מבוא להאקינג

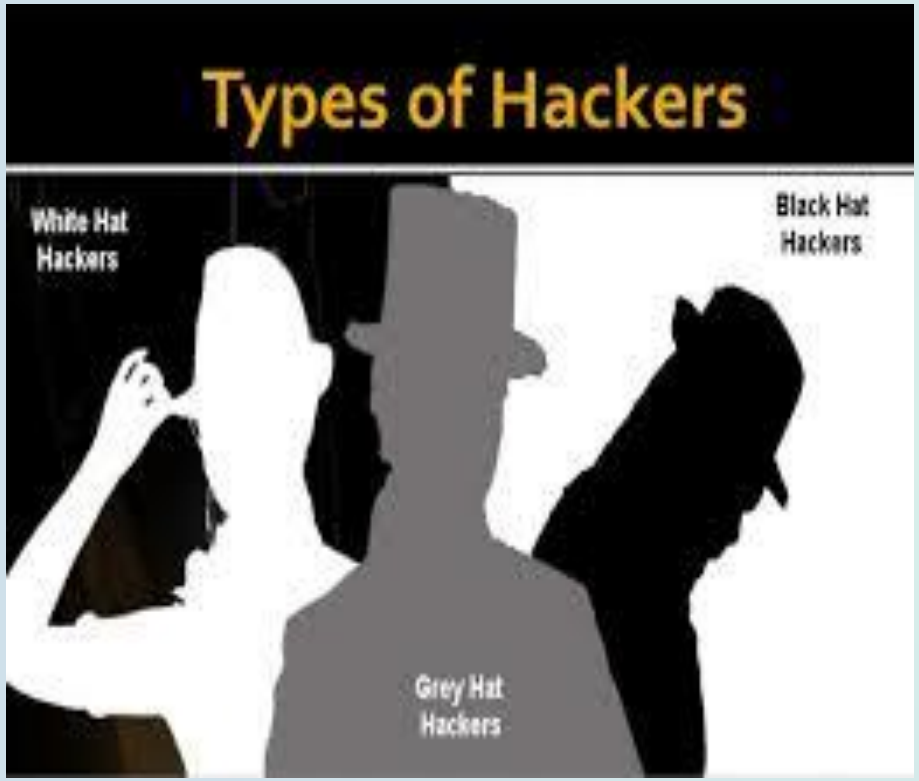
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

נושאי הלימוד

- האקרים – סוגי האקרים
- מתודולוגיות תקיפה של האקרים
- כלי האקינג על קצה המזלג
  - SHODAN
  - Mac Spoofing Attack
  - סניפרים (רחרחנים) – WIRESHARK
  - KALI LINUX
  - Google hack
  - פריצת סיסמאות

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

סוגי האקרים



Black Hat

White Hat

Grey Hat

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

סוגי האקרים

Black Hat

מבצע חדירות לרשתות, ולמחשבים על מנת:

- להשיג את מטרות מסוימות:
  - מטרות כלכליות – וירוסי כופרה
  - מטרות פוליטיות – ארגון אנונימוס
  - פעולות נקם – ביצוע פעולות טרור
- יצר ונדליזם – להרוס , לשבש סתם בשביל הכיף
- יצר אתגרי – הפריצה מבחינתו זה הוכחת יכולת טכנולוגית

פעולותיהם הם עבירה על החוק

סוגי האקרים

White Hat נקרא גם "מאבטח מידע"

מבצע בדיקות לרשתות, ולמחשבים על מנת:

- לשפר רמת האבטחה במערכות רשתות ומחשבים
- למצוא פרצות ולהתריע עליהן בקרב האחראים
- לבצע פעולות בדיקת חדירות בארגונים (PEN TEST)
- להגן בפני אנשי הכובע השחור (צבא: מגן סייבר)
- יצר אתגרי – איתור הפירצה מבחינתו זה הוכחת יכולת טכנולוגית

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

סוגי האקרים

Grey Hat

כוונתו לא לגמרי ברורה שכן הוא לא מזיק אך גם לא מסייע

- מטרתם היא לרוב למידת הטכנולוגיות והאתגר של ההתנסות בהן.
- חוקר מערכות ותוכנות, מחפש חולשות ובעיות.
- כאשר הוא מוצא פרצה הוא לא פוגע אך גם לא תורם (מדווח וכדומה)
- יכול להפוך ל-WHITE HAT או ל- BLACK HAT תלוי במניעים שלו.

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

סוגי האקרים

Script kiddies

משתמשים בתוכנות קיימות (סקריפטים) כדי לעשות דברים רעים

- מטרתם בעיקר לגרום לנזקים
- הם לא מתוחכמים ולא מבינים במחשבים
- הופכים את עצמם למטרה, כי ברגע שהם מנסים לפרוץ לא בחכמה הם חושפים את עצמם.
- הסקריפטים שהם מורידים על מנת לתקוף לפעמים מכילים וירוסים וכך הם הופכים לקורבן

איזה כובע הם חובשים??

Script kiddies

הם רוצים להראות כך...

אבל הם נראים כך....

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Israeli Hackers Strike Back at Anonymous OpIsrael, Expose Participants With Their Own Webcams (PHOTOS)

By The Pie Overlord!

TECHNOLOGY • 4/10/14 6:24:11 pm • Views: 6,653

0 Share

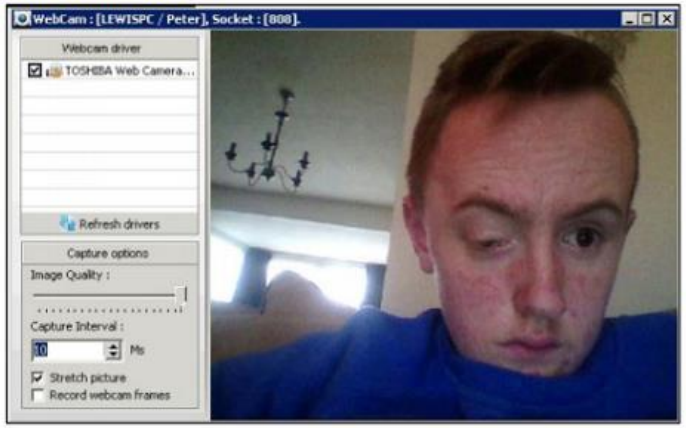
More: **Israeli Hackers Strike Back at Anonymous OpIsrael, Expose Participants With Their Own Webcams (PHOTOS)**

10. Peter Lewis

IP: 79.141.173.62

Location: United Kingdom

https://twitter.com/AnonLw6



An Israeli hacker team published on Tuesday images and personal details of members of the Anonymous hacker collective who participated in the OpIsrael attack against Israeli sites earlier this week, Israel's Channel 2 reported.

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

כיצד פועל ההאקר ? (כובע שחור)

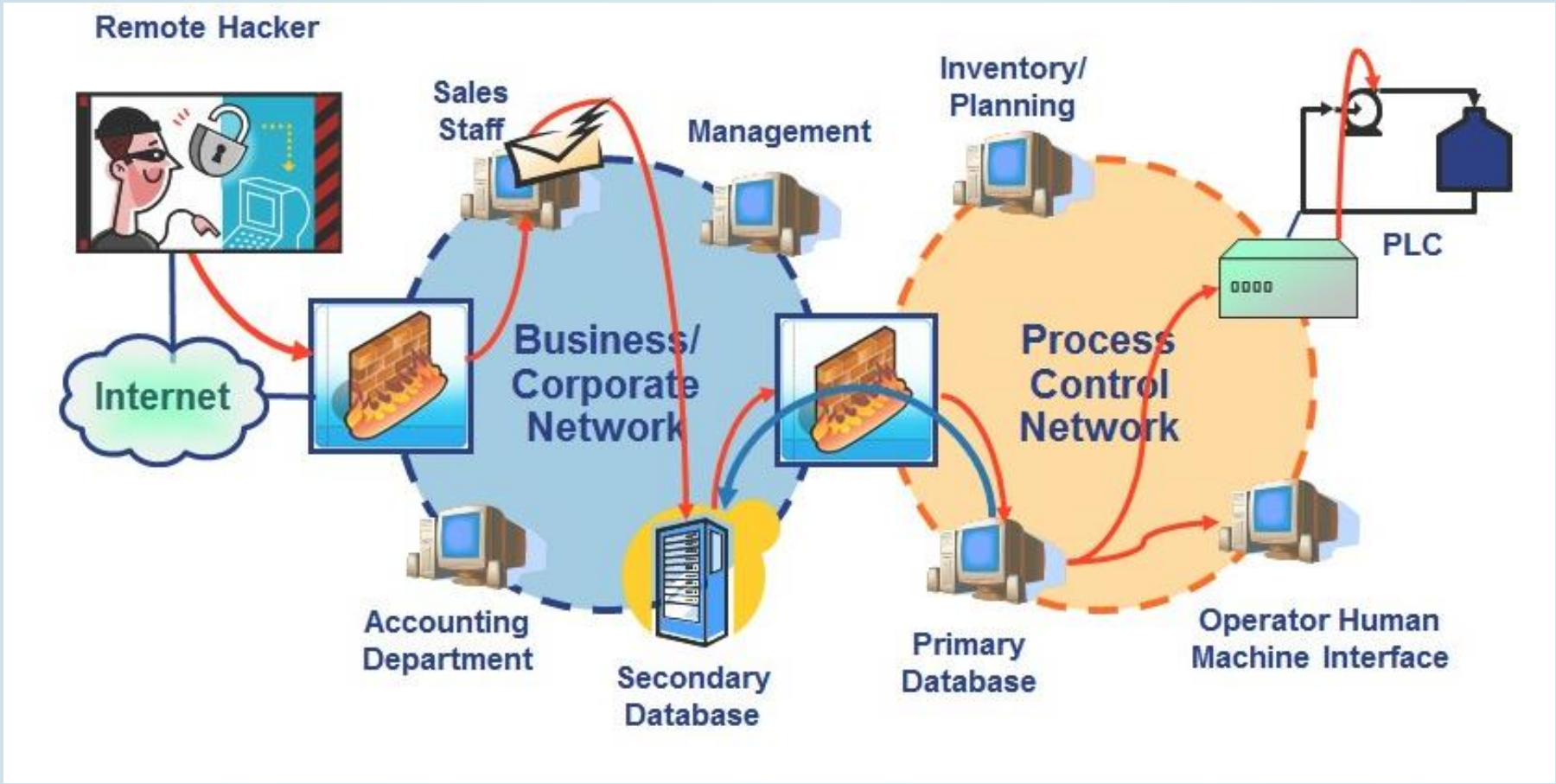
מתודולוגית תקיפה אופיינית

- חיפוש אחר יעד לתקיפה / איתור היעד לתקיפה
- איתור חולשה מסויימת (Vulnerability)
- ניצול החולשה – הורדת תכנה (Exploit) או כתיבת התכנה
- ביסוס אחיזה – למשל התקנת Service שעולה עם מערכת ההפעלה
- ביצוע "תנועה צידית" (Lateral Movement) – מעבר ממחשב למחשב
- טישטוש עקבות – מחיקת לוגים שנרשמים ב- Event Viewer

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתודולוגיות תקיפה

מבט כללי על רשת טיפוסית במפעל

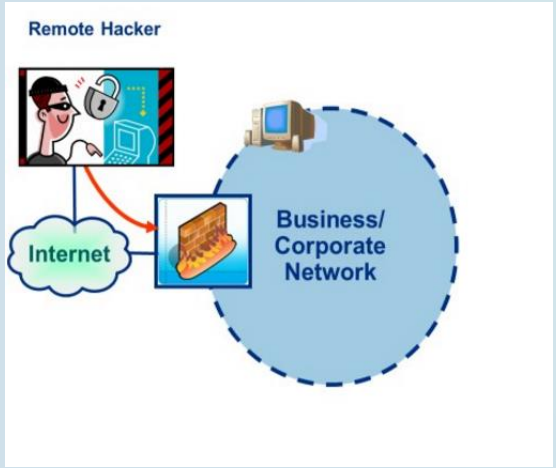


Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתודולוגיית התקיפה – חדירה ראשונית

