

מבוא להאק ינג חלק א'



נושאי הלימוד



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

Black Hat



White Hat



Grey Hat



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

נקרא גם "מאבטח מידע"

White Hat


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 

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.



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??

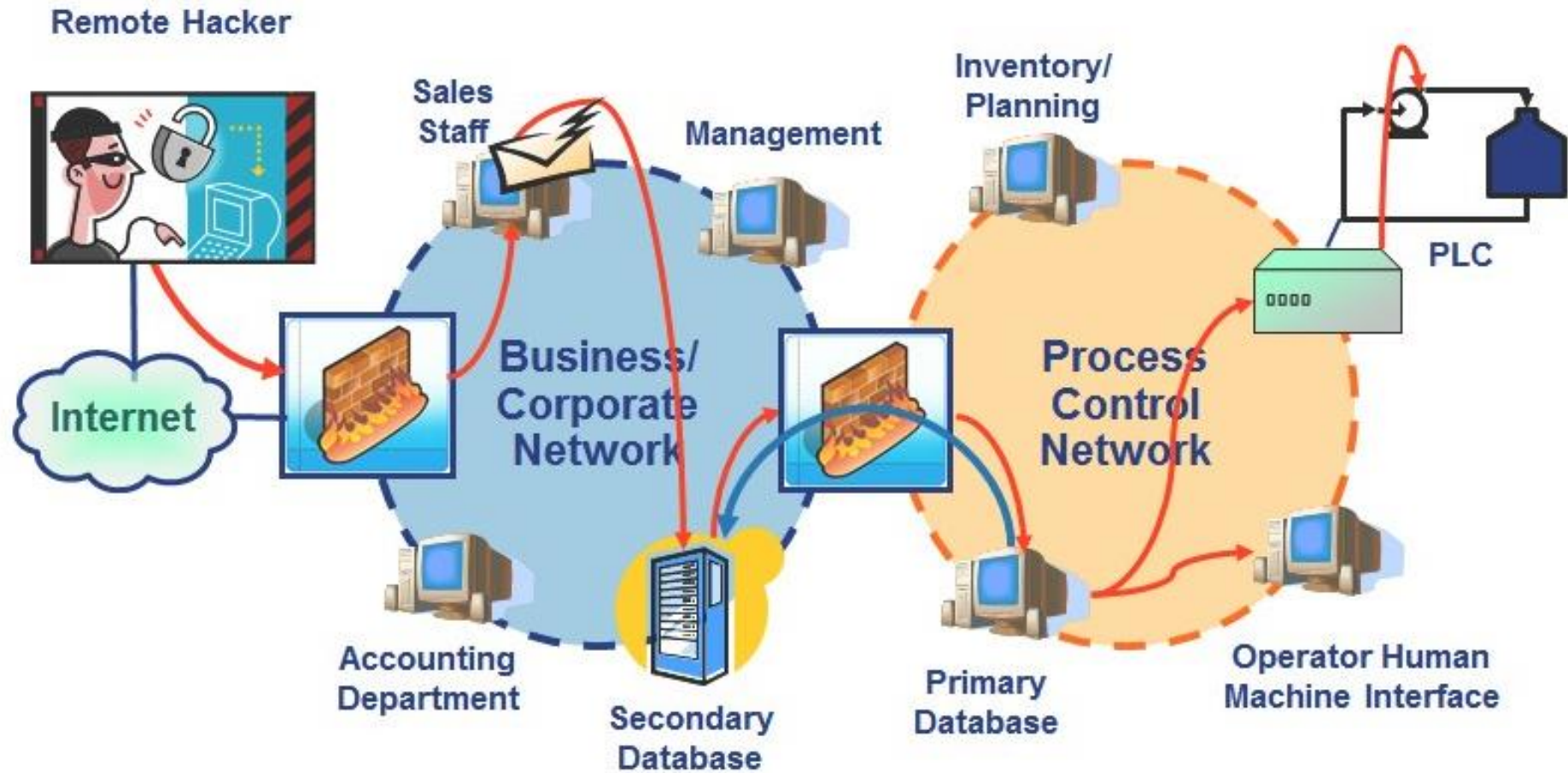
כיצד פועל ההאקר ? (כובע שחור)

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

מבט כללי על רשת טיפוסית במפעל



מתודולוגיית התקיפה – חדירה ראשונית

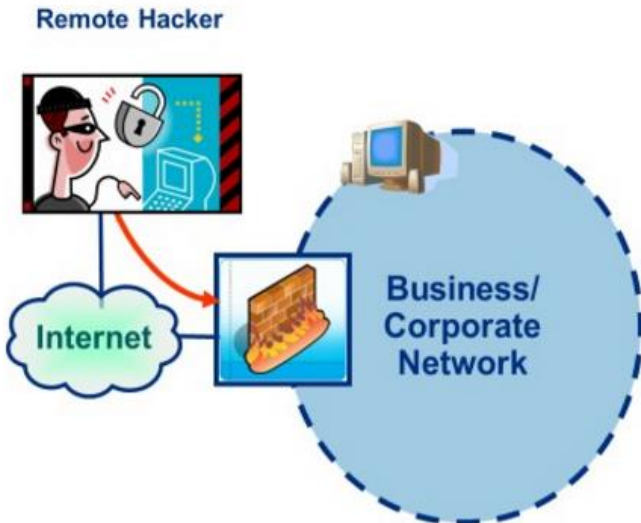
חדירה ראשונית:

