

RECON for Bug Bounty



Let's Recon with Chaos

⚠ warning

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

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



فهرست

4	Introduction
4	Types of Recon
5	ACTIVE VS PASSIVE
5	شناسایی فعال (Active Reconnaissance)
6	شناسایی غیرفعال (Passive Reconnaissance)
7	ASSET DISCOVERY
7	1. دارایی‌های متحرک (Movable Assets)
8	2. دارایی‌های ثابت (Immovable Assets)
9	ابزارهای مورد استفاده در کشف دارایی‌ها
10	CONTENT DISCOVERY
11	Content Discovery Tools
12	IP ADDRESS DISCOVERY
12	دسته‌بندی ابزارهای کشف و تحلیل IP
14	DNS RECORDS
14	رکوردهای پر کاربرد DNS
16	کاربردهای کلیدی رکوردهای DNS
17	BGP
17	پیش‌نیازهای یادگیری BGP
18	اهمیت پروتکل BGP
19	ابزارهای تحلیل BGP



20	BGP Hijacking تهدید
21	DOMAIN / SUBDOMAIN DISCOVERY
21	دسته‌بندی ابزارهای کشف زیردامنه
24	روش‌های پیشرفته کشف Subdomain
25	EMAIL&Username DISCOVERY
25	ابزارهای کشف Email
26	ابزارهای کشف Username
27	BUSINESS COMMUNICATION
27	INFRASTRUCTURE DISCOVERY
28	SOURCE CODE AGGREGATORS
28	SEARCH - INFORMATION DISCOVERY
29	CLOUD INFRASTRUCTURE DISCOVERY
30	COMPANY INFORMATION AND ASSOCIATIONS
31	INTERNET SURVEY DATA
32	SOCIAL MEDIA \ EMPLOYEE PROFILING
33	DATA LEAKS
35	Archived Information
35	موتورهای جستجوی دستگاه‌های متصل



Introduction

شناسایی (**Recon**) به فرآیند جمع‌آوری اطلاعات درباره یک سازمان، فرد یا سیستم گفته می‌شود. این مرحله یکی از مهم‌ترین مراحل در تست نفوذ، تحقیقات امنیتی و فعالیت‌های مرتبط با امنیت سایبری است. هدف اصلی شناسایی، کشف نقاط ضعف و آسیب‌پذیری‌های احتمالی قبل از حمله یا ارزیابی امنیتی است.

Types of Recon

به طور کلی، شناسایی به دو دسته اصلی تقسیم می‌شود:

1. شناسایی غیرفعال (**Passive Recon**)

در این روش، اطلاعات بدون تعامل مستقیم با هدف جمع‌آوری می‌شود. یعنی هکر یا محقق از طریق منابع عمومی مانند موتورهای جستجو، شبکه‌های اجتماعی، **DNS**، **WHOIS** و سایر ابزارهای **OSINT (Open Source Intelligence)** اطلاعات را استخراج می‌کند.

- مزایا: کم خطر، غیرقابل تشخیص توسط سیستم‌های دفاعی
- معایب: اطلاعات محدودتر نسبت به روش فعال

2. شناسایی فعال (**Active Recon**)

در این روش، اطلاعات با تعامل مستقیم با هدف (مانند اسکن پورت، ارسال درخواست‌های خاص به سرور) جمع‌آوری می‌شود.

- مزایا: اطلاعات دقیق‌تر و جزئی‌تر
- معایب: احتمال تشخیص توسط سیستم‌های امنیتی مانند فایروال و **IDS/IPS**



ACTIVE VS PASSIVE

شناسایی فعال (Active Reconnaissance)

شناسایی فعال به روشی از جمع‌آوری اطلاعات گفته می‌شود که در آن مستقیماً با هدف تعامل صورت می‌گیرد و ردپایی (Footprint) از فعالیت باقی می‌گذارد. این ردپا می‌تواند توسط سیستم‌های امنیتی مانند فایروال‌ها، سیستم‌های تشخیص نفوذ (IDS/IPS) و لگ‌های سرور شناسایی شود.

