



Ai powered Recon with Chaos

⚠ warning

**This document is only for
educational purposes.**

**The author will approve of
no abusage.**



فهرست

4	جمع‌آوری اطلاعات (Intelligence Gathering) با بهره‌گیری از هوش مصنوعی
5	3 . ابزارها و روش‌های مبتنی بر AI برای Recon
7	5 . استفاده از هوش مصنوعی برای کدنویسی ابزار Recon
8	جمع‌آوری اطلاعات خارج از سازمان (External Recon) با استفاده از هوش مصنوعی
10	ترکیب ابزارهای کلاسیک با LLM ها برای تحلیل سریع‌تر
10	هدف نهایی Recon خارجی چیست؟
11	جمع‌آوری اطلاعات داخل سازمان (Internal Recon) با استفاده از هوش مصنوعی
11	سناریو 1: مشاور خارجی (بدون دسترسی به شبکه داخلی)
13	سناریو 2: کاربر با دسترسی اولیه به شبکه داخلی (مثلاً نقش کارمند)
15	بررسی شبکه LAN سیمی در Recon داخلی
15	سناریو 1: فعال است و IP اختصاص داده می‌شود
15	سناریو 2: غیرفعال است، اما کابل فعال است
16	سناریو 3: Network Access Control (NAC) فعال است
17	سناریو 4: پورت LAN به صورت کامل غیرفعال است
17	هوش مصنوعی در تحلیل وضعیت شبکه
18	بررسی شبکه بی‌سیم (Wireless LAN) در Recon داخلی
21	استخراج هش‌های LLMNR/NBNS Spoofing با طریق NTLM از ابزارهای Inveigh و Responder



21	سناريو پايه: جعل پاسخدهنده به نام دامنه اشتباه
23	تفاوت Net-NTLM و NTLM
25	جمع آوري اطلاعات غيرفعال (Passive Fingerprinting)
28	نقش هوش مصنوعي در Passive Recon
29	شناسي فعال (Active Fingerprinting)
29	هدف اصلی در Active Recon
31	نقش هوش مصنوعي در Active Fingerprinting



جمع‌آوری اطلاعات با (Intelligence Gathering)

بهره‌گیری از هوش مصنوعی

جمع‌آوری اطلاعات یکی از مهم‌ترین مراحل در تست نفوذ و عملیات‌های امنیتی است. در عصر جدید، استفاده از هوش مصنوعی (AI)، مدل‌های زبانی بزرگ (LLM) و ابزارهای خودکار می‌تواند فرآیند شناسایی هدف را بسیار سریع‌تر و هوشمندتر انجام دهد.

۱. سناریوهای پایه در جمع‌آوری اطلاعات

• سناریو اول: خارج از سازمان (External Recon)

اطلاعات قابل دسترسی از طریق اینترنت، پایگاه‌داده‌های عمومی، شبکه‌های اجتماعی، **Shodan**، **WHOIS** و غیره.

• سناریو دوم: داخل سازمان (Internal Recon)

دسترسی از طریق نفوذ اولیه، ابزارهای شبکه داخلی، **Enumeration**، سیستم‌عامل‌ها، کشف دارایی‌ها و تحلیل لاغ‌ها.

۲. نقش هوش مصنوعی در جمع‌آوری اطلاعات

• پردازش سریع داده‌های حجمی

• تحلیل رفتار دامنه‌ها، ایمیل‌ها، و ساختار زیرساخت

• خودکارسازی تولید پرامپت‌ها و اسکریپت‌های مخصوص جمع‌آوری داده

• استخراج اطلاعات از منابع متنی، مانند وبسایتها، گزارش‌ها یا چت‌ها



3 . ابزارها و روش‌های مبتنی بر AI برای Recon

1.3 . ابزارها و خدمات آنلاین:

Shodan + GPT-based analysis .

ارسال خروجی **GPT** به **Shodan** برای تحلیل سریع سرویس‌ها و آسیب‌پذیری‌ها.

Maltego + AI Integration .

افزودن ماژول‌های تحلیل هوش مصنوعی به **Maltego** برای بررسی ارتباطات پیچیده.

Recon-ng + LLM .

استفاده از پرامپت‌هایی برای خلاصه‌سازی نتایج و پیشنهاد گام‌های بعدی.

SpiderFoot + GPT Summarizer .

پس از **Crawl** اطلاعات، ارسال خروجی به مدل برای تحلیل خودکار تهدیدها.

Google Dorks + LLM .