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:

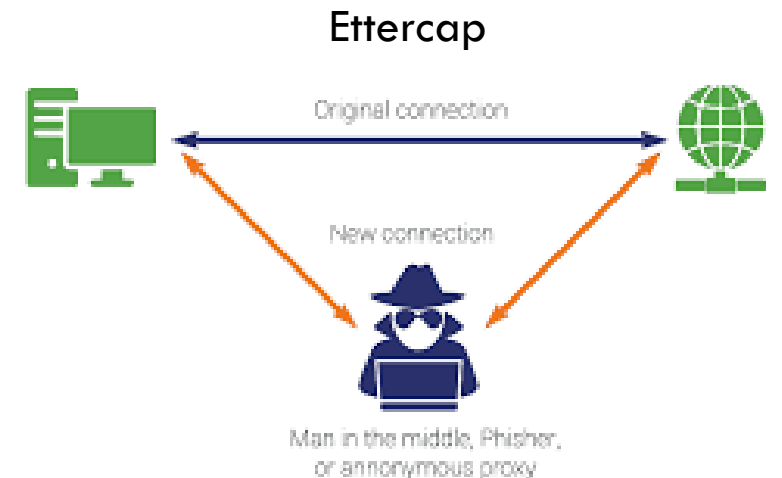
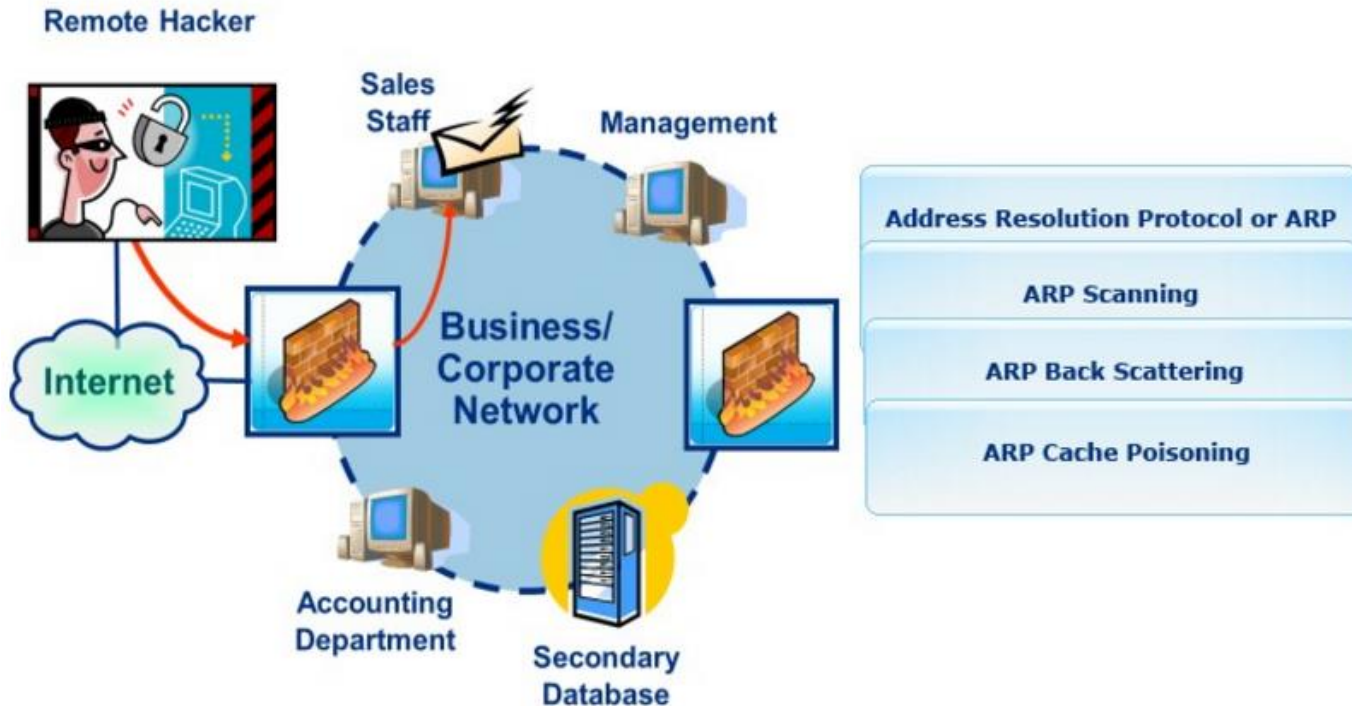


