گزارشِ راه‌اندازیِ IVRE

تهیه و تنظیم: مبین خیری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در این گزارش قصد داریم ابتدا برنامه IVRE را نصب و راه اندازی کرده و سپس 100 آی‌پیِ رندوم را به کمکِ امکاناتِ موجود در این ابزار آنالیز کرده و با انتقالِ اطلاعاتِ استخراج‌شده به دیتابیسِ این ابزار، نتایجِ کلی را به کمکِ نمودارها به نمایش بگذاریم.

اما پیش از ورود به بحث اصلی لازم است که با مفاهیمِ Nmap و Recon آشنایی پیدا کنیم.

امروزه با افزایش تهدیدات سایبری، انجام اسکن‌های امنیتی منظم شبکه، برای سازمان‌ها و شرکت‌ها به یک ضرورت تبدیل شده است. هر چند برای این منظور ابزارها و نرم افزارهای نظارتی زیادی وجود دارد، اما Nmap نرم افزاری است که هیچ چیز دیگری نمی‌تواند جایگزین امکانات مفید و کاربردی آن شود.

Nmap چیست؟

ابزار Nmap یاNetwork Mapper ، بهترین و پرکاربردترین نرم افزار Open Source و رایگان برای بازرسی امنیتی و اسکن شبکه است Nmap .را می‌توان به عنوان ابزاری در نظر گرفت که قادر به شناسایی و عیب‌یابی سرویس‌های فعال و در حال اجرا بر روی یک سیستم متصل به اینترنت است.

مسئولان شبکه از انمپ برای شناسایی دستگاه‌هایی که بر روی سیستم‌های آن‌ها در حال اجرا هستند، پیدا کردن پورت‌های آزاد، شناسایی خطرات امنیتی و... استفاده می‌کنند.

نرم افزارNmap ، ابتدا بسته‌های IP خام را برای شناسایی host های موجود در سیستم شبکه، ارسال می‌کند. همچنین این برنامه می‌تواند سرویس‌های ارائه شده به وسیله این host ها، سیستم عامل آنها و سایر ویژگی‌ها را نیز شناسایی کند.

دلیل استفاده از ابزار Nmap چیست؟

مدیران شبکه باید به طور منظم و مستمر به تست و بررسی هاست، تشخیص پورت‌های آزاد و اشغال شده، انجام تست و اسکن برای شناسایی حفره‌ها و آسیب‌پذیری‌های امنیتی و... اقدام کنند. ابزار Nmapهمه این امکانات را به صورت یکجا در اختیار شما قرار می‌دهد.

ابزار Nmap چگونه به آسان‌تر شدن کارها کمک می‌کند؟

- نرم افزارNmap ، علاوه بر جمع‌آوری جزئیات شبکه، در تعیین حفره‌های امنیتی موجود در سیستم نیز بسیار سودمند و موثر است.
- سیستمNmap ، مستقل از سیستم عامل است و بر روی بسیاری از سیستم عامل‌های معمول و متداول مانندLinux ، Windows، Macو... قابل اجرا و استفاده است.
- ابزار Nmap برای تست نفوذ در سیستم‌های تحت شبکه، بسیار مفید کارآمد است.
- استفاده از نرم افزار Nmap بسیار ساده بوده و محیط این پلتفرم به دو صورت-command lineو رابط گرافیکی در دسترس است.

اهداف نرم افزار Nmap چیست؟

- یکی از اهداف نرم افزار Nmap ،گزارش‌گیری‌های منظم از شبکه است. همچنین می‌توان از این سیستم برای انجام کارهای دیگری مانند مدیریت موجودی شبکه، به‌روزرسانی سرویس‌ها، نظارت بر زمان Up time و down time سرویس‌های مختلف نیز استفاده کرد.