ویژگی‌های شناسایی فعال:

تعامل مستقیم با هدف: مانند اسکن پورت‌ها، ارسال درخواست‌های خاص به سرور، یا تست آسیب‌پذیری‌ها

کشف جزئیات فنی: مانند شناسایی سیستم عامل (OS)، سرویس‌های فعال، نسخه نرم‌افزارها و نقاط ورود احتمالی

مثال‌های رایج

- استفاده از **Nmap** برای اسکن شبکه
 - اجرای **Nikto** برای بررسی آسیب‌پذیری‌های وب‌سرور
 - تست **Brute Force** روی فرم‌های ورود
- مزایا
- اطلاعات دقیق‌تر و به‌روزتر
 - امکان شناسایی آسیب‌پذیری‌های عمیق‌تر

معایب

- احتمال بالای تشخیص توسط سیستم‌های امنیتی
- ممکن است باعث افزایش سطح حفاظت هدف شود



شناسایی غیرفعال (Passive Reconnaissance)

شناسایی غیرفعال به روشی از جمع‌آوری اطلاعات گفته می‌شود که بدون تعامل مستقیم با هدف انجام می‌شود و هیچ ردپایی از فعالیت باقی نمی‌گذارد. این روش معمولاً اولین مرحله در فرآیند شناسایی است، زیرا هدف را از تحت نظر بودن آگاه نمی‌کند.

ویژگی‌های شناسایی غیرفعال:

عدم تعامل مستقیم: داده‌ها از منابع عمومی (**OSINT**) جمع‌آوری می‌شوند.

تمرکز بر اطلاعات موجود: مانند اطلاعات دامنه، پست‌های شبکه‌های اجتماعی، مستندات عمومی و داده‌های تاریخی

مثال‌های رایج:

◦ جستجوی **Google Dorks** برای یافتن اطلاعات حساس

◦ بررسی **WHOIS** برای مالکیت دامنه

◦ تحلیل پروفایل‌های **LinkedIn** برای شناسایی کارکنان سازمان

مزایا

◦ غیرقابل تشخیص توسط هدف

◦ کم خطر و بدون ریسک شناسایی شدن

معایب

◦ اطلاعات محدود و گاهی قدیمی

◦ نیاز به تحلیل دقیق برای استخراج داده‌های مفید



ASSET DISCOVERY

فرآیند کشف دارایی‌ها (**Asset Discovery**) یکی از مراحل اساسی در ارزیابی امنیتی و تست نفوذ محسوب می‌شود. این مرحله شامل شناسایی تمامی اجزای مرتبط با یک سازمان است که ممکن است در معرض تهدیدات امنیتی قرار گیرند. دارایی‌ها به طور کلی به دو دسته دارایی‌های متحرک (**Movable Assets**) و دارایی‌های ثابت (**Immovable Assets**) تقسیم می‌شوند.

انواع دارایی‌ها در امنیت سایبری

۱. دارایی‌های متحرک (**Movable Assets**)

این نوع دارایی‌ها شامل منابعی هستند که به راحتی قابل جابجایی یا تغییر مکان هستند. این دارایی‌ها معمولاً به صورت فیزیکی یا دیجیتالی وجود دارند و ممکن است در محیط‌های مختلف مورد استفاده قرار گیرند.

مثال‌هایی از دارایی‌های متحرک

- دستگاه‌های همراه مانند لپ‌تاپ‌ها، تلفن‌های هوشمند، تبلت‌ها
- حافظه‌های قابل حمل مانند فلاش‌درایوها، هاردیسک‌های اکسترنال
- توکن‌های امنیتی مانند کلیدهای رمزگاری سخت‌افزاری
- دستگاه‌های IoT قابل حمل مانند دوربین‌های تحت شبکه متحرک

ملاحظات امنیتی

- احتمال سرقت یا گم شدن این دارایی‌ها بیشتر است.
- نیاز به مکانیزم‌های احراز هویت و رمزگاری قوی دارند.
- نظارت بر دسترسی به این دارایی‌ها چالش‌برانگیز است.



۲. دارایی‌های ثابت (Immovable Assets)

این دارایی‌ها معمولاً در مکان ثابتی قرار دارند و جابجایی آن‌ها دشوار یا غیرممکن است. این نوع دارایی‌ها اغلب زیرساخت‌های اصلی یک سازمان را تشکیل می‌دهند

مثال‌هایی از دارایی‌های ثابت:

- سرورهای فیزیکی مانند سرورهای داخلی سازمان
- تجهیزات شبکه مانند روترهای، سوئیچ‌ها، فایروال‌های ثابت
- دیتاسترها و اتاق‌های سرور
- سیستم‌های نصب شده ثابت مانند دوربین‌های مداربسته ثابت

ملاحظات امنیتی:

- معمولاً دارای حفاظت فیزیکی هستند
- نیاز به پایش مداوم وضعیت امنیتی دارند
- به روزرسانی و وصله‌گذاری این سیستم‌ها حیاتی است

فرآیند کشف دارایی‌ها

۱. شناسایی اولیه: تعیین محدوده ارزیابی و جمع‌آوری اطلاعات اولیه

۲. اسکن شبکه: استفاده از ابزارهایی مانند **Nmap** برای شناسایی دستگاه‌های متصل

۳. بررسی سوابق: تحلیل مستندات شبکه و فهرست دارایی‌های موجود

۴. تایید دستی: بازبینی نتایج به صورت دستی برای اطمینان از صحت داده‌ها

۵. مستندسازی: ثبت دقیق تمام دارایی‌های شناسایی شده



ابزارهای مورد استفاده در کشف دارایی‌ها

• برای اسکن شبکه و شناسایی دستگاه‌ها **Nmap**

• برای شناسایی دارایی‌ها و آسیب‌پذیری‌های مرتبط **Nessus**

• برای کشف خودکار دارایی‌های شبکه **Lansweeper**

• برای شناسایی تجهیزات **SolarWinds Network Device Scanner**

شبکه

• برای کشف دستگاه‌های متصل به اینترنت **Shodan**

چالش‌های کشف دارایی‌ها

وجود دستگاه‌های قدیمی که ممکن است در فهرست‌های رسمی ثبت نشده باشند

دستگاه‌های **BYOD (Bring Your Own Device)** که به شبکه متصل می‌شوند

دارایی‌های ابری که ممکن است خارج از کنترل مستقیم سازمان باشند

تغییرات مداوم در پیکربندی شبکه



CONTENT DISCOVERY

پیدا کردن دایرکتوری‌های حساس، البته با گوگل شروع کنید، اگر مشکلی ندارید با اطلاعات آشنا شروع کنید

Extensions

site:<http://example.com> filetype:php
site:<http://example.com> filetype:aspx
site:<http://example.com> filetype:swf
site:<http://example.com> filetype:wsdl

Directory structure

site:<http://example.com> intext:"index of /"

Juicy stuff

site: <http://target.com> filetype:txt
site: <http://target.com> inurl:.php.txt
site: <http://target.com> ext:txt

کشف داده‌ها می‌تواند به هر شکلی از داده باشد، بگذارید چند روش رایج کشف محتوا را بگویم

- **News Discovery Apps and tools**
- **Social Search**
- **Twitter News Discovery**
- **Social news Discovery**
- **Startup And New tools discovery**
- **Video Content Discovery**
- **Content Trends**
- **RSS search Engines**
- **Alerts make use of google alerts**
- **Image Discovery & Search Discovery**



Content Discovery Tools

۱. ابزارهای مبتنی بر دایرکتوری و فایل

این ابزارها برای یافتن فایل‌ها و دایرکتوری‌های پنهان یا حساس استفاده می‌شوند:

- ابزاری ساده برای **brute force** دایرکتوری‌ها و فایل‌ها
- نسخه پیشرفته‌تر با قابلیت‌های بیشتر **Dirbuster**
- ابزاری سریع و کارآمد برای کشف منابع **Gobuster**
- ابزار انعطاف‌پذیر برای تست وب اپلیکیشن‌ها **WFuzz**

۲. ابزارهای کشف زیردامنه

شناسایی زیردامنه‌ها می‌تواند منجر به کشف سیستم‌های کمتر محافظت شده شود:

- ابزاری برای کشف زیردامنه‌ها از منابع عمومی **Sublist3r**
- ابزار پیشرفته برای نقشه‌برداری از زیردامنه‌ها **Amass**
- ابزاری ساده و مؤثر برای کشف دارایی‌ها **Assetfinder**
- ابزاری سریع برای کشف زیردامنه‌ها **Findomain**

منابع جامع ابزارهای کشف محتوا

یکی از منابع مفید برای آشنایی با ابزارهای مختلف، لینک زیر است که مجموعه‌ای گسترده از ابزارهای کشف محتوا را معرفی کرده است

Content Discovery Tools Collection:

content-discovery-tools.zeef.com/robin.good



IP ADDRESS DISCOVERY

کشف و تحلیل آدرس‌های IP یکی از مراحل اساسی در فرآیند شناسایی و ارزیابی امنیتی شبکه‌ها محسوب می‌شود. این فرآیند شامل تبدیل نام دامنه به آدرس IP، بررسی اطلاعات WHOIS، تحلیل مسیریابی BGP و جمع‌آوری اطلاعات مرتبط با زیرساخت شبکه می‌باشد.