تولید داینامیک **Dork**‌های پیشرفته بر اساس کلمات کلیدی هدف.



4. پرامپت‌های هوش مصنوعی برای کمک به Recon به فارسی

نمونه 1: تحلیل دامنه

دامنه **example.com** را بررسی کن و اطلاعاتی مثل ایمیل‌های مرتبط، سرویس‌های فعال و هر نشانه‌ای از تکنولوژی‌های استفاده شده را استخراج کن.

نمونه 2: تولید لیست subdomain

با استفاده از ابزارهایی مثل **VirusTotal**، **crt.sh** و منابع دیگر یک لیست **subdomain** برای دامنه **x.com** تولید کن.

نمونه 3: تحلیل ساختار سازمان

با بررسی لینک‌دین و شبکه‌های اجتماعی، ساختار کارکنان و نقش‌های کلیدی در سازمان **X** را شناسایی کن.

نمونه 4: تحلیل تاریخچه DNS

تاریخچه **DNS** دامنه **x.org** را بررسی کن و تغییرات مهم **A Record** و **NS** را گزارش بده.

نمونه 5: تهییه پروفایل هدف

با استفاده از اطلاعات عمومی در دسترس، یک پروفایل فنی برای شرکت **X** تهییه کن شامل دامنه‌ها، سرویس‌های ابری، ایمیل‌ها، شماره تلفن‌ها و فناوری‌های مورد استفاده.



5 . استفاده از هوش مصنوعی برای کدنویسی ابزار Recon

- مثال: ساخت ابزار **subdomain scanner** ساده با کمک **GPT**

با دادن پرامپت زیر:

- یه اسکریپت پایتون بنویس که با استفاده از دیکشنری مشخص، **subdomain**‌های دامنه‌ای را بررسی کنه و وضعیت پاسخدهی آونها رو مشخص کنه.

خروجی می‌تواند یک ابزار نیمه‌خودکار باشد برای شناسایی سریع دامنه‌های فعال.

- پیشنهادهای پیشرفته: استفاده از **GPT** برای تولید ماژول‌های **Nmap** به گزارش قابل‌خواندن برای تحلیل‌گر امنیتی.

6 . ترکیب ابزارهای کلاسیک و هوش مصنوعی

ابزار سنتی	نقش AI در بهبود عملکرد
Nmap	تحلیل خروجی به زبان طبیعی، اولویت‌بندی اهداف
theHarvester	خلاصه‌سازی ایمیل‌ها و دامنه‌ها و دسته‌بندی شان
OSINT Framework	خودکارسازی انتخاب ابزار مناسب با توجه به هدف



جمع‌آوری اطلاعات خارج از سازمان (External Recon) با

استفاده از هوش مصنوعی

هنگامی که تست نفوذ یا عملیات شناسایی از بیرون سازمان انجام می‌گیرد، اولین قدم شناسایی سطح حمله (**Attack Surface**) است. این مرحله شامل پاسخ به پرسش‌های کلیدی زیر است که با کمک ابزارهای هوش مصنوعی و زبان‌های بزرگ (**LLM**) می‌توان آن را هوشمند، سریع و دقیق انجام داد.

پرسش‌هایی برای تعیین سطح حمله

۱. چه دامنه/زیر دامنه‌هایی وجود دارند؟

ابزارها **Assetfinder**, **Sublist3r**, **crt.sh**

پرامپت **AI**

با استفاده از اطلاعات منابع عمومی، دامنه‌ها و زیر دامنه‌های مرتبط با **example.com** را شناسایی کن.

۲. چه **IP**، رنج شبکه، یا شماره **ASN** به سازمان اختصاص دارد؟

ابزارها **whois**, **IPinfo**, **bgp.he.net**

پرامپت **AI**

با استفاده از اطلاعات **ASN** و **BGP** و **WHOIS** مربوط به دامنه **example.com** را استخراج کن.



۳. چه سرویس‌هایی (پورت‌های باز) روی این IP‌ها اجرا می‌شوند؟

ابزارها **Nmap, Masscan, Shodan**

پرامپت AI

خروجی Nmap روی IP‌های **X.X.X.X** بررسی کن و سرویس‌های آسیب‌پذیر یا مشکوک را لیست کن.

۴. چه آدرس‌های ایمیل یا افرادی با سازمان در ارتباط هستند؟

ابزارها **Hunter.io, theHarvester**

پرامپت AI

لیستی از ایمیل‌ها و افراد مرتبط با **example.com** بر اساس داده‌های عمومی و شبکه‌های اجتماعی تهیه کن.