- از دیگر اهدافNmap ، کمک به امن کردن شبکه است. به این ترتیب که این نرم افزار با اسکن دیوایس‌های موجود در شبکه با استفاده از Ip packet های منحصربفرد، هاست‌های فعال در شبکه را شناسایی کرده و اطلاعاتی از باز و بسته بودن پورت‌های TCp وUDP ، نوع سیستم عامل موجود روی هاست، نام و آدرس دیوایس‌ها، نوع فیلتر، Firewallموجود بر روی دیوایس‌ها و... را در اختیار مدیران شبکه قرار می‌دهد.
- علاوه بر موارد نام برده شده، سیستم Nmap گزارش‌هایی ارائه می‌دهد که در آن تمام هاست‌های اسکن شده هدف با تمام اطلاعات موجود در command مربوطه به یک لیست تبدیل می‌شوند. همچنین وضعیت سرویس‌ها (آزاد، فیلتر شده، فیلتر نشده و...) نیز مشخص می‌شود. علاوه بر این در این سیستم می‌توانید خروجی را به شکلی توسعه دهید تا نوع سیستم عامل، آدرس سخت افزاری(MAC Address) ، نوع دستگاه و نام reverse DNS نیز در گزارش ارائه شود.

کاربرد Nmap چیست؟

همان طور که بیان کردیم، برنامه Nmap ابزاری بسیار مفید و کارآمد برای اسکن و گزارش‌گیری از شبکه است. اما سایر کاربردهای انمپ چیست؟ در این بخش می‌خواهیم بدانیم با دستورات Nmap چه کارهای دیگری می‌توان انجام داد.

- نرم افزار Nmap می‌تواند هاست‌های متصل به شبکه را شناسایی کند.
- Nmapمی‌تواند پورت‌های آزاد در هاست مورد نظر را مشخص کند.
- ابزار Nmap قادر است تمامی سرویس‌های موجود بر روی یک هاست را همراه با سیستم عامل و نسخه‌های آن شناسایی کند.
- سیستم Nmap می‌تواند هر گونه حفره امنیتی یا آسیب پذیری بالقوه در شبکه را تشخیص دهد.

مزایای نرم افزار Nmap چیست؟

در این بخش مزایای نرم افزار Nmap را بررسی می‌کنیم. پیش‌تر هم اشاره کردیم که متن باز و رایگان بودن این سیستم نخستین و مهم‌ترین مزیت آن به شمار می‌رود. برخی از دیگر مزایای این نرم افزار عبارت است از:

- می‌تواند برای گزارش‌گیری سیستم شبکه مورد استفاده قرار گیرد.
- سیستم Nmap قادر است سرورهای جدید را تشخیص دهد.
- می‌تواند در دامنه‌ها و زیردامنه‌ها به جستجو بپردازد.
- Nmapبا کمک Nmap scripting engine (NSE) می‌تواند با هاست مورد نظر تعامل داشته باشد.
- نرم افزار Nmap می‌تواند ماهیت سرویسی که اکنون در هاست در حال اجر است را تعیین کند.

ویژگی‌های سیستم Nmap چیست؟

ابزار Nmap ویژگی‌های زیادی دارد که آن را از سایر ابزارهای اسکن شبکه متمایز می‌کند. در ادامه ویژگی‌های این سیستم را بررسی خواهیم کرد.

انعطاف پذیری

این سیستم از چندین تکنیک پیشرفته برای استخراج نقشه شبکه استفاده می‌کند. این نقشه ازIP filter ، فایروال، مسیریاب و سایر موانع تشکیل شده است. همچنین نقشه شبکه شامل بسیاری از پورت‌های اسکن شده TCP) و(UDP ، امکانات تشخیص سیستم عامل، ping sweepها و... است.

سادگی

نرم افزارNmap ، دو نسخه command line و GUI بر اساس نیاز شما در دسترس قرار می‌دهد. نسخه باینری نیز برای افرادی که مایل به کامپایل کردن کدهای Nmapنیستند موجود است. در ضمن Nmap مجموعه‌ای از ویژگی‌های پیشرفته را نیز با دستور «nmap –O –sS targethost» برای کاربرانی که توانمندی بیشتری دارند ارائه می‌دهد.

