מועבר מפתח בכל חבילה באוויר, לכן הצפנה זו דורשת אך ורק 16 מילון אופציות של Bruteforce.
בהצפנות חדשות יותר כמו WPA ה-bruteforce יותר קשה והוא תלוי באורך הסיסמה, במקרה הגרוע ביותר ברשת המוגנת WPA PSK יקח שנה לפרוץ לרשת מוגנת מסוג זו.

1. Airmon -
    a. >airmon-ng start <NIC name>
    b. כלי זה הופך את כרטיס הרשת ל-monitor mode.
2. > airodump-ng <NIC name>
    a. BSSID - NIC MAC Address
        i. PWR - power
            1. Beacons - כמה פקטות האנטנה תפסה
                a. #Data - כמה מידע האנטנה תפסה
                i. #/S - is WPS open
                1. CH - Channel
                a. ENC - Encryption
                i. ESSID - network Name
    b. > airodump-ng <NIC name> -c <channel #> --bssid<MAC> --essid <network Name> -w

c. כלי זה תפקידו להסניף תעבורת רשת גם כאשר אינו מחובר ל-wifi.

3. > aireplay-ng -3 -b <MAC> <NIC Name> = asking to reset the router
    a. > aireplay -0 = jamming
4. > aircrack-ng <.cap file>
    a. > aircrack-ng -b <MAC> <.cap file> -w <wordlist>

i. בכדי לראות את תעבורת הרשת ב-wireshark ניתן

Handshake:

ישנם ארבע חבילות בתהליך האותנטיקציה נקרא- eapol ומתחלק ל-4 שלבים:

1. Authentication request.
2. Clear text that needs to be encrypted with the key from the client.
3. Sending the encrypted password the the AP.
4. Success message.

Evil twin:

מדובר על מתקפה שבה התוקף מתחזה לראוטר, אנשים מתחברים אליו במקום לראוטר ולתוקף תהיה שליטה מסוימת על מי שיתחבר אליו.

Fake AP:

Configuration file for the router:

```
> nano hostapd.conf
        Interface wlan0mon
        Driver <antena driver>
        ssid=cafe_cafe
        hw_mode=g
        channel=6
        ignore_broadcast_ssid=0
        auth_algs=1
        wpa=2
        wpa_key_agnt=WPA-PSK
        rsn_pairwise=TKIP
        wpa_pasphrase=123123
```

DNS configuration file:

```
> nano dnsmasq.conf
        interface=wlan0mon
        dhcp-range=192.168.2.2.192.168.2.60.255.255.255.0.12h
        dhcp-options=3.192.168.2.1
        dhcp-options=6.192.168.2.1.8.8.8.8
        log-queries
        log-dhcp
        listen-address=127.0.0.1
```

Configuring the NIC:

```
> ifconfig wlan0mon up 192.168.2.1 netmask 255.255.255.0
> route add -net 192.168.2.0 netmask 255.255.255.0 gw [static route address]
>echo 1 > /proc/sys/net/ipv4/ip_forward
```

https://www.shellvoide.com/media/files/

>dnsspoof -i <NIC name>

>apt install hostapd
> hostapd <fakeAP file.conf>

Man In The Middle:

זהו מונח מקצועי המתאר מצב שתוקף מעביר דרכו מידע, ברגע שהמידע עובר אצל התוקף... לתוקף יש יכולת להשפיע על מידע זה.
ישנם 4 מניפולציות שונות בכדי להגיע לתקיפת - Man In The Middle.

ישנם 2 מצבים ל- Man In The Middle:

1. WLAN
2. LAN

מצב של Man In The Middle אפשרי רק ברשת פנימית, אז איך אפשר לפרוץ מבחוץ?
תשובה: ע"י שרת proxy.
מניפולציות שניתן להפעיל במצב של -

1. לגנוב מידע כי כל התעבורה עוברת אצל התוקף
2. לשנות את המידע כשמגיע לתוקף.

3. Denial of service

a. מניעת שירות.

ARP Spoofing / ARP Poisoning:

זו היא מתקפה

מה זה ARP?
זהו פרוטוקול העובד בשכבה השניה שתפקידו לקשר בין כתובת MAC לבין כתובת IP.
פרוטוקול ARP בעייתי בשני סיבות:

1. הוא אינו מוודא שהמידע נכון.
2. יש מצב שנקרא generus ARP כלומר שהראוטר שולח מידע נדיב לדוגמא "אני הראוטר והכתובת IP שלי היא 10.0.0.1 , מה שאומר שאין בדיקה לתזמון.
   a. בהנחה שהתוקף מתחזה לראוטר הוא יכול לשלוח מידע נדיב שישלח לכל המחשבים את כתובת ה-IP שלו וכל המחשבים ברשת ישנו את ה-Default Gateway שלהם לכתובת של התוקף וכך כל התעבורה תעבור דרך התוקף.