חדירה ראשונית:
פעולות לגיטימיות (שימוש בפורט 25 המשמש לשליחת מיילים לארגון ופתוח בחומת האש)
שימוש ב-
SOCIAL ENGINEERING
SPEAR PHISHING EMAIL

- התוקף שולח קובץ POWERPOINT המכיל מצגת
- בתוך המצגת מוחדרת פיסת קוד שמכילה MALEWARE
- הוירוס פותח תקשורת החוצה אל מחשב התוקף שמאפשרת לו להשתלט על המחשב הנפגע



וקטורי התקיפה אפשריים לתקיפה מסוג זה:

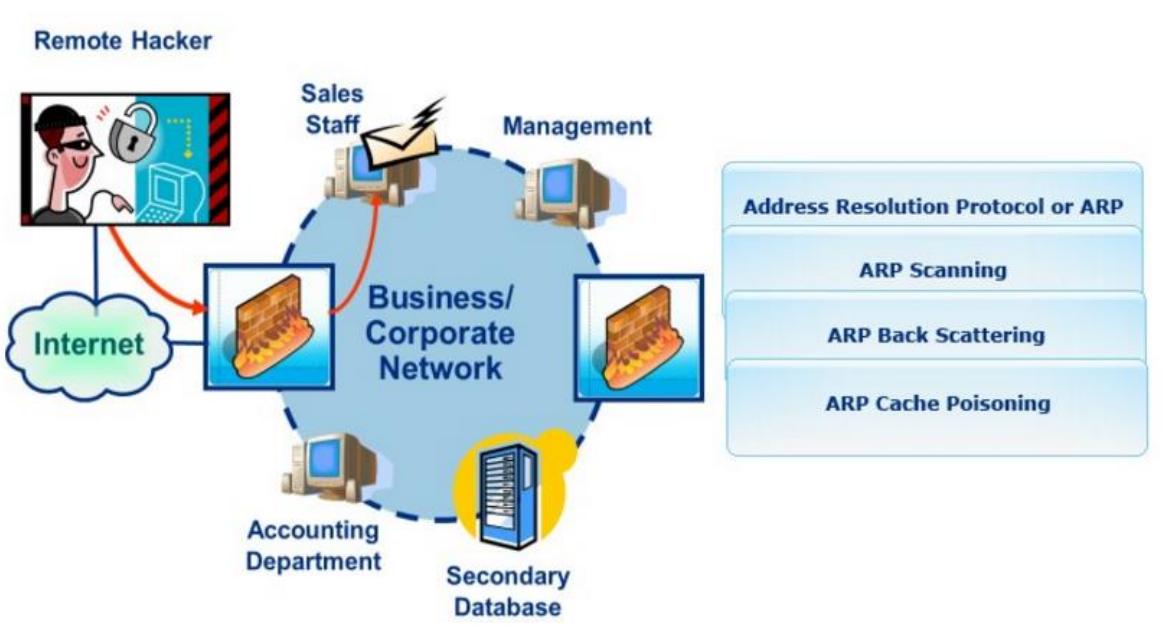
- משלוח מייל לארגון
- הורדת קובץ מהאינטרנט
- שיטוט באתר שנפל קורבן

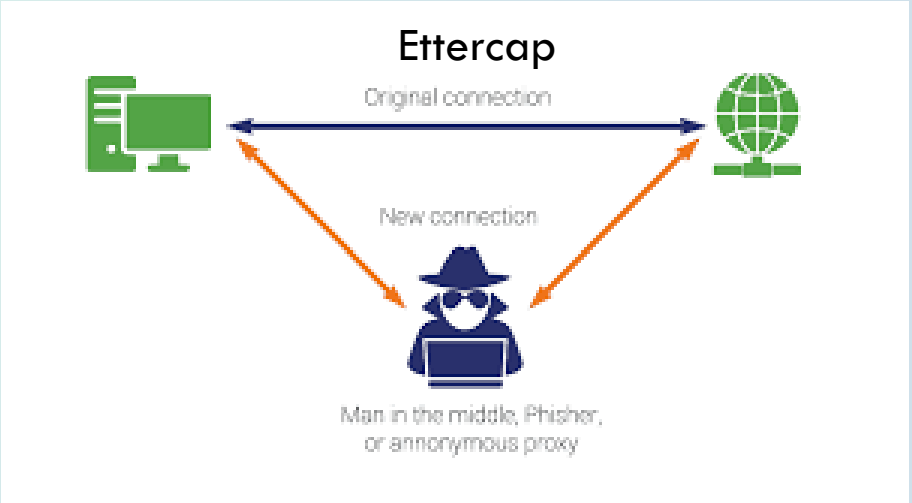
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתודולגית התקיפה – שליטה על התקשורת ברשת

לאחר החדירה

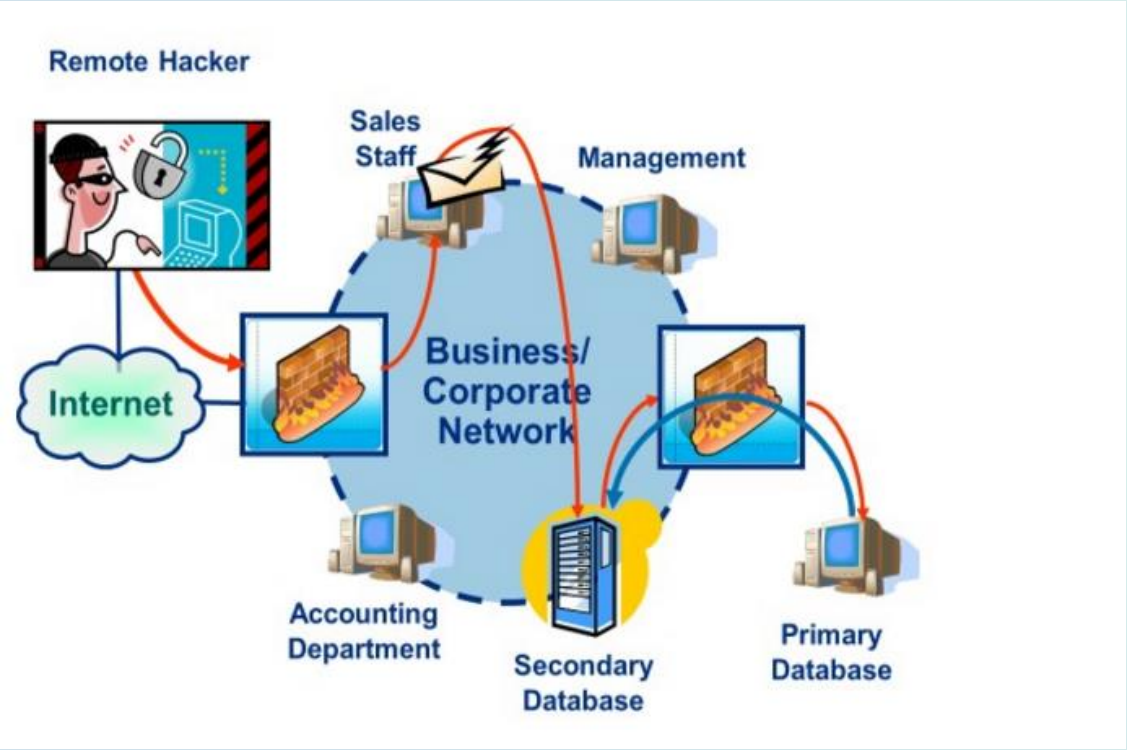
- התוקף מבצע LATERAL MOVEMENT בתוך רשת הארגון באמצעות ARP
- שינוי ב–ARP שמחזיקים המחשבים בארגון יעביר את כל התעבורה למחשב הנשלט (הופך אותו ל DEFAULT GATEWAY).
- בשלב זה השיג התוקף שליטה על התעבורה של התקשורת בארגון.





מתודולגיית התקיפה – השתלטות על בסיס הנתונים

- התוקף מבצע מעקב אחרי תעבורת התקשורת בין שרתי בסיס הנתונים.
- התוקף מזריק קוד עוין אל שרת ה-DB ברשת ה-ICS



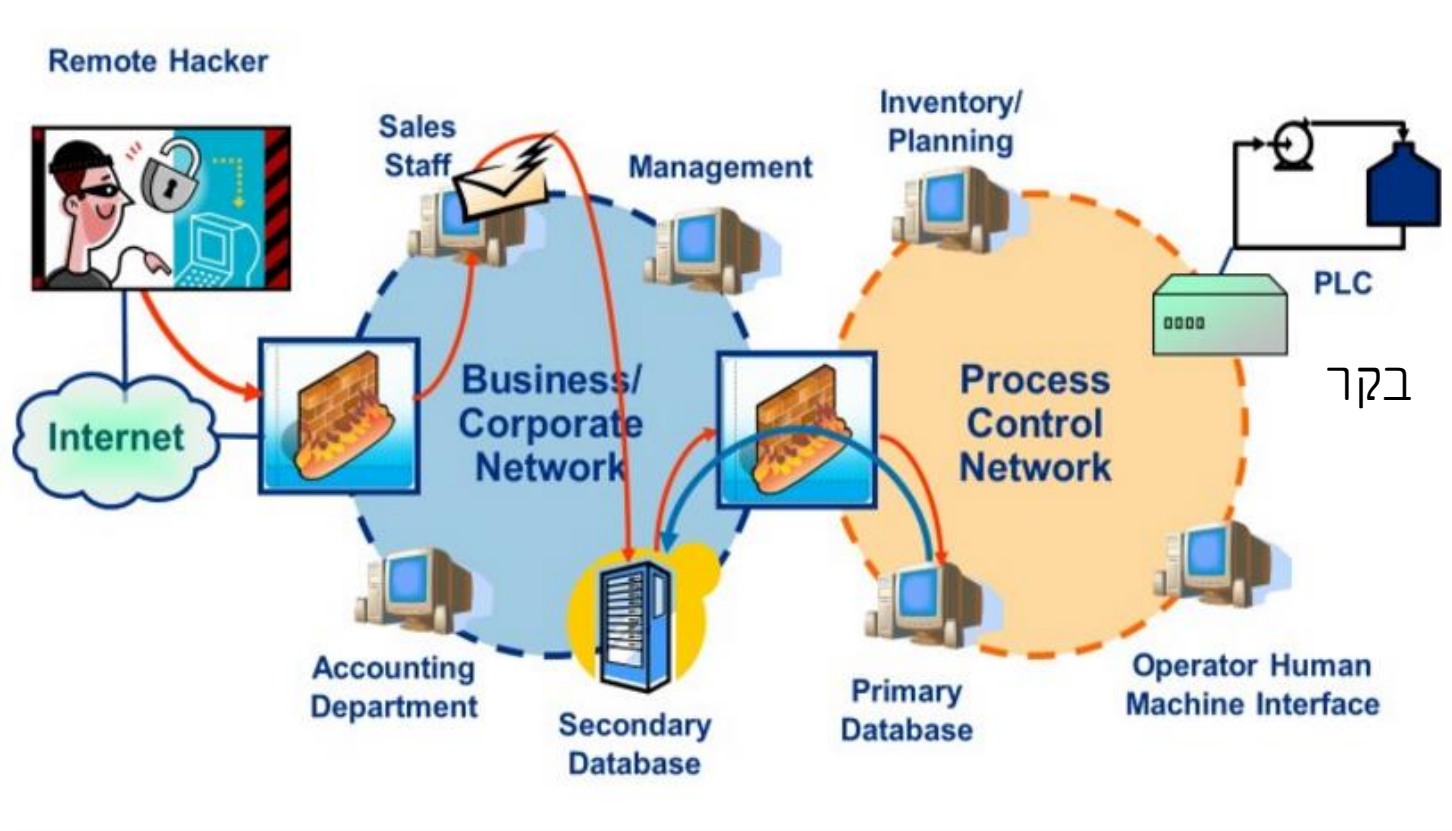
SQL = TCP 1433

ORACLE = TCP 1521

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

מתודולגית התקיפה – השתלטות על רשת ICS

התוקף משלים את ההשתלטות
משיג שליטה ברשת ה-ICS



חומרים מסוכנים

בקר

Game Over!