دسته‌بندی ابزارهای کشف و تحلیل IP

۱. ابزارهای تبدیل دامنه به IP

IP ابزار جامع برای جستجوی گروهی دامنه و MXToolbox .

IP تبدیل گروهی دامنه به آدرس DomainToIPConverter .

DNS ابزار رفع DNS برای جستجوی گروهی MassDNS .

Dig ابزار آنلاین GoogleApps Dig ارائه شده توسط گوگل .

۲. ابزارهای تحلیل اطلاعات شبکه

IP بررسی دامنه‌ها و آدرس‌های Domain Dossier .

IPv4/IPv6، ASN جستجوی BGPView یا نام منبع .

ASN جستجوی Hurricane Electric BGP Toolkit بر اساس کلمه کلیدی



۳. ابزارهای چندمنظوره

IPViewDNS مجموعه‌ای از ابزارهای مختلف برای دامنه و **IPv6** اطلاعات جامع مربوط به آدرس‌های .

۴. ابزارهای **WHOIS** و جستجوی **DNS**

ابزار خط فرمان برای یافتن اطلاعات ثبت شده منابع اینترنتی **Whois:** .

۵. ابزارهای تحلیل مسیریابی

ارائه‌دهنده مسیریابی اینترنت با تاخیر کم و **BGP (Hurricane Electric)** .

دسترسی به هزاران شبکه

زیرساخت جهانی اینترنت با پشتیبانی **Hurricane Electric IP Transit** .

از **IPv6** و **IPv4**



DNS RECORDS

رکوردهای پر کاربرد DNS

1. رکوردهای اصلی

IPv4 نگاشت نام دامنه به آدرس **A (Host Address)** .

IPv6 نگاشت نام دامنه به آدرس **AAAA (IPv6 Host Address)** .

رکوردي که به صورت خودکار به رکورد **A/AAAA** تبدیل می شود **ALIAS** .

ایجاد نام مستعار برای یک دامنه **CNAME (Canonical Name)** .

مشخص کننده سرورهای ایمیل برای دامنه **MX (Mail Exchange)** .

تعیین سرورهای **DNS** مسئول برای دامنه **NS (Name Server)** .

Reverse DNS نگاشت معکوس IP به نام دامنه برای **PTR (Pointer)** .

DNS اطلاعات پایه درباره منطقه **SOA (Start of Authority)** .

مشخص کننده موقعیت سرویس های خاص **SRV (Service)** .

اطلاعات متنی (اغلب برای تأیید مالکیت یا امنیت) **TXT (Text)** .

2. رکوردهای مربوط به DNSSEC

DNSSEC کلید عمومی برای احراز اصالت **DNSKEY** .

DNS اطلاعات تأیید بین مناطق **DS (Delegation Signer)** .

اثبات عدم وجود رکورد خاص **NSEC/NSEC3** .

امضای دیجیتال برای **RRSIG (Resource Record Signature)** .

رکوردها



۳. رکوردهای تخصصی

AFS موقعیت پایگاه داده **AFSDB** .

ATM آدرس **ATMA** .

CAA تعیین مراجع صدور گواهی مجاز

CERT ذخیره گواهی‌های **SSL/TLS** .

DHCID اطلاعات **DHCP** .

DNAME تغییرنام غیرترمینال در **DNS** .

HINFO اطلاعات سختافزاری/نرمافزاری میزبان .

ISDN آدرس **ISDN** .

LOC اطلاعات جغرافیایی .

NAPTR تبدیل نام به **URI** یا دیگر شناسه‌ها .

TLSA احراز اصالت **TLS** .



کاربردهای کلیدی رکوردهای DNS

۱. مدیریت ترافیک شبکه

A/AAAA مسیریابی درخواستها

CNAME ایجاد نامهای مستعار

MX مدیریت سرورهای ایمیل

۲. امنیت و احراز هویت

DNSSEC Records جلوگیری از حملات جعل

DMARC , DKIM , SPF TXT ذخیره اطلاعات

CAA کنترل مراجع صدور گواهی

۳. سرویس‌دهی تخصصی

SRV شناسایی سرویس‌های خاص

NAPTR تبدیل پروتکل‌ها و شناسه‌ها

نکات فنی مهم

۱. resolver مدت زمان کش شدن رکورد TTL (Time To Live) را تعیین می‌کند.