قدرتمندی

قدرت نرم افزار Nmap تا اندازه‌ای است که می‌توان از آن برای اسکن شبکه‌های بسیار بزرگ استفاده کرد.

پشتیبانی از سیستم عامل‌های مختلف

سیستم Nmap از اکثر سیستم عامل‌ها پشتیبانی می‌کند و بر روی آن‌ها قابل استفاده است. این سیستم عامل‌ها عبارتند ازLinux ، Solaris، Mac OS، HP-UXو...

رایگان بودن

ابزار Nmap برای دانلود رایگان به همراه کدهای کامل و قابل تغییر در دسترس است. همچنین شما می‌توانید این کدها را تغییر داده و تحت عنوان GNU General Public License (GPL) در اختیار دیگران قرار دهید.

امنیت

پیش‌تر هم اشاره کردیم که هدف پروژهNmap ، تجهیز مدیران شبکه و کمک به امنیت بیشتر شبکه تحت کنترل است.

ارائه مستندات قابل اتکا

متخصصانNmap ، سعی کرده‌اند که مستندات و manual page های ارائه شده توسط نرم افزار Nmap کاملا گویا، قابل فهم و به روز باشد. همچنین این مستندات و manual page ها به چندین زبان موجود است.

روش‌های اسکن در سیستم Nmap چیست؟

انتخاب روش اسکن مناسب باعث افزایش سرعت و دقت در اسکن شبکه می‌شود. به طور کلی 3 روش اسکن در سیستم Nmap وجود دارد که شامل موارد زیر است.

ICMP Scan

Protocol Scan

SYN/ACK Scan

در صورتی که شبکه به بسته‌های ICMP جواب بدهد، استفاده از روش ICMP Discovery گزینه مناسبی است. با استفاده از پارامترهای PM– PP– PE می‌توانید درخواست‌های ICMP را بررسی کنید.

اگر شبکه توسط Stateful Firewallمحافظت شود، روش Syn/ACK Scan با استفاده از پارامتر PS و اگر با فایروال Statelessمحافظت شود، از پارامتر PA برای اسکن شبکه استفاده می‌شود. این دو پارامتر برای ارسال بسته SYN/ACK نیاز به یک شماره پورت دارند.

چگونه از Nmap استفاده کنیم؟

در Nmap مجموعه گسترده‌ای از برنامه‌های کاربردی بررسی وضعیت شبکه و ابزارهای رایگان و اپن سورس اسکن سطح آسیب پذیری برای مسئولان شبکه وجود دارد. اما همان طور که اشاره کردیم، انعطاف پذیری و قدرت Nmap آن را به ابزاری برتر تبدیل کرده است. هر چند Nmap به عنوان یک ابزار اسکن پورت در نظر گرفته شده، قابلیت‌های دیگری هم برای استفاده در اختیار شما قرار می‌دهد که شامل موارد زیر است.

نقشه برداری شبکه:

Nmapقادر است دستگاه‌های موجود در شبکه از جمله سرورها، روترها، سوییچ‌ها و همچنین نحوه اتصال فیزیکی آن‌ها با یکدیگر را شناسایی کند(host discovery) .

شناسایی سیستم عامل:

Nmapمی‌تواند سیستم عامل‌های در حال اجرا روی دستگاه‌های شبکه را شناسایی کند OS) . fingerprint)

شناسایی سرویس:

این نرم افزار می‌تواند میزبان‌های موجود در شبکه و همچنین نوع کاری که انجام می‌دهند را شناسایی کند.

نظارت امنیتی:

با بررسی سیستم عامل‌ها و اپلیکیشن‌های در حال اجرا بر روی میزبان‌های شبکه، مدیران می‌توانند آسیب پذیری‌ها و نقاط ضعف را مشخص کنند.