MODBUS= TCP 502

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

השתלטות על רשת בקרה במפעל – משמעויות

התוקף מסוגל לבצע את הפעילויות הבאות:

- העלאת הורדת לחצים לערכים לא סבירים עד לדליפה ולעיתים פיצוץ צנרת או מיכלים
- שינוי ערכי קירור וחימום והגעה לטמפרטורות קיצוניות
- סגירת / פתיחת ברזים לא מבוקרת עד כדי גלישת חומר מסוכן
- העלאת / הורדת רמת PH במתקני טיהור שפכים – הוצאת שפכים ברמת רעילות מסוכנת
- כל פעילות אחרת שקשורה בתפעול מערך בקרה תעשייתית במפעל (ICS).

התוצאות:

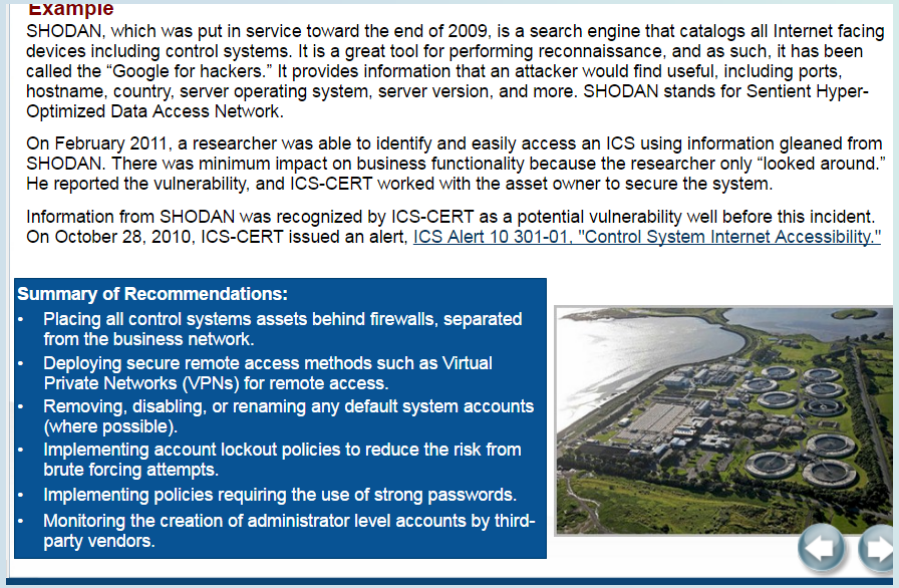
- ❑ פגיעה בבריאות הציבור ובסביבה
- ❑ פגיעה עסקית קשה ברצפת הייצור

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

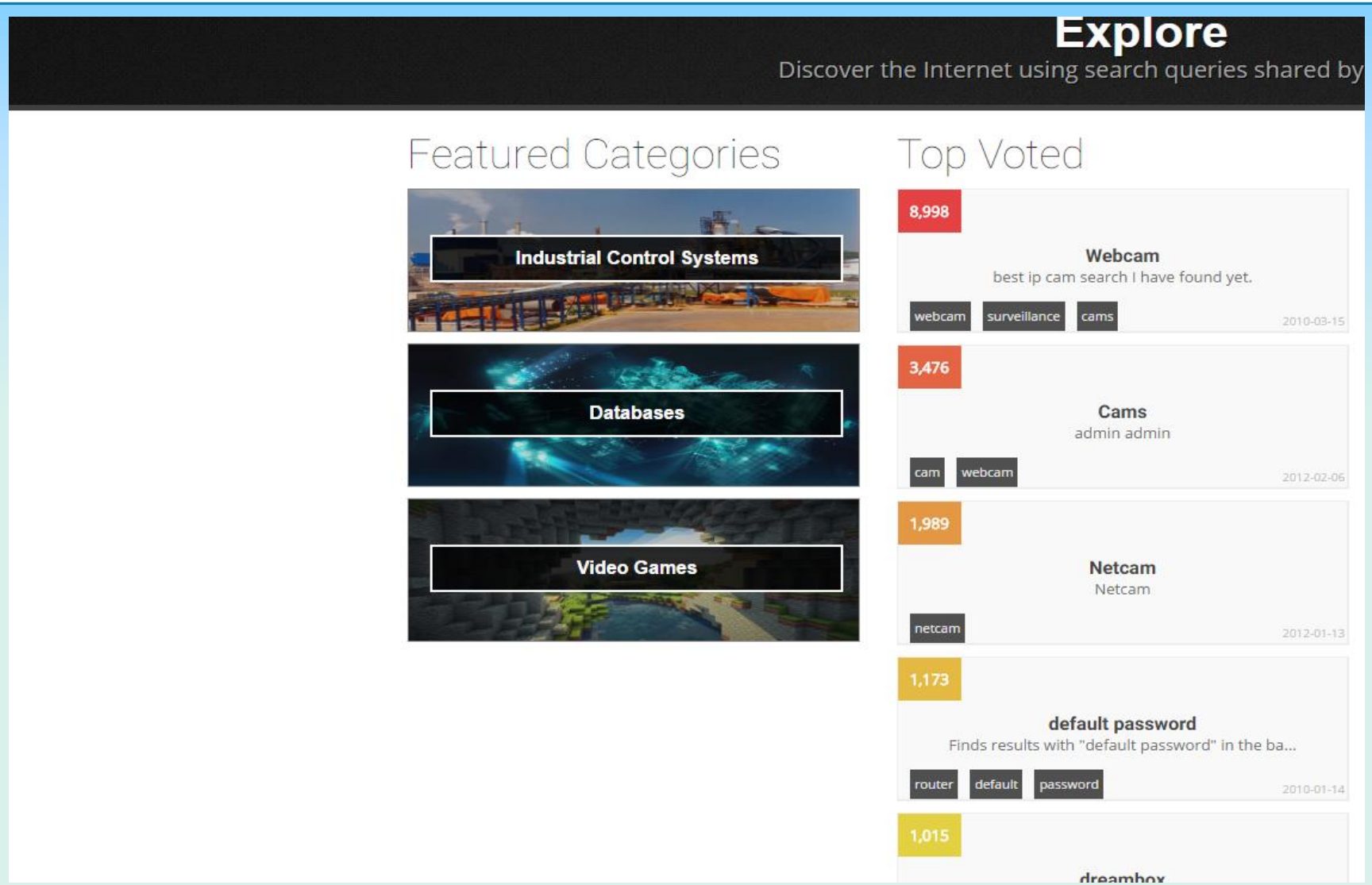
קצת על כלי / עזרי תקיפה.....

SHODAN

- אתר שעלה לאוויר בסוף 2009
- מנוע חיפוש שמקטלג רכיבים שמחוברים לאינטרנט כמו רכיבי ICS (בקרים, אביזרים מערכות סקאדה), מצלמות .
- כלי מצויין להאקרים לביצוע מעקב אחרי רכיבים שפתוחים לעולם ומספק להם נתונים על מיקום, כתובות IP פורטים פתוחים, מערכות הפעלה וכדומה.