۲. تقدم MX عدد اولویت در رکورد MX هرچه کمتر، مهم‌تر

۳. DNSSEC Chain of Trust ارتباط سلسله مراتبی رکوردهای امنیتی

۴. رکوردهای ترکیبی: امکان استفاده همزمان از چند رکورد برای یک دامنه

توجه: تنظیم صحیح رکوردهای DNS برای عملکرد بهینه شبکه و سرویس‌ها ضروری است.

خطا در تنظیمات می‌تواند منجر به اختلال در دسترسی به سرویس‌ها شود.



پیش‌نیازهای یادگیری BGP

۱. درک پروتکل TCP

پروتکل لایه **trasnport** که ارتباط قابل اطمینان بین دستگاهها ایجاد می‌کند

- ویژگی‌های کلیدی:

- ارتباط اتصال‌گرا (**Connection-oriented**)

- تضمین تحويل داده‌ها (با استفاده از تصدیق‌ها)

- کنترل ازدحام و جریان داده

- رابطه با **BGP**: **BGP** از **TCP** برای ارتباط بین روترهای استفاده می‌کند

۲. مفهوم Peering

- همتاگذاری (**Peering**) ارتباط مستقیم بین سیستم‌های مستقل (**AS**)

- انواع

- از طریق اتصال مستقیم خصوصی (**Private Peering**)

- از طریق نقاط تبادل اینترنت (**IXPs**)

- مزايا

- کاهش هزینه‌های ترانزیت

- بهبود عملکرد شبکه

- افزایش افزونگی



3. خطای RIB (Routing Information Base)

- پایگاه داده‌ای که تمام مسیرهای شناخته شده را نگهداری می‌کند
- **RIB Failure** هنگامی رخ می‌دهد که
 - ظرفیت پردازشی روتر کافی نباشد و تعداد پیشوندهای دریافتی از حد مجاز بیشتر شود همچنین مشکلات حافظه روتر وجود داشته باشد
- تأثیرات: ممکن است منجر به از دست دادن مسیرها یا ناپایداری **routing** شود

اهمیت پروتکل BGP

1. نقش BGP در اینترنت

- پروتکل دروازه مرزی: پروتکل مسیریابی بین دامنه‌ای (**EGP**)
- کاربرد اصلی: تبادل اطلاعات مسیریابی بین سیستم‌های مستقل (**AS**)
 - سیاستمحور (**Policy-based**)
 - مسیریابی **path-vector**
 - مقیاس‌پذیری بالا

2. دلایل حیاتی بودن BGP

1. ستون فقرات اینترنت: بیش از ۹۰٪ مسیریابی اینترنت روی **BGP** انجام می‌شود
2. انعطاف‌پذیری: مکان اعمال سیاست‌های پیچیده مسیریابی
3. تحمل خطا: مکانیزم‌های بازیابی خودکار
4. توزیع ترافیک: امکان **load balancing** بین مسیرهای مختلف



ابزارهای تحلیل **BGP**

ابزار **BGP-recon**

bgp-recon .

• کاربردها:

◦ جمع آوری اطلاعات توپولوژی **BGP**

◦ شناسایی تغییرات مسیریابی

◦ تحلیل همتاگذاری‌ها

◦ قابلیت‌های کلیدی

◦ پایش تغییرات **RIB**

◦ شناسایی ناهنجاری‌های مسیریابی

◦ تولید گزارش‌های تحلیلی



تهدید BGP Hijacking

1. مفهوم BGP Hijacking

• تعریف: اعلام مسیرهای جعلی به منظور انحراف ترافیک

• انواع

◦ اعلام مالکیت IP متعلق به دیگران ادعای Prefix Hijacking

◦ اعلام پیشوندهای جزئی Subprefix Hijacking

◦ دستکاری مسیر اعلام شده AS Path Hijacking

2. نمونه‌های واقعی سال‌های اخیر

• حملات به YouTube (2008) انحراف ترافیک به پاکستان

• حمله به Amazon Route 53 (2018) سرقت ارز دیجیتال

• حمله به روسیه (2017) انحراف ترافیک مالی

3. راهکارهای مقابله

1. RPKI (Resource Public Key Infrastructure)

◦ سیستم اعتبارسنجی مبتنی بر رمزنگاری

2. BGP Monitoring Tools

◦ ابزارهایی مانند ARTEMIS و BGPStream

3. فیلتر پیشوندها

◦ اعتبارسنجی پیشوندهای اعلام شده



DOMAIN / SUBDOMAIN DISCOVERY

کشف دامنه‌ها و زیردامنه‌ها مرحله حیاتی در تست نفوذ و ارزیابی امنیتی است. این فرآیند به شناسایی سطح حمله (Attack Surface) کمک می‌کند. ابزارهای مختلفی برای این منظور توسعه یافته‌اند که هر کدام روش‌های متفاوتی را به کار می‌گیرند.