- משלוח מייל לארגון
- הורדת קובץ מהאינטרנט
- שיטוט באתר שנפל קורבן

מתודולגית התקיפה – שליטה על התקשורת ברשת

לאחר החדירה

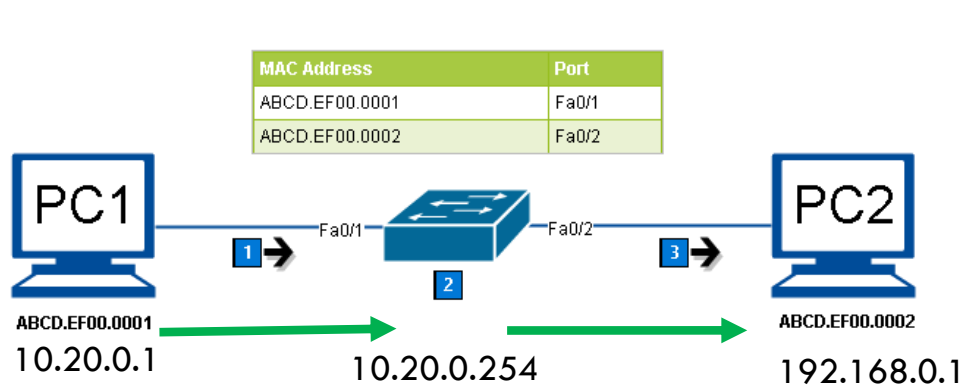
- התוקף מבצע LATERAL MOVEMENT בתוך רשת הארגון באמצעות ARP
- שינוי ב-ARP שמחזיקים המחשבים בארגון יעביר את כל התעבורה למחשב הנשלט (הופך אותו ל DEFAULT GATEWAY).
- בשלב זה השיג התוקף שליטה על התעבורה של התקשורת בארגון.



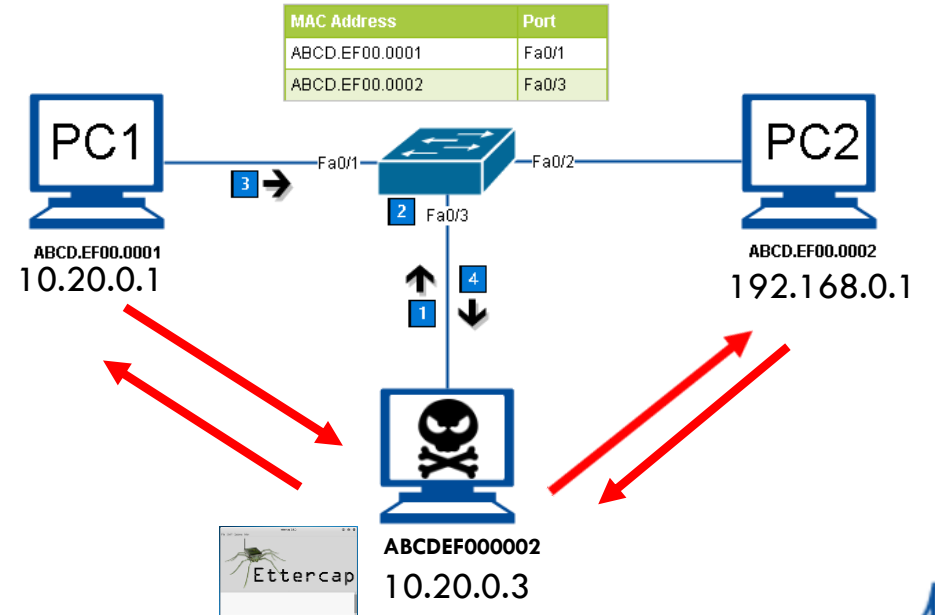
Mac Spoofing Attack

תוקף מסניף את הרשת (ע"י סניפר שניתן להוריד חינם מהרשת) לאיתור MAC ADDRESS לגיטימי ומנסה להתנהג כמוהו.

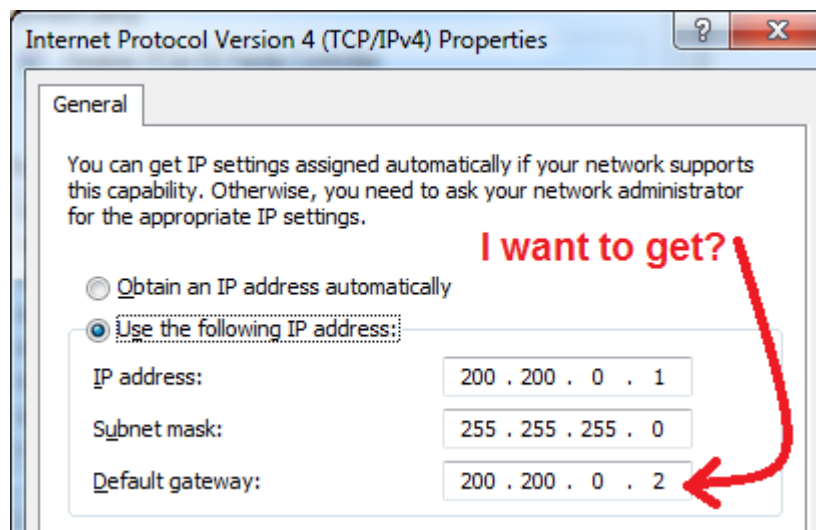
התוקף מציג עצמו כ- DEFAULT GATEWAY וכך עוברת כל התעבורה דרכו.