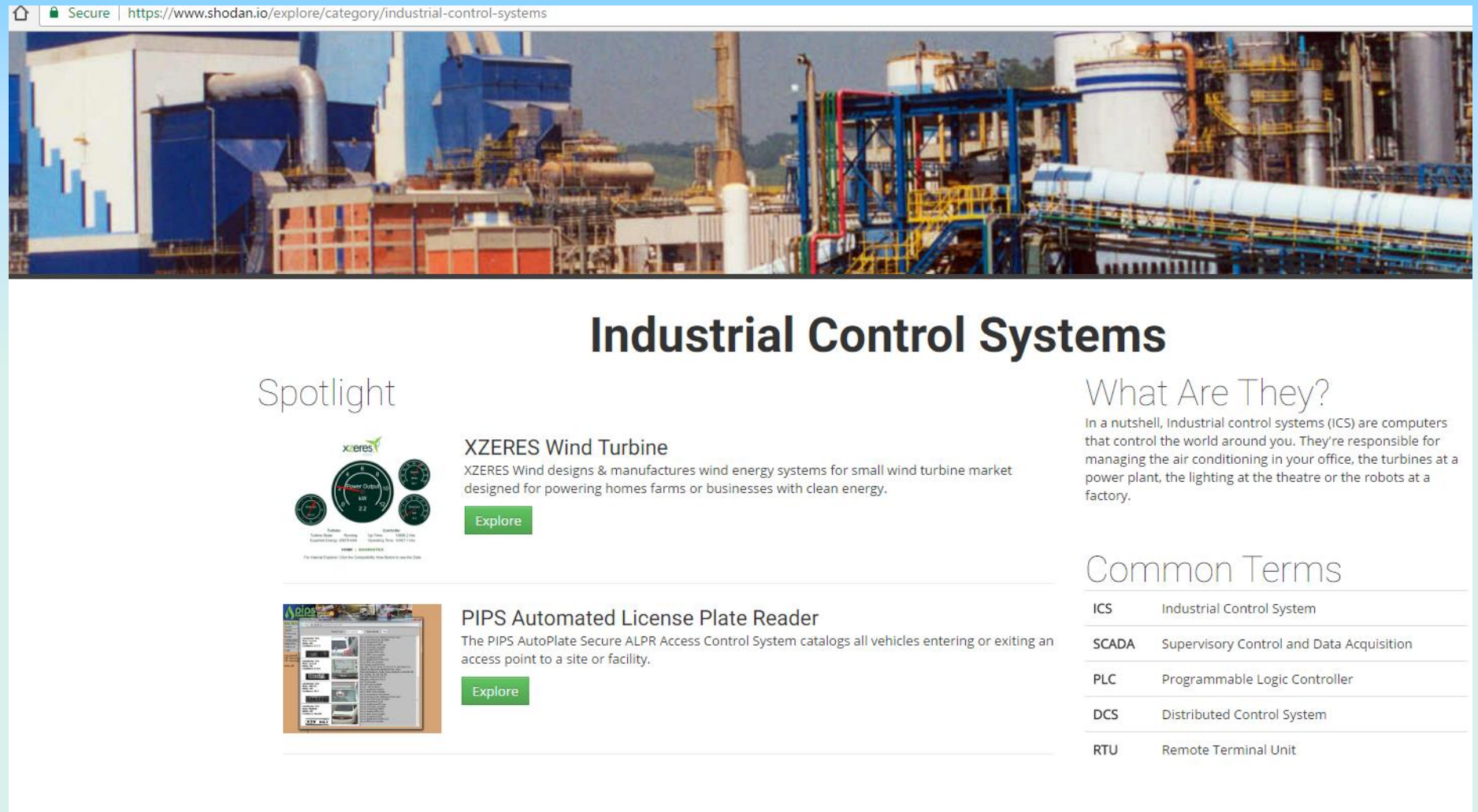


https://www.shodan.io/



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

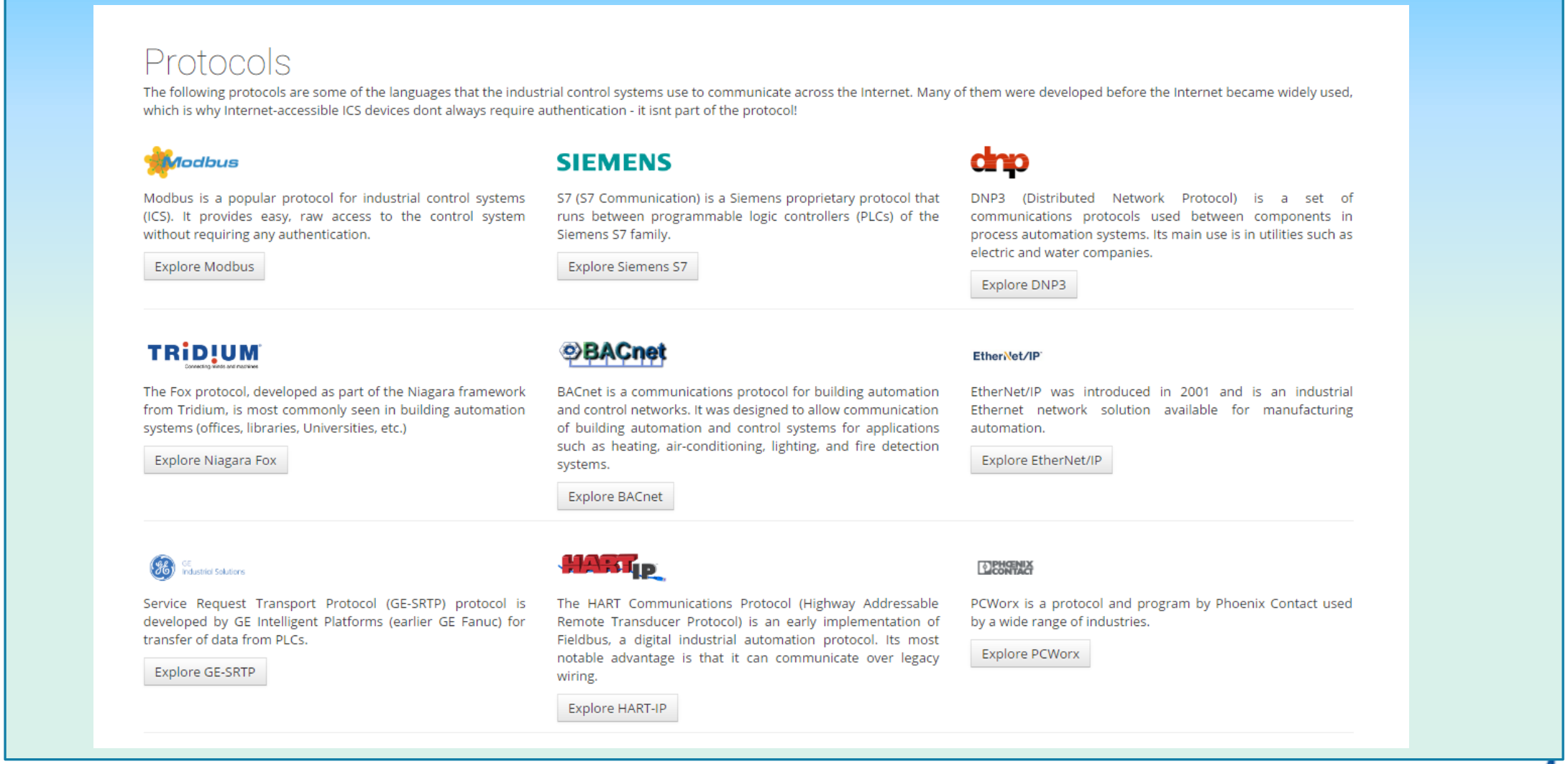
מערכות ICS



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פרוטוקולים פתוחים

בדרך כלל פרוטוקולים ללא הזדהות – בימים שנוצרו לא חשבו על הרכיב הזה....



Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

GE Industrial Solutions

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

HART IP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

Explore HART-IP

PHOENIX CONTACT

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

פרוטוקול MODBUS הנפוץ בתעשייה

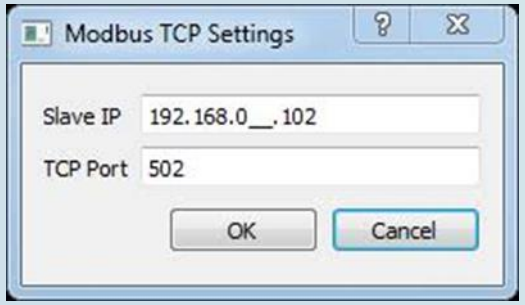
MODBUS נועד להעביר מידע מסנסורים ובקרים ופאנלים לוקאליים לניטור תעבורה

פרוטוקול בסטנדרט תעשייתי לכן תומך במערכות תעשייתיות רבות ומיצרנים שונים

הפרוטוקול הופיע לראשונה ב-1979 ופותח ע"י חברת MODICON (היום שניידר אלקטריק)

בתחילתו תמך בתווך-RS232 (כבלים סריאליים) , לאחר מכן ב- RS485 תוך שימוש בפרוטוקול TCP/IP

כברירת מחדל עובד על TCP PORT 502

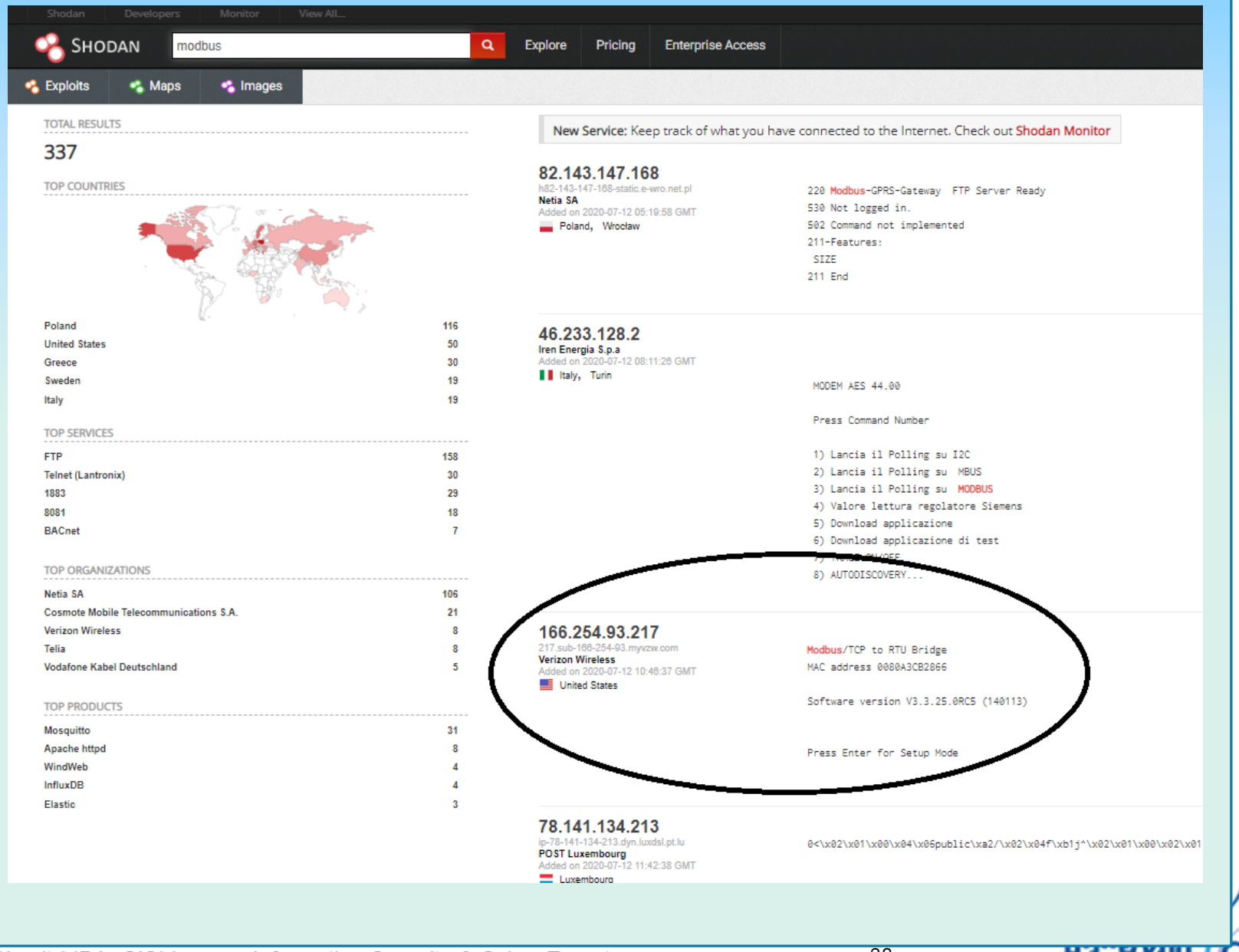


<u>החסרונות הגדולים של הפרוטוקול:</u>

- אינו תומך בהזדהות (authentication)
- אינו תומך בהצפנה (encryption) – לכן יש להשתמש ב-VPN מוצפנים

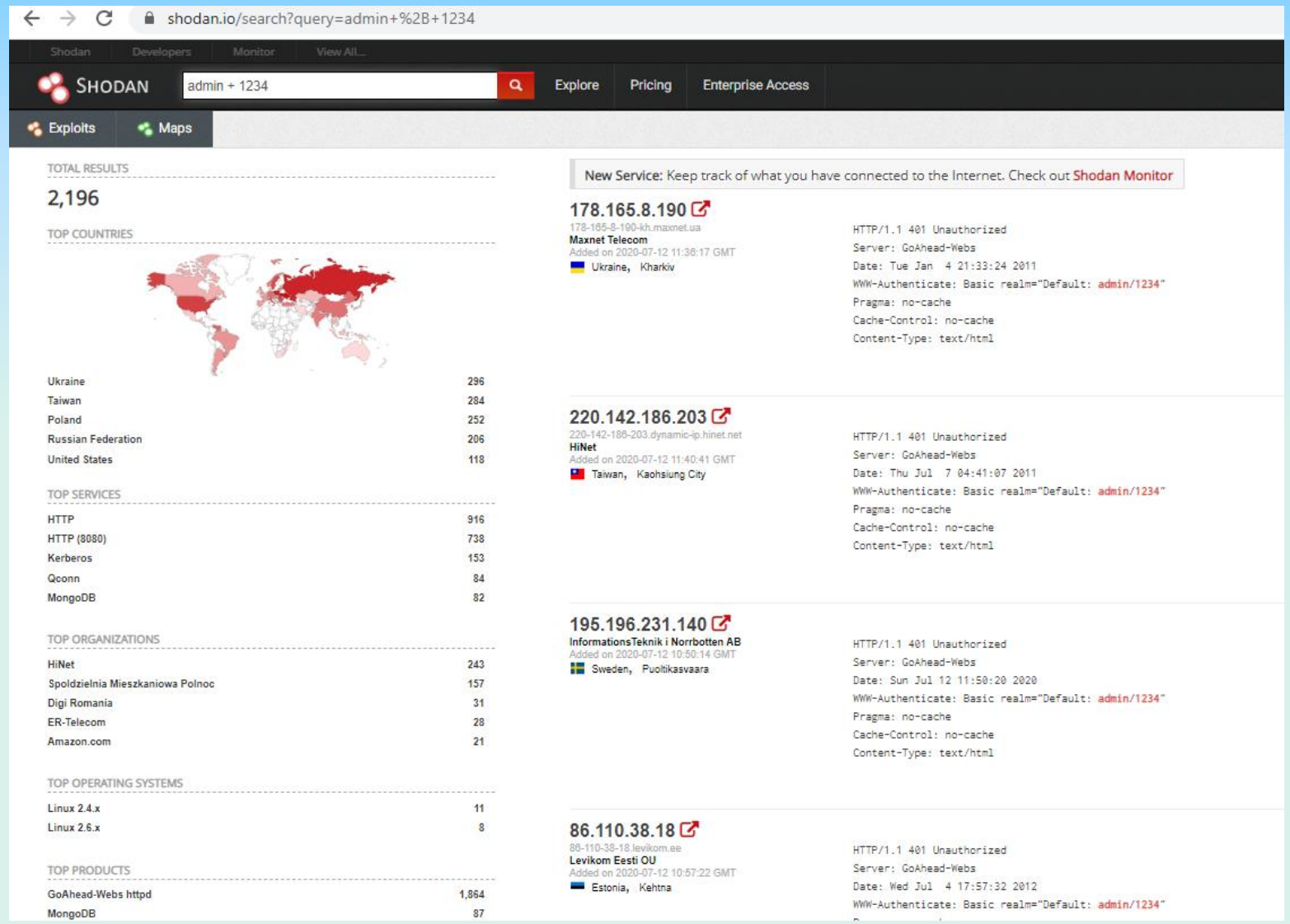
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