یکی از مزایای بزرگ Nmap این است که افرادی که دانش کمی درباره شبکه دارند، می‌توانند کار با این ابزار را برای اسکن مقدماتی به سادگی آغاز کنند. کاربران حرفه‌ای نیز می‌توانند از امکانات پیچیده‌تر نرم افزار استفاده کنند که به نمایش دقیق‌تر وضعیت شبکه کمک می‌کند.

Reconچیست؟

به تکنیک ها و فرایندهای جمع آوری اطلاعات مرتبط با یک وب سایت، Reconnaissance و به اختصار Recon گفته می شود. انجام این کار در بخش های مختلف و با استفاده از ابزارهای متفاوتی صورت می پذیرد که IVRE نیز یکی از این ابزارهاست.

IVRE چیست؟

IVRE یک چارچوب شناسایی شبکه پیشرفته است که با پایتون و MongoDB ساخته شده است. IVRE به تعدادی بسته (Nmap، Masscan، Zmap، Zeek، Argus، Nfdump، ZDNS) متکی است و همه آنها را از طریق CLI و یک رابط وب گرد هم می آورد.

یک محقق می‌تواند شناسایی فعال یا غیرفعال یک شبکه را انجام دهد، سپس از طریق CLI یا رابط وب، تحقیق کرده و تجزیه و تحلیل بیشتری انجام دهد.

IVREرا می توان برای تحقیقات تیم قرمز و آبی استاندارد، ایجاد Shodan/Censys خصوصی یا حتی سرویس DNS غیرفعال خود استفاده کرد.

ویژگی های اصلی:

چارچوب IVRE :چرخ را دوباره اختراع نمی کند - با ترکیب آنها و ایجاد بر روی آن پایه، به نرم افزارهای موجود متکی است .رابط وب: رابط کاربری گرافیکی مبتنی بر وب فیلتر کردن و کاوش داده ها را آسان میکند مصورسازی‌ها: با افزودن به رابط وب، تجسم های متعدد و مکانیسم های مرتب سازی وجود دارد که امکان تجزیه و تحلیل بیشتر (از جمله تجسم جریان های شبکه) را فراهم می کند. API: اگر محدودیت‌هایی در چارچوب پیدا کردید، می‌توانید از API برای صادر کردن داده‌های خود و تجسم/تحلیل آن در جای دیگری استفاده کنید.

IVRE به درد چه کسانی می‌خورد؟

درست مانند Masscan وJok3r ، IVREهم برای تحقیقات تیم قرمز تهاجمی و هم برای تحقیقات دفاعی عالی است.

همانطور که در بالا ذکر شد، شما همچنین می توانید از IVRE برای ایجاد سرویس Shodan خصوصی یا غیرفعال DNS خود استفاده کنید .سرویس غیرفعال برای هر نوع سازمانی عالی است تا بر شبکه های خود نظارت داشته باشند و جریان فعالیت شبکه را برای تشخیص هر گونه رفتار غیرعادی ببینند.

نصب IVRE روی لینوکس

IVREگزینه های نصب بسیاری را ارائه می دهد .بر اساس مستندات، IVREاز Docker پشتیبانی می کند و بر روی تعدادی از توزیع های لینوکس بسته بندی شده است، همانطور که در اینجا مشاهده می کنید.

با این حال، این ابزار به تعدادی بسته مختلف متکی است که نیاز به نصب خود دارند .اینها عبارتند از MongoDB، Nmap، Zmap، Masscan، Apache/Nginx(اختیاری) و بسیاری دیگر .ما سعی خواهیم کرد که نصب ناب را تنها با استفاده از بسته های مورد نیاز دنبال کنیم.