Source: <https://www.jannet.hk/en/post/mac-address-table-attack/>

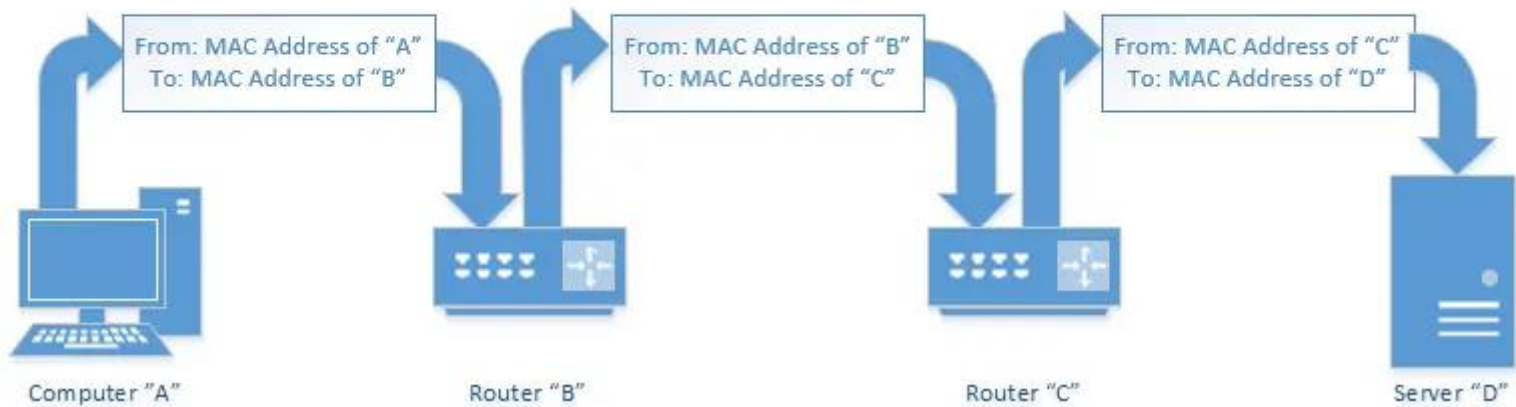


Default Gateway



במידה והמחשב אליו אני מתקשר לא ברשת שלי, התקשורת תצא אל "יציאת ברירת המחדל", בד"כ כתובת של ה-ROUTER שדרכו יוצאים לרשת אחרת.

IP vs Mac Address



Source: https://askleo.com/whats_the_difference_between_a_mac_address_and_an_ip_address/

זו – MAC ADDRESS
הכתובת הפיזית

MAC
Media Access Control Address



Organizationally Unique Identifier Universally Administered Address

Arp Table

ARP = Address Resolution Protocol

```
<FW>display arp
2017-11-07 17:27:54.130 +02:00
IP ADDRESS          MAC ADDRESS          EXPIRE (M)  TYPE  INTERFACE          VPN-INST
                   VLAN
-----
192.168.1.1         48fd-8e10-4680      I -         GE0/0/0          default
1.1.1.1             48fd-8e10-4681      I -         GE0/0/1
1.1.1.5             2047-47af-f37f      6           D-0             GE0/0/1
1.1.1.255           Incomplete          1           D-0             GE0/0/1
1.1.1.1             48fd-8e10-4683      I -         GE0/0/3          cata
192.168.3.5         48fd-8e10-4684      I -         GE0/0/4          cata
5.5.5.1             48fd-8e10-4685      I -         GE0/0/5
10.10.10.10        48fd-8e10-4686      I -         GE0/0/6
192.168.3.5         48fd-8e10-4687      I -         GE0/0/7
-----
Total:9             Dynamic:2            Static:0      Interface:7
```

טבלאות ARP

נמצאות בכל רכיבי התקשורת: מחשבים, שרתים, נתבים רכיבי אבטחת מידע

```
C:\Users\yossefs>arp -a

Interface: 10.200.10.133 --- 0x9
 Internet Address      Physical Address      Type
 10.200.10.12          98-e7-43-2b-14-a0    dynamic
 10.200.10.15          3c-2c-30-b9-e1-56    dynamic
 10.200.10.42          98-e7-43-0f-67-ce    dynamic
 10.200.10.254         08-97-34-de-34-65    dynamic
 10.200.10.255         ff-ff-ff-ff-ff-ff    static
 224.0.0.22            01-00-5e-00-00-16    static
 224.0.0.251           01-00-5e-00-00-fb    static
 224.0.0.252           01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

מציאת ה- DEFAULT GATEWAY

```
C:\Users\yossefs>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : sviva.gov.il

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : sviva.gov.il
    Link-local IPv6 Address . . . . . : fe80::d8c9:5520:e35a:bc56%9
    IPv4 Address. . . . . : 10.200.10.133
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.10.254