באופן דיפולטיבי מכונת הלינוקס לא מאפשרת מצב של forwarding, כדי להיכנס למצב של forwarding יש להריץ:
> echo 1 > /proc/sys/net/ipv4/ip_forward

להפעלת התקיפה:
> arpspoof -i <NIC> -t <Target IP> <Router’s IP>
בכדי להפנות את הבקשה של הנתקף לראוטר יש להריץ את הפקודה:
> arpspoof -i <NIC> -t <Target IP> <Router’s IP> -r

MAC Flooding attack:

ידוע שבמתגים ישנה רשומה בשם MAC Table ששומרת את כל הכתובות הפיזיות של המחשבים בארגון ומקשרת את כתובות ה-MAC למחשבים עצמם.
מתקפה זו מתבצעת ע"י שליחה כמות אדירה של מידע (Ethernet Frames) המכיל וריאציות של כתובות פיזיות שהמתג יוסיף אותם לרשומה ויציף את מקום הזיכרון במתג.
המטרה היא שהמתג יקרוס, וברגע שמתג קורס הוא נכנס למצב גיבוי בתור Hub מה שאומר שהמידע חשוף לתוקף לגמרי.
> macof

DNS:

זהו פרוטוקול שמתרגם בין כתובת IP ל-Domain והפוך.

רשומות DNS:

לכל בקשה או תשובה לשאילתת DNS יש טיפוס אשר מגדיר מה היא בעצם מכילה. כמו כן, השרת אשר שלח את התשובה מגדיר עבורה גם TTL (Time to live) שהוא הזמן המקסימלי שלמקבל התשובה מותר לשמור אותה במטמון שלו ולהניח שהיא נכונה.

- A -
  - רשומה זו היא כתובת IPv4 (**A**ddress) המשויכת לשם דומיין מסוים.
- AAAA -
  - בדומה לטיפוס A, רשומה זו היא כתובת IPv6.
- NS -
  - רשומה אשר מציינת שרת אשר משמש כאחראי למסירת מידע על הדומיין המבוקש.
- PTR -
  - רשומה זו מכילה דומיין אשר משויכת לו כתובת IP מסוימת (על מנת ששרת ה-DNS יוכל לחפש דומיינים על פי כתובות IP).
- MX -
  - מכילה את הכתובת של השרת המשמש את הדומיין לשליחה וקבלה של דואר אלקטרוני.
- CNAME -
  - רשימה המכילה שם נוסף לאותו דומיין "Canonical name".
- TXT -
  - רשומה זו מאפשרת לצרף לכתובת ה-IP של הדומיין גם טקסט חופשי (משמשת למימוש שירותים שונים הקשורים בדומיין, כגון DomainKeys).
- SPF -
  - סוג מיוחד של רשומת TXT המציינת את שמות ה-hosts מהם מותר למסור מייל בשם אותו דומיין.
- SOA - start of authority -
  - הרשומה אשר מצביעה על הימצאותו של ה- ZONE.

DNS Poisoning:

היא מתקפה של MITM המאפשרת לתוקף לשבש את התעבורת DNS בין המותקף לשרת וע"י כך יכול להגיע לרמה של התחזות שרת DNS ולהשתיל תרגום דומיינים לאתרים אחרים שהתוקף חפץ שהקורבן יופנה אליהם.

מתקפה זו דורשת קובץ בשם <host>
פקודות התקיפה:

```
> dnsspoof -i <NIC> -f [host]
```

עוד מספר כלים ל-man in the middle:

urlsnarf

driftnet
filesnarf
webspy
dsniff

Urlsnarf :

כלי זה מציג לאילו כתובות המותקף נכנס.

Driftnet:

כלי זה מציג את התמונות של התעבורה של הנתקף.

Filesnarf:

מציג את הקבצים של האתר.

Webspy:

יציג את האתר במלואו.

SSL Strip:

הפשטה של SSL מ-client.

דרישות:

```
>echo 1 > /proc/sys/net/ipv4/ip_forward
> arpspoof -i <NIC> -t [target] [router's IP] -r
> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <port#>
>sslstrip -l 1000
```

הגנה מפני SSL Strip:

נקראת HSTS - Http Strict Transport Security הוא header המתרגם לאתר שאם מנסים לפנות אליו ב-http תחסום את התעבורה.

כלים אוטומטיים לMIT:

Eettercap:

```
>ettercap -Tq -M ARP -i <NIC> //<IP>// /<Router's IP>/
```

Bettercap:

הוא מודול framework שלם לכל מה שקשור ל-MITM

```
> apt install bettercap
```