دسته‌بندی ابزارهای کشف زیردامنه

۱. ابزارهای شمارش پیشرفته

SubFinder .

- ابزار کشف غیرفعال زیردامنه
- مناسب برای برنامه‌های باگ بانتی
- طراحی شده برای تست نفوذ ایمن

Amass .

- ابزار جامع شمارش زیردامنه
- ترکیبی از تکنیک‌های brute force و OSINT
- قابلیت نقشه‌برداری از شبکه

Sublist3r .

- جمع‌آوری زیردامنه‌ها از منابع مختلف
- پشتیبانی از موتورهای جستجو و API ها
- خروجی قابل یکپارچه‌سازی با ابزارهای دیگر



2. ابزارهای **Brute Force**

Aiodnsbrute .

DNS brute force .

- عملکرد سریع با استفاده از برنامه نویسی ناهمگام

- قابلیت تنظیم نرخ درخواست

GoBuster .

ابزار چندمنظوره برای **brute force** .

VHost ، دایرکتوری و **DNS** پشتیبانی از .

نوشته شده در زبان **Go** .

3. ابزارهای تحلیل گواهی **SSL**

crt.sh .

SSL جستجوی دامنه ها از طریق گواهی های .

(**Certificate Transparency**) استفاده از شفافیت گواهی .

Ct-exposer .

CT کشف زیردامنه ها از طریق لاغ های .

شناسایی دامنه های جدید و تغییرات .

Certgraph .

تحلیل گراف نامهای جایگزین گواهی .

شناسایی ارتباط بین دامنه ها .



4. ابزارهای تخصصی DNS

LDNS .

◦ کتابخانه DNS برای توسعه ابزارها

◦ قابلیت‌های پیشرفته DNS query

Dns-nsec3-enum .

◦ اسکریپت NSE برای NSEC3 walking

◦ مفید برای شناسایی زیردامنهای مناطق امن DNSSEC

Nsec3map .

◦ ابزار تخصصی برای NSEC/NSEC3 walking

◦ شناسایی تمام نامهای موجود در منطقه

5. منابع داده عمومی

Project Sonar .

◦ داده‌های DNS مستقیم و معکوس

◦ منبع ارزشمند برای شناسایی دارایی‌ها

Wolframalpha .

◦ موتور دانش محاسباتی

◦ ارائه اطلاعات جانبی درباره دامنه‌ها



روش‌های پیشرفته کشف Subdomain

۱. شمارش ترکیبی

Amass + SubFinder استفاده همزمان از چند ابزار مثلاً

- ترکیب نتایج و حذف موارد تکراری

- افزایش پوشش کشف زیردامنه‌ها

۲. تحلیل عمیق گواهی‌ها

- استخراج نام‌های جایگزین از گواهی‌های SSL

- ردیابی تغییرات در طول زمان

- شناسایی ارتباط بین دامنه‌های مختلف یک سازمان

۳. تکنیک‌های NSEC Walking

- استفاده از ضعف طراحی در DNSSEC

- بازیابی تمام رکوردهای منطقه

- نیاز به تنظیمات خاص DNS



EMAIL&Username DISCOVERY

ابزارهای کشف Email

1. جستجوی پیشرفته (Google Dorks)

استفاده از عملگرهای جستجوی گوگل برای یافتن آدرس‌های ایمیل مرتبط با دامنه خاص

2. ابزارهای تخصصی ایمیل یابی

Hunter .

- سرویس جستجوی ایمیل‌های مرتبط با دامنه‌ها

- ارائه اطلاعات تماس سازمانی

Skrapp .

- افزونه مرورگر برای استخراج ایمیل‌ها از پروفایل‌های LinkedIn

- مناسب برای تحقیقات کسب‌وکار

Email Extractor .