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Mobile Broadband adapter Cellular:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```

```
C:\Users\yossefs>tracert www.ynet.co.il

Tracing route to e12476.b.akamaiedge.net [23.195.10.161]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms   10.200.10.254
  1  <1 ms    <1 ms    <1 ms   10.30.250.249
  2  1 ms     1 ms     1 ms    172.17.1.14
  3  3 ms     2 ms     2 ms    172.30.12.13
  4  3 ms     2 ms     2 ms    172.30.1.5
  5  3 ms     3 ms     3 ms    172.17.1.2
```

מציאת כתובת פיסיית

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1214467	224.039208925	172.16.1.2	172.16.1.254	ICMP	116	Echo (ping) request id=0x...
1214696	224.062466172	172.16.1.2	172.16.1.254	ICMP	114	Echo (ping) request id=0x...
1236738	226.044383693	172.16.1.2	172.16.1.254	ICMP	116	Echo (ping) request id=0x...
1236949	226.066464998	172.16.1.2	172.16.1.254	ICMP	114	Echo (ping) request id=0x...
1376853	238.577461725	172.16.1.2	172.16.1.254	ICMP	116	Echo (ping) request id=0x...
1377089	238.602675214	172.16.1.2	172.16.1.254	ICMP	114	Echo (ping) request id=0x...
1399115	240.580919267	172.16.1.2	172.16.1.254	ICMP	116	Echo (ping) request id=0x...
1399316	240.602473039	172.16.1.2	172.16.1.254	ICMP	114	Echo (ping) request id=0x...
1421510	242.585849188	172.16.1.2	172.16.1.254	ICMP	116	Echo (ping) request id=0x...
1421646	242.602516834	172.16.1.2	172.16.1.254	ICMP	114	Echo (ping) request id=0x...

Frame 1192625: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0

- Ethernet II, Src: Cisco_37:c8:e5 (00:1e:7a:37:c8:e5), Dst: Cisco_8f:c3:c0 (00:16:46:8f:c3:c0)
 - Destination: Cisco_8f:c3:c0 (00:16:46:8f:c3:c0)
 - Source: Cisco_37:c8:e5 (00:1e:7a:37:c8:e5)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.16.1.254, Dst: 172.16.1.2
- Internet Control Message Protocol

Frame (frame), 114 bytes Packets: 1952692 · Displayed: 2

*eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

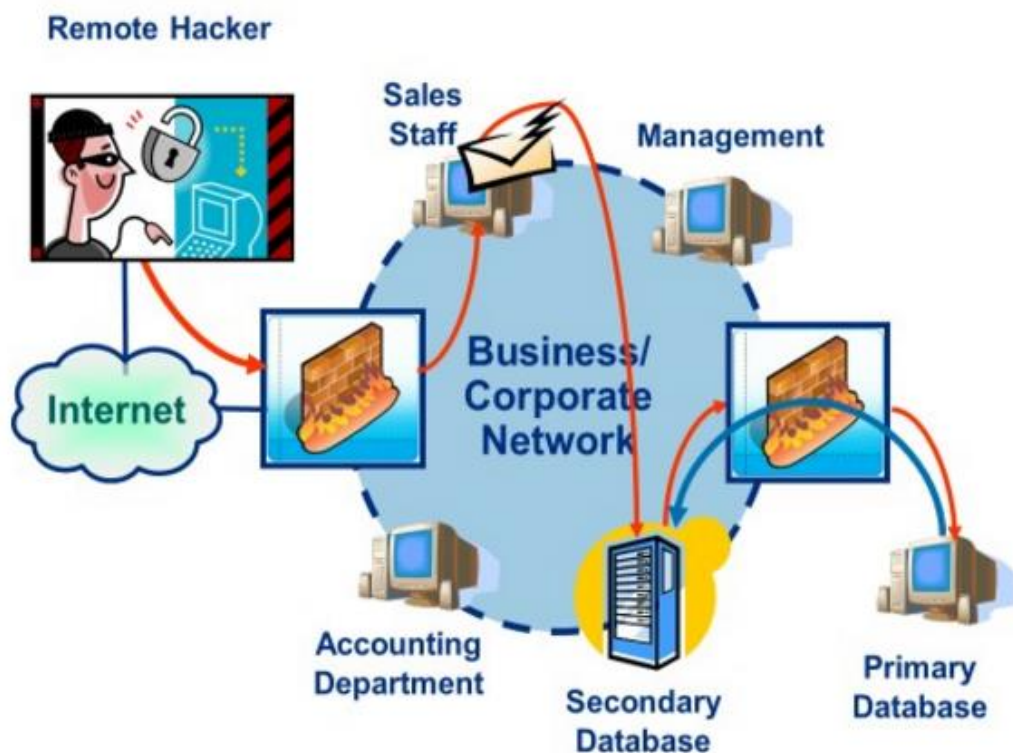
No.	Time	Source	Destination	Protocol	Length	Info
1192608	222.088832865	00:14:1c:0e:43:c0	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192609	222.088963807	00:1e:7a:37:c8:e5	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192610	222.089031190	00:14:1c:0e:43:c0	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192611	222.089161945	00:1e:7a:37:c8:e5	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192612	222.089229433	00:14:1c:0e:43:c0	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192613	222.089360403	00:1e:7a:37:c8:e5	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192614	222.089428023	00:14:1c:0e:43:c0	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192615	222.089558960	00:1e:7a:37:c8:e5	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192616	222.089626328	00:14:1c:0e:43:c0	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...
1192617	222.089757333	00:1e:7a:37:c8:e5	f0:1e:34:12:0f:4d	ARP	42	Gratuitous ARP for 0...