همیشه مهم است که در هنگام نصب نرم افزار جدید از نوعی محیط سندباکس استفاده کنید. می توانید یک ماشین مجازی (VM)، کانتینر یا یک سرور تست از راه دور را انتخاب کنید. ما از اوبونتو 20.04 برای این بررسی استفاده کردیم، و هر دستوری که در اینجا استفاده می‌شود باید برای توزیع‌های مبتنی بر دبیان (و با چند تغییر جزئی، برای توزیع‌های دیگر نیز اعمال شود).

ابتدا تعدادی بسته‌ی سیستمی را نصب می‌کنیم:

```
sudo apt install mongodb nmap zmap gcc make libpcap-dev python3-virtualenv
```

دستور بالا دو اسکنر (Nmap و ZMap) را نصب می‌کند و از بسته‌های دیگر برای ساخت Masscan استفاده می‌شود که به صورت زیر قابل انجام است:

```
git clone https://github.com/robertdavidgraham/masscan
  cd masscan
  make
```

می‌توانید دستورالعمل‌های نصب کامل ما را برای Masscan در اینجا ببینید.

اکنون یک محیط مجازی پایتون ایجاد کرده و IVRE را نصب می کنیم:

```
  mkdir IVRE-install
  virtualenv --python=python3.8 IVRE-install/
  cd IVRE-install/
  source bin/activate
  pip install ivre
```

اکنون باید IVRE را روی تمام سیستم نصب کرده باشید، که می توانید با اجرای دستورِ زیر از آن مطمئن شوید:

```
  ivre –help
```

```
(IVRE-install) root@box5:~/IVRE-install# ivre --help
IVRE - Network recon framework
Copyright 2011 - 2020 Pierre LALET <pierre@droids-corp.org>
Version 0.9.15

Python 3.8.2 (default, Apr 27 2020, 15:53:34)
[GCC 9.3.0]

Linux box5 5.4.0-40-generic #44-Ubuntu SMP Tue Jun 23 00:01:04 UTC 2020 x86_64

Dependencies:
    Python module pymongo: 3.10.1
    Python module py2neo: missing
    Python module sqlalchemy: missing
    Python module psycopg2: missing
    Python module cryptography: 2.9.2
    Python module krbV: missing
    Python module PIL: missing
    Python module MySQLdb: missing
    Python module dbus: missing
    Python module matplotlib: 3.2.2
    Python module bottle: 0.12.18
    Python module OpenSSL: 19.1.0
    Python module tinydb: missing
```

اکنون می توانیم با اجرای دستورات زیر IVRE را مقداردهی اولیه کنیم:

ivre ipinfo --init

ivre scancli --init

ivre view --init

ivre flowcli --init

sudo ivre runscansagentdb –init

```
(IVRE-install) root@box5:~# ivre ipinfo --init
This will remove any passive information in your database. Process ? [y/N] y
(IVRE-install) root@box5:~# ivre scancli --init
This will remove any scan result in your database. Process ? [y/N] y
(IVRE-install) root@box5:~# ivre view --init
This will remove any view in your database. Process ? [y/N] y
(IVRE-install) root@box5:~# ivre flowcli --init
This will remove any flow result in your database. Process ? [y/N] y
(IVRE-install) root@box5:~# ivre runscansagentdb --init
This will remove any agent and/or scan in your database and files. Process? [y/N] y
(IVRE-install) root@box5:~#
```

با این کار داده های موجود از پایگاه داده حذف می شود .این دستورات را می توان در بین تحقیقات برای پاکسازی داده ها استفاده کرد.

آخرین مرحله واکشی داده های IP خواهد بود:

```
ivre ipdata –download
```

این دستور داده های IP را از وب سایت IVRE و Maxmind واکشی می کند .اگر می‌خواهید آدرس‌های IPرا از یک AS یا هر کشور اسکن یا فهرست کنید، به این داده‌ها نیاز است.