modbus



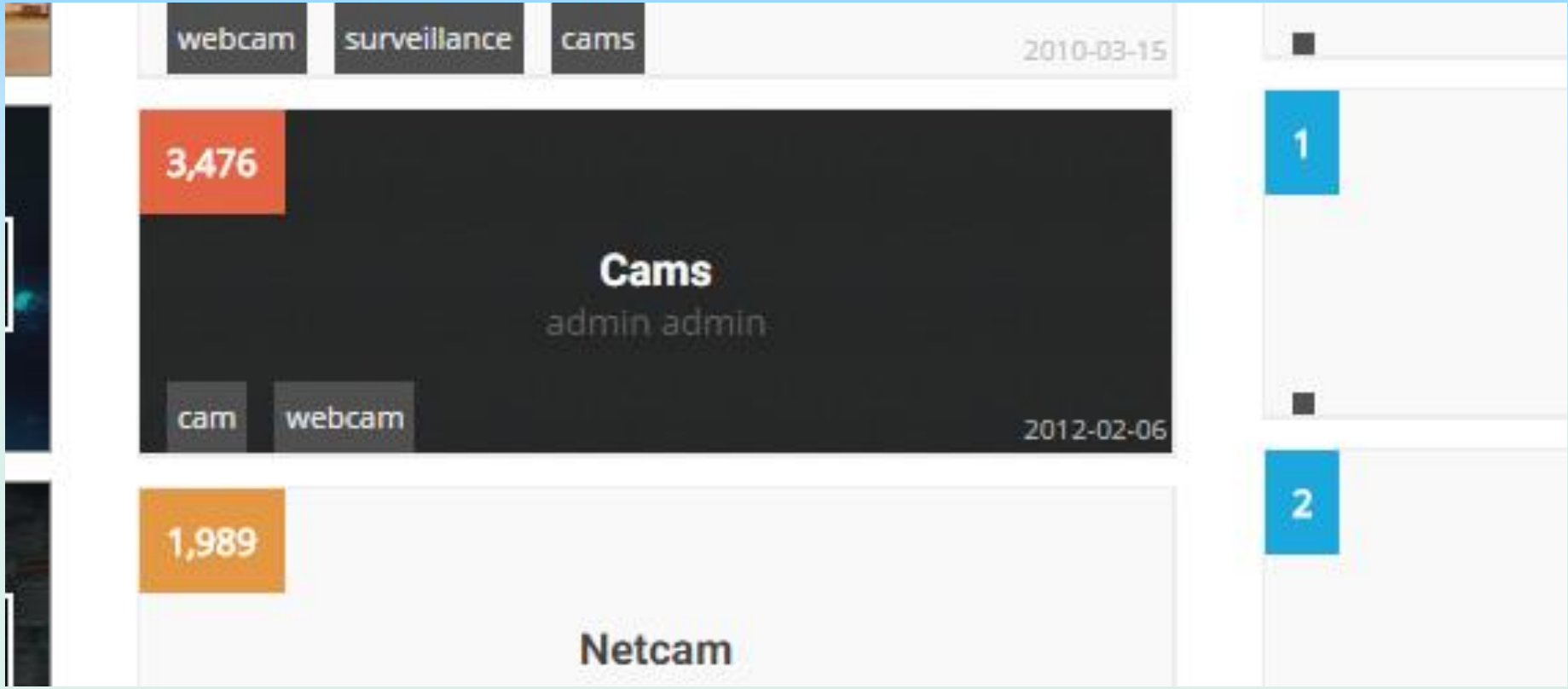
Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Admin + 1234