Frame 1192608: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

- Ethernet II, Src: 00:14:1c:0e:43:c0, Dst: f0:1e:34:12:0f:4d
 - Destination: f0:1e:34:12:0f:4d
 - Source: 00:14:1c:0e:43:c0
 - Type: ARP (0x0806)
- Address Resolution Protocol (request/gratuitous ARP)

מתודולגיית התקיפה – השתלטות על בסיס הנתונים

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

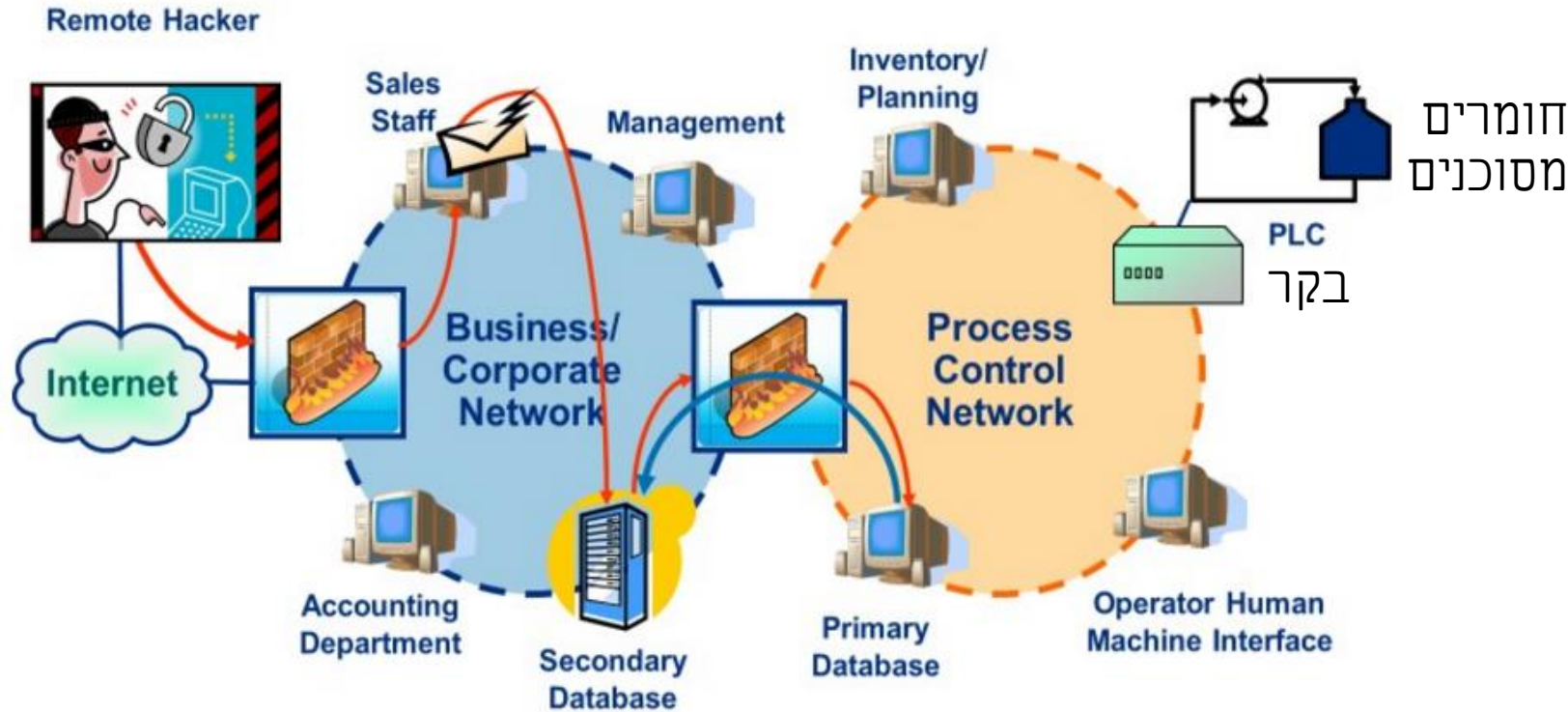


SQL = TCP 1433

ORACLE = TCP 1521

מתודולגית התקיפה – השתלטות על רשת ICS

התוקף משלים את ההשתלטות
משיג שליטה ברשת ה-ICS



MODBUS= TCP 502

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).



התוצאה: פגיעה בבריאות הציבור ואיכות הסביבה

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.

Example

SHODAN, which was put in service toward the end of 2009, is a search engine that catalogs all Internet facing devices including control systems. It is a great tool for performing reconnaissance, and as such, it has been called the "Google for hackers." It provides information that an attacker would find useful, including ports, hostname, country, server operating system, server version, and more. SHODAN stands for Sentient Hyper-Optimized Data Access Network.