۵. از چه سیستم‌عامل‌ها یا نرم‌افزارهایی استفاده می‌شود؟

ابزارها **Wappalyzer, Netcraft, BuiltWith**

پرامپت AI

مشخص کن وب‌سایت **example.com** از چه تکنولوژی‌ها، سرورها، زبان‌ها یا فریمورک‌هایی استفاده می‌کند.

۶. آیا در گذشته نقض امنیتی‌ای (**Data Breach**) رخ داده؟

ابزارها **Have I Been Pwned, DeHashed, LeakCheck**

پرامپت AI

بررسی کن آیا دامنه یا ایمیل‌های مرتبط با **example.com** در دیتابیس‌های نشت اطلاعات دیده شده‌اند؟



ترکیب ابزارهای کلاسیک با LLM ها برای تحلیل سریع تر

هوش مصنوعی می‌تواند خروجی ابزارهای سنتی مانند **Nmap, theHarvester** یا **Shodan** را تجزیه و تحلیل کرده و به زبان طبیعی گزارشی قابل فهم تولید کند. مثلاً:

مثال:

ورودی : خروجی **Nmap** برای دامنه یا IP

پرامپت:

تحلیل کن کدام سرویس‌ها روی پورت‌های باز اجرا می‌شوند و آیا آسیب‌پذیری شناخته‌شده‌ای دارند یا نه؟

خروچی هوش مصنوعی:

پورت **21** (FTP) باز است و نسخه **vsFTPd 2.3.4** در حال اجرا است که دارای بکدور شناخته‌شده **CVE-2011-2523** است.

هدف نهایی Recon خارجی چیست؟

با گردآوری این اطلاعات، مهاجم یا تحلیل‌گر امنیتی می‌تواند:

- **Credential** های فاش شده را برای دسترسی اولیه استفاده کند.
- از آسیب‌پذیری‌های شناخته‌شده روی سرویس‌های باز بهره‌برداری کند.
- مهندسی اجتماعی را با اطلاعات کارکنان دقیق‌تر انجام دهد.
- ساختار زیرساخت سازمان را حدس زده و قدم بعدی برای دسترسی به شبکه داخلی بردارد.



جمع‌آوری اطلاعات داخل سازمان (Internal Recon) با استفاده از هوش مصنوعی

زمانی که در داخل سازمان حضور داریم (به صورت فیزیکی یا از طریق دسترسی اولیه)، سناریوهای متفاوتی وجود دارد که هر کدام نیاز به تکنیک‌ها و ابزارهای مخصوص خود دارند. در اینجا ما ابتدا به حالت مشاور خارجی می‌پردازیم که هنوز به شبکه داخلی سازمان دسترسی ندارد، ولی داخل ساختمان حضور دارد.

سناریو ۱: مشاور خارجی (بدون دسترسی به شبکه داخلی)

فرض کنیم به عنوان مشاور امنیتی در اتاق جلسه حضور داریم. اقدامات اولیه می‌تواند شامل موارد زیر باشد:

۱. اسکن شبکه‌های بی‌سیم اطراف (**WiFi Enumeration**)
 - ابزارها : **Kismet, airodump-ng, WiFi Analyzer**
 - کاربرد **AI**
 - تحلیل نام شبکه‌ها (**SSID**) برای شناسایی نامهای سازمانی یا تستی
 - استخراج الگوهای نام‌گذاری که نشان‌دهنده ساختار داخلی باشد
- پرامپت پیشنهادی:
 - لیستی از **SSID**‌های شناسایی شده را تحلیل کن و مشخص کن کدامیک می‌توانند مربوط به شبکه‌های سازمانی باشند.



۲ - بررسی کانال‌های ارتباطی باز (Bluetooth, NFC)

• ابزارهای **hcitool, bluetoothctl, nfc-list**:

• پaramپت:

- خروجی ابزارهای **Bluetooth Scan** را تحلیل کن و مشخص کن آیا دستگاه‌های شناسایی شده متعلق به کارمندان هستند یا تجهیزات زیرساختی؟

۳ - بررسی دستگاه‌های متصل به شبکه (در صورت دسترسی محدود)

• ابزارهای **Netdiscover, ARP-scan, Fing**:

- خروجی این ابزارها را می‌توان به مدل‌های **LLM** داد تا نوع دستگاه، سازنده و ریسک را مشخص کند.

• پaramپت:

- خروجی **arp-scan** را تحلیل کن و مشخص کن کدام IP‌ها مربوط به پرینتر، دوربین، سرور یا لپ‌تاپ هستند.

