مبانی رایانش امن
قدم‌های هک

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

امنیت در پشتهٔ پروتکل شبکه

لایه فیزیکی
- محدود کردن شنود سیم با روکش‌های پرس شده با گاز ساکن خطوط انتقال
- تلاش برای باز کردن خروج گاز و کاهش فشار و شلیک هشدار

لایه پیوند داده
- پیوند نقطه به نقطه
- رمزگذاری در حین خروج و کشف در حین ورود.
- خطر در گشایش در هر مسیریاب
- رمزگذاری پیوند

لایه شبکه
- دیوارآتش جهت ممانع از حمله ورود و خروج ترافیک به شبکه
- IPsec: پروتکلی برای امنیت IP که محمولهٔ بسته‌ها را رمز می‌کند.

لایه انتقال
- رمز کل انتها به انتهای اتصالات (یا متناظرا فرایند به فرایند)

لایه کاربرد
- حل مسائلی چون احراز هویت کاربر و عدم‌انکار
- امکان انجام احراز هویت در لایه‌های پایین‌تر (شبکه‌های بی‌سیم)

- مشکل ضمانت امنیت
- در عوض بهبود امنیت به میزانی اعمال اصول امنیت
- تدوین اصول امنیت در سال ۱۹۷۵ به وسیلهٔ جرومی سالتزر و مایکل شروءدر
  - اصل سازوکار مقتصدانه یا اصل سادگی
    - سیستم پیچیده دارای اشکلات بیشتر از سیستم ساده‌تر
    - راحتی فهم کاربر از آن
    - کاهش سطح حمله attack surface
  - اصل پیش‌فرض‌های شکست ایمن
    - ایمن‌تر بودن فرض عدم اجازه
  - اصل تامل کامل
    - بررسی اجازهٔ هر دسترسی به هر منبع
    - داشتن روش معین‌کردن منبع درخواست
  - اصل کمترین اجازه معروف به POLA
    - دسترسی در حد انجام وظیفه و نه بیشتر
  - اصل جدایی اعتبار
    - دسته‌بندی اجازه‌ها
  - اصل کمترین سازوکار مشترک
    - مانند متغیر محلی در مقابل سراسری. مورد مقدم معتبر است
  - اصل طراحی باز
    - براساس سخنان کرکهوف سیستم‌رمز بایدد امن باشد حتی اگر همه سیستم به جز کلید را بشناسند.
    - عدم تکیه بر امنیت با ابهام و مخفی‌کاری یا نامعلوم گذاشتن
  - اصل قابل‌قبولی روانی
    - سادگی کاربرد و فهم سازوکارها و قواعد امنیت

امنیت شبکه ترکیبی از مفهوم‌های در دامنه کاربرد و مهندسی و مفاهیمی ریشه در نظریه، ریاضی و رمزنگاری

پینگ مرگ

- استفاده از گزینه قطعه سازی IP جهت شکستن اکوی ICMP بزرگتر از بیشترین اندازه مجاز بسته IP
- عدم پیش‌بینی بسته‌های چنین بزرگ در هدف
- رونویسی روی داده‌های دیگر در بافر
- سرریز بافر

اصول بنیادی حمله

جهت حفاظت بیشتر نیاز به فهم نحوه حمله

۱- شناسایی Reconnaissance

- اولین گام مهاجم داشتن دانش هر چه بیشتر از هدف
- در صورت داشتن برنامه حمله با استفاده از اسپم یا مهندسی اجتماعی: نیاز به اختصاص زمان به چهره‌نماهای برخط افرادی هدف
- فنی
  - به چه ماشین‌هایی از بیرون دسترسی داریم
  - استفاده از کدام پروتکل
  - شناخت توپولوژی شبکه
  - شناخت خدمات در حال کار در هر ماشین

اصول بنیادی حمله

۲- بوکشیدن و جاسوسی Sniffing and Snooping

- ادراک بسته‌های شبکه
- بدون رمز داده‌های مهم و حتی داده‌های رمزشده جهت یافتن نشانی MAC عناصر در ارتباط

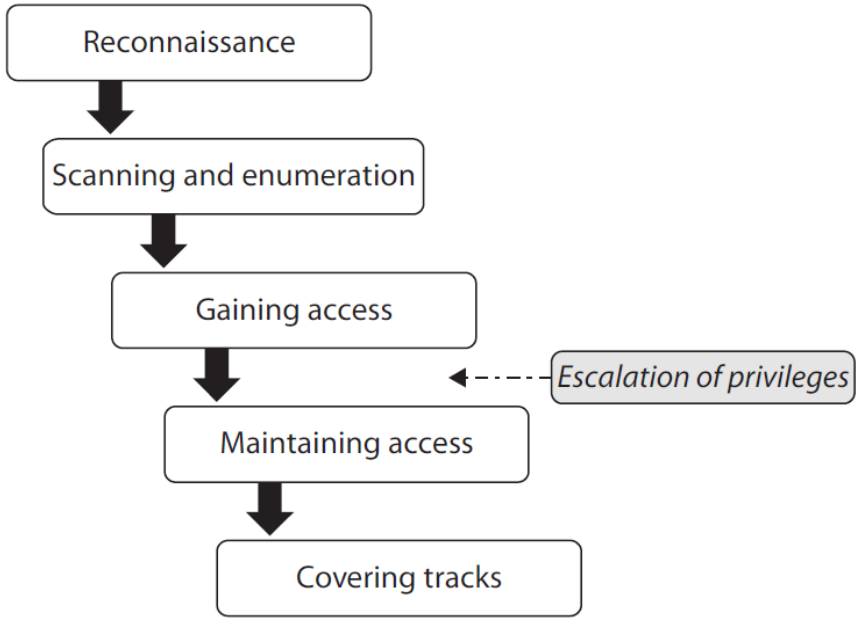
۳- جعل spoofing

- ترافیک جعلی شبکه به منزلهٔ منشا از ماشینی دیگر
- ارسال قاب اترنت یا بسته آی‌پی با نشانی مبدا متفاوت
  - جهت عبور کردن از دفاع یا انجام حملات بندآوری خدمت
  - دلیل امر سادگی چنین پروتکل‌هایی