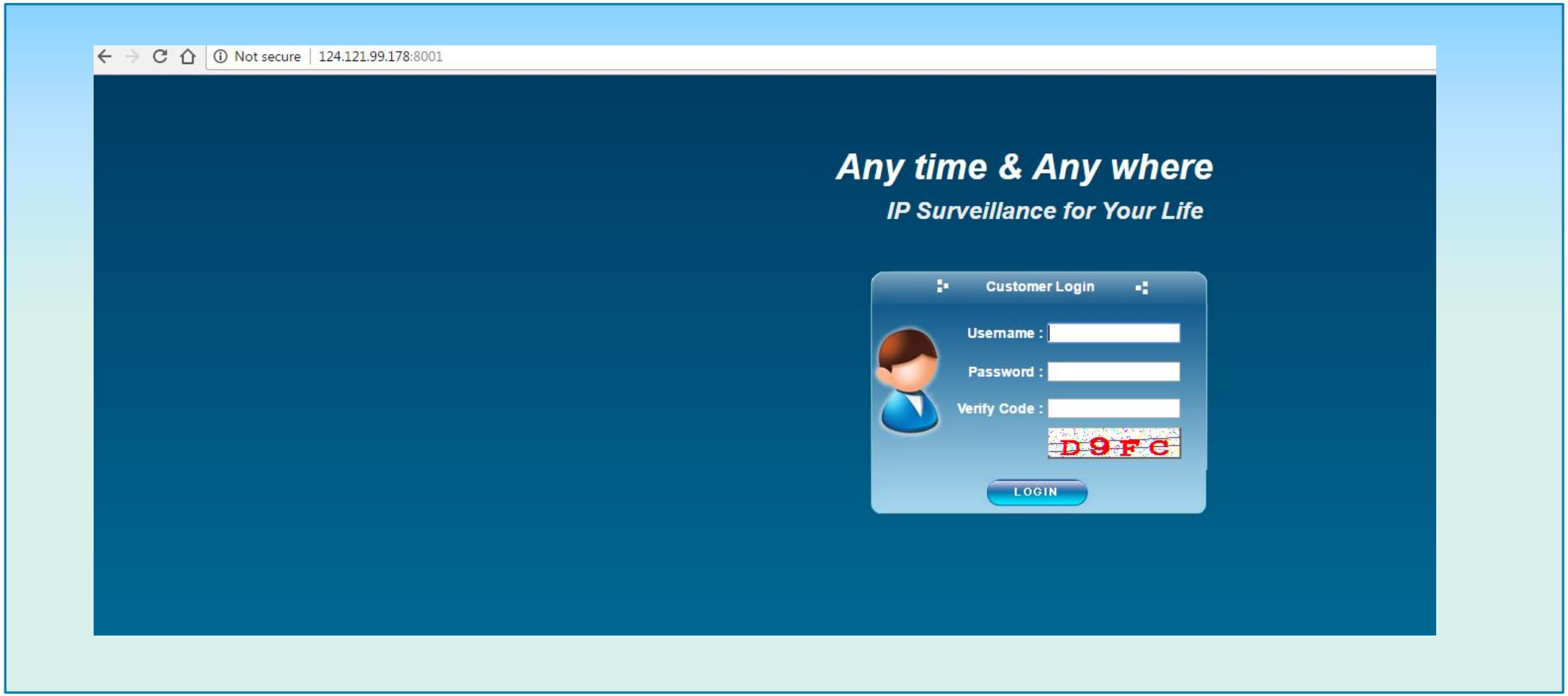


Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

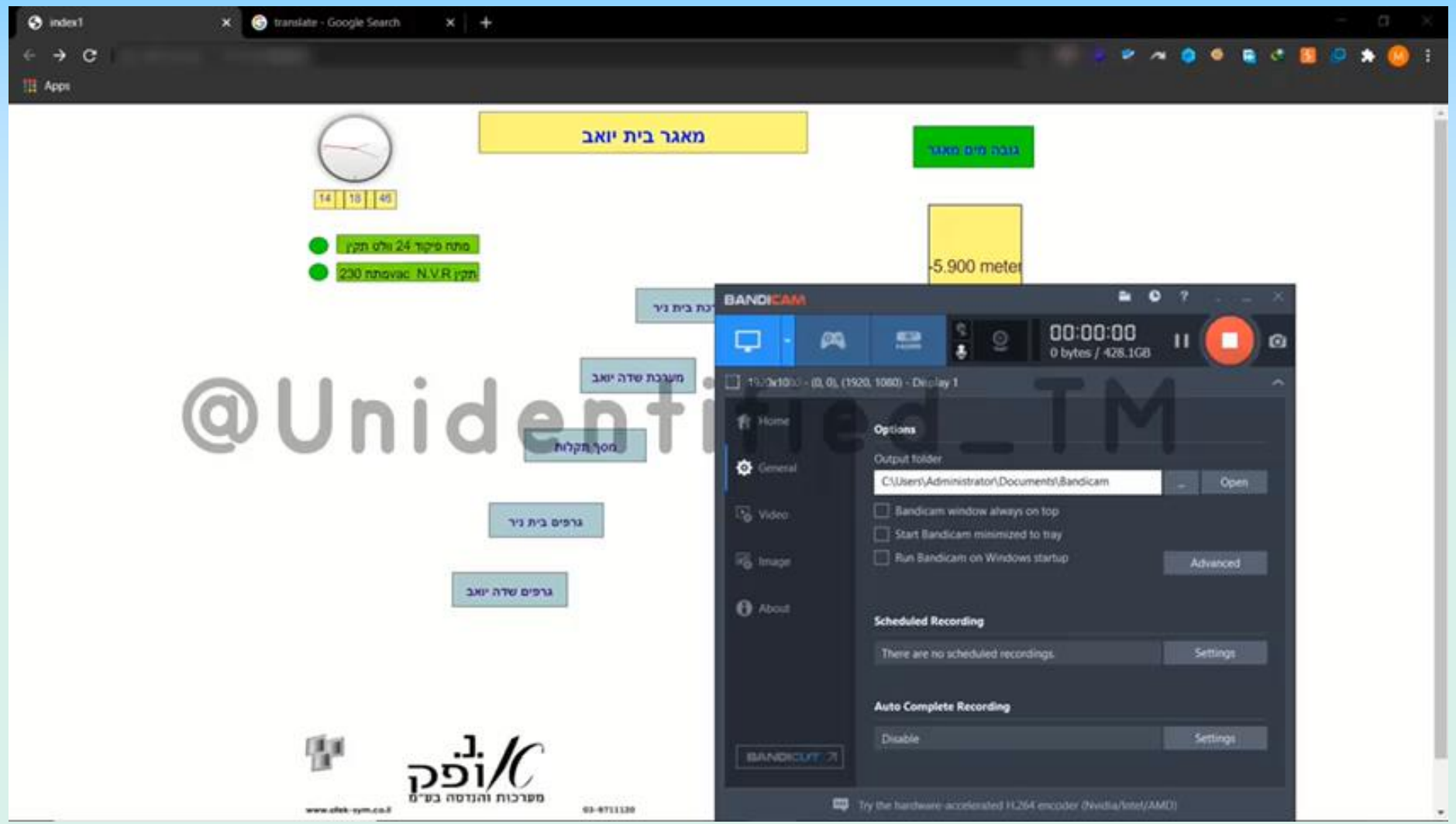
מצלמות פתוחות עם משתמש וסיסמא ידועים



מצלמה פתוחה לעולם



תקיפת מתקני מים בישראל – ע"י שימוש במידע שהגיע משודן



Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

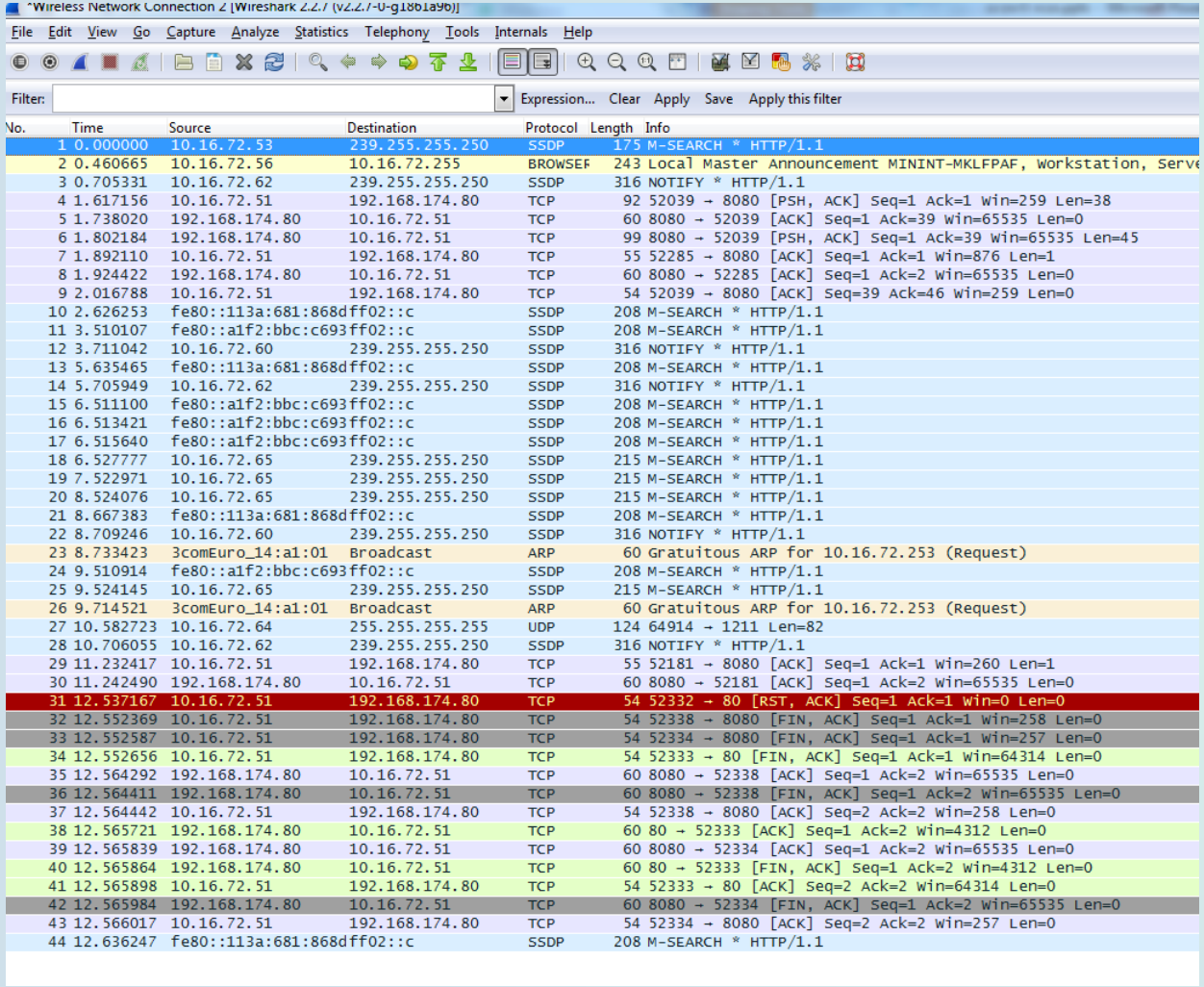

91.135.106.243
Country
Israel
Organization
Pelephone
Ports
80
502
View Host Details
@UnidentifiedTM
1.4 bar
0 RPM
0 Kub\Hr
50 Hz
-5.900 meter

SNIFFER – רחרחן

תוכנה שיודעת לראות מה עובר ברשת המחשבים

לדוגמא:

WIRESHARK



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.16.72.53	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	0.460665	10.16.72.56	10.16.72.255	BROWSER	243	Local Master Announcement MININT-MKLFPAF, Workstation, Serve
3	0.705331	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
4	1.617156	10.16.72.51	192.168.174.80	TCP	92	52039 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=259 Len=38
5	1.738020	192.168.174.80	10.16.72.51	TCP	60	8080 → 52039 [ACK] Seq=1 Ack=39 Win=65535 Len=0
6	1.802184	192.168.174.80	10.16.72.51	TCP	99	8080 → 52039 [PSH, ACK] Seq=1 Ack=39 Win=65535 Len=45
7	1.892110	10.16.72.51	192.168.174.80	TCP	55	52285 → 8080 [ACK] Seq=1 Ack=1 Win=876 Len=1
8	1.924422	192.168.174.80	10.16.72.51	TCP	60	8080 → 52285 [ACK] Seq=1 Ack=2 Win=65535 Len=0
9	2.016788	10.16.72.51	192.168.174.80	TCP	54	52039 → 8080 [ACK] Seq=39 Ack=46 Win=259 Len=0
10	2.626253	fe80::113a:681:868d	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
11	3.510107	fe80::a1f2:bbc:c693	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
12	3.711042	10.16.72.60	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
13	5.635465	fe80::113a:681:868d	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
14	5.705949	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
15	6.511100	fe80::a1f2:bbc:c693	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
16	6.513421	fe80::a1f2:bbc:c693	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
17	6.515640	fe80::a1f2:bbc:c693	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
18	6.527777	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
19	7.522971	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20	8.524076	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
21	8.667383	fe80::113a:681:868d	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
22	8.709246	10.16.72.60	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
23	8.733423	3comEuro_14:a1:01	Broadcast	ARP	60	Gratuitous ARP for 10.16.72.253 (Request)
24	9.510914	fe80::a1f2:bbc:c693	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
25	9.524145	10.16.72.65	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
26	9.714521	3comEuro_14:a1:01	Broadcast	ARP	60	Gratuitous ARP for 10.16.72.253 (Request)
27	10.582723	10.16.72.64	255.255.255.255	UDP	124	64914 → 1211 Len=82
28	10.706055	10.16.72.62	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
29	11.232417	10.16.72.51	192.168.174.80	TCP	55	52181 → 8080 [ACK] Seq=1 Ack=1 Win=260 Len=1
30	11.242490	192.168.174.80	10.16.72.51	TCP	60	8080 → 52181 [ACK] Seq=1 Ack=2 Win=65535 Len=0
31	12.537167	10.16.72.51	192.168.174.80	TCP	54	52332 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	12.552369	10.16.72.51	192.168.174.80	TCP	54	52338 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
33	12.552587	10.16.72.51	192.168.174.80	TCP	54	52334 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
34	12.552656	10.16.72.51	192.168.174.80	TCP	54	52333 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64314 Len=0
35	12.564292	192.168.174.80	10.16.72.51	TCP	60	8080 → 52338 [ACK] Seq=1 Ack=2 Win=65535 Len=0
36	12.564411	192.168.174.80	10.16.72.51	TCP	60	8080 → 52338 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
37	12.564442	10.16.72.51	192.168.174.80	TCP	54	52338 → 8080 [ACK] Seq=2 Ack=2 Win=258 Len=0
38	12.565721	192.168.174.80	10.16.72.51	TCP	60	80 → 52333 [ACK] Seq=1 Ack=2 Win=4312 Len=0
39	12.565839	192.168.174.80	10.16.72.51	TCP	60	8080 → 52334 [ACK] Seq=1 Ack=2 Win=65535 Len=0
40	12.565864	192.168.174.80	10.16.72.51	TCP	60	80 → 52333 [FIN, ACK] Seq=1 Ack=2 Win=4312 Len=0
41	12.565898	10.16.72.51	192.168.174.80	TCP	54	52333 → 80 [ACK] Seq=2 Ack=2 Win=64314 Len=0
42	12.565984	192.168.174.80	10.16.72.51	TCP	60	8080 → 52334 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
43	12.566017	10.16.72.51	192.168.174.80	TCP	54	52334 → 8080 [ACK] Seq=2 Ack=2 Win=257 Len=0
44	12.636247	fe80::113a:681:868d	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

כלי האקינג נוספים

KALI LINUX

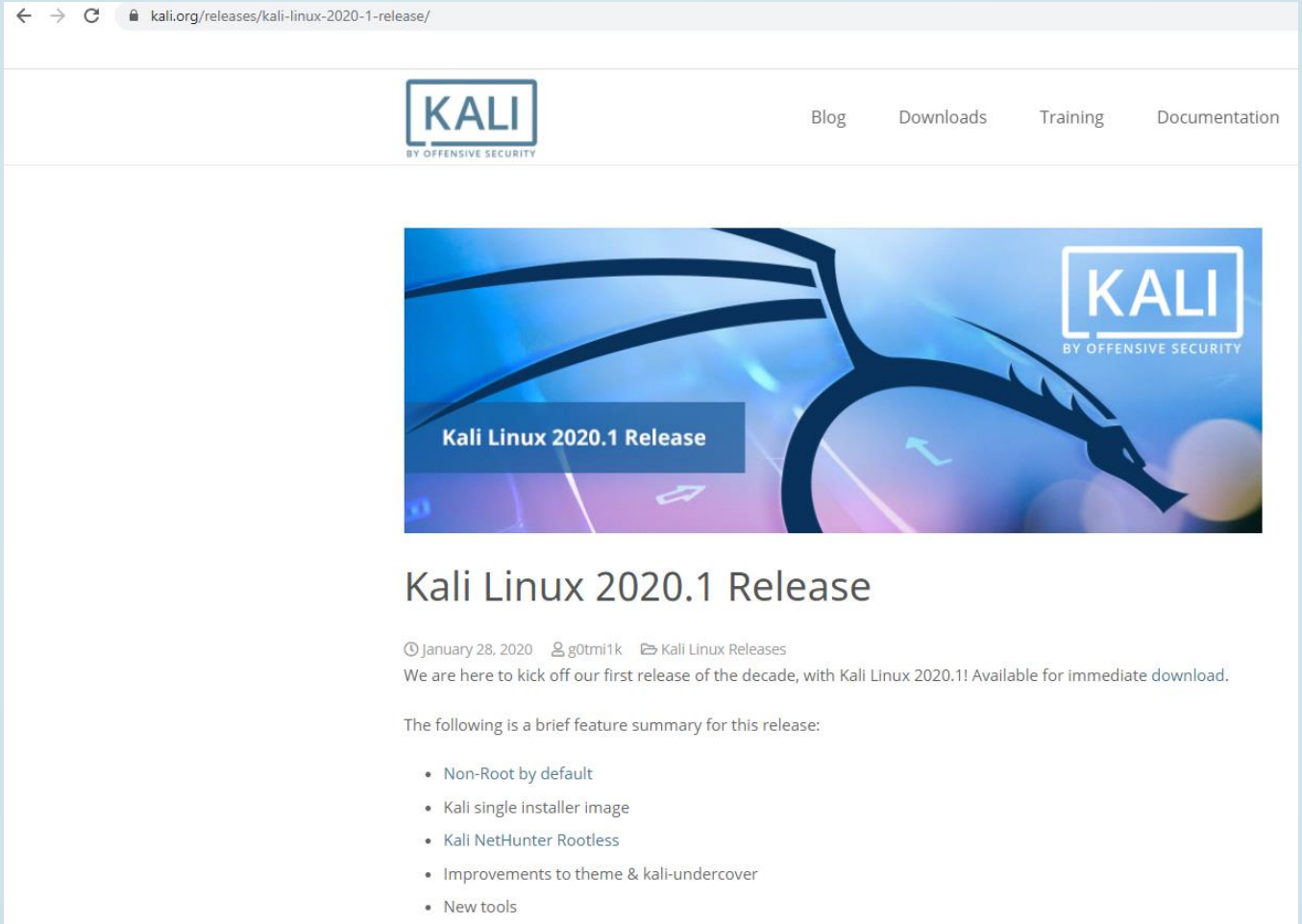
Back - Track היה בעבר

- כלי האזנה לתעבורת רשת
- כלי סריקת חורי אבטחה במערכות שונות
- כלי פיצוח סיסמאות
- כלי פריצת רשתות אלחוטיות
- כלים ליצירת תקיפת פישינג
- כלים למתקפות MAN IN THE MIDDLE
- כלי תקיפה נוספים

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

הורדה פשוטה וחינמית

https://www.kali.org/releases/kali-linux-2020-1-release/



PORT SCANNING – כלי סריקה

Common TCP Ports

According to the Nmap classification, these are the most common TCP ports:

- 21 - FTP (File Transfer Protocol)
- 22 - SSH (Secure Shell)
- 23 - Telnet
- 25 - SMTP (Mail)
- 80 - HTTP (Web)
- 110 - POP3 (Mail)
- 143 - IMAP (Mail)
- 443 - HTTPS (Secure Web)
- 445 - SMB (Microsoft File Sharing)
- 3389 - RDP (Remote Desktop Protocol)

Our TCP Port Scanner with Nmap

The **Full Scan** allows you to perform portscans with **custom parameters**, easily configured from the web interface:

- Specify custom TCP ports to scan (1-65535)
- Enable/disable service detection
- Enable/disable operating system detection
- Enable/disable host discovery
- Do Traceroute

המטרה:

מציאת שירות פתוח (פורט פתוח)

הכלי: NMAP

65,535 TCP Ports
65,535 UDP Ports

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

בעזרת תכנה שנקראת hydra נמצאת בחבילת ה-KALI LINUX - BRUTE FORCE

Password Protection

This table illustrates maximum times for a brute force attack for passwords of 96 character complexity (upper and lower case, numbers, and special characters). If your passwords cannot be this complex, the amount of time would be greatly reduced.