۴ - تحلیل رفتار کاربران و سیستم‌ها

با مشاهده مستقیم رفتار کارکنان، اطلاعاتی مانند موارد زیر قابل استخراج است:

- نوع سیستم‌عامل استفاده شده
- نحوه اتصال به شبکه با **VPN** یا مستقیم
- استفاده از ابزارهای خاص مثل **SSH, Outlook, SAP** و ...



سناریو 2: کاربر با دسترسی اولیه به شبکه داخلی (مثال نقش کارمند)

در این حالت، فرصت‌های بیشتری برای جمع‌آوری اطلاعات وجود دارد:

1. شناسایی ساختار شبکه

: **Nmap, Netdiscover, Ping Sweep** • ابزارها

- هوش مصنوعی می‌تواند پس از اسکن، تopoلوجی تقریبی شبکه را ترسیم کند.
- پرامپت:
- از خروجی **Nmap** یک نقشه ساده از شبکه تهیه کن و IP هایی که به نظر مهم یا حیاتی هستند را جدا کن.

2. بررسی اشتراک‌های شبکه (Network Shares)

: **smbclient, smbmap, enum4linux** • ابزارها

- پرامپت:
- مسیرهای اشتراک‌گذاری شده را تحلیل کن و مشخص کن کدامیک ممکن است حاوی اطلاعات حساس باشند.

3. دسترسی به پالیسی‌ها و مستندات

• جستجو در پوشه‌های عمومی مانند \\domain\public یا دسکتاپ کاربران

- اسناد **HR**، اسکریپت‌های خودکار، لیست‌های رمز عبور ذخیره شده و غیره
- هوش مصنوعی می‌تواند این اسناد را خلاصه و تحلیل کند.

پرامپت:

- محتواهای فایل‌های **Word** و **PDF** را بررسی کن و اطلاعات کلیدی مثل رمز عبور، دسترسی‌ها یا ساختار تیم را استخراج کن.



۴. تحلیل لاغها و ابزارهای مانیتورینگ محلی

• ابزارهای **Event Viewer, Syslog, Log Parser**:

- پرامپت:
- از لاغها خطاها را که با سرویس‌های داخلی یا تلاش‌های دسترسی مشکوک را استخراج کن.

نقش AI در شناسایی الگوهای دسترسی

با دادن خروجی‌ها به یک مدل زبانی یا گراف تحلیلی، می‌توان مسیرهای احتمالی حمله را شبیه‌سازی کرد:

- کاربر X به پوشه Y دسترسی دارد که روی سرور Z میزبانی می‌شود.
- سرور Z یک سرویس RDP با پورت باز دارد.
- روی سرور Z لگی حاکی از تلاش ناموفق ورود دیده می‌شود.



بررسی شبکه LAN سیمی در Recon داخلی

زمانی که در محل سازمان حضور فیزیکی داریم و به کابل **LAN** دسترسی پیدا می‌کنیم، فرصت بسیار مناسبی برای جمع‌آوری اطلاعات داخلی فراهم می‌شود. بسته به پیکربندی شبکه، چند سناریوی مختلف ممکن است پیش بیاید که هر کدام تکنیک‌ها و راهکارهای خاصی دارند. در ادامه این سناریوها را بررسی می‌کنیم.

سناریو 1: DHCP فعال است و IP اختصاص داده می‌شود

اگر **DHCP** فعال باشد، سیستم ما به صورت خودکار یک آدرس **Subnet**، **IP**، **DNS** و **Gateway** دریافت می‌کند.

- اقدامات بعدی:

- اسکن شبکه با ابزارهایی مثل **Nmap**، **Netdiscover**
- تحلیل ساختار شبکه، شناسایی گره‌ها، سرورها و سرویس‌های حساس
- پرامپت **AI** پیشنویس‌هایی مثل **DHCP log** و **ifconfig/ipconfig**
- از خروجی **DHCP** یک نمای کلی از ساختار شبکه و کلاس **IP** استخراج کن.

سناریو 2: DHCP غیرفعال است، اما کابل فعال است

در این حالت می‌توان ترافیک را **sniff** کرد و اطلاعاتی مانند **IP** همسایه‌ها، **Netmask** و **Gateway** را استخراج کرد.

- ابزارها

Wireshark, **tcpdump**, **arp-scan**



• اقدامات:

- تنظیم **IP** استاتیک به صورت دستی و تلاش برای ارتباط **AI**.
- خروجی **Wireshark** را بررسی کن و مشخص کن کدام **IP** و **Gateway** در شبکه تکرار شده‌اند و قابل استفاده برای تنظیم دستی هستند.