۴- برهم‌زدن Disruption

- بندآوری خدمت

نوع دیگر از مراحل و فازهای حمله



شناسایی
- تعقیب ردپا

اسکن و شمارش

دستیابی به دسترسی

نگهداری دسترسی

دوری از تعقیب

شناسایی

استیلای درنده بر جونده

دزدی

دستگیری
- ردپاگیری

مدرن و جستجو

انجام درست کار
- یادگرفتن چگونگی جمع‌آوری اطلاع از هدف پیش از تلاش بر حمله بر وی

در پی دو پرسش
- به دنبال چه اطلاعی
- چگونگی جمع‌آوری چنین اطلاعی

شناسایی

به دنبال هر اطلاع دیددهنده از هدف

- عدم لزوم فنی بودن داده
- اطلاعات سطح بالای معماری شبکه
  - مسیریاب‌ها و سرورها
- کاربردها و تارمانه‌ها
- امنیت فیزیکی
  - ورود
  - رویه‌های روزانهٔ کارمندان
- همچنین
  - کارکردهای فیاوری اساسی
  - دارایی‌های مجازی کلیدی
  - اطلاعات حساس سازمان
  - اطلاع از کارمندان

سادگی نسبی جمع‌آوری چنین اطلاعاتی

شناسایی

ردپاگیری

- غالبا منفعلانه
- دردسترسی آزادانه اطلاعات

ردپا ناشناس

ردپا شبه ناشناس

مزایای ردپاگیری

- فهم وضعیت و حالت امنیتی
- کاهش ناحیهٔ تمرکز
- آشکاری آسیب‌پذیری‌ها
- رسم نقشهٔ شبکه

شناسایی

ردپاگیری

- فعال در مقابل منفعل
- دسترسی مستقیم به منابع در مقابل جمع‌آوری از منابع عموما در دستری
- منفعل
  - اطلاعات رقابتی Competitive intelligence
  - موتور جستجو
  - پیگیری رسانه‌های جمعی
  - آشغال‌گردی Dumpster Diving
  - دست‌یابی به بازه شبکه
  - بررسی DNS

شناسایی

فعال

- مهندسی اجتماعی
- تعاملات انسانی
- هر مورد نیازمند به تهامل نفوذگر با سازمان
- به معنای در معرض دید قرار دادن تلاش کشف نفوذگر

شناسایی- مهندسی اجتماعی

ساده و خام به نظر آمدن

هنر دوست‌یابی!

وجود کتاب در این مورد

مهندسی اجتماعی

- مهندسی اجتماعی social engineering
  - روش غیرفنی نفوذ به سیستم یا شبکه
  - فرایند فریب کاربران سیستمی
    - ترغیب آنان به افشای اطلاعاتی که منجر به شکست یا تحویل سازوکار امنیت
    - به منظور فریب آنها به انجام عملی که منجر به پیاده‌کردن بدافزار
    - معمولا بدون اینکه شخص افشاکننده متوجه شود
- مورد استفاده جهت جمع‌آوری اطلاعات قبل یا حین حمله

مهندسی اجتماعی

- استفاده از تلفن یا اینترنت
  - جهت فریب افراد به آشکارکردن اطلاعات حساس
  - یا متعاقدسازی افراد به انجام عملی منافی سیاسات امنیتی سازمان
- اعتقاد به ضعیف بودن افراد در امنیت
- خطر عمدهٔ آن
  - با وجود فرایندهای احرازهویت، دیواره‌های آتش، شبکه‌های مجازی خصوصی، نرم‌افزارهای نظارت شبکه
  - مهندسی اجتماعی موجبات محل اعراب نداشتن هیچ یک و تعقیب عامل انسانی در سازمان

مهندسی اجتماعی

- تکیه بر کنجکاوی و طمع و زودباوری و ترس بشر
- کوین میتنیک
  - بدست آوردن اطلاعات بدون فناوری‌های پیچیده
  - کوید ۱۹ و نقشه‌ها
  - کتاب سازمان بهداشت جهانی
-

مهندسی اجتماعی

- انواع مهندسی اجتماعی
  - انسان‌محور
    - تعاملات انسان با انسان جهت دستیابی به اطلاع مقصود
    - تماس و تلاش برای یافتن رمز
  - رایانه‌محور
    - استفاد از نرم‌افزارهای رایانه‌ای جهت بازیابی اطلاعات مقصود
    - ارسال ایمیل و درخواست وارد کردن دوبارهٔ رمز در تارنامه
      - طله‌گذاری **phishing**

مهندسی اجتماعی انسان‌محور

دسته‌بندی

- تظاهر به کاربر یا کارمند معتبر
  - خدمات،کارمند یا پیمان‌کار
- وانمود به کاربر مهم
  - مدیر اجرایی یا مدیر میانی و نیازمند فوری به اطلاعات
  - ارعاب کارمند سطح پایین
  - عدم پرسش از کارمند سطح بالا
- استفاده از شخص ثالث
  - وانمود به داشتن اجازه از منبع مجاز
  - کارآمد هنگام در سفر بودن منبع مجاز یا عدم امکان تاییدگیری از وی
- تماس با پشتیبان فنی
- تقلب از روی دست shoulder surfing، بررسی اطلاعات دیرریخته شده

مهندسی اجتماعی وارون

جازدن نفوذگر به عنوان صاحب موقعیت و اجازه

پرسش کارمندان از نفوذگر

خود را پشتیبان فنی جا زدن

مهندسی اجتماعی رایانه‌محور

شامل

- پیوست‌های ایمیل
- تارمانه‌های جعلی
- پنجره‌های پاپ‌آپ

مهندسی اجتماعی

گمان بر حملهٔ عامل خارجی
- حملات داخلی

بیشترین خطرات به نهادهای فیاوری درون‌سازمانی
- کارمندان نهاد مالی دزدی پول بیشتر نسبت به رباینده‌گان بانک

در صورت نیافتن روش نفوذ
- استخدام کارمند یا پیدا کردن کارمند ناراضی جهت دستیاری در حمله
- روشی قدرتمند
- دسترسی کارمند به اطلاعات محرمانه
- رویه‌های امنیتی ضعیف
  - امکان بررسی اطلاعات بدون گذاشتن ردی از خود
- خودی‌ها محتملا منبع حملهٔ سایبری نسبت به خارجی‌ها
  - لزوما نه برای جرم خودشان بلکه عامل پخش ناآگاهانهٔ اطلاعات

