# CYBER DEFENSE

## ❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering


www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH


**By. Hossein Malekzadeh**

**Cyber Security Consultant and Manager**

**www.Hosseinmalekzadeh.com**

**Mobile : 09153133217**

# نقشه شبکه سازمان (دفتر مرکزی)

## سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

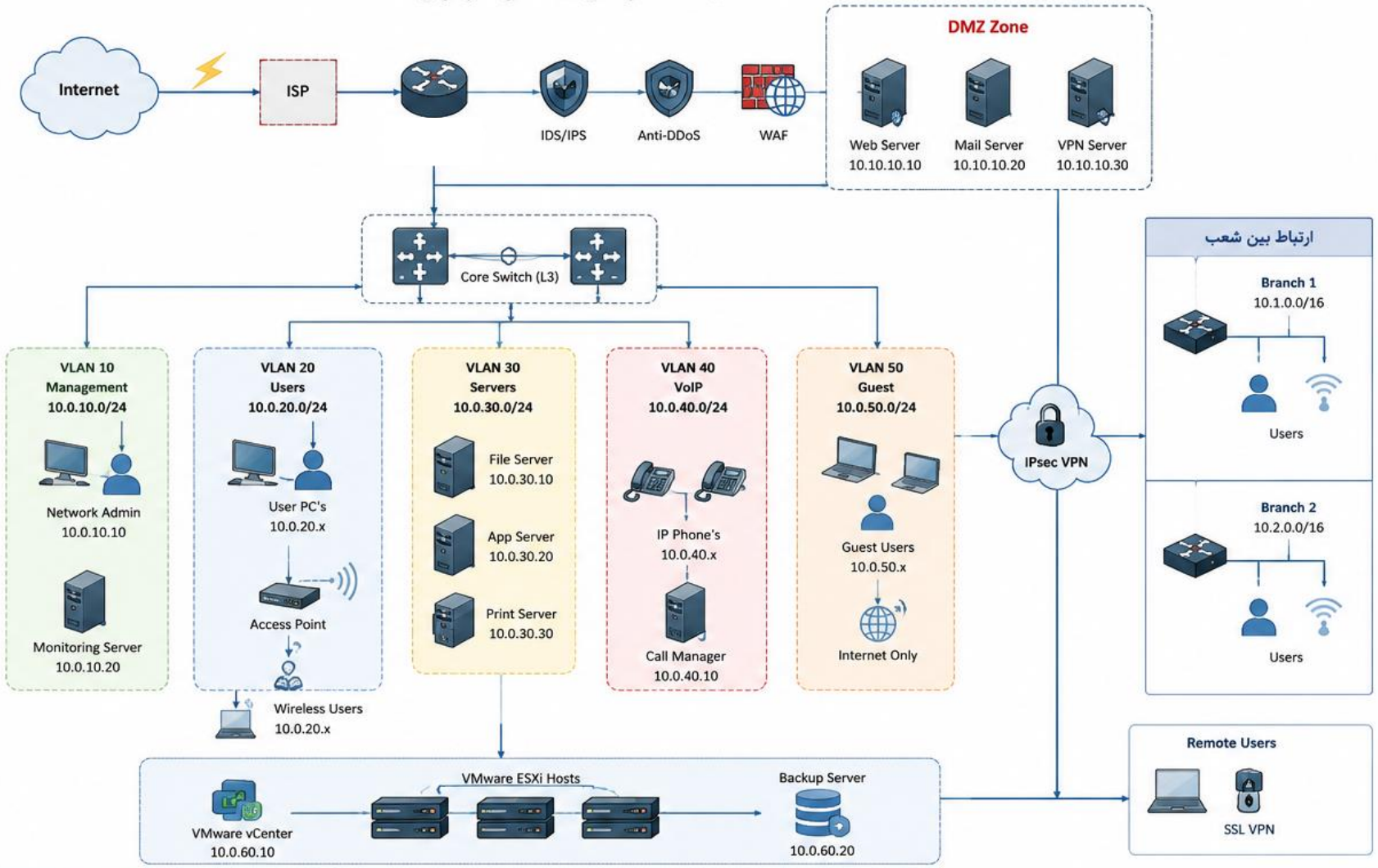
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

## اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

## چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها




### راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

### نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

### جدول آدرس دهی

| VLAN | Network | Gateway | Description |
|---|---|---|---|
| 10 | 10.0.10.0/24 | 10.0.10.1 | Management |
| 20 | 10.0.20.0/24 | 10.0.20.1 | Users |
| 30 | 10.0.30.0/24 | 10.0.30.1 | Servers |
| 40 | 10.0.40.0/24 | 10.0.40.1 | VoIP |
| 50 | 10.0.50.0/24 | 10.0.50.1 | Guest |
| 60 | 10.0.60.0/24 | 10.0.60.1 | Virtualization/Backup |
| DMZ | 10.10.10.0/24 | 10.10.10.1 | DMZ Zone |

# Project-Based Cyber Defense Lifecycle

- **Hardening** یکی از حیاتی‌ترین کارهایی است که باید در زیرساخت شبکه سازمانی انجام شود. به زبان ساده، امن سازی یعنی کم کردن سطح حمله و کاهش نقاط ضعف تا حد ممکن.
- **دلیل اینکه سازمان‌ها باید حتماً این کار را انجام دهند، چند محور اصلی دارد:**

- **کاهش سطح حمله (Attack Surface Reduction)**
- هر **سیستمی که سرویس اضافه دارد**، پورت باز دارد، نرم‌افزار قدیمی دارد یا تنظیمات پیش‌فرض را نگه داشته، یک درِ باز برای مهاجم است. **امن سازی** این درهای اضافه را می‌بندد.

- **جلوگیری از نفوذ و کاهش ریسک**
- بیشتر حملات موفق نه به خاطر پیچیدگی، بلکه به‌خاطر سهل‌انگاری در تنظیمات یا سرویس‌های غیرضروری اتفاق می‌افتد. **Hardening** جلوی این ریسک‌ها را می‌گیرد.

- **حفاظت از داده‌های سازمان**
- شبکه سازمانی قلب اطلاعات است. با سخت‌سازی، احتمال دسترسی غیرمجاز، نشت اطلاعات و تخریب داده‌ها به شدت کاهش می‌یابد.

- **افزایش پایداری و عملکرد سیستم‌ها**
- وقتی سرویس‌های اضافی حذف و منابع آزاد می‌شوند، سیستم‌ها هم پایدارتر کار می‌کنند و هم سریع‌تر می‌شوند.

- **کاهش آثار حمله در صورت نفوذ (Damage Control)**
- حتی اگر مهاجم وارد شود، با تنظیمات سخت‌سازی شده، دسترسی محدودی دارد و نمی‌تواند آزادانه در شبکه حرکت (Lateral Movement) انجام دهد.

- **انطباق با استانداردهای امنیتی و الزامات قانونی**
- استانداردهایی مثل ISO 27001 ، NIST، CIS Benchmark و GDPR همگی الزام یا توصیه شدید به Hardening دارند. بدون آن، سازمان از نظر بازرسی یا ممیزی مردود می‌شود.