- اکستنشن کروم برای استخراج خودکار ایمیل‌ها از صفحات وب

- پردازش صفحات بازدید شده

Convertcsv .

- ابزار آنلاین استخراج ایمیل از متن، صفحات وب و فایل‌های داده

- پشتیبانی از فرمتهای مختلف خروجی



ابزارهای کشف Username

1. ابزارهای مبتنی بر LinkedIn

linkedin2username .

- تولید لیست نامهای کاربری احتمالی بر اساس پروفایل‌های کارمندان در LinkedIn

OSINT استفاده در تحقیقات

2. ابزارهای شمارش کاربران

Office365UserEnum .

- شمارش کاربران معتبر در سرویس Office 365

- استفاده از پروتکل ActiveSync برای تأیید وجود حساب‌ها



BUSINESS COMMUNICATION INFRASTRUCTURE DISCOVERY

ابزارهای کلیدی

MXToolbox .1

- بررسی رکوردهای **MX** و وضعیت سرورهای ایمیل
- تشخیص مشکلات تحویل ایمیل

MicroBurst .2

- اسکریپتهای پاورشل برای ارزیابی امنیتی **Azure**
- شناسایی تنظیمات ناامن در محیط ابری

LyncSmash .3

- ابزار شمارش و تست امنیتی **Lync/Skype for Business**
- شناسایی آسیب‌پذیری‌های سیستم‌های میزبانی شده داخلی

Enumeration-as-a-Service .4

- شمارش سرویس‌های **SaaS** از طریق کوئری‌های **DNS**
- شناسایی سرویس‌های ابری مورد استفاده سازمان

Ruler .5

- ابزار تست امنیتی سرویس **Exchange**
- شناسایی و سوءاستفاده از آسیب‌پذیری‌های احتمالی



SOURCE CODE AGGREGATORS

SEARCH - INFORMATION DISCOVERY

کشف کد منبع و اطلاعات فنی

پلتفرم‌های جستجوی کد

1. GitHub Advanced Search جستجوی پیشرفته در مخازن عمومی

GitHub

2. Bitbucket Search یافتن پروژه‌ها در Bitbucket با استفاده از

عملگرهای گوگل

3. GitLab Search جستجو در پروژه‌های عمومی GitLab

ابزارهای تخصصی

• Gitrob ابزار شناسایی سازمان‌های GitHub و تحلیل مخازن

• PublicWWW موتور جستجوی کد منبع در وبسایت‌ها

• BuiltWith شناسایی تکنولوژی‌های استفاده شده در وبسایت‌ها

نکته: این ابزارها برای تحقیقات امنیتی و کشف اطلاعات حساس احتمالی در کدهای عمومی مفید هستند.



CLOUD INFRASTRUCTURE DISCOVERY

CloudScraper .1

DigitalOcean , Azure Blobs , S3 ◦ شناسایی منابع ابری با

◦ کراولینگ خودکار و بسایتها

InSp3ctor .2

AWS , S3 ◦ جستجوی سطوح و اشیاء در

◦ کشف باکت‌های در معرض خطر

Grayhatwarfare .3

S3 ◦ موتور جستجوی باکت‌های باز

◦ نمایش محتوای عمومی باکت‌ها

Spaces-finder .4

DigitalOcean Spaces ◦ شناسایی های عمومی

◦ کشف منابع ذخیره‌سازی در معرض خطر

GCPBucketBrute .5

Google Cloud Storage ◦ شمارش باکت‌های

◦ تشخیص تنظیمات نادرست دسترسی

CloudStorageFinder .6

◦ جستجوی داده‌های عمومی در سیستم‌های ذخیره‌سازی ابری

◦ پشتیبانی از پلتفرم‌های مختلف



COMPANY INFORMATION AND ASSOCIATIONS

Crunchbase .1

- پایگاه داده تخصصی اطلاعات شرکتها
- شامل تاریخچه تأمین مالی، ادغامها و تصاحبها
- مثال: پیگیری تصاحب واتس‌اپ توسط فیسبوک

Companies House .2

- سامانه رسمی ثبت شرکت‌های بریتانیا
- دسترسی به اسناد قانونی و اطلاعات مالی

Overseas Registries .3

- فهرست جهانی سامانه‌های ثبت شرکت
- دسترسی به داده‌های شرکتی بین‌المللی

OpenCorporates .4

- بزرگترین پایگاه داده باز شرکتی جهان
- پوشش بیش از **200** میلیون شرکت ثبت‌شده



INTERNET SURVERY DATA

منابع اصلی داده‌های تحقیقاتی

Project Sonar . 1

- مجموعه داده‌های حاصل از اسکن‌های اینترنت‌گستر
- پوشش سرویس‌ها و پروتکل‌های مختلف
- شامل داده‌های **SSH**، **SSL**، **HTTP**، **DNS** و