طله‌گزاری

- طله‌گذاری PHISHING
  - هرگونه تلاش برخط، فریبندهٔ شخصی ثالث
  - جهت دست یافتن به اطلاعات محرمانه یا سود مالی
  - معمولا بدون کد مخرب بلکه مبنی بر فنون و روش‌های مهندسی اجتماعی
  - نامهٔ نیجریه‌ای

طله‌گزاری

- طله‌گذاری کلاهبرداری ایمیلی فیاوری
  - نوعی از نامه نیجریه‌ای
  - معرفی خود به عنوان کارمند رتبه بالاتر در شرکت و در خواست از کارمند سطح پایین جهت انتقال مبلغ به حساب کلاهبرداری
  - طبق گزارش پلیس فدرال سرقت سه میلیون دلار در طول سه سال تا ۱۳۹۶
- طله‌گزاری نیزه
  - وانمود کردن به جای پی‌پل و ای‌بی و امثالهم و جهت اعتبار حساب
  - کنترل بر پیوند هدایت به مانه‌ای تحت کنترل کلاهبردار و مجبور به افشای اطلاعات شخصی و محرمانه
- تکیهٔ طله‌گذار بر فنون شیادی
  - اما استفاده از ایمیل
  - معمولا ایجاد تارمانه‌ای که شبیه نهاد مالی معتبر و کلک زدن جهت وارد کردن اطلاعات مالی
    - یا بارگذاری بدافزاری بر رایانه قربانی
    - استفاده جهت کلاهبرداری هویتی و دزدی
    - دزدی هویت

طله‌گزاری

- تغییر رمز گوگل
  - دستیابی به حساب معاون هیلاری کلینتون و دیگر اعضای کمیته ملی دمکرات
- طبق گزارش ورایزن
  - باز شدن ۳۰ درصد ایمیل‌ها
  - کلیک شدن پیوست دوازده درصد آنها
- مبارزه با طله
  - DMARC
  - موفقیت آن در سال‌های گذشته

مقابله با مهندسی اجتماعی

سیاسات امنیتی اجباری و مستند شده

برنامه‌های آگاهی-افزایی امنیتی

برگزاری دوره‌های هم‌افزایی

- تحلیل زمان پایان فرایند
- تغییر رمزها
- ازبین بردن کاغذ
- محدودیت‌های دسترسی فیزیکی
- آموزش نحوه نگهداری اطلاعات محرمانه
- گزارشات ماهانه آگاهی‌بخشی امنیتی

- مزیت
  - عدم تعهد پاسخگویی کارمند در موارد امنیتی در قبال تماس

ردپایابی روش‌ها و ابزارها

موتورهای جستجو

منبع ردگیری

در صورت استفاده درست عدم هشدار به هدف

نقشه-گوگل، نقشه-بینگ، نقشه-زمین

Netcraft

- حتی گاهی اوقات اطلاعات سیستم عامل

گوگل

- جانی لانگ در ۱۳۸۳
- توجه به چگونگی کار با رشته‌های جستجو در گوگل
- عملگرهای اضافی در موتور جستجو جهت تسهیل دقت مناسب رشته جستجو
  - استفاده از چنین منطقی جهت اهداف نفوذ

ردپایابی روش‌ها و ابزارها

موتور جستجو

- یافتن سیستم‌های استفاده کننده از اتصالات راه دور
- یافتن چند نمایش تاریخ MySQL جهت رهگیری چند رمز
- نفوذ گوگل Google Hacking
- استفاده از رشته جستجو با چند عملگر اضافه جهت جستجو آسیب‌پذیری‌ها
- وجود مانه‌های فراوان برای رشته جستجو

ردپایابی روش‌ها و ابزارها

allinurl:tsweb/default.htm

؟

به دنبال صفحات با TSWEB در URL

- نمایش صفحه دسترسی از راه‌دور

صرفا آنهایی که پیش‌فرض صفحه HTML استفاده می‌کنند

ردپایابی روش‌ها و

- تمرین جستجوی هر چه بیشتر «نفوذ گوگل»

Operator	Syntax	Description
filetype	filetype:*type*	Searches only for files of a specific type (DOC, XLS, and so on). For example, the following will return all Microsoft Word documents: `filetype:doc`
index of	index of */string*	Displays pages with directory browsing enabled, usually used with another operator. For example, the following will display pages that show directory listings containing *passwd*: `"intitle:index of" passwd`
info	info:*string*	Displays information Google stores about the page itself: `info:www.anycomp.com`

intitle	intitle:*string*	Searches for pages that contain the string in the title. For example, the following will return pages with the word *login* in the title:
		`intitle: login`
		For multiple string searches, you can use the allintitle operator. Here's an example:
		`allintitle:login password`

inurl	inurl:*string*	Displays pages with the string in the URL. For example, the following will display all pages with the word *passwd* in the URL:
		`inurl:passwd`
		For multiple string searches, use allinurl. Here's an example:
		`allinurl:etc passwd`

link	link:*string*	Displays linked pages based on a search term.
related	related:*webpagename*	Shows web pages similar to *webpagename*.
site	site:*domain or web page string*	Displays pages for a specific website or domain holding the search term. For example, the following will display all pages with the text *passwds* in the site anywhere.com: `site:anywhere.com passwds`

ردپایابی روش‌ها و ابزارها

- تمرین جستجوی هر چه بیشتر «نفوذ گوگل»

امکان استفاده در گستره‌ای وسیع از اهداف

- مثال- یافتن پیاده کردن (دانلود) رایگان موسیقی
- "intitle:index of" nameofsong.mp3
- یافتن آسیب‌پذیری‌های باز روی شبکه
  - مثال- یافتن نتایج پویش و اسکن آسیب‌پذیری با استفاده از Nessus
  - "intitle:Nessus Scan Report" "This file was generated by Nessus"
- امکان استفاده برای VoIP و VPN
  - امکان استفاده از VoIP از Trivial FTP (TFTP) بدون ایمنی
- جستجوی "login," یا "login page," یا "welcome" در عملگر "intitle:"
- استفاده از "D-Link VIP Router" برای پرتال مسیریاب D-Link
- استفاده از "SPA504G" برای آسان‌سازی‌های پیکربندی سیسکو