- **کاهش هزینه‌های بلندمدت**
- هزینه Hardening بسیار کمتر از هزینه یک نفوذ، حمله باج‌افزاری، یا از دست رفتن داده‌هاست

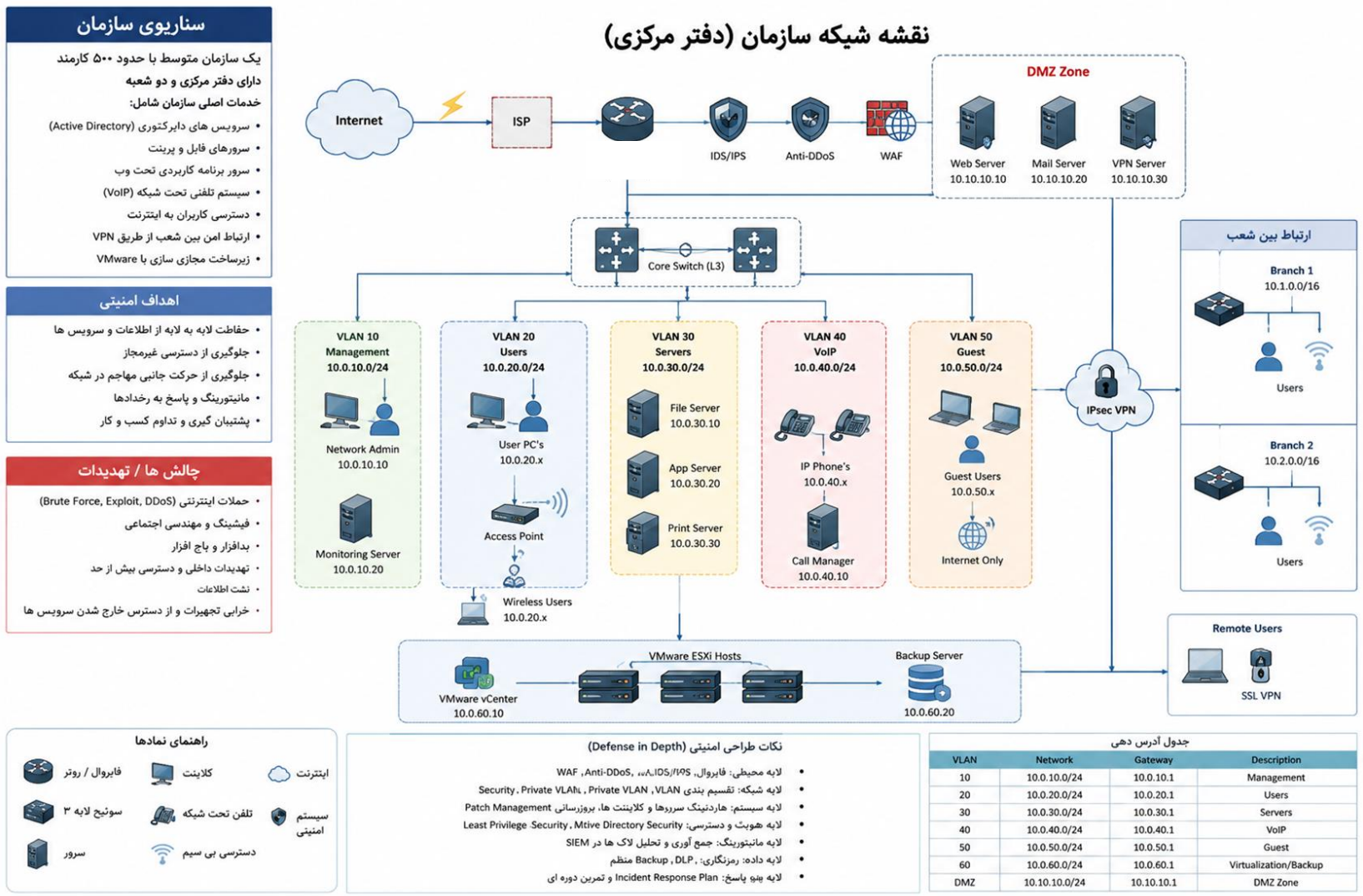
- **دفاع چندلایه (Defense in Depth)**
- حتی بهترین فایروال یا IDS کافی نیست. اگر سیستم‌های داخلی امن نباشند، مهاجم با یک مدخل کوچک می‌تواند به همه جا دسترسی بگیرد.

# هدف اصلی در پروژه های Cyber Defense

- **کارشناس فنی باید بتواند:**
- دارایی‌های مهم سازمان را شناسایی کند
- مسیرهای حمله را درک کند
- تهدیدات واقعی را تحلیل کند
- ریسک‌ها را اولویت‌بندی کند
- برای هر تهدید دفاع مناسب طراحی کند

# سناریوی واقعی سازمانی دوره

- **اجزای اصلی:**
- Active Directory
- File Server
- VMware
- VoIP
- Cisco Router Edge
- Cisco Core
- VPN
- شعب
- کاربران داخلی
- DMZ
- WiFi



# شناسایی دارایی‌ها مهم در این پروژه (Assets)

- اول باید بدانیم چه چیزی ارزش محافظت دارد.

- «شما تازه وارد تیم امنیت یک سازمان
- شده‌اید و هیچ مستندی وجود ندارد.»

- **وظیفه:**
- کشف تجهیزات
- شناسایی سرویس‌ها
- تشخیص سیستم‌های حیاتی
- ساخت Asset Inventory

| Asset | اهمیت |
| --- | --- |
| Active Directory | بسیار حیاتی |
| Backup Server | حیاتی |
| File Server | حیاتی |
| ERP/Application | حیاتی |
| VoIP | متوسط |
| User PCs | متوسط |
| WiFi | پرریسک |
| VPN | بسیار حساس |

- جدول Asset Inventory بسازید

| Criticality | Role | IP | Device |
|---|---|---|---|
| Critical | Domain Controller | 10.0.30.5 | DC01 |
| High | File Server | 10.0.30.10 | FS01 |
| Medium | VoIP | 10.0.40.10 | PBX01 |

- نکته مهم :
- «هکرها همیشه مستقیم سراغ **Domain Admin** می‌روند.»

# ابزارهای حرفه‌ای پیشنهادی

- **Excel / Google Sheets**
- بهترین گزینه برای شروع کار است.
- چرا؟
- ساده
- قابل فهم
- مناسب مفاهیم اولیه

**ساختار پیشنهادی فایل**

**Sheet 1 — Servers**
**Sheet 2 — Network Devices**
**Sheet 3 — Users**
**Sheet 4 — Wireless**
**Sheet 5 — Risk Matrix**

# اسکن پورت‌ها و سرویس‌ها

- شناسایی همه پورت‌های باز روی یک IP خاص
- nmap -p- 192.168.1.10
- شناسایی سرویس‌های اجرا شده روی پورت‌ها
- nmap -sV 192.168.1.10
- اسکن کل شبکه برای یافتن هاست‌های فعال
- nmap -sn 192.168.1.0/24
- اسکن همه پورت‌ها TCP و UDP
- nmap -sS -sU -p- 192.168.1.10
- تشخیص سیستم عامل
- nmap -O 10.0.30.10

- این دستور یک **ARP broadcast** در شبکه می‌فرستد و تمام دستگاه‌هایی که در همان subnetهستند را پیدا می‌کند.
- **به عبارتی:**
  - تمام IPهای فعال شبکه
  - MAC Address دستگاه‌ها
  - Vendor کارت شبکه
  - را نمایش می‌دهد.
- **sudo** arp-scan –l
- اگر arp-scan نصب نباشد
- **sudo** apt install arp-scan