Scans.io (ZMap) . 2

- مخزن داده‌های اسکن گسترده اینترنت
- حاوی نتایج اسکن پورت‌ها و سرویس‌ها
- پشتیبانی از فرمتهای مختلف داده

Portradar . 3

- داده‌های اسکن پورت رایگان و متن باز
- اطلاعات به روز از وضعیت پورت‌های عمومی
- قابلیت جستجوی پیشرفته بر اساس معیارهای مختلف



SOCIAL MEDIA \ EMPLOYEE PROFILING

ابزارهای تخصصی تحقیقات اجتماعی

۱. ابزارهای شبکه‌های حرفه‌ای

LinkedIn .

- اسکریپر پیشرفته برای جمع‌آوری اطلاعات از **LinkedIn**

- استخراج پروفایل‌های کارکنان و ساختار سازمانی

Glassdoor .

- پایگاه داده نظرات و ارزیابی‌های شرکت‌ها

- اطلاعات حقوق و مزايا، فرهنگ سازمانی و نظرات کارکنان

۲. ابزارهای تحلیل رسانه‌های اجتماعی

SocialBlade .

- ردیابی آمار کاربران در یوتیوب، توییتر و دیگر پلتفرم‌ها

- تحلیل رشد فالوورها و تعاملات

Social-Searcher .

- موتور جستجوی یکپارچه رسانه‌های اجتماعی

- پوشش چندین پلتفرم شامل توییتر، فیسبوک و ردیت

۳. ابزارهای تأیید هویت

Checkuser .

- بررسی وجود کاربر در پلتفرم‌های مختلف

- تأیید یکپارچگی اطلاعات پروفایل‌ها



DATA LEAKS

پایش خودکار پایگاههای انتشار موقت

۱. سیستم‌های مانیتورینگ عمومی

Dumpmon .

- ربات توییتری ردیاب دامپ‌های اطلاعاتی
- پایش چندین سایت پیست (**Paste sites**) برای کشف پسوردها و اطلاعات حساس

Pastebin_scaper .

- ابزار خودکار مانیتورینگ
- شناسایی محتوای حاوی اطلاعات مهم

Scavenger .

- کراولر تخصصی سایت‌های پیست
- تمرکز بر کشف اعتبارنامه‌های لو رفته

۲. ابزارهای جستجوی پیشرفته

Pwnbin .

- کراولر پایتونی برای
- جستجوی هوشمند بر اساس کلمات کلیدی

PwnedOrNot .

- ابزار بررسی پسوردهای افشاشه
- تأیید وجود حساب‌های کاربری به خطر افتاده



3. پایگاه‌های داده عمومی

HavelBeenPwned.com .

◦ سرویس معتبر بررسی نشت اطلاعات

◦ پوشش گسترده دیتابیس‌های لو رفته

GhostProject.fr .

◦ پایگاه داده جایگزین برای بررسی نشت‌ها

◦ ارائه نتایج تکمیلی نسبت به سرویس‌های دیگر



Archived Information

منابع داده آرشیو شده

Cachedviews . 1

◦ نمایش نسخه‌های کش شده صفحات از منابع مختلف

◦ امکان مشاهده محتوا حذف شده یا تغییر یافته

Wayback Machine . 2

◦ آرشیو اینترنت با بیش از **468** میلیارد صفحه ذخیره شده

◦ قابلیت بازبینی تغییرات وبسایت‌ها در طول زمان

موتورهای جستجوی دستگاه‌های متصل

Shodan . 3

◦ موتور جستجوی تخصصی دستگاه‌های متصل به اینترنت

◦ شناسایی سیستم‌های **ICS** ، دوربین‌ها، سرورها و دستگاه‌های **IoT**

Censys . 4

◦ پلتفرم تحلیل دارایی‌های اینترنتی

◦ ارائه داده‌های **SSL/TLS** ، گواهی‌ها و پیکربندی‌های شبکه

Zoomeye . 5

◦ موتور جستجوی فضای سایبری

◦ پوشش گسترده دستگاه‌های چینی و بین‌المللی