استفاده گاه به گاه گوگل از کپچا

- امکان استفاده از موتور جستجوهای دیگر

جستجوی پیشرفته

ردپایابی روش‌ها و ابزارها

شدان Shodan

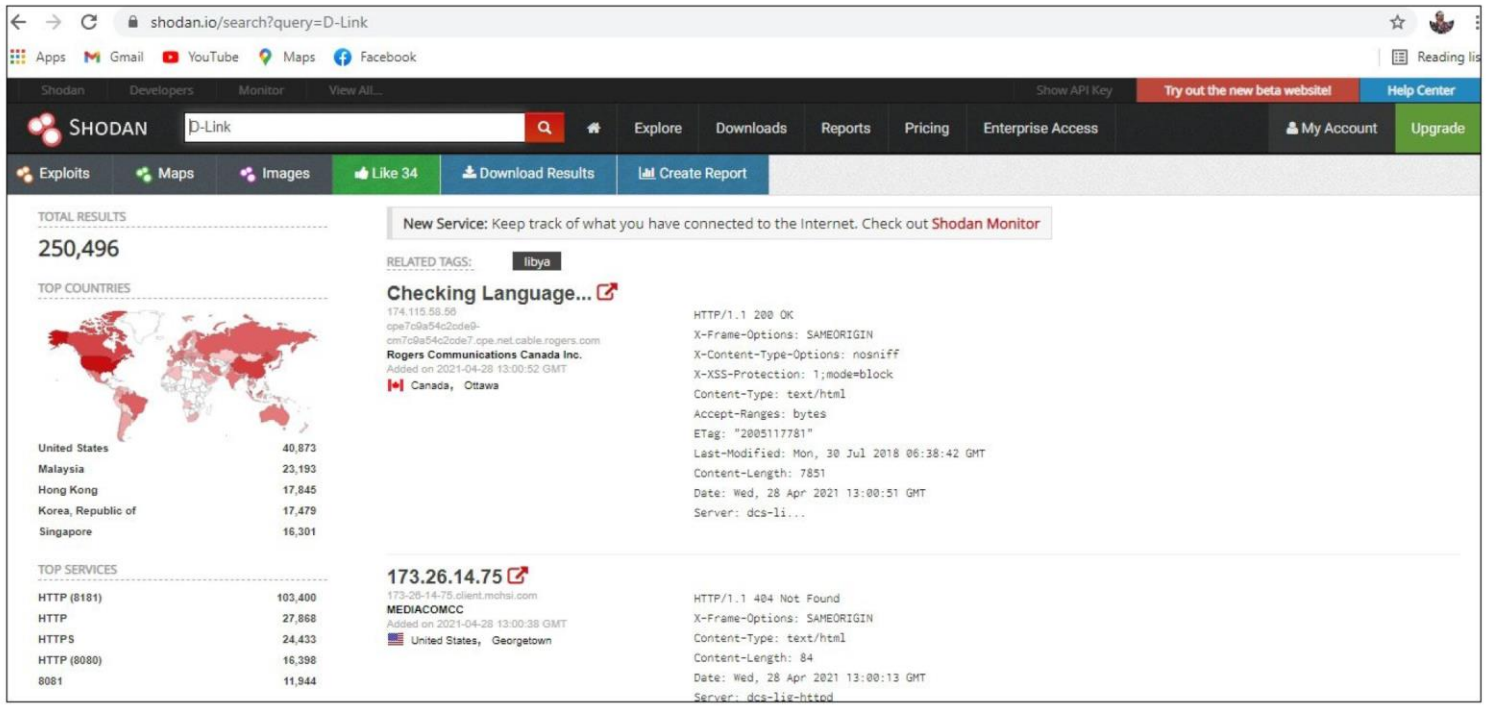
- موتورهای جستجو اندیس‌سازی؟

ردپایابی روش‌ها و ابزارها

شدان Shodan

- موتورهای جستجو اندیس‌سازی؟ تارمانه‌ها

ردپایابی روش‌ها



شدان Shodan

- موتورهای جستجو اندیس‌سازی؟ تارمانه‌ها
- شدان shodan.io
  - اندیس‌سازی هر چیز دیگر
  - به بیان دیگر، یافتن هر چیز متصل به اینترنت و در دسترسی در شدان
  - مسیریاب‌ها، سرورها، دوربین‌های وب، امکانات تصفیه آب، تلویزیون‌ها، یخچال‌ها، ابزارهای پزشکی،
  - تلاش برای اتصال هر نشانی IP روی اینترنت
- امکان کوچک کردن حوزه جستجو
- Apache city: Washington
- country:
- hostname:
- net:
- port:
- before/after:

ردپایابی روش‌ها و ابزارها

ردیابی تارمانه و ای‌نامه

- نیاز به تلاش و دانش بیشتر

ردیابی DNS

سیستم نام‌گذاری دامنه Domain Name Server

معرفی در سال ۱۳۶۳ شمسی

نوعی پایگاه داده توزیع شده شامل نام دامنه و نشانی آی‌پی معادل آن

متشکل از سرورهای در پهنهٔ گیتی

هر سرور مخزن و مدیر رکوردهایی منطقهٔ استقرار خود ← مشهور به namespace

هر یک نیازمند

- نگهداری رکوردهای منطقه خود
- همچنین چگونگی اتصال به فضای نمونه سطح بالاتر جهت اجابت درخواست پرس‌وجوی مشتری