- 192.168.1.1 00:50:56:c0:00:01 **VMware**, Inc.
- 192.168.1.10 00:15:5d:3a:21:10 **Microsoft** Corp
- 192.168.1.20 00:0c:29:11:22:33 **VMware**
- 192.168.1.30 00:50:56:ab:cd:ef **Dell**

- از روی این خروجی می‌توانیم حدس بزنیم :
- کدام سیستم **Domain Controller** است
- کدام **Server**
- کدام **Workstation**

- اما هنوز نمی‌دانیم :
- چه سرویس‌هایی باز هستند؟
- کدام سیستم Domain Controller است؟
- کدام File Server است؟
- چه نسخه‌ای از سیستم‌عامل اجرا می‌شود؟

- **در این مرحله می توانیم لیست IPهای مهم را جدا کنیم**
- اسکن سرویس انجام می‌دهیم :

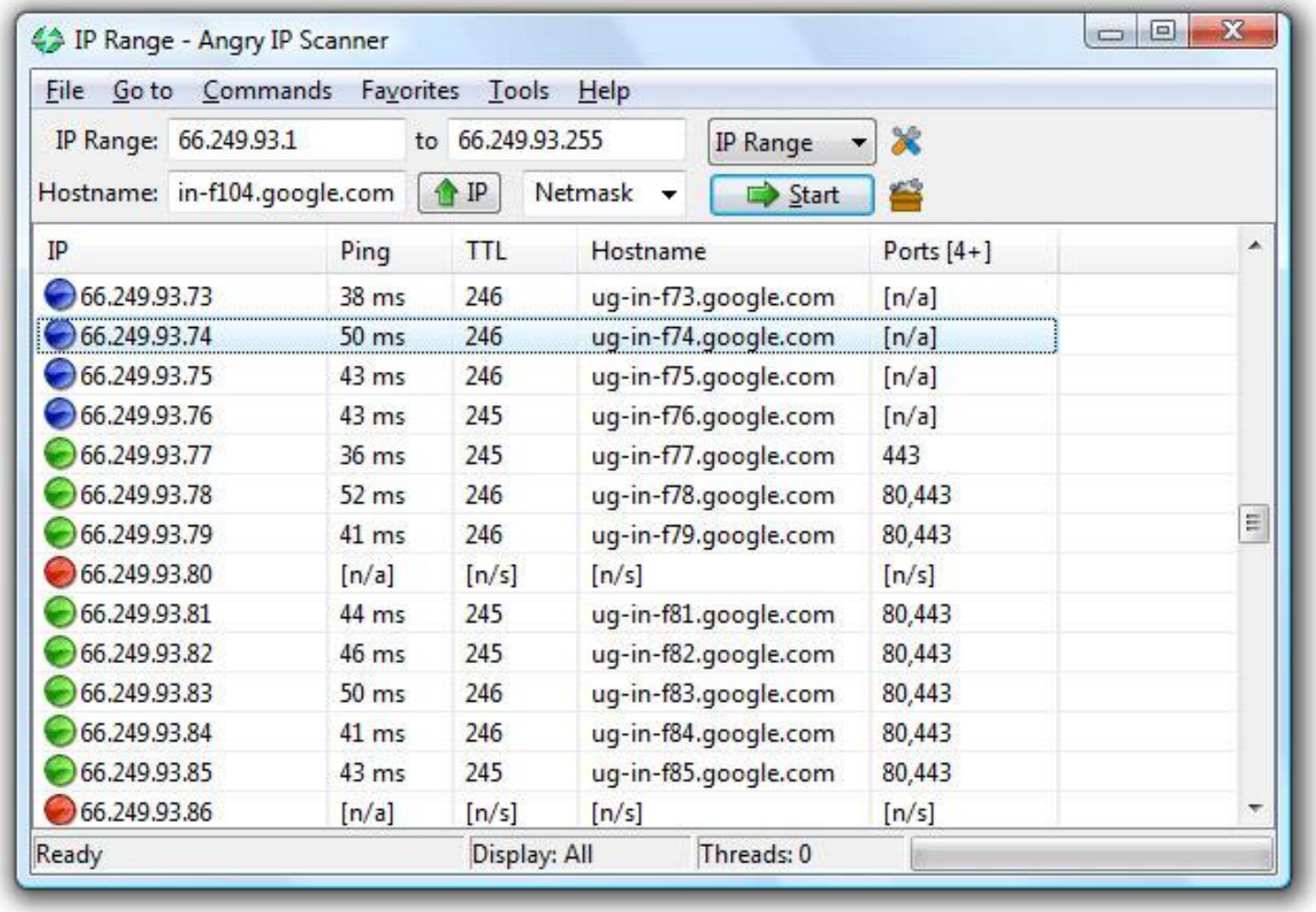
- **nmap -sS -sV -T2 192.168.1.10**

**توضیح:**

- **-sS** → TCP SYN Scan (نسبتاً مخفی‌تر)
- **-sV** → تشخیص نسخه سرویس
- **-T2** → سرعت پایین‌تر برای stealth