The calculations are based on 96 to the power of the password characters. So a password of length 8 characters has 96^8 complexity or 7.2 quadrillion possible combinations. The table further shows 4 columns of brute force password processing attempts in units per second. The first column is 10 million per second, which is possible to do with a modern quad core processor. The last column is 76 billion per second, which is possible to do with a botnet. The table lists the maximum amount of time. It is possible to reduce this time using different password- cracking technologies such as dictionaries and look-up tables.

Number of Characters	Complexity (96^x)	QUAD CORE 10 Million / sec	100 Million / sec	BOT NET 76 Billion / sec	2.5 Quadrillion / sec
4	84.9 Million	8.49 seconds	< 1 second	< 1 second	< 1 second
6	782.8 Billion	21.7 hours	2.2 hours	10.3 seconds	< 1 second
7	75.1 Trillion	87 days	8.7 days	16.5 minutes	< 1 second
8	7.2 Quadrillion	22.9 years	2.3 years	1.1 days	2.9 seconds
9	692.5 Quadrillion	> 100 years	> 100 years	105.5 days	4.6 minutes

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

איך עובד BTUTE FORCE

מכינים קובץ txt וקוראים לו בשם : wordlist.txt

הקובץ מכיל: שורות המכילות אותיות או מספרים שעשויים להיות בסיסמא

הנטיה הטבעית להכניס לסיסמא מאפיינים אישיים

שם ומשפחה

תאריך לידה

שמות ילדים

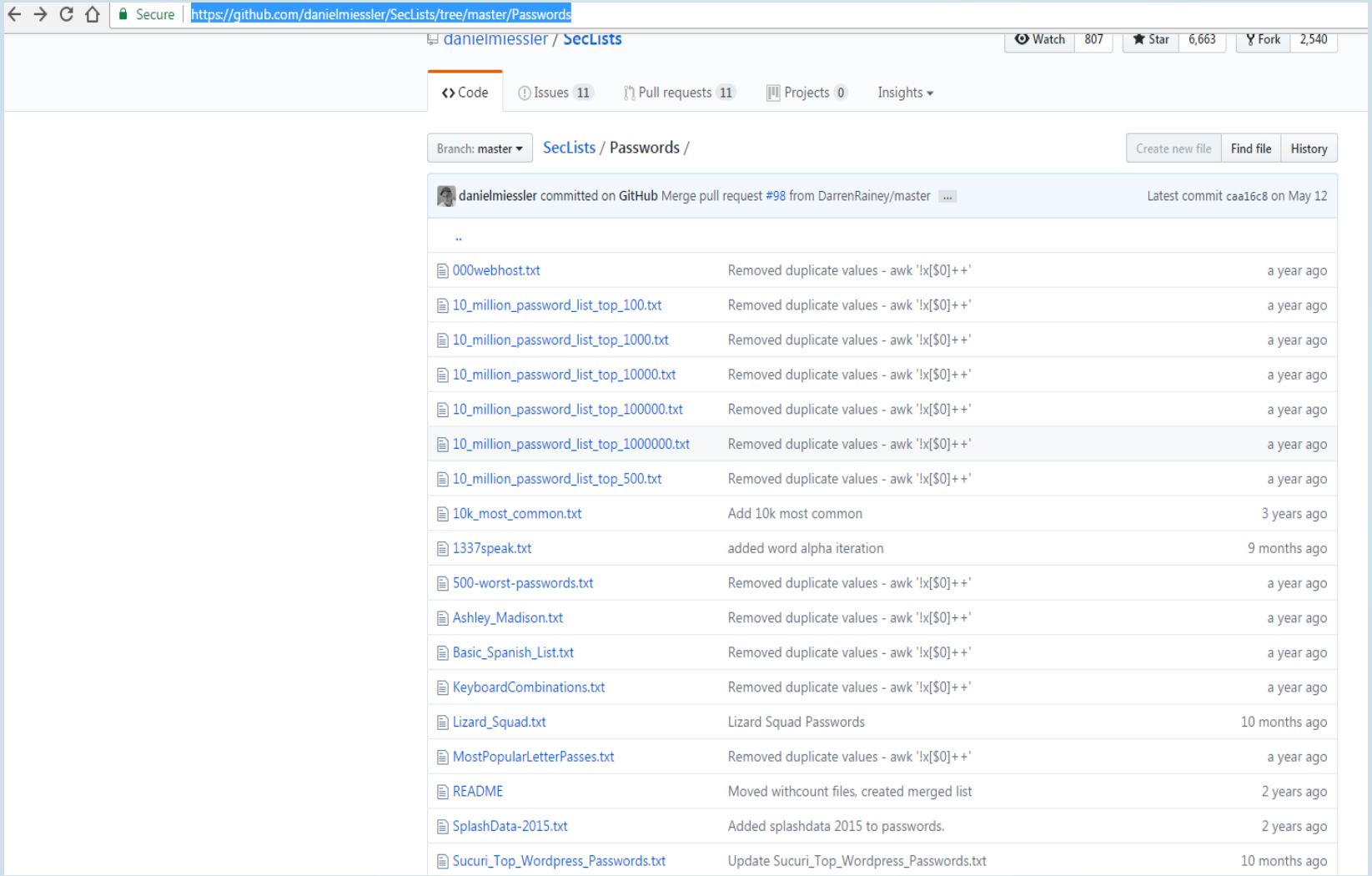
וכדומה

ישנם רשימות מוכנות ברשת שמכילות סיסמאות או קומבינציות שעשויות להביא לסיסמא :

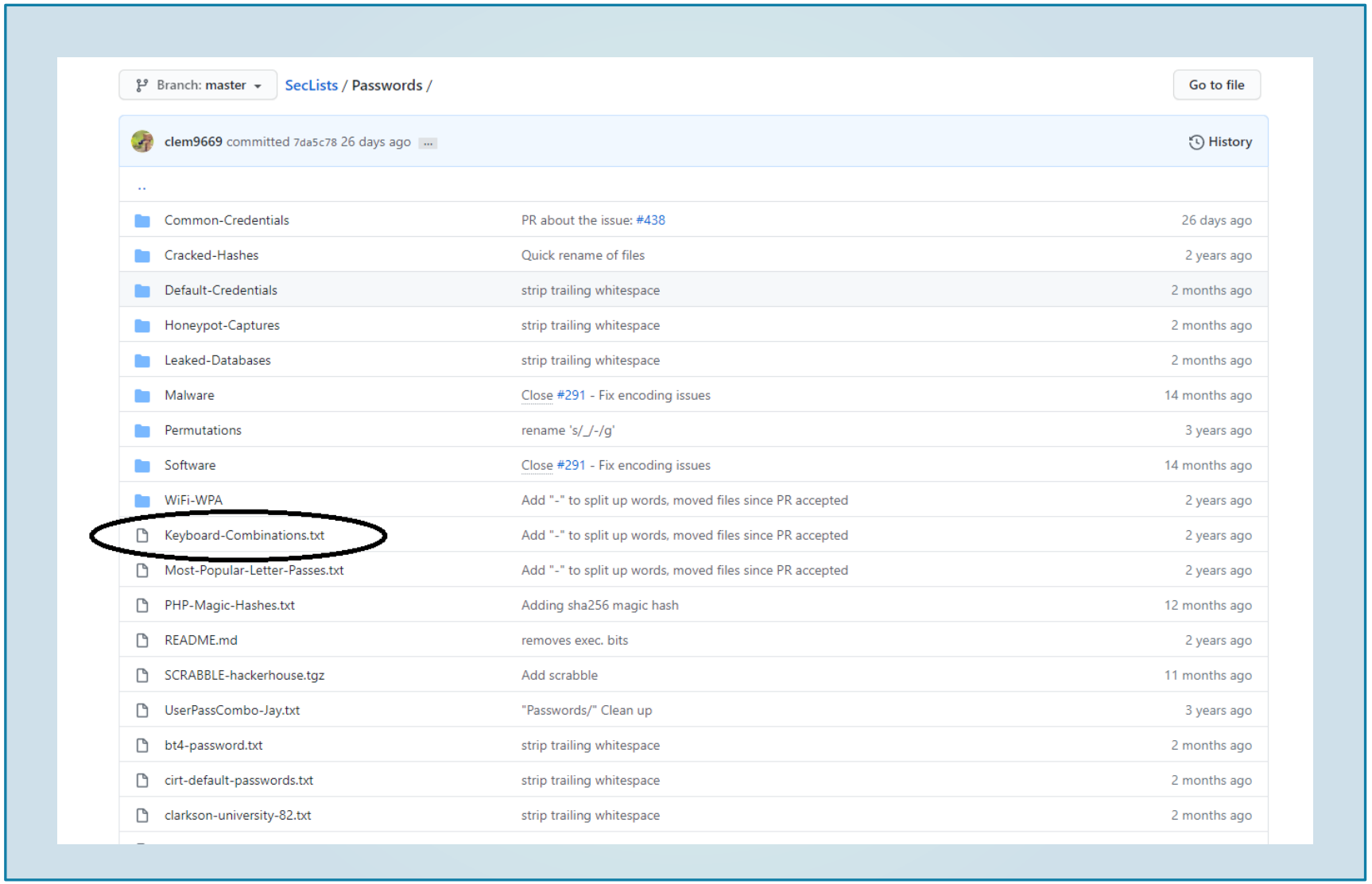
https://github.com/danielmiessler/SecLists/tree/master/Passwords

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דוגמאות לקבצי סיסמאות מהרשת



דוגמאות לקבצי סיסמאות מהרשת



Branch: master ▾ SecLists / Passwords / Go to file

clem9669 committed 7da5c78 26 days ago ... History

..		
Common-Credentials	PR about the issue: #438	26 days ago
Cracked-Hashes	Quick rename of files	2 years ago
Default-Credentials	strip trailing whitespace	2 months ago
Honeypot-Captures	strip trailing whitespace	2 months ago
Leaked-Databases	strip trailing whitespace	2 months ago
Malware	Close #291 - Fix encoding issues	14 months ago
Permutations	rename 's/_/-/g'	3 years ago
Software	Close #291 - Fix encoding issues	14 months ago
WiFi-WPA	Add "-" to split up words, moved files since PR accepted	2 years ago
Keyboard-Combinations.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
Most-Popular-Letter-Passes.txt	Add "-" to split up words, moved files since PR accepted	2 years ago
PHP-Magic-Hashes.txt	Adding sha256 magic hash	12 months ago
README.md	removes exec. bits	2 years ago
SCRABBLE-hackerhouse.tgz	Add scrabble	11 months ago
UserPassCombo-Jay.txt	"Passwords/" Clean up	3 years ago
bt4-password.txt	strip trailing whitespace	2 months ago
cirt-default-passwords.txt	strip trailing whitespace	2 months ago
clarkson-university-82.txt	strip trailing whitespace	2 months ago

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

קומבינציות עוקבות על המקלדת

Branch: master ▾ SecLists / Passwords / Keyboard-Combinations.txt

g0tmi1k Add "-" to split up words, moved files since PR accepted ...