ساختاری درختی

پورت ۵۳ UDP برای یافتن lookup نام‌ها و انتقال ناحیه zone transfer با پورت ۵۳ TCP

ردیابی DNS

جهت بدست‌آوردن نشانی IP

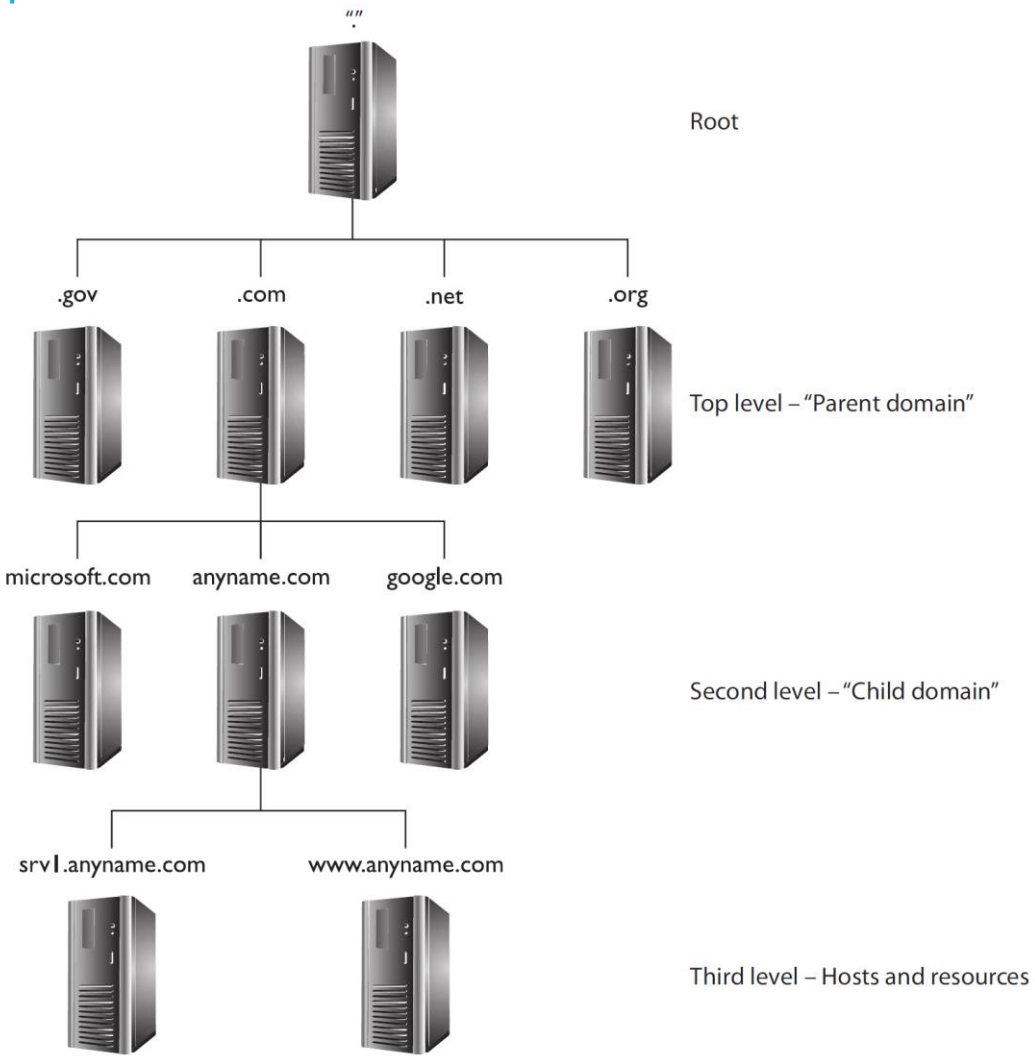
- صدا زدن تابع تطبیق نام Name resolver
- پارامتر ورودی نام دامنه
- تولید بسته درخواست Query packet با UDP
- ارسال به سرویس‌دهندهٔ DNS
- هر سیستم نیازمند به داشتن حداقل یک سروی‌دهندهٔ نام
- برگرداندن نشانی IP با سرور محلی

عدم تمرکز

ردیابی DNS

روشی سلسله‌مراتبی

- مثال www.cs.iasbs.ac.ir
  - کشور ایران
  - هویت: دانشگاهی
  - نام‌دانشگاه
  - نام دانشکده
  - هر نقطه مشخص کننده یک سطح از حوزه



ردیابی DNS

DNS Record Type	Label	Description
SRV	Service	This record defines the hostname and port number of servers providing specific services, such as a Directory Services server.
SOA	Start of Authority	This record identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
PTR	Pointer	This maps an IP address to a hostname (providing for reverse DNS lookups). You don't absolutely need a PTR record for every entry in your DNS namespace, but these are usually associated with e-mail server records.
NS	Name Server	This record defines the name servers within your namespace. These servers are the ones that respond to your clients' requests for name resolution.
MX	Mail Exchange	This record identifies your e-mail servers within your domain.
CNAME	Canonical Name	This record provides for domain name aliases within your zone. For example, you may have an FTP service and a web service running on the same IP address. CNAME records could be used to list both within DNS for you.
A	Address	This record maps an IP address to a hostname and is used most often for DNS lookups.

دارای انواع رکوردها:

- نشانی آی‌پی هر سیستم
- بعضی حاوی سرور ای‌نامه
- بعضی حاوی اشاره‌گر به DNS دیگر – چرا؟