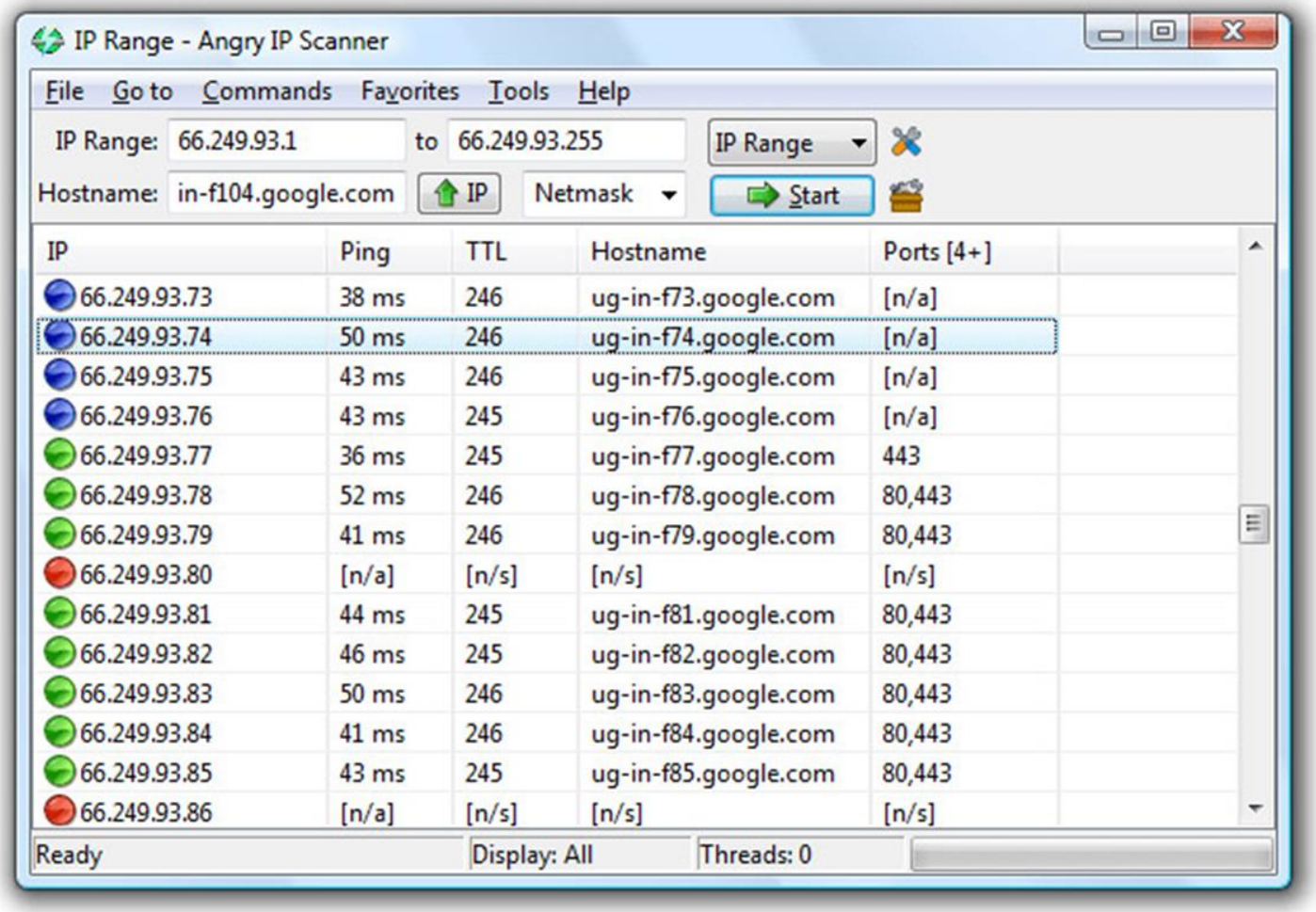
# Angry IP Scanner

- https://www.yasdl.com/232895/%d8%af%d8%a7%d9%86%d9%84%d9%88%d8%af-angry-ip-scanner.html



1.نرم‌افزار را باز کن.
2.محدوده‌ی IP شبکه‌ات را وارد کن (مثلاً ۱۹۲.۱۶۸.۱.۰ – ۱۹۲.۱۶۸.۱.۲۵۵).
3.در تنظیمات (Menu → Preferences → Ports) محدوده‌ی پورت‌هایی که باید بررسی شوند را تعیین کن (مثلاً ۱–۶۵۵۳۵).
4.دکمه‌ی **Start** را بزن.

- بعد از پایان اسکن، ستون‌های مربوط به **پورت‌های باز (Open Ports)** را ببین.
- می‌توانی خروجی را به CSV یا TXT صادر کنی.



# Netdiscover

- **ابزار سبک برای پیدا کردن دستگاه‌های فعال در شبکه (ولی نه پورت‌ها)**
- Netdiscover خودش فقط **هاست‌های زنده (Active Hosts)** را شناسایی می‌کند، نه پورت‌ها
- netdiscover -r 192.168.1.0/24
- سپس آدرس‌های IP شناسایی‌شده را با Nmap اسکن کن:
- nmap -p- -sV -iL live_hosts.txt

- **هر سرویس فعال = یک ریسک امنیتی**

- **در این مرحله از پروژه دنبال چه مواردی بودیم ؟**
- چه تجهیزاتی در شبکه هستند
- چه Portهایی باز است
- چه سرویس‌هایی اجرا می‌شوند
- چه سیستم‌هایی پرریسک هستند

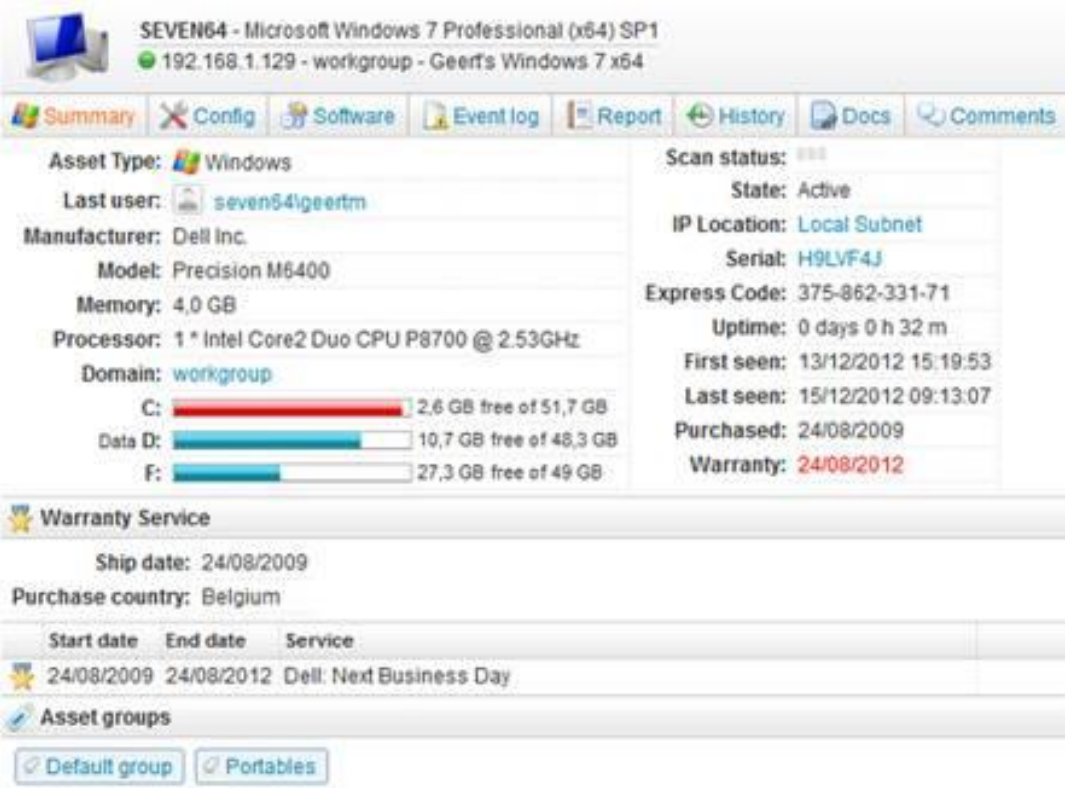
# Lansweeper

https://www.digiboy.ir/12759/lansweeper-12-5-0-7/

- Asset Managementواقعی سازمانی
- چه چیزی پیدا می‌کند؟

- Windows
- Linux
- Switch
- VMware
- Printer
- Software
- Patch Status

Lansweeper
NETWORK MANAGEMENT



Main page - Lansweepe

localhost:81/Default.aspx

Lansweeper

Built-in admin

Dashboard | Assets | Reports | Software | Scanning | Helpdesk | Knowledgebase | Calendar | Deployment | Configuration | Enterprise | Community

v. 8.0.130.10

Main page | Servers | Software | Hardware | Active Directory | General | Helpdesk | Add Widgets | Add New Tab

## My Teams

| | |
|---|---|
| Open | 3 |
| In Progress | 1 |
| Awaiting Reply | 2 |
| Pending 3rd party | 1 |
| Waiting for approval | 1 |
| Confirm resolution | 1 |

## Windows Domain Overview

| Domain | | |
|---|---|---|
| Workgroup | 0 | 1 |
| Total | 0 | 1 |

## IP Locations Overview

| | |
|---|---|
| Undefined | 1 |

## Asset Group Overview

| Static | |
|---|---|
| Default group | 1 |
| **Dynamic** | |
| .NET Framework 4 Missing | 0 |
| 64-bit Windows | 0 |
| All Except Routers & Switches | 2 |
| Firefox Installed | 0 |
| Laptops | 0 |
| Manufacturer Dell | 0 |
| Non-Active | 0 |
| Printers | 0 |
| Windows 7 | 0 |

config

## Chart: Asset type summary

## News

Welcome to Lansweeper

You just powered up your network!