سناریو ۳ Network Access Control (NAC) فعال است

در این حالت، اتصال ساده به شبکه کافی نیست. سازمان ممکن است **NAC** یا **X 802.1** فعال کرده باشد. در این سناریو، گزینه‌هایی مانند زیر مطرح می‌شود:

- شناسایی و کلون کردن **MAC** آدرس از یک دستگاه متصل (مثل چاپگر)
 - ابزارها: **Wireshark, arp, macchanger**
 - پرامپت:
- آدرس‌های متصل به شبکه را شناسایی کن و یکی از آن‌ها را که مربوط به دستگاه غیر حیاتی است، برای کلون کردن پیشنهاد بده.
- بررسی دستگاه‌های **Hub** یا **IP Phone** یا **Phone** های متصل
- برخی تلفن‌های **VoIP** دارای پورت **LAN** اضافی هستند و ممکن است اتصال از طریق آن‌ها ممکن باشد.
- استفاده از **USB-to-LAN Adapter** به دستگاه متصل
- با استفاده از **USB Ethernet Adapter** می‌توان به دستگاه متصل، دسترسی جانبی ایجاد کرد.



سناریو 4 : پورت LAN به صورت کامل غیرفعال است

- شرح: در صورت غیرفعال بودن پورت، عملأً راهی برای دسترسی وجود ندارد (مگر از طریق دسترسی فیزیکی به سوییچ).
- اقدامات احتمالی: بررسی سایر پورت‌ها، دستگاه‌های باز، یا شبکه WiFi موجود در محل.

هوش مصنوعی در تحلیل وضعیت شبکه

با استفاده از ابزارهای GPT مانند LLM، می‌توان خروجی ابزارهای شبکه را تحلیل کرده و تصمیم‌گیری سریع‌تری داشت. به عنوان مثال:

وروودی:

خروچی arp-scan

192.168.1.10 00:1A:2B:3C:4D:5E HP Printer

192.168.1.20 00:1F:22:33:44:55 Cisco IP Phone

پرامپت:

کدامیک از این MAC آدرس‌ها را می‌توان برای کلون کردن انتخاب کرد تا احتمال شناسایی پایین‌تر باشد؟

خروچی:

HP Printer (00:1A:2B:3C:4D:5E) مربوط به MAC زیرا دستگاه‌های چاپ‌گر معمولاً ترافیک خاصی ندارند و بررسی سخت‌تری دارند.



بررسی شبکه بی‌سیم (Wireless LAN) در Recon داخلی

شبکه‌های **Wi-Fi** یکی از رایج‌ترین و آسیب‌پذیرترین نقاط ورودی در سازمان‌ها هستند. در عملیات‌های جمع‌آوری اطلاعات داخل سازمان، شناسایی و بررسی دقیق شبکه‌های بی‌سیم می‌تواند اطلاعات مهمی درباره ساختار و امنیت سازمان به دست دهد.

۱ - بررسی اتصال به شبکه Wi-Fi باز (Open/Guest)

اقدامات:

- اتصال به شبکه مهمان (در صورت عدم نیاز به رمز عبور)

• بررسی محدوده آدرس‌دهی داخلی (**Private IP Range**)

• بررسی امکان **resolve** شدن نام دامنه‌های داخلی

ابزارها:

ipconfig/ifconfig, netstat, nslookup, dig, ping, traceroute

پaramپت پیشنهادی:

من به شبکه **Wi-Fi** مهمان متصل شده‌ام. بررسی کن که آیا می‌توانم به شبکه داخلی سازمان دسترسی داشته باشم یا خیر، و آیا نام دامنه‌های داخلی **resolve** می‌شوند؟

نکته:

برخی سازمان‌ها فقط اینترنت را روی شبکه **Guest** ارائه می‌دهند، ولی اگر **DNS** داخلی نادرست پیکربندی شده باشد، ممکن است نام‌های داخلی **resolve** شوند مثلًا **intranet.company.local**



2 . بررسی شبکه‌های دارای رمز عبور **WEP / WPA / WPA2**

اگر شبکه‌هایی با رمز عبور شناسایی شوند، می‌توان آن‌ها را هدف تحلیل قرار داد:

- شناسایی شبکه‌های اطراف (**SSID, BSSID, Channel**)

• ابزارها : **airodump-ng, Kismet, WiFi Explorer**

- تحلیل نوع رمزگذاری

• شناسایی نوع رمزگذاری (**WEP, WPA, WPA2, WPA3**)

• پaramپت:

• خروجی **airodump-ng** را تحلیل کن و مشخص کن کدام شبکه‌ها رمزگذاری

ضعیفتری دارند و احتمال کرک شدن آن‌ها بیشتر است.