دارای دو دسته سرور

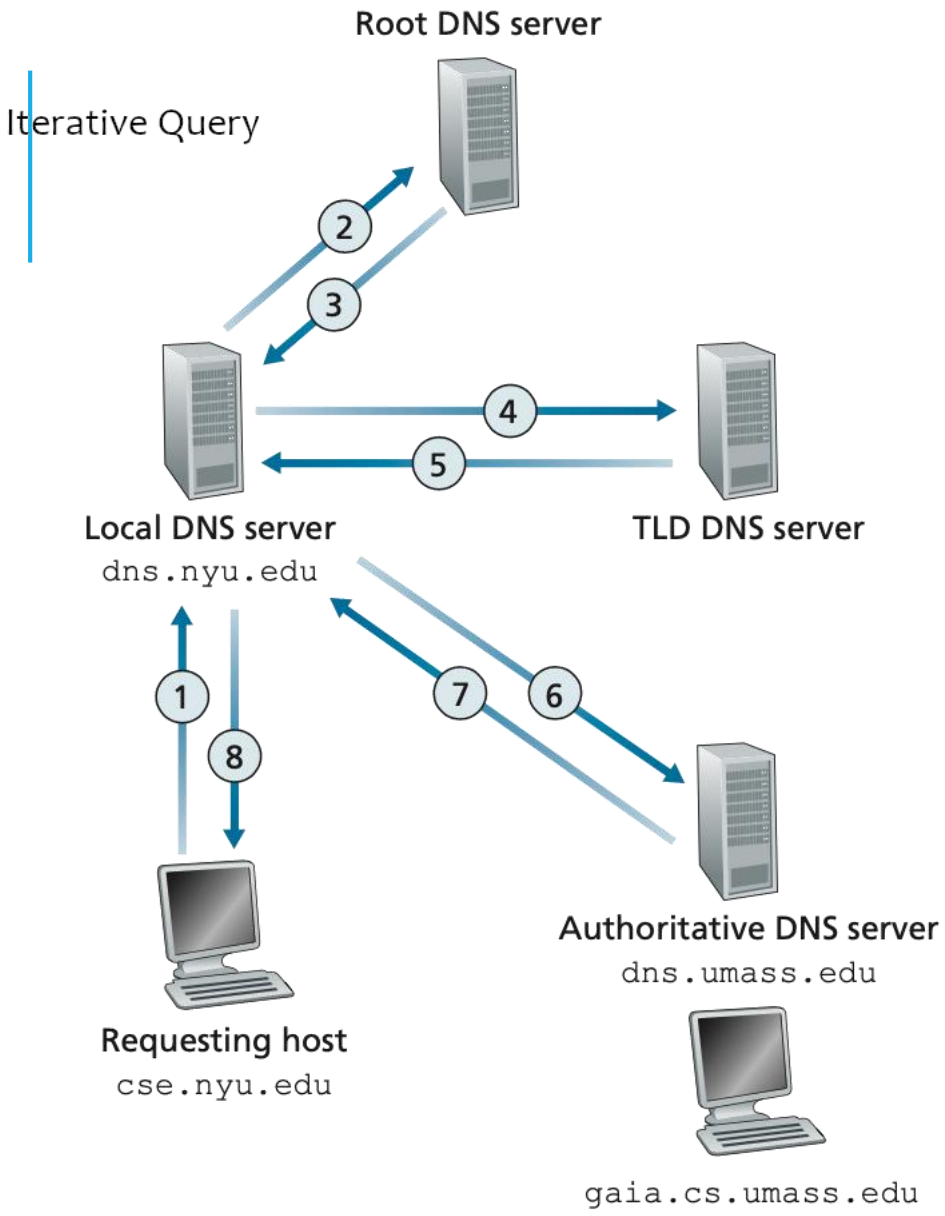
- Name resolver
  - پاسخ به درخواست‌ها
- Authoritative server
  - نگهادارری رکوردهای فضانام

ردیابی DNS

روش‌های پرس‌وجو در خدمت‌دهندگان نام

- پرس وجوی تکراری Iterative Query
- پرس‌وجوی بازگشتی Recursive Query
- پرس‌وجوی معکوس Reverse Query