The contents of this news widget are visible to all Lansweeper users and fully customizable.

config

## Alert Report: Dashboard

***High priority***

- Error: WMI access denied (0)
- OS: End of lifetime (no longer supported) (0)
- Disk: Servers less than 1 GB free HD (0)
- Disk: Workstations less than 1 GB free HD (0)
- Workstation: All workstations without anti-virus software (0)
- Server: All servers without anti-virus software (0)
- Device: Printer out of toner (0)

***Important***

- Asset: Hard drive S.M.A.R.T. status not OK (0)
- Error: RPC server unavailable (0)
- Computer: Not seen in the last 30 days (0)
- Asset: Out of warranty (0)
- Asset: Out of warranty in 60 days (0)
- Device: Printer almost out of toner (0)
- Workstation: Antivirus disabled (0)
- Workstation: Antivirus expired (0)

***Informational***

- OS: Not latest Service Pack Vista (0)
- OS: Not latest Service Pack Win2008 (0)
- OS: Not latest Service Pack Win2008 R2 (0)
- OS: Not latest Service Pack Windows 7 (0)
- OS: Not latest Service Pack Windows 8 (0)
- OS: Not latest Service Pack Win2012 (0)
- OS: Not latest Service Pack Windows 8.1 (0)
- OS: Not latest Service Pack Windows 2012 R2 (0)
- OS: Not latest Build of Windows 10 (0)
- OS: Not latest Build of Windows 2016 (0)
- OS: Not latest Build of Windows 2019 (0)

config

## Chart: Asset manufacturer

## Scanning Status

| Server | | |
|---|---|---|
| desktop-tuurnm6 | 1 (0) | 14 (86) |

Database size:

10214 MB free of 10240 MB

## Calendar events

**Test Lansweeper**
18/03/2020 15:20:00
Due in 4 minutes
5 minutes before start | Snooze | Dismiss

## Team follow ups (1)

**#20: [DEMO] New database backup server**
15 days

## Last Seen Assets

| | |
|---|---|
| Default location | 18/03/2020 15:11:58 |
| DESKTOP-TUURNM6 | 18/03/2020 15:10:49 |

## Last Seen Users

## Lansweeper news

- Emergency Patch Released for SMBv3 Vulnerability 2020-03-13T13:18:35
- Microsoft Patch Tuesday Audit – March 2020 2020-03-11T12:06:01
- Are You Prepared for Office 2010 End of Support? 2020-03-03T09:00:00
- Critical Chrome Zero-Day Vulnerability Under Active Attac 2020-02-25T14:48:03
- Top 10 Vulnerability Audit Reports of 2019 2020-02-20T12:38:22
- Why You Should Dump Your IT Inventory Spreadsheets

Lansweeper network inventory

Trial version [redacted]. Contact us for a trial extension. Default user

Dashboard | Assets | Reports | Licenses | Deployment | Configuration | Community | v. 6242

**Asset options**

- New asset
- Edit asset
- Rescan Asset
- Wake on Lan
- Refresh Warranty
- QR Code
- Deploy Package

**Basic actions**

- Ping
- Pathping
- Traceroute
- NBTstat
- HTTP
- HTTPS
- SSH (putty)
- Remote desktop
- Open C$
- Open Admin$
- Computer management
- Services management
- Event viewer
- Shared folders
- Reboot
- Shutdown
- Abort shutdown

**Advanced actions**

- Device tester

**CHI-DC01** GLOBOMANTICS.local - Microsoft Windows Server 2008 R2 Enterprise (x64) SP1

172.16.30.200 - globomantics

Summary | Config | Software | Event log | Report | History | Deployments | Docs | Comments | Scan

| | | | |
|---|---|---|---|
| Asset Type: | Windows | Scan status: | |
| Last user: | Jeff Hicks | Scan server: | chi-win81 |
| OS: | Microsoft Windows Server 2008 R2 Enterprise (x64) SP1 | State: | Active |
| Manufacturer: | Microsoft Corporation | IP Location: | Local Subnet |
| Model: | Virtual Machine | Asset location: | Undefined |
| Memory: | 1.0 GB | Serial: | 8489-9638-6902-1028-1552-2278-75 |
| Processor: | 1 * Intel Core i7-4500U CPU @ 1.80GHz | Uptime: | 22 days 4 h 23 m |
| Domain: | globomantics | First seen: | 24/03/2015 13:50:20 |
| OU: | OU=Domain Controllers, DC=GLOBOMANTICS, DC=local | Last seen: | 24/03/2015 14:03:09 |
| C: | 0.9 GB free of 14.9 GB | Purchased: | unknown |
| | | Warranty: | unknown |

**Asset groups**

Default group

**Anti-Virus**

| Name | Status | Virus Signature |
|---|---|---|

No antivirus installed

**Recent eventlog entries**

No event log information scanned

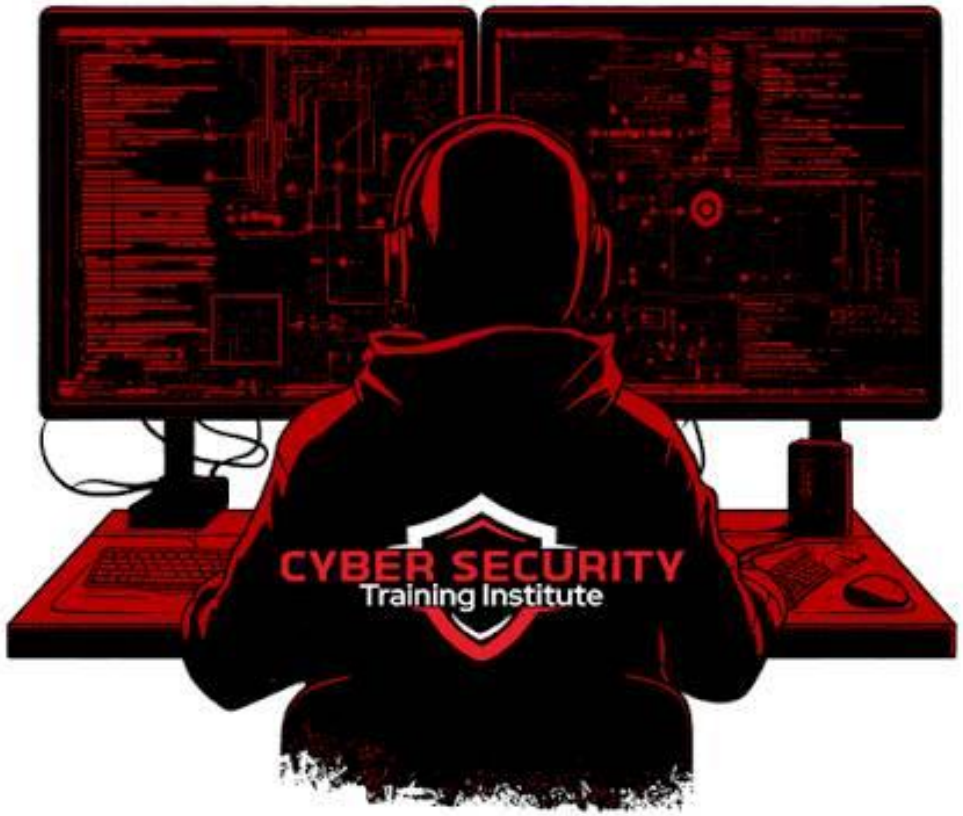
**Event summary of last week**

No event log information scanned

**Uptime calendar**

2:00 4:00 6:00 8:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 Asset on

# تحلیل تجهیزات ناشناس




- **برسی موارد زیر در پروژه :**

- **MAC Vendor** را تشخیص می‌دهد
- **Broadcast** ها را تحلیل می‌کند
- **Rogue Device** را پیدا می‌کند

- **بهترین برنامه برای بررسی امن بودن اتصال شبکه و اینترنت چیست؟**
- **فینگ Fing**

- **احتمالاً شما هم ناخودآگاه** به این موضوع فکر کرده‌اید که آیا اتصال اینترنت من امن است یا نه؟
- **آیا شخص دیگری** به شبکه و دستگاه ADSLمن متصل شده است؟
- **و همیشه دنبال راهکاری باشید** که امنیت شبکه و اینترنت خود را بررسی کنید، تا با انجام اقدامات لازم، نگرانی شما رفع شود.