1 contributor

9604 lines (9604 sloc) | 82.5 KB

```
zaq1zaq1
zaq1xsw2
zaq1cde3
zaq1vfr4
zaq1bgt5
zaq1nhy6
zaq1mju7
zaq1,ki8
zaq1.lo9
zaq1/;p0
zaq1ZQ!
zaq1XW@
zaq1DE#
zaq1FR$
zaq1BGT%
zaq1NHY^
zaq1JU&
zaq1<KI*
zaq1LO(
zaq1?:P)
zaq1qwer
zaq11234
zaq1asdf
zaq1zxcv
zaq1!@#$
zaq12345
zaq13456
zaq14576
zaq15678
zaq16789
zaq17890
zaq1890-
zaq190=-
zaq10-=\
```

סיסמאות נפוצות

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]	2019[11]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou	123123
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess	abc123
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin	qwerty123
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome	1q2w3e4r
14	master	sunshine	letmein	abc123	111111	abc123	login	666666	admin
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123	qwertyuiop
16	ashley	123123	1234	mustang	dragon	121212	starwars	football	654321
17	bailey	welcome	monkey	access	master	flower	123123	123123	555555
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey	lovely
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321	7777777
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*	welcome
21	654321	jesus	password1	superman	princess	master	hello	charlie	888888
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456	princess
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald	dragon
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123	123qwe

https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

המשרד להגנת הסביבה

סייבר בתעשייה
המשרד להגנת הסביבה

סיסמאות נפוצות – 2023

The top 10 most common passwords list in 2023:

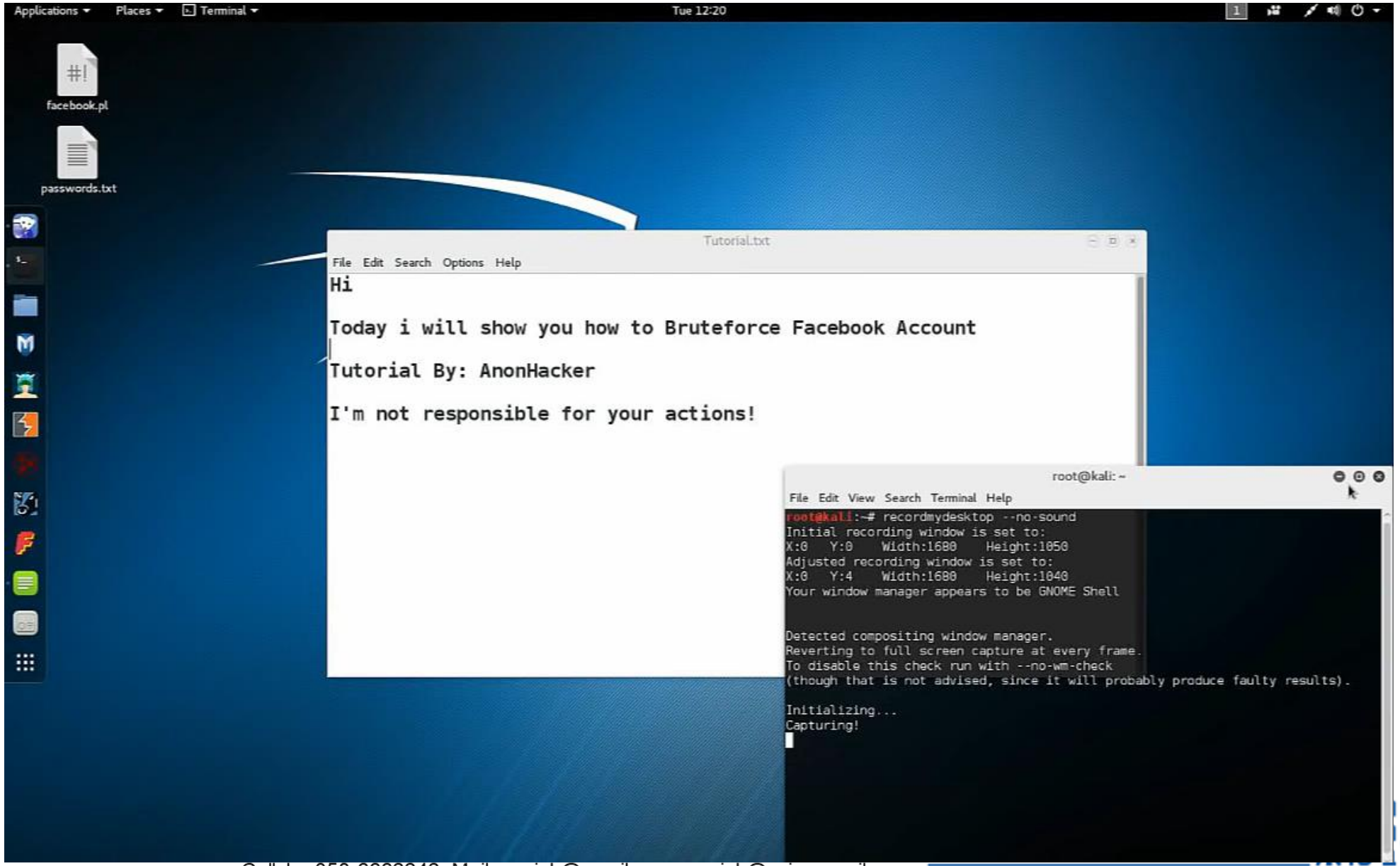
1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

התאחדות התעשיינים בישראל

סרטון האקר בפעולת פריצת סיסמא...

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il



Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Google Hack

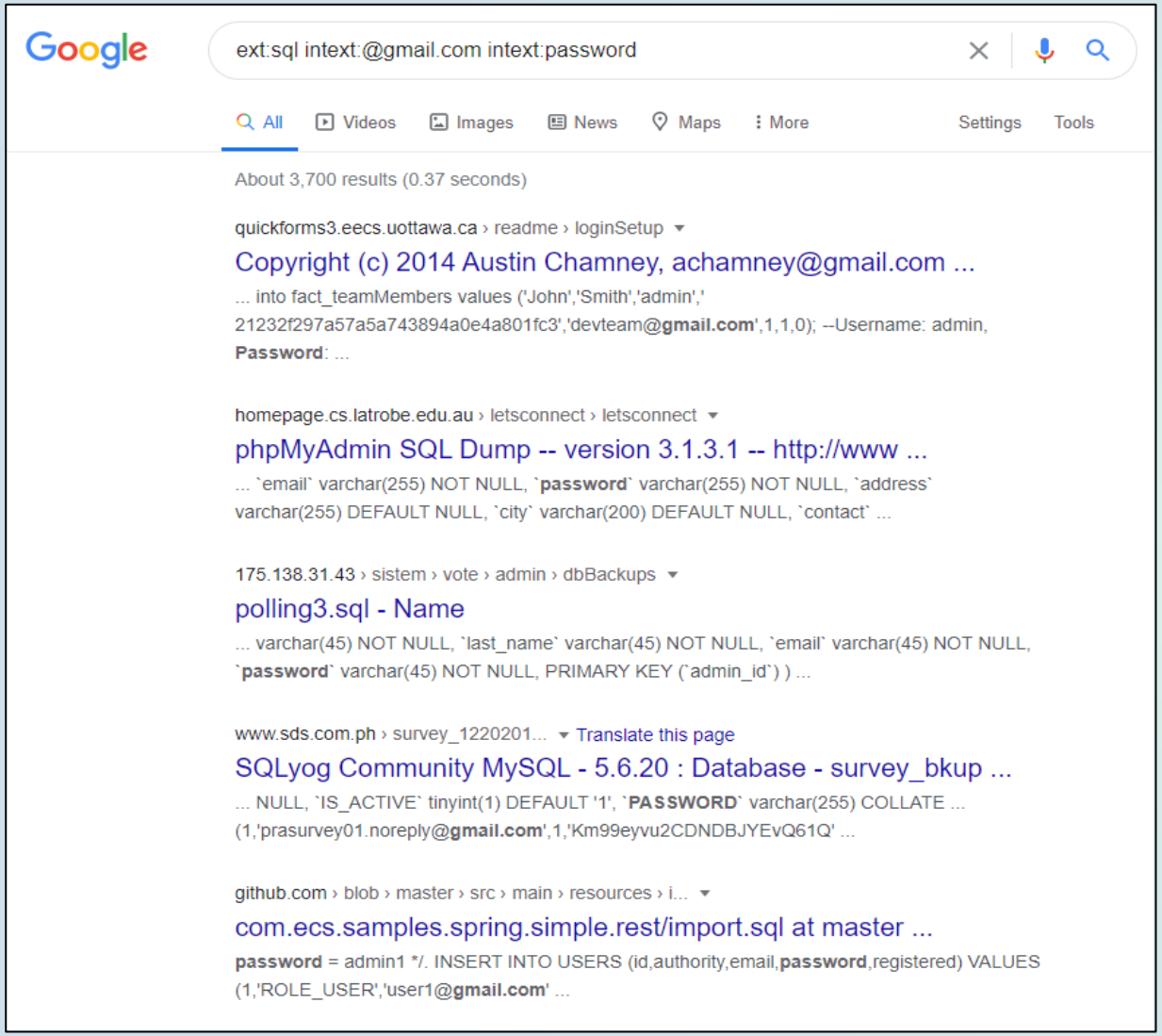
ניצול יכולות החיפוש בגוגל לצורך קבלת מידע על סיסמאות, משתמשים, חולשות וכדומה

Advanced Operator	Description	Examples
site:	Limit the search query to a specific domain or web site.	• site:example.com
filetype:	Limit the search to text found in a specific file type	• mysqldump filetype:sql
link:	Search for pages that link to the requested URL	• link:www.example.com
cache:	Search and display a version of a web page as it was shown when Google crawled it.	• cache:example.com
intitle:	Search for a string text within the title of a page.	• intitle:"index of"
inurl:	Search for a string within a URL	• inurl:passwords.txt

Logical Operator	Description	Examples
AND or +	Used to include keywords. All the keywords need to be found.	• web **AND** application **AND** security • web **+**application **+**security
NOT or –	Used to exclude keywords. All the keywords need to be found.	• web application **NOT** security • web application **–**security
OR or |	Used to include keywords where either one keyword or another is matched. All the keywords need to be found.	• web application **OR** security • web application **|**security
Tilde (~)	Used to include synonyms and similar words.	• web application ~security
Double quote (")	Used to include exact matches.	• "web application security"
Period (.)	Used to include single-character wildcards.	• .eb application security
Asterisk (*)	Used to include single-word wildcards.	• web * security
Parenthesis (())	Used to group queries	• ("web security" | websecurity)

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

דוגמא לחיפוש



ext:sql intext:@gmail.com intext:password

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Google hacking

Advanced operator table:

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

הוצאת רשימת סיסמאות

filetype:txt username pa... | Full text of "OpIsrael Of... | www.fu...

thonthao6.sextgem.com/files/superhit.txt

```
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWARD:rahulhina111';
?><?php
='USER ID:rahul9267671167bimt@gmail.com';
='PASSWARD:rahulhina111';
?><?php
='USER ID:yar yeh phisher kon kon use krha hai';
='PASSWARD:????';
?><?php
='USER ID:dvirus_ajju@yahoo.in';
='PASSWARD:';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:Prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:prakashpsm@live.in';
='PASSWARD:akshaykatrina';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWARD:divyaps';
?><?php
='USER ID:ashukp584@yahoo.com';
='PASSWARD:divyaps';
?><?php
='USER ID:shrishesha@gmail.com';
='PASSWARD:9900878675';
?><?php
='USER ID:shrishesha@gmail.com';
='PASSWARD:9900878675';
?><?php
='USER ID:Bhinda18@yahoo.com';
='PASSWARD:';
?><?php
='USER ID:Dhiraj.suryavanshi';
='PASSWARD:585523';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWARD:akibakib';
?><?php
='USER ID:akibbagwan007@yahoo.com';
='PASSWARD:786786';
?><?php
```


```
beithamaayan@walla.com  679239
hodaka1@gmail.com       1q2w3e4r
aviv_rent1@bezeqint.net 7233826
inbalims@zahav.net.il   301084
etl88@walla.co.il       340867
contact@ekdesign.co.il  123456
adi.tzachar@gmail.com   adi123456
yeudit@green1realestate.com     123456
eve@vayax.co.il e1234567
stevenalina@walla.com   eldorado
shimixxxx@walla.com     1122
shayn@nioi.gov.il       dba621
alon@ekdesign.co.il     123456
karnona@yahoo.com       23307maya
elie_asaraf@walla.co.il 1q2w3e
kifkef@kifkef.co.il     458123
coolit@inn.co.il        tamar15
yardenbp@gmail.com      tulli2000
joel70@walla.com        123456
talizh@gmail.com        tal1234
orit_nakar2003@yahoo.com        tuxyrkhv
liormaaam@walla.com     0528546365
shacharf1@bezeqint.net  ys321948
drreshef@gmail.com      a355v411
```

you are wathcing user and password

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

כלי האקינג נוספים בתוך ה-KALI - LINUX

– Minikatz לקחת הרשאות , לבצע תנועה צידית (Lateral Movement)

– MetaSploit סט כלי תקיפה בעיקר כדי להפוך exploits למודולרים

– Ettercap – Mac Spoofing , ARP Poisioning
תקיפת "אדם באמצע" – MAN IN THE MIDDLE

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il

Yosi Shavit MBA, CISM - Information Security & Cyber Expert
Cellular:058-6662242 Mail: yosish@gmail.com, yosish@sviva.gov.il