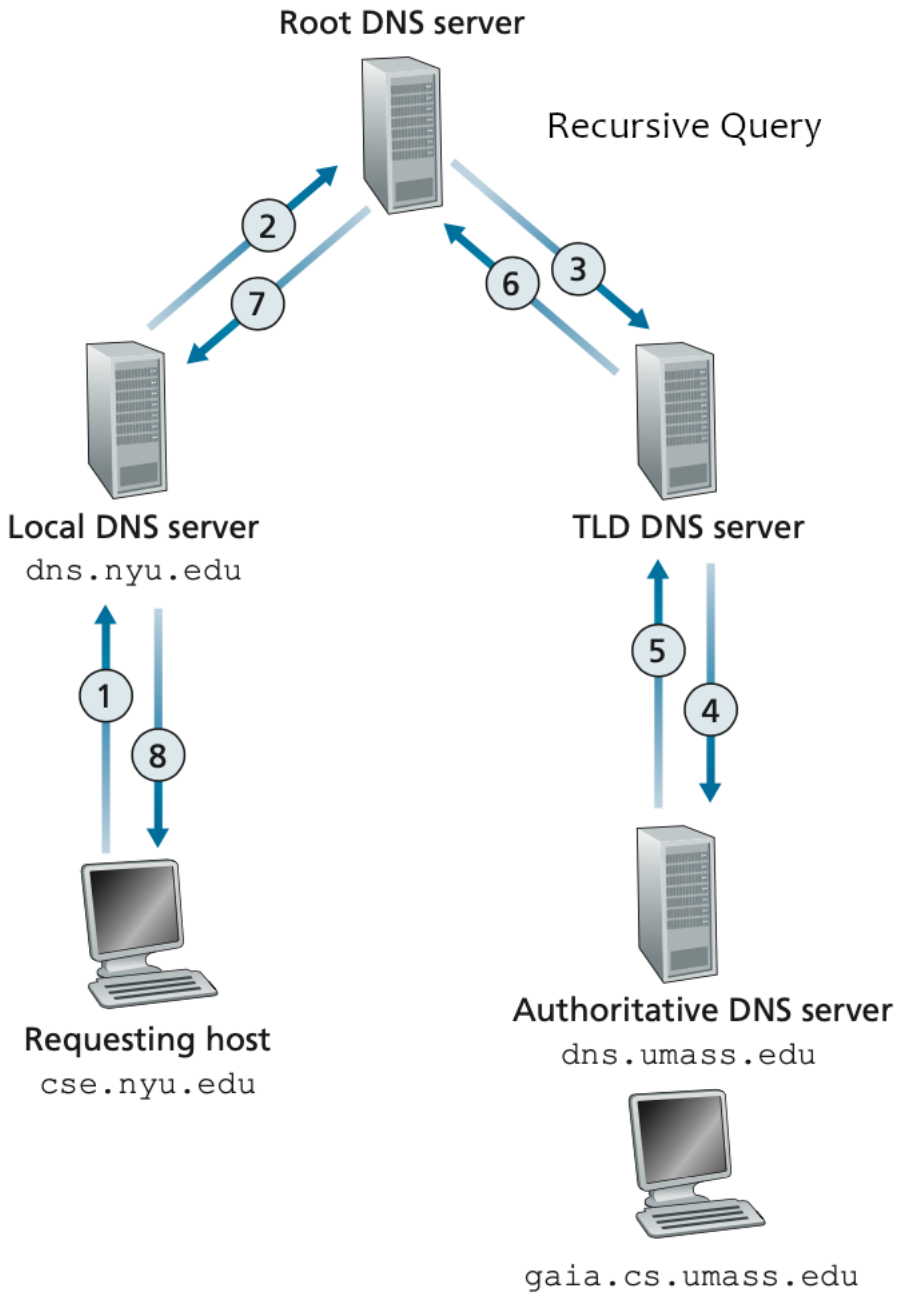
ردیابی DNS



پرس وجوی تکراری Iterative Query

- غالب کار بر عهدهٔ سرور محلی است
- نیاز به ماشین ریشه جهت شروع کار

ردیابی DNS



پرس وجوی بازگشتی

- در پرس‌وجوی تکراری
  - بیشتر حجم عملیات بر عهدهٔ سرور محلی
  - ساده‌تر بودن مدیریت خطا و پیگیری روند کار
  - روشی منطقی برای استفاده در اینترنت
- کاربرد پرس‌وجوی بازگشتی در شبکه‌های کوچک

ردیابی DNS

DNS بازگوی تمامی طرح شبکه ⟸ نفوذگر

فرض اتصال به ftp.acom.com

- روش
  - جستجوی کش در نزدیک‌ترین سرور DNS نزدیک به کاربر
  - کدام نزدیک‌ترین است؟
  - در صورت نبودن:استفاده از ساختار معماری DNS جهت یافتن نشانی
  - برگشت پاسخ به کاربر
- فرضا نفوذگر به دنبال داده
  - تغییر کش روی سرور محلی جهت اشاره به سروری جعلی به جای نشانی حقیقی
  - مسموم‌سازی DNS یا DNS poisoning
  - چنان خطرناک که منجر به تغییر کل DNS در سال ۱۳۷۸
  - دن کامینسکی متوفی در سال گذشته در ۴۲ سالگی
- DNSSEC
  - IETF
  - استفاده از امضاء دیجیتال و امضای دادهٔ DNS
  - افزودن دو ویژگی مهم
  - احراز هویت اصلی داده و یکپارچگی داده

مسموم‌سازی DNS یا DNS poisoning
جعل DNS یا DNS spoofing
ربایش DNS یا DNS hijacking

ردیابی DNS

رکورهای SOA

- مشخص کنندهٔ بارهای اطلاعات
  - از میزبان در سرور ابتدایی در فضا DNS(منطقه یا zone) تا زمانی که سرورهای نام رکوردها را در کش نگه دارند.
- میزبان مبدا Source host
  - نام میزبان سرور دی‌ان‌اس بنیادی zone
- ایمیل تماس
- شماره سریال
- زمان رفرش Refresh time
- زمان بازتلاش retry time
- زمان انقضا expire time
- زمان زنده ماندن TTL

ردیابی DNS

جادوی راه‌انداز ماشین‌ها

عدم امکان پیشبرد اینترنت بدون ترجمات سریع و کارآمد نام به نشانی آی‌پی

نوشتن نام و کلیک
- بدون دانستن اینکه به کجا روان است
- موجب دردسر و استرس کارمندان امنیت
- اما این تمامی ماجرا نیست

با نوشتن URL در مرورگر ماشین ویندوز
- سیستم عامل بررسی اینکه درخواست برای خود است یا نه (localhost)
- در غیر صورت بالا جسجو در فایل HOSTS محلی
- در صورت نبودن مراجعه به DNS محلی
- بررسی کش محلی DNS و سپس کل DNS

توقف فرایند و جستجو در صورت انطباق در هر یک از مراحل
- C:\Windows\System32\Drivers\etc\
- HOSTS

- # 50.62.134.34 google.com

ردیابی DNS

تمرین Wireshark

تمرین جستجوی مانه‌های سیاه‌چاله

ردیابی DNS

اهمیت ردگیری DNS

مدیریت نشانی IP

- IANA و سپس به ICANN
- مدیریت تخصیص نشانی IP
- پنج ناحیهٔ ثبت اینترنتی

- **American Registry for Internet Numbers (ARIN)** Canada, Caribbean, North Atlantic islands, United States
- **Asia-Pacific Network Information Center (APNIC)** Asia, Pacific
- **Réseaux IP Européens (RIPE) NCC** Europe, Middle East, Central Asia/Northern Africa
- **Latin America and Caribbean Network Information Center (LACNIC)** Latin America, Caribbean
- **African Network Information Center (AfriNIC)** Africa

```
Domain Name: mheducation.com
Registry Domain ID: 28866363_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2021-06-04T01:14:05Z
Creation Date: 2000-06-08T17:53:21.000-04:00
Registrar Registration Expiration Date: 2022-06-08T21:53:21Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/
epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: McGraw-Hill Global Education Holdings, LLC
Registrant Street: 2 Penn Plaza
Registrant City: New York
Registrant State/Province: NY
Registrant Postal Code: 10121
Registrant Country: US
Registrant Phone: +1.6094265291
Registrant Phone Ext:
Registrant Fax: +1.6094265291
Registrant Fax Ext:
Registrant Email:
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: McGraw-Hill Global Education Holdings, LLC
Admin Street: 2 Penn Plaza
Admin City: New York
Admin State/Province: NY
Admin Postal Code: 10121
Admin Country: US
Admin Phone: +1.6094265291
Admin Phone Ext:
Admin Fax: +1.6094265291
Admin Fax Ext:
Admin Email:
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: McGraw-Hill Global Education Holdings, LLC
Tech Street: 2 Penn Plaza
Tech City: New York
Tech State/Province: NY
Tech Postal Code: 10121
Tech Country: US
Tech Phone: +1.6094265291
Tech Phone Ext:
Tech Fax: +1.6094265291
Tech Fax Ext:
Tech Email:
Name Server: pdns85.ultradns.biz
Name Server: pdns85.ultradns.com
Name Server: pdns85.ultradns.net
Name Server: pdns85.ultradns.org
DNSSEC: unsigned
```

ردیابی DNS

مراجعه به سایت‌های آنها

- whois
  - www.whois.sc
  - Mheducation.com
- Nslookup
- nslookup [-options] {hostname | [-server]}
- مثال – تبدیل به مد تعاملی با nslookup
- ورود set query = MX
- اطلاع جهت اینکه به دنبال ذخیره‌های سرورهای ایمیل هستید.