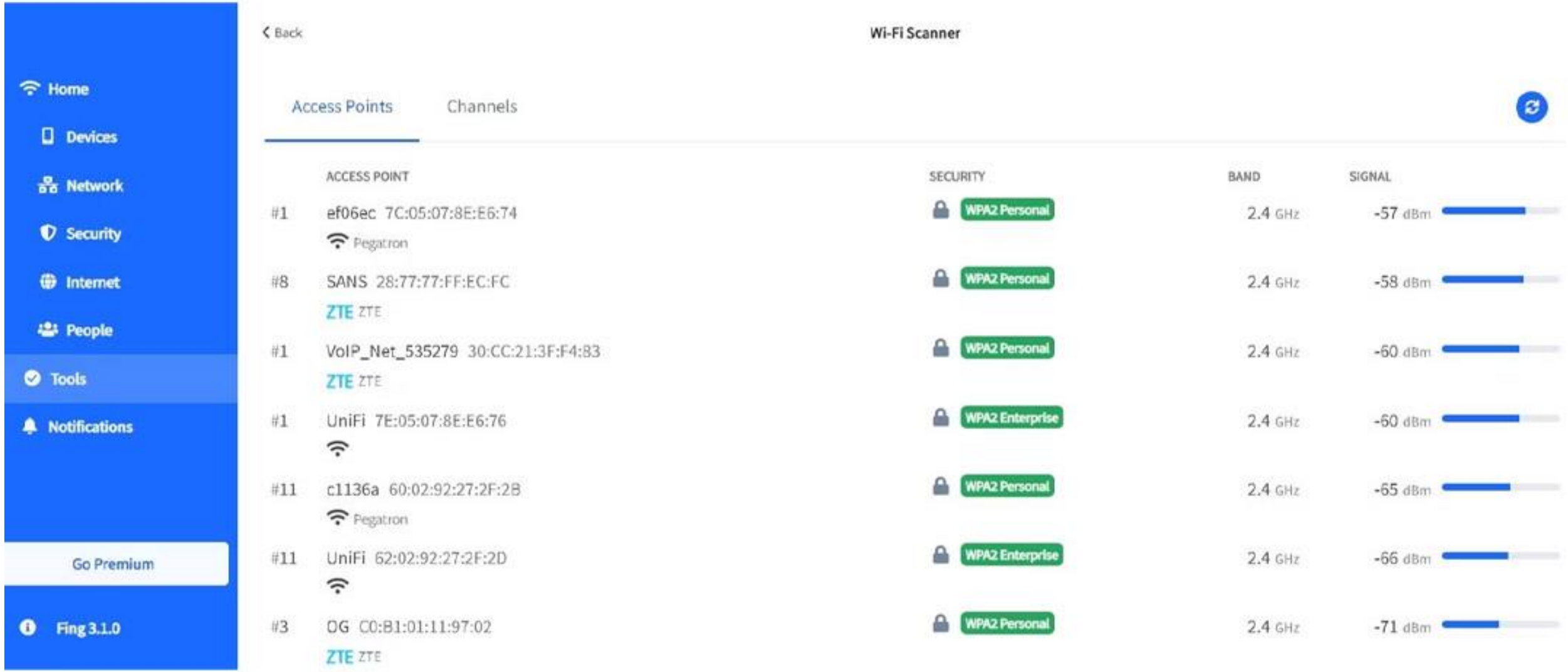
- **مهم نیست** که چقدر اقدامات احتیاطی انجام می‌دهید، اگر شبکه‌ای که به آن متصل هستید به درستی ایمن نباشد، در معرض خطر و آسیب پذیری در برابر حملات سایبری هستید. اما چگونه می‌توانید بررسی کنید که یک شبکه ایمن است؟

- **یکی از بهترین روش‌های بررسی امنیت اتصال اینترنت شما، استفاده از اپلیکیشنی به نام فینگ Fing می‌باشد**

- **Fing** که در **Android, iOS, Windows**و **macOS** سیستم‌های مبتنی بر ویندوز، سیستم‌های مبتنی اندروید و تمام دستگاه‌های اپل مانند مک بوک پرو، مک مینی، آیفون و...) موجود است
- **ابزاری نسبتا سبک اما قدرتمند است** که قادر به انجام تجزیه و تحلیل شبکه کامل است. یک نسخه رایگان از برنامه و یک نسخه پریمیوم با ویژگی‌های اضافی وجود دارد.

- **برای شروع، می‌توانید بررسی کنید** که کدام دستگاه‌ها به شبکه شما متصل هستند، که قطعاً تشخیص افراد مزاحم را بسیار آسان‌تر می‌کند.
- اما مهمتر از آن، می‌توانید امنیت شبکه خود را آزمایش کنید. این شامل آزمایش خود نقطه دسترسی، اسکن پورت‌ها، مشاهده دستگاه‌های تایید نشده و غیره است.

- **بعد از اینکه برنامه فینگ را نصب کردید**، آن را اجرا کنید تا به طور خودکار، تمام دستگاه‌های متصل به شبکه شما را شناسایی کند.
- **این شناسایی شامل**: نام **دستگاه‌ها** و **آی پی** آن‌ها و همچنین **آیکون** مرتبط (مانند: لپ تاپ، گوشی، دوربین و...) خواهد بود.




**علاوه بر این، با استفاده از Fing**، می‌توانید آزمایش‌های پینگ انجام دهید، نقاط دسترسی بی‌سیم اطراف را اسکن کنید، دستگاه را فقط بر اساس آدرس MAC آن بررسی کنید، جستجوی DNS انجام دهید، سرعت اینترنت خود را آزمایش کنید، ارائه‌دهنده خدمات اینترنت (ISP )خود را با سایر ارائه‌دهندگان در منطقه خود مقایسه کنید، و قطع یا اختلال را شناسایی کنید.