On February 2011, a researcher was able to identify and easily access an ICS using information gleaned from SHODAN. There was minimum impact on business functionality because the researcher only "looked around." He reported the vulnerability, and ICS-CERT worked with the asset owner to secure the system.

Information from SHODAN was recognized by ICS-CERT as a potential vulnerability well before this incident. On October 28, 2010, ICS-CERT issued an alert, [ICS Alert 10 301-01, "Control System Internet Accessibility."](#)

Summary of Recommendations:

- Placing all control systems assets behind firewalls, separated from the business network.
- Deploying secure remote access methods such as Virtual Private Networks (VPNs) for remote access.
- Removing, disabling, or renaming any default system accounts (where possible).
- Implementing account lockout policies to reduce the risk from brute forcing attempts.
- Implementing policies requiring the use of strong passwords.
- Monitoring the creation of administrator level accounts by third-party vendors.



<https://www.shodan.io/>

Explore

Discover the Internet using search queries shared by

Featured Categories



Top Voted

8,998

Webcam
best ip cam search I have found yet.

webcam surveillance cams

2010-03-15

3,476

Cams
admin admin

cam webcam

2012-02-06

1,989

Netcam
Netcam

netcam

2012-01-13

1,173

default password
Finds results with "default password" in the ba...

router default password

2010-01-14

1,015

dreambox

Secure | <https://www.shodan.io/explore/category/industrial-control-systems>



Industrial Control Systems

Spotlight



XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore



PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

Explore

What Are They?

In a nutshell, industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit

Protocols

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

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 don't always require authentication - it isn't part of the protocol!



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](#)



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](#)



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 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](#)



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](#)



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](#)

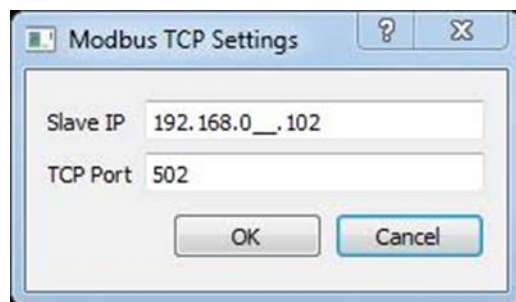


PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)

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 תומך בתווק-RS232 (כבלים סריאלים), לאחר מכן ב-RS485 תוך שימוש בפרוטוקול TCP/IP כברירת מחדל עובד על TCP PORT 502



החסרונות הגדולים של הפרוטוקול:

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

modbus

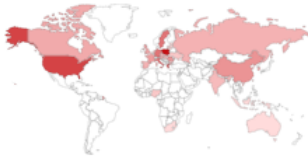
Shodan Developers Monitor View All...

SHODAN modbus [Search] Explore Pricing Enterprise Access

Exploits Maps Images

TOTAL RESULTS
337

TOP COUNTRIES



Poland	116
United States	50
Greece	30
Sweden	19
Italy	19

TOP SERVICES

FTP	158
Telnet (Lantronix)	30
1883	29
8081	18
BACnet	7

TOP ORGANIZATIONS

Netia SA	106
Cosmote Mobile Telecommunications S.A.	21
Verizon Wireless	8
Telia	8
Vodafone Kabel Deutschland	5

TOP PRODUCTS

Mosquitto	31
Apache httpd	8
WindWeb	4
InfluxDB	4
Elastic	3

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

82.143.147.168
h82-143-147-168-static.e-wro.net.pl
Netia SA
Added on 2020-07-12 05:19:58 GMT
Poland, Wroclaw

220 Modbus-GPRS-Gateway FTP Server Ready
530 Not logged in.
502 Command not implemented
211-Features:
SIZE
211 End

46.233.128.2
Iren Energia S.p.a
Added on 2020-07-12 08:11:28 GMT
Italy, Turin

MODEM AES 44.00

Press Command Number

- 1) Lancia il Polling su I2C
- 2) Lancia il Polling su MBUS
- 3) Lancia il Polling su **MODBUS**
- 4) Valore lettura regolatore Siemens
- 5) Download applicazione
- 6) Download applicazione di test
- 7) ...
- 8) AUTOISCOVERY...

166.254.93.217
217_sub-168-254-93.myvzw.com
Verizon Wireless
Added on 2020-07-12 10:48:37 GMT
United States

Modbus/TCP to RTU Bridge
MAC address 0080A3CB2866

Software version V3.3.25.0RC5 (140113)

Press Enter for Setup Mode

78.141.134.213
ip-78-141-134-213.dyn.luxdsl.pt.lu
POST Luxembourg
Added on 2020-07-12 11:42:38 GMT
Luxembourg

0<\x02\x01\x00\x04\x06public\wa2/\x02\x04f\bx1j*\x02\x01\x00\x02\x01

shodan.io/search?query=admin+%2B+1234

SHODAN admin + 1234

Exploits Maps

TOTAL RESULTS
2,196

TOP COUNTRIES

Ukraine	296
Taiwan	284
Poland	252
Russian Federation	206
United States	118

TOP SERVICES

HTTP	916
HTTP (8080)	738
Kerberos	153
Qoon	84
MongoDB	82

TOP ORGANIZATIONS

HiNet	243
Spoldzielnia Mieszkaniowa Polnoc	157
Digi Romania	31
ER-Telecom	28
Amazon.com	21