- حملات روی **WEP / WPA**

• **aircracking** قابل کرک با جمع‌آوری تعداد کافی **IV** ها با ابزار **WEP**

• **Deauthentication** با حمله **WPA/WPA2 (PSK)** و گرفتن

• **Dictionary** و سپس استفاده از **aireplay-ng** با **Handshake**

Attack

مثال پaramپت:

من یک **SSID "office_wifi"** از شبکه **Wi-Fi** با **Handshake** گرفتم. لطفاً با استفاده از یک لیست رمز عبور، بررسی کن آیا می‌توان آن را کرک کرد یا نه.



3. نقش AI در تحلیل شبکه‌های Wi-Fi

موارد کاربردی:

- طبقه‌بندی شبکه‌ها براساس نوع رمزگذاری، قدرت سیگنال، و احتمال نفوذ
- پیشنهاد روش مناسب برای کرک رمز عبور
- پیشنهاد بهترین wordlist یا dictionary براساس نام شبکه و محل

مثال ترکیبی:

SSID = Office_Guest

Signal = -40 dBm

Encryption = WPA2

نام شبکه شامل کلمه "Guest" است. احتمال دارد رمز ساده باشد.

پیشنهاد: استفاده از لیست رمزهای رایج مخصوص شبکه‌های مهمان.

جدول خلاصه سناریوهای Wi-Fi

نقش AI	اقدام مناسب	وضعیت	نوع شبکه
تحلیل نام دامنه‌ها	بررسی Subnet و DNS	متصل	Open/GUEST
تحلیل احتمال موفقیت	جمع‌آوری IV و کرک با aircrack	رمز دارد	WEP
پیشنهاد wordlist مناسب	گرفتن Handshake و Dictionary حمله	رمز دارد	WPA/WPA2
تحلیل ترافیک اولیه	نیاز به کرک EAP یا مهندسی اجتماعی	پیچیده	WPA2 Enterprise



استخراج هش‌های LLMNR/NBNS از طریق NTLM

Inveigh Responder با ابزارهای Spoofing

پس از دسترسی به شبکه داخلی سازمان، یکی از مؤثرترین روش‌ها برای استخراج اطلاعات احراز هویت، استفاده از آسیب‌پذیری‌های مرتبط با پروتکل‌های Broadcast مانند **LLMNR**، **Inveigh Responder** و **NBNS** است. ابزارهایی مانند **mDNS** برای بهره‌برداری از این پروتکل‌ها طراحی شده‌اند و می‌توانند به راحتی هش‌های کاربران شبکه را جمع‌آوری کنند.

سناریو پایه: جعل پاسخ‌دهنده به نام دامنه اشتباه

مثالی ساده:

1. کاربری قصد دارد به فایل‌서ور دسترسی پیدا کند: \\NAS001

2. اشتباهًا تایپ می‌کند: \\NAS01

3. DNS نمی‌تواند NAS01 را resolve کند.

4. کاربر درخواست را روی شبکه Broadcast می‌کند:

"کسی هست که NAS01 باشه؟"

5. مهاجم با Inveigh Responder یا فعال پاسخ می‌دهد:

"192.168.1.66" من! آدرس من:

6. کلاینت اطلاعات خود را از جمله نام کاربری و هش NTLMv2 به مهاجم ارسال می‌کند.



ابزارهای اصلی

مناسب لینوکس **Responder**

- پایتون بیس، سازگار با ابزارهای **Red Team** مثل **Kali, Parrot**
- شبیه‌سازی سرورهای **FTP**, **HTTP**, **SMB** و ...
- استخراج هش‌های **NTLMv1/v2** و تحلیل ترافیک داخلی

مناسب ویندوز **Inveigh**

- نسخه ویندوزی **Responder**
- عملکرد مشابه برای تست در شبکه‌های مبتنی بر **Windows**
- مناسب برای موقعی که ابزارهای لینوکسی در دسترس نیستند

نمونه هش **Net-NTLMv2** استخراج می‌شود:

DOMAIN\username::domain:[random challenge]:[NT response hash]:[blob]:[challenge]

پرامپت هوش مصنوعی برای تحلیل:

این هش **NTLMv2** را بررسی کن و مشخص کن با کدام ابزار **(john, hashcat)** و کدام فرمت می‌توان آن را کرک کرد؟



تفاوت Net-NTLM و NTLM

نوع هش	محل استفاده	پشتیبانی	کرک پذیری
Pass-the-Hash			
NTLM	ذخیره شده در SAM یا NTDS.dit	بله	بله
Net-NTLMv1/v2	احراز هویت شبکه (Challenge-Response)	خیر	بله (Offline)

کاربرد عملی برای تست

• پیش نیاز: حضور در شبکه داخلی و شنود ترافیک **Broadcast**

• مراحل:

1. اجرای **Analyze** یا **Inveigh** یا **Responder**

Poison

2. انتظار برای خطای تایپ یا **Broadcast** از طرف کلاینت

3. دریافت هش و ذخیره آن در فایل خروجی

4. کرک هش به صورت آفلاین با ابزارهایی مانند **john** یا **hashcat**



پرامپت‌های پیشنهادی برای تحلیل هوشمندانه:

:1 مثال

خروجی **Responder** را بررسی کن. کدام کاربران بیشترین درخواست را ارسال کرده‌اند و کدام هش‌ها احتمال کرک شدن بیشتری دارند؟

:2 مثال

بر اساس دامنه و نام کاربری، یک لیست **wordlist** احتمالی تولید کن که احتمال کرک شدن **Net-NTLM** را افزایش دهد.

منابع پیشنهادی برای مطالعه بیشتر:

- [**The Practical Guide to NTLM Relaying - Byt3bl3d3r**](#)
- [**SMB Relay Demystified \(SANS\)**](#)



جمع آوری اطلاعات غیرفعال (Passive Fingerprinting)

در **Passive Fingerprinting**، شما مستقیماً با سیستم هدف ارتباط برقرار نمی‌کنید. به جای آن، با استفاده از اطلاعات موجود در اینترنت مانند کش موتورهای جستجو، **DNS**، **WHOIS**، و پایگاهداده‌های عمومی (ساختار، دامنه‌ها، **IP**‌ها و آسیب‌پذیری‌های احتمالی را بررسی می‌کنید.

ابزارها و روش‌ها

ابزارهای خط فرمان و **API**



فریم‌ورک مژوولار برای انجام **reconnaissance** با مژوول‌های **WHOIS**، **DNS** و **Google Dork** وغیره.



ابزار **OSINT** برای جمع آوری ایمیل‌ها، دامنه‌ها، و حساب‌های عمومی در شبکه‌های اجتماعی.



برای استخراج **DNS Records (A, MX, TXT, NS)** و گراف شبکه دامنه.



مثال‌های کاربردی:

curl -s

http://api.hackertarget.com/hostsearch/?q=example.com > hostsearch

curl -s

http://api.hackertarget.com/dnslookup/?q=example.com > dnslookup



Google Dorking Techniques

تکنیک	کاربرد
site:example.com	نتایج فقط از example.com
filetype:pdf	جستجوی فایل‌های PDF مثلاً سندهای سازمانی
inurl:admin یا allinurl:login intitle:index.of	یافتن صفحات لاغین دسترسی به دایرکتوری‌های باز

پرامپت 

با استفاده از ترکیب **Dork** های گوگل، صفحاتی از **example.com** را که شامل فایل‌های اکسل، دایرکتوری‌های باز یا صفحات لاغین هستند لیست کن.

ابزارهای تحلیلی و پیشرفتی

McAfee SiteDigger

بررسی کش گوگل برای یافتن آسیب‌پذیری‌ها و **misconfiguration** های احتمالی.

SearchDiggity

مجموعه کامل ابزارهای **OSINT** شامل:

GoogleDiggity :

BingDiggity :

CodeSearchDiggity :

SHODANDiggity :

...PortScanDiggity :



Shodan.io + CLI

برای مشاهده سرویس‌ها و پورت‌های باز مرتبط با IP/دامنه.

shodan host example.com

Exfiltrated (Internet Census 2012)

نمایی از IP‌ها و پورت‌های باز در سال ۲۰۱۲، مناسب برای تحلیل تاریخی و مقایسه وضعیت امنیت.