- نمایش تمام دستگاه های متصل به شبکه، عدم محدودیت در نمایش تعداد دستگاه ها و شبکه ها
- نمایش MAC Addressو کارخانه تولید کننده دستگاه
- امکان جستجو بر اساس IP، Mac، نام، توزیع کننده و یادداشتها
- امکان به اشتراک گذاری از طریق ایمیل و شبکه های اجتماعی
- قابلیت اسکن سرویس و یافتن پورت های باز در عرض چند ثانیه
- قابلیت :Wake On LANروشن نمودن کامپیوتر متصل به شبکه از طریق گوشی یا تبلت اندرویدی
- بررسی عملکرد شبکه از طریق Pingو Traceroute
- امکان چک کردن وضعیت دسترسی به شبکه
- ردیابی دستگاهها هنگام ورود و خروج از شبکه
- اجرای برنامه ها برای پورتهای خاص مثل مرورگر، SSHو FTP
- نمایش نامهای NetBIOSو مشخصات آنها
- امکان شناسایی از طریق آدرس IPبرای شبکه های Bridge

# Active Directory Discovery

- برای شناسایی دارایی‌های Domain

- PowerShell
- Get-ADComputer -Filter *

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADComputer -Filter *


DistinguishedName : CN=SERVER1,OU=Domain Controllers,DC=test,DC=local
DNSHostName       : server1.test.local
Enabled           : True
Name              : SERVER1
ObjectClass       : computer
ObjectGUID        : bc297ccc-1976-4dde-a441-abcaabc79187
SamAccountName    : SERVER1$
SID               : S-1-5-21-2328314914-3034131014-599688784-1001
UserPrincipalName :

DistinguishedName : CN=PC-1,CN=Computers,DC=test,DC=local
DNSHostName       : pc-1.test.local
Enabled           : True
Name              : PC-1
ObjectClass       : computer
ObjectGUID        : c426124d-9b60-428a-aa61-145ca23fc51b
SamAccountName    : PC-1$
SID               : S-1-5-21-2328314914-3034131014-599688784-1107
UserPrincipalName :

DistinguishedName : CN=SERVER2,CN=Computers,DC=test,DC=local
DNSHostName       : Server2.test.local
Enabled           : True
Name              : SERVER2
ObjectClass       : computer
ObjectGUID        : 0d587cba-d804-4303-af54-f5be176fa09b
SamAccountName    : SERVER2$
SID               : S-1-5-21-2328314914-3034131014-599688784-1108
UserPrincipalName :
```

- Get-ADUser -Filter *

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADUser -Filter *


DistinguishedName : CN=Administrator,CN=Users,DC=test,DC=local
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : cb151d82-36b2-4548-891d-9effbfbcdc99
SamAccountName    : Administrator
SID               : S-1-5-21-2328314914-3034131014-599688784-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=test,DC=local
Enabled           : False
GivenName         :
Name              : Guest
ObjectClass       : user
ObjectGUID        : 95e18922-12c0-49b3-b54d-5223f1c1ea80
SamAccountName    : Guest
SID               : S-1-5-21-2328314914-3034131014-599688784-501
Surname           :
UserPrincipalName :

DistinguishedName : CN=Hesam,CN=Users,DC=test,DC=local
Enabled           : True
GivenName         :
Name              : Hesam
ObjectClass       : user
ObjectGUID        : e8ee250f-54c5-4823-9252-6f2fe9dd1468
SamAccountName    : Hesam
SID               : S-1-5-21-2328314914-3034131014-599688784-1000
```

- **دراین مرحله از پروژه دنبال چه مواردی هستیم :**
- چه سیستم‌هایی عضو Domain هستند
- چه کاربران فعالی وجود دارند
- سیستم‌های بلااستفاده کدام‌اند

# نکته بسیار حرفه‌ای

- «اگر Asset Inventory نداشته باشید، امنیت ندارید.»

| Risk | Role | IP | Asset |
|---|---|---|---|
| Critical | Domain Controller | 10.0.30.5 | DC01 |
| High | File Server | 10.0.30.10 | FS01 |
| Medium | VoIP | 10.0.40.10 | PBX01 |
| Critical | Edge Router | 10.0.0.1 | MikroTik01 |

- برای اینکه شما به عنوان کارشناس **واقعاً بتوانید Risk را تشخیص دهید**، باید یاد بگیرد از روی **رفتار شبکه، سرویس‌های فعال و ترافیک** تحلیل کنید.
- یعنی فقط دیدن MAC کافی نیست؛ باید بررسی کند دستگاه چه کاری در شبکه انجام می‌دهد.

- **بررسی سرویس‌های فعال دستگاه** (Service Enumeration ) اول باید بفهمید دستگاه چه سرویس‌هایی اجرا می‌کند.
- nmap -sV 192.168.1.77
- nmap -A 192.168.1.77

- **خروجی ممکن است چیزی مثل این باشد:**

- 22/tcp open ssh
- 80/tcp open http
- 67/udp open dhcp

- **تحلیل**:
- اگر **DHCP ٦٧** باز باشد → احتمال **Rogue DHCP Server**
- اگر **HTTP Proxy یا SSH** باشد → ممکن است ابزار حمله باشد
- اگر سرویس‌های غیرعادی باشد → دستگاه مشکوک است

# NETWORK TRAFFIC ANALYSIS

## Why packet ?

**چرا پکت ها را باید برسی کنیم**

در صورتی که در ساختار شبکه ما طراح هایی برای جلوگیری و شناسایی حملات مانند IDS , IPS داریم

در ساختار شبکه ما فایروال داریم که می تونه جلوی پکت های مخرب را بگیرد .

یا فضای مانیتورینگ داریم – SIEM را داریم .

**و این ها مواردی هست که شاید نیاز نباشد که ما خیلی پکت ها را برسی کنیم**

- **جواب سوال این هست** که سیستم های IDS , IPS و حتی مانیتورینگ هم خطا پذیری بالایی دارند و هم اینکه هرکدام دارای محدودیت هایی هستند

- **حتی solution هایی که گران هستند** دارای خطا پذیری هستند false positive دارند اینها همه مواردی هست که ما نتونیم پکت ها را کامل دریافت کنیم و یا خیلی از این پکت ها را در شبکه از دست می دهیم .

- **اینجاست که اگر یک متخصص** آنالیز ترافیک شبکه داشته باشیم می تونه برسی کند اینکه پکت ها واقعی هست یا خیر

- اولویت ترافیک و Alert که ایجاد شده در شکل زیر با کدام لاگ هست ؟ کدام مهمتر و کدام کم اهمیت تر هست ؟

## Prioritize Traffic and Generated Alerts

```
[**] [1:10000005:0] nmap SYN scan [**] [Priority: 0] {TCP}
192.168.11.62:52999 -> 192.168.11.46:212

[**] [1:10000003:0] ICMP tunnel [**] [Priority: 0] {ICMP}
192.168.122.132 -> 192.168.122.131

[**] [1:10000003:0] ICMP tunnel [**] [Priority: 0] {ICMP}
192.168.122.132 -> 192.168.122.131

[**] [1:10000004:0] ICMP ping sweep [**] [Priority: 0] {ICMP}
92.242.140.21 -> 192.168.11.6
```

Which one is the most important?
Which one is least important?
Our initial focus is the highlighted message that accompanies the alert

# Prioritize Traffic and Generated Alerts

---

```
[**] [1:10000005:0] nmap SYN scan [**] [Priority: 0] {TCP}
192.168.11.62:52999 -> 192.168.11.46:212
```
2

```
[**] [1:10000003:0] ICMP tunnel [**] [Priority: 0] {ICMP}
192.168.122.132 -> 192.168.122.131
```
1

```
[**] [1:10000003:0] ICMP tunnel [**] [Priority: 0] {ICMP}
192.168.122.132 -> 192.168.122.131
```

```
[**] [1:10000004:0] ICMP ping sweep [**] [Priority: 0] {ICMP}
92.242.140.21 -> 192.168.11.6
```
3

Which one is the most important?
Which one is least important?
Our initial focus is the highlighted message that accompanies the alert

همیشه در نتورک آنالیز باید به چند سوال حتما پاسخ داد
اول اینکه مهاجم کیست و چه هدفی دارد ؟
دوم اینکه آیا نشانه ای وجود دارد بابت اینکه متوجه شویم مهاجم از چه ابزاری استفاده می کند .
سوم اینکه آیا پاسخی برای Attacker ارسال شده است یا خیر ؟
نکته آخر ارزیابی ما ازحمله هست ؟

Who is the attacker, and who is the target?