تست / استفاده

اولین آزمایش ما اجرای اسکن روی 100 میزبان تصادفی با اجرای پنج فرآیند Nmap موازی خواهد بود:

```
ivre runscans --routable --limit 100 --output=XMLFork --processes 5
```

```
Scanning 170.66.195.245 [2 ports]
Scanning 213.171.214.87 [2 ports]
Scanning 97.33.132.196 [2 ports]
Initiating Ping Scan at 11:35
Scanning 50.189.164.12 [2 ports]
Initiating Ping Scan at 11:35
Scanning 99.174.28.58 [2 ports]
NSE: Loaded 267 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:35
NSE: [targets-ipv6-wordlist] Need to be executed for IPv6.
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
Completed NSE at 11:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
Initiating Ping Scan at 11:35
Scanning 168.21.44.128 [2 ports]
Completed Ping Scan at 11:35, 3.20s elapsed (1 total hosts)
Nmap scan report for 50.189.164.12 [host down, received no-response]
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
```

اکنون می‌توانیم نتایج را به پایگاه داده وارد کرده و یک نما از آن را ایجاد کنیم:

```
ivre scan2db -c ROUTABLE-001 -s MySource -r scans/ROUTABLE/up
```

```
ivre db2view nmap
```

با خروجی فرمان 'scan2db' می توانید تأیید کنید که اسکن شما با موفقیت انجام شده است، که باید چیزی شبیه به خط زیر باشد:

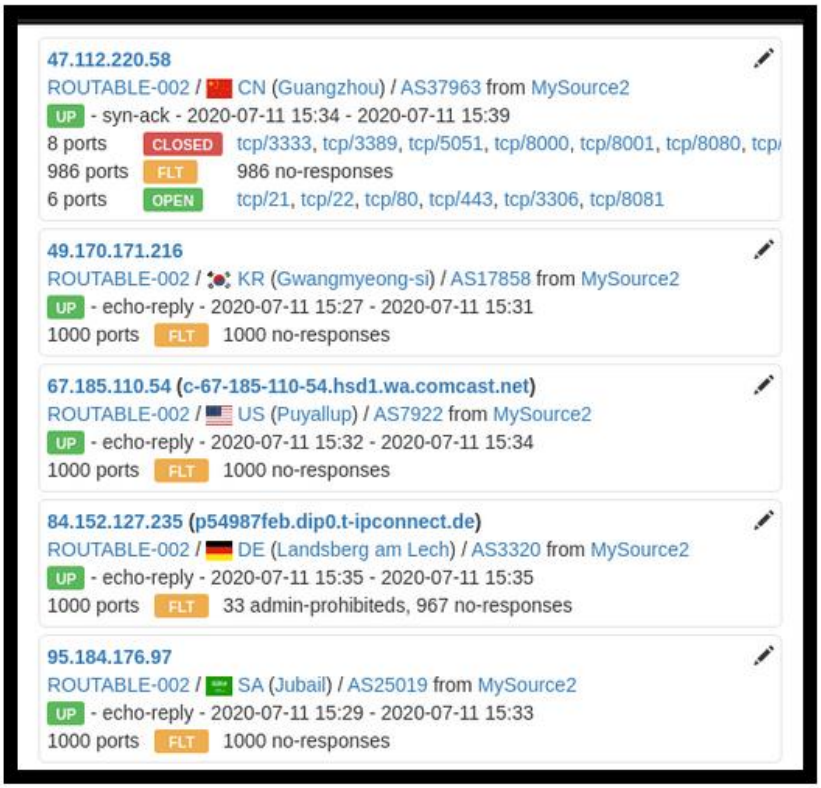
```
INFO:ivre:9 results imported.
```

ما می‌توانیم نتایج را با اجرای زیر تجزیه و تحلیل سریع انجام دهیم:

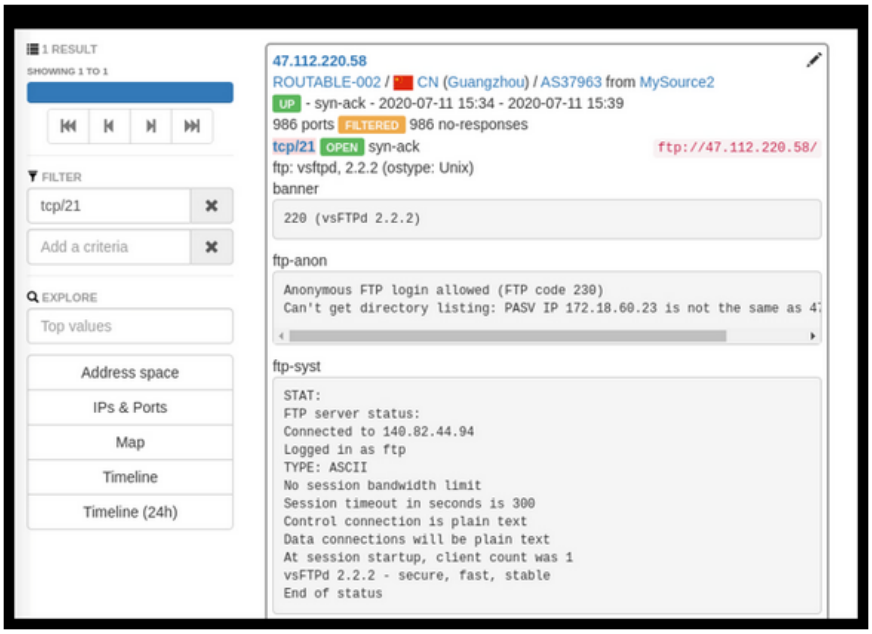
```
ivre scancli --port 22
```

اما این خیلی مفید نیست مگر اینکه با CLI راحت باشید .بنابراین بیایید ببینیم که رابط وب به جای آن چه چیزی را به ما نشان می دهد .سرور اصلی httpd را راه اندازی کنید (اگر سرور آزمایشی را از راه دور اجرا می کنید، مطمئن شوید که از فایروال محافظت می کنید) همانطور که در پایین نشان داده شده است:

```
ivre httpd --bind-address 0.0.0.0
```



نتایج در رابط وب بسیار آموزنده است و به ما نشان می دهد که کدام پورت ها در حال استفاده هستند، از جمله اینکه کدام یک باز و کدام یک بسته است. همچنین مکان آدرس IP به ما نشان داده شده است. حال هجازه دهید یک فیلتر اضافه کنیم تا ببینیم برنامه چگونه آن را مدیریت می کند. فیلتر کردن بر اساس پورت 21:



این نیز کاملا گویا است، و اطلاعات ارزشمند زیادی در مورد پورت (که FTP است) و نسخه نرم افزار مورد استفاده در پورت ارائه می دهد.

اکنون تمام داده های موجود را پاک می کنیم و سعی می کنیم اسکن مشابهی را در یک زیر شبکه خاص اجرا کنیم:

```
rm -rf scans/ROUTABLE/*
```

اگر می خواهید یک تحقیق شناسایی فعال جدید را بدون هیچ گونه داده موجود در پایگاه داده یا نما شروع کنید، می توانید داده ها را با اجرای دو دستور زیر حذف کنید:

```
ivre scancli --init
```

```
ivre view –init
```

ما اسکن خود را در برابر زیرشبکه‌ای اجرا می‌کنیم که دارایIP های تبلیغاتی مضری است که ما ردیابی می‌کنند:

```
ivre runscans --routable --categories MALVERT --network 139.45.192.0/20 --output=XMLFork --processes 5
```

در دستور بالا، ما:

دسته بندی خودمان 'MALVERT' را ایجاد کردیم که در /scans/MALVERT/ ظاهر می شود.

یک زیر شبکه کامل تحت "شبکه" اسکن می‌شود.

و فقط از پنج فرآیند Nmap همزمان استفاده می‌کند.