DNS Intelligence, Reverse Lookup ابزارهای

ابزار	عملکرد
DomainTools	WHOIS , مانیتورینگ تغییرات Reverse IP Lookup
PassiveTotal	تحلیل تهدید، زیرساخت و DNS
Server Sniff	DNS Trace , Reverse IP , IP Lookup
Robtex	بررسی جامع دامنه، AS , IP ، و مسیرهای شبکه

Robtex برای **Nmap NSE Script**

nmap –script http-robtex-reverse-ip –script-args http-robtex-reverse-ip.host='XX.XX.78.214'



نقش هوش مصنوعی در Passive Recon

با استفاده از مدل‌های زبانی مانند **GPT** می‌توان:

- خروجی ابزارها را خلاصه و تفسیر کرد
- بین داده‌ها ارتباط ایجاد کرد مثلاً یک **subdomain** خاص به چه **IP**‌ها متصل است؟
- پیشنهاد هدف‌های مناسب‌تر بر اساس ضعف احتمالی ارائه داد

پرامپت‌های پیشنهادی:

خروجی **hostsearch** را بررسی کن و مشخص کن کدام زیردامنه‌ها ممکن است دارای لاگین، پنل ادمین یا اسناد حساس باشند.

از میان ۱۰۰ دامنه استخراج شده، ۱۰ دامنه‌ای را انتخاب کن که احتمال وجود صفحه ورود در آن‌ها بیشتر است.



شناسایی فعال (Active Fingerprinting)

پس از اتمام مرحله‌ی شناسایی غیرفعال، نوبت به بررسی‌های تعاملی می‌رسد. در این مرحله ما مستقیماً با زیرساخت سازمان هدف ارتباط برقرار می‌کنیم تا اطلاعاتی مانند رکوردهای **DNS**، سرویس‌های فعال، IP‌های اختصاصی، و نام میزبان‌ها را شناسایی کنیم.

برخلاف شناسایی غیرفعال، این روش ممکن است در لگ‌ها ثبت شده و شناسایی شود.

هدف اصلی در Active Recon

- دریافت اطلاعات کامل‌تر از سرور DNS در صورت misconfiguration

- شناسایی IP-to-Hostname Mapping

- کشف Subdomain‌ها و دامنه‌های داخلی یا زیرساختی

ابزارها و دستورات کلیدی در Active DNS Fingerprinting

host -l

host -l example.com ns1.example.com

در صورتی که Zone Transfer از DNS Server پشتیبانی کند، لیست کامل رکوردها را برمی‌گرداند.

dig axfr

dig axfr example.com @ns1.example.com

اجرای دستور AXFR برای انجام Zone Transfer

اگر پیکربندی سرور ضعیف باشد، تمام رکوردهای A, MX, TXT, NS و... دریافت می‌شود.



dnsrecon

dnsrecon -d example.com -t axfr

ابزار کامل‌تر برای شناسایی **DNS Records**

انواع تست‌های **cache, brute, standard, axfr, zonewalk** و **snooping** را پشتیبانی می‌کند.

dnsenum

dnsenum example.com

جمع‌آوری **WHOIS info**، سرورهای ایمیل، و تلاش برای **Subdomain** و **Zone Transfer**

قابلیت استفاده در هر دو سناریوی داخلی و خارجی

منابع خارجی و داخلی

محیط اجرا	اطلاعات قابل استخراج	احتمال موفقیت Zone Transfer
خارج از سازمان	دامنهای عمومی، رکوردهای باز، برخی Subdomain	کم
داخل شبکه	دامنهای داخلی، رکوردهای مخفی، سیستم‌های داخلی	زیاد



نقش هوش مصنوعی در Active Fingerprinting

هوش مصنوعی می‌تواند:

- خروجی‌های ابزارها را تحلیل و اولویت‌بندی کند
- الگوهایی در نام میزبان‌ها پیدا کند مثلاً **dev-, test-, vpn-**
- پیشنهاد حملات بعدی بر اساس اطلاعات کشف شده ارائه دهد

پرامپت‌های پیشنهادی برای AI

:1 مثال

خروجی **dig axfr** را بررسی کن و مشخص کن کدام IP‌ها مربوط به سرورهای ایمیل، **VPN** یا سرورهای داخلی هستند.

:2 مثال

خروجی **dnsenum** شامل چندین زیردامنه است. لطفاً آن‌ها را بر اساس کاربرد (تست، ایمیل، وب، توسعه) دسته‌بندی کن.

نمونه خروجی جذاب از Zone Transfer

dev01.example.com. A 192.168.1.10

vpn.example.com. A 192.168.1.25

mail1.example.com. MX 10 mail1.example.com.

ftp.example.com. A 192.168.1.20

این اطلاعات، دید کاملی از زیرساخت شبکه در اختیار تحلیل‌گر امنیتی قرار می‌دهد.