Any signs the attacker is using some kind of software tool?

Are there any responses from the target?

What is your assessment of the attack: harmless, worth investigating, 911?

- tcpdump -D
- پس از وارد کردن دستور بالا لیستی از اینترفیس‌های لینوکی خود را خواهید دید

```
┌──(hesam㉿kali)-[~]
└─$ sudo -s
[sudo] password for hesam:
┌──(root㉿kali)-[/home/hesam]
└─# tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0) [Wireless, Association status unknown]
5.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.dbus-system (D-Bus system bus) [none]
9.dbus-session (D-Bus session bus) [none]

┌──(root㉿kali)-[/home/hesam]
└─#
```

- توسط پارامتر -i می‌توانید یک اینترفیس خاص را انتخاب کرده و داده‌های ارسالی و دریافتی آن اینترفیس را اسنیف کنید.

- tcpdump -i eth0

```
┌──(root㉿kali)-[/home/hesam]
└─# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
04:17:59.370855 IP 192.168.100.61.61975 > 239.255.255.250.1900: UDP, length 175
04:17:59.382790 IP 192.168.100.150.52973 > dns.google.domain: 47594+ PTR? 250.255.255.239.in-addr.arpa. (46)
04:17:59.465687 IP dns.google.domain > 192.168.100.150.52973: 47594 NXDomain 0/1/0 (103)
04:17:59.466247 IP 192.168.100.150.38423 > dns.google.domain: 37906+ PTR? 61.100.168.192.in-addr.arpa. (45)
04:17:59.613519 IP dns.google.domain > 192.168.100.150.38423: 37906 NXDomain 0/0/0 (45)
04:17:59.614427 IP 192.168.100.150.54400 > dns.google.domain: 39038+ PTR? 8.8.8.8.in-addr.arpa. (38)
04:17:59.680118 IP dns.google.domain > 192.168.100.150.54400: 39038 1/0/0 PTR dns.google. (62)
04:17:59.680626 IP 192.168.100.150.43589 > dns.google.domain: 24058+ PTR? 150.100.168.192.in-addr.arpa. (46)
04:17:59.886675 IP dns.google.domain > 192.168.100.150.43589: 24058 NXDomain 0/0/0 (46)
04:18:00.394752 IP 192.168.100.61.61975 > 239.255.255.250.1900: UDP, length 175
04:18:02.330891 IP6 fe80::3f58:dd71:45f2:c65a.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit
04:18:02.396578 IP 192.168.100.150.37809 > dns.google.domain: 1370+ PTR? 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.0.2.0.f.f.ip6.arpa. (90)
04:18:02.463184 IP dns.google.domain > 192.168.100.150.37809: 1370 NXDomain 0/1/0 (154)
04:18:02.463567 IP 192.168.100.150.45324 > dns.google.domain: 63371+ PTR? a.5.6.c.2.f.5.4.1.7.d.d.8.5.f.3.0.0.0.0.0.0.0.0
.0.0.0.0.0.8.e.f.ip6.arpa. (90)
04:18:02.589454 IP dns.google.domain > 192.168.100.150.45324: 63371 NXDomain 0/1/0 (154)
```

- با استفاده از پارامتر -c شما قادر خواهید بود تعداد مشخصی از پکت‌ها را اسنیف کنید. به طور پیشفرض tcpdump تا کنسل نکردن دستور شبکه را اسنیف خواهد کرد.

- **tcpdump -c 10 -i eth0**

```
┌──(root㉿kali)-[/home/hesam]
└─# tcpdump -c 10 -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
04:20:55.927028 IP 192.168.100.61.60707 > 239.255.255.250.1900: UDP, length 175
04:20:56.029063 IP 192.168.100.150.59898 > dns.google.domain: 30936+ PTR? 250.255.255.239.in-addr.arpa. (46)
04:20:56.142038 IP dns.google.domain > 192.168.100.150.59898: 30936 NXDomain 0/1/0 (103)
04:20:56.142588 IP 192.168.100.150.34679 > dns.google.domain: 31590+ PTR? 61.100.168.192.in-addr.arpa. (45)
04:20:56.241092 IP dns.google.domain > 192.168.100.150.34679: 31590 NXDomain 0/0/0 (45)
04:20:56.241843 IP 192.168.100.150.33506 > dns.google.domain: 55239+ PTR? 8.8.8.8.in-addr.arpa. (38)
04:20:56.475102 IP dns.google.domain > 192.168.100.150.33506: 55239 1/0/0 PTR dns.google. (62)
04:20:56.475643 IP 192.168.100.150.54585 > dns.google.domain: 23262+ PTR? 150.100.168.192.in-addr.arpa. (46)
04:20:56.644301 IP dns.google.domain > 192.168.100.150.54585: 23262 NXDomain 0/0/0 (46)
04:20:56.950205 IP 192.168.100.61.60707 > 239.255.255.250.1900: UDP, length 175
10 packets captured
10 packets received by filter
0 packets dropped by kernel

┌──(root㉿kali)-[/home/hesam]
└─#
```

- جهت ذخیره سازی خروجی کپچر در یک فایل ، از پارامتر -w استفاده می‌شود.
- tcpdump -w file1.pcap -i eth0

```
┌──(root㉿kali)-[/home/hesam]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root㉿kali)-[/home/hesam]
└─# cd Desktop

┌──(root㉿kali)-[/home/hesam/Desktop]
└─# ls
log

┌──(root㉿kali)-[/home/hesam/Desktop]
└─# cd log

┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─#
```

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# tcpdump -w file1.pcap -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

در مثال بالا ، خروجی دستور tcpdump در فایل file1.pcap ذخیره سازی می‌شود.

برای خواندن فایل‌های کپچر شده که توسط دستور بالا تولید می‌شود ، از پارامتر -r استفاده می‌گردد.

tcpdump -r file1.pcap

```
┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# tcpdump -w file1.pcap -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

^C101 packets captured
101 packets received by filter
0 packets dropped by kernel

┌──(root㉿kali)-[/home/hesam/Desktop/log]
└─# tcpdump -r file1.pcap
reading from file file1.pcap, link-type EN10MB (Ethernet), snapshot length 262144
06:41:01.381154 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 38, length 40
06:41:01.381251 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 38, length 40
06:41:02.397120 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 39, length 40
06:41:02.397187 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 39, length 40
06:41:03.409700 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 40, length 40
06:41:03.409779 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 40, length 40
06:41:04.422276 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 41, length 40
06:41:04.422340 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 41, length 40
06:41:05.434606 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 42, length 40
06:41:05.434694 IP 192.168.100.150 > 192.168.100.60: ICMP echo reply, id 1, seq 42, length 40
06:41:06.353504 ARP, Request who-has 192.168.100.150 (50:76:af:e4:37:39 (oui Unknown)) tell 192.168.100.60, length 46
06:41:06.353546 ARP, Reply 192.168.100.150 is-at 00:0c:29:5f:30:0e (oui Unknown), length 28
06:41:06.447245 IP 192.168.100.60 > 192.168.100.150: ICMP echo request, id 1, seq 43, length 40
```