ردیابی DNS

- انتقال منطقه Zone transfer
  - برگرداندن تمامی ذخیرهای (رکوردهای) سرور DNS

- nslookup
- server نام خدمت‌دهندهٔ هدف
- set type=any
- ls –d [نام منطقهٔ مدنظر]

```
Listing domain [anycomp.com]
Server: dn1234.anycomp.com
Host or domain name     Resource    Record Info.
anycomp.com.            SOA         dn1234.anycomp.com
hostmaster.anycomp.com  (2013090800 86400 900 1209600 3600)
anycomp.com.            NS     DN1234.anycomp.com
anycomp.com.            NS     DN5678.anycomp.com
anycomp.com.            A      172.16.55.12
anycomp.com.            MX     30     mailsrv.anycomp.com
mailsrv                 A      172.16.101.5
www                     CNAME  anycomp.com
fprtone                 A      172.16.101.15
fprttwo                 A      172.16.101.16
```

- یا دریافت کد خطا یا چیزی شبیه به مورد روبرو
  - 2013090800 شماره سریال
  - 86400 بازه رفرش
  - 900 زمان بازتلاش
  - 1209600زمان انقضاء
  - 3600 زمان زنده ماندن

دیگر موارد دستور dig

ردیابی شبکه

یافتن بازهٔ شبکه

محدود کردن زمان برای کارهای بعدی با یافتن نشانی‌های شروع و پایان شبکه

امتحان نام mheducation.com با 54.164.59.97

- در arin.net

Network: NET-54-144-0-0-1

Source Registry	ARIN
Net Range	54.144.0.0 - 54.221.255.255
CIDR	54.144.0.0/12 54.160.0.0/11 54.192.0.0/12 54.208.0.0/13 54.216.0.0/14 54.220.0.0/15
Name	AMAZON
Handle	NET-54-144-0-0-1
Parent	NET-54-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	*not provided*
Registration	Thu, 23 Oct 2014 04:00:00 GMT (Wed Oct 22 2014 local time)
Last Changed	Wed, 10 Feb 2021 14:46:13 GMT (Wed Feb 10 2021 local time)
Self	https://rdap.arin.net/registry/ip/54.144.0.0
Alternate	https://whois.arin.net/rest/net/NET-54-144-0-0-1
Port 43 Whois	whois.arin.net

Source Registry	ARIN
Kind	Org
Full Name	Amazon Technologies Inc.
Handle	AT-88-Z
Address	410 Terry Ave N. Seattle WA 98109 United States
Roles	Registrant
Registration	Thu, 08 Dec 2011 18:34:25 GMT (Thu Dec 08 2011 local time)
Last Changed	Tue, 31 Mar 2020 13:49:42 GMT (Tue Mar 31 2020 local time)
Comments	All abuse reports MUST include: * src IP * dest IP (your IP) * dest port * Accurate date/timestamp and timezone of activity * Intensity/frequency (short log extracts) * Your contact details (phone and email) Without these we will be unable to identify the correct owner of the IP address at that point in time.
Self	https://rdap.arin.net/registry/entity/AT-88-Z
Alternate	https://whois.arin.net/rest/org/AT-88-Z
Port 43 Whois	whois.arin.net

ردیابی شبکه

Traceroute

- لزوم شناخت خدمات فعالی روی ماشین اما ناکافی
- شناخت دیگر ماشین‌ها
- بررسی IPهای همسایه مثلا با داشتن نشانی ۱۳۰,۳۷,۱۹۳,۱۹۱ احتمال بررسی ۱۳۰,۳۷,۱۹۳,۱۹۲ و ۱۳۰,۳۷,۱۹۳,۱۹۳ و دیگر نشانی‌های ممکن روی شبکه محلی
- استفاده از traceroute جهت یافتن مسیر به نشانی آی‌پی اصلی
- Traceroute
  - ارسال دسته کوچک از بسته‌های UDP به هدف با زمان زندگی یک. سپس دسته‌ای دیگر با زمان زندگی دو و به همین منوال
  - کاهش مقدار زمان زندگی در اولین مسیریاب و دورریزی فی‌الفور اولین بسته‌ها و ارسال خطای ICMP
    - خود خوان حدیث مفصل
  - ادامه کار تا رسیدن بسته UDP به مقصد.
  - جمع‌آوری بسته‌های خطای ICMP و آی‌پی فرستندهٔ خطا شناخت کل مسیر
- امکان استفادهٔ مهاجمان از نتایج جهت اسکن اهداف بیشتر
  - با جستجوی بازهٔ نشانی مسیریاب‌های نزدیک به هدف
  - کسب اطلاع زیاد از توپولوژی شبکه

```
C:\>tracert xxxxxx.com
Tracing route to xxxxxx.com [xxx.xxx.xxx.xxx] over a maximum of 30 hops:
  1     1 ms     1 ms     1 ms  192.168.1.1
  2    11 ms    13 ms     9 ms  10.194.192.1
  3     9 ms     8 ms     9 ms  ten2-3-orld28-ear1.noc.bhn.net [72.31.195.24]
  4     9 ms    10 ms    38 ms  97.69.193.12
  5    14 ms    17 ms    15 ms  97.69.194.140
  6    25 ms    13 ms    14 ms  ae1s0-orld71-cbr1.noc.bhn.net [72.31.194.8]
  7    19 ms    21 ms    42 ms  72-31-220-0.net.bhntampa.com [72.31.220.0]
  8    37 ms    23 ms    21 ms  72-31-208-1.net.bhntampa.com [72.31.208.1]
  9    23 ms    22 ms    27 ms  72-31-220-11.net.bhntampa.com [72.31.220.11]
 10    19 ms    19 ms    19 ms  66.192.139.41
 11    20 ms    27 ms    20 ms  orl1-ar3-xe-0-0-0-0.us.twtelecom.net
[66.192.243.186]
 12     *        *        *     Request timed out.
 13    21 ms    27 ms    31 ms  ssl7.cniweb.net [xxx.xxx.xxx.xxx]
Trace complete
```

ردیابی

ابزارهای دیگر

- OSRFramework
- Web spiders

منابع

[لاودن]

[استالینگز]

[تنن‌باوم]

[ملکیان]

[واکر]