TOP OPERATING SYSTEMS

Linux 2.4.x	11
Linux 2.6.x	8

TOP PRODUCTS

GoAhead-Webs httpd	1,854
MongoDB	87

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

178.165.8.190
178-165-8-190-kh.maxnet.ua
Maxnet Telecom
Added on 2020-07-12 11:36:17 GMT
Ukraine, Kharkiv

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Tue Jan 4 21:33:24 2011
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

220.142.186.203
220-142-186-203.dynamic-ip.hinet.net
HiNet
Added on 2020-07-12 11:40:41 GMT
Taiwan, Kaohsiung City

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Thu Jul 7 04:41:07 2011
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

195.196.231.140
InformationsTeknik i Norrbotten AB
Added on 2020-07-12 10:50:14 GMT
Sweden, Puoltikasvaara

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Sun Jul 12 11:50:20 2020
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html

86.110.38.18
86-110-38-18.levikom.ee
Levikom Eesti OU
Added on 2020-07-12 10:57:22 GMT
Estonia, Kehtna

HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Wed Jul 4 17:57:32 2012
WWW-Authenticate: Basic realm="Default: admin/1234"

מצלמות פתוחות עם משתמש וסיסמא ידועים

webcam surveillance cams 2010-03-15

3,476

Cams
admin admin

cam webcam 2012-02-06

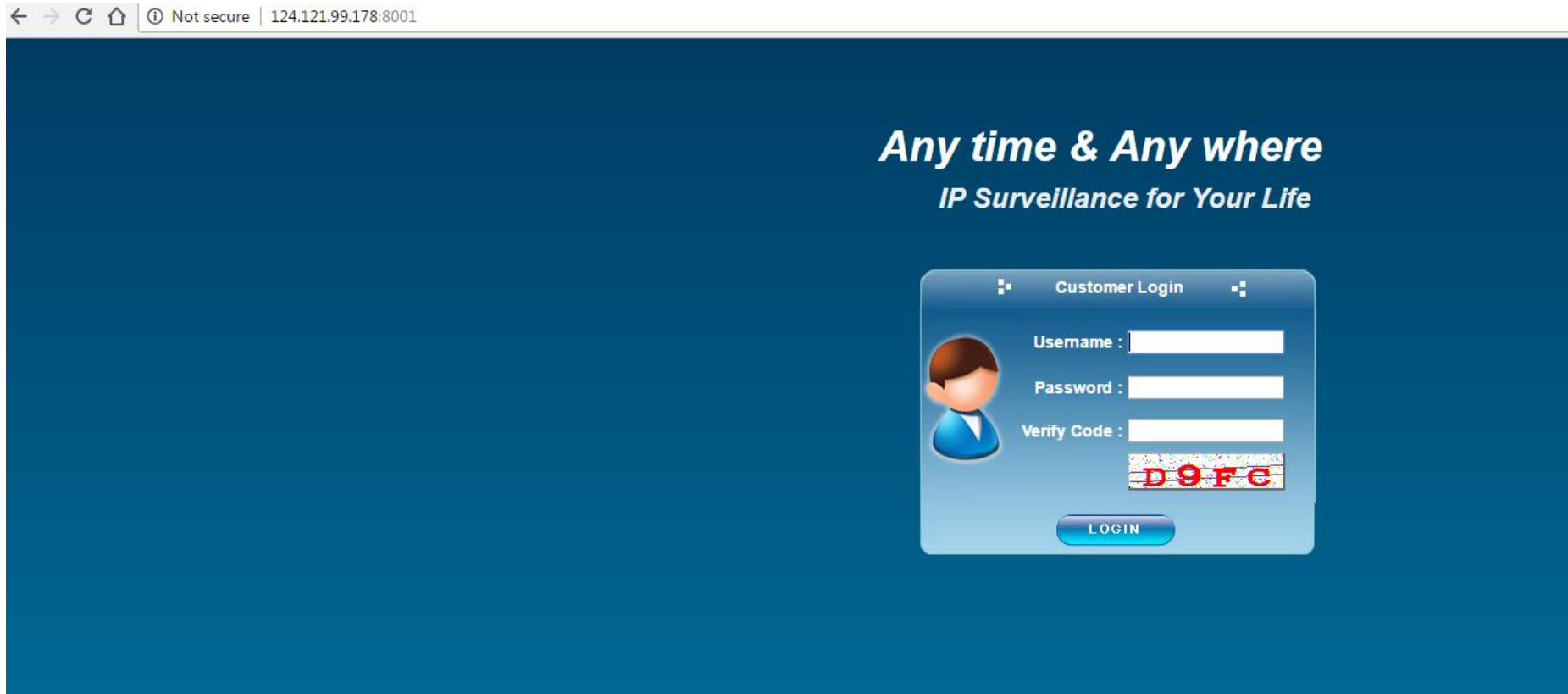
1,989

Netcam

1

2

מצלמה פתוחה לעולם



תוכנה שיוזעת 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	BROWSE	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