اولین چیزی که هنگام اجرای این اسکن اصلاح شده کشف کردیم این بود که فرآیند اسکن برای یک زیرشبکه نسبتاً کوچک چقدر کند است .این ممکن است به دلیل تعداد فرآیندهایی باشد که ما استفاده کردیم (که پنج مورد بسیار کم است) .کل زمان اجرا تقریباً بیشتر از 3 ساعت طول کشید.

اکنون داده ها را در پایگاه داده وارد می کنیم تا بتوانیم بررسی های بیشتری انجام دهیم:

```
ivre scan2db -c MALVERT -s test2 -r scans/MALVERT/up
```

```
ivre db2view nmap
```

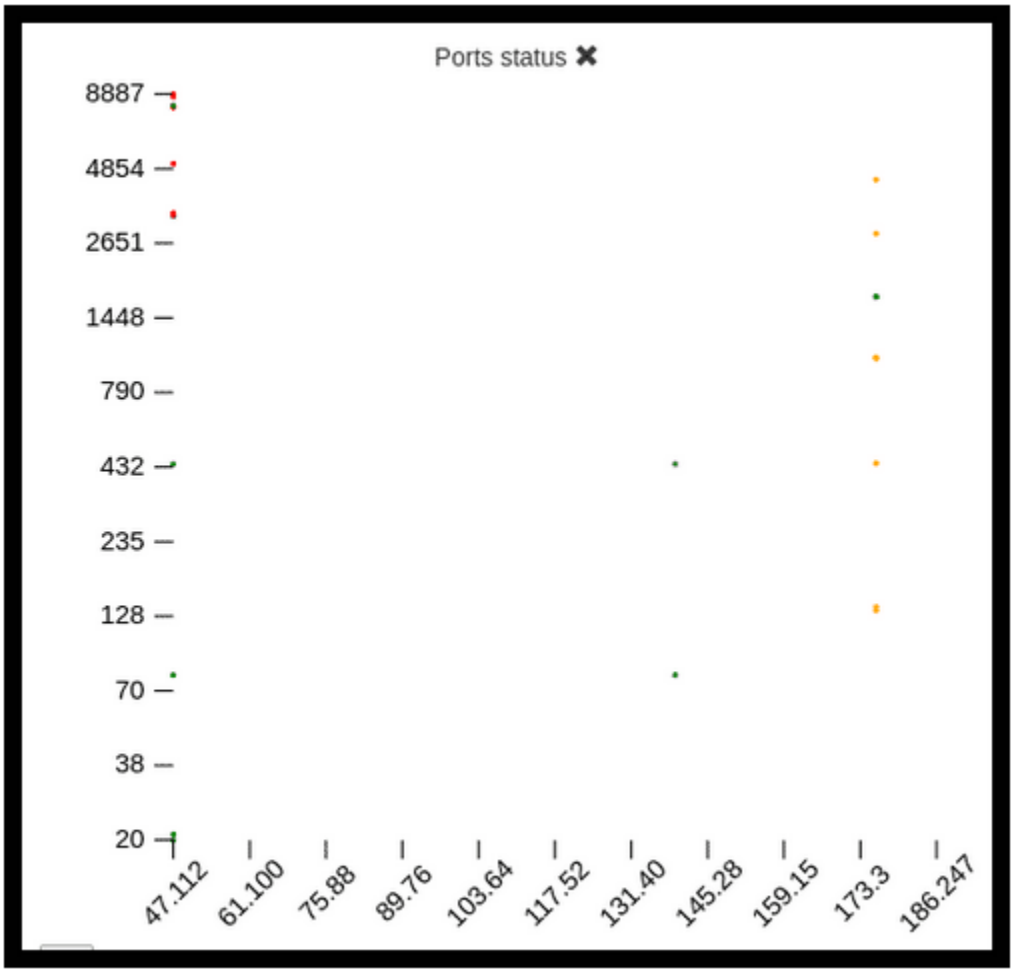
با اجرای دستورِ:

```
ivre scancli –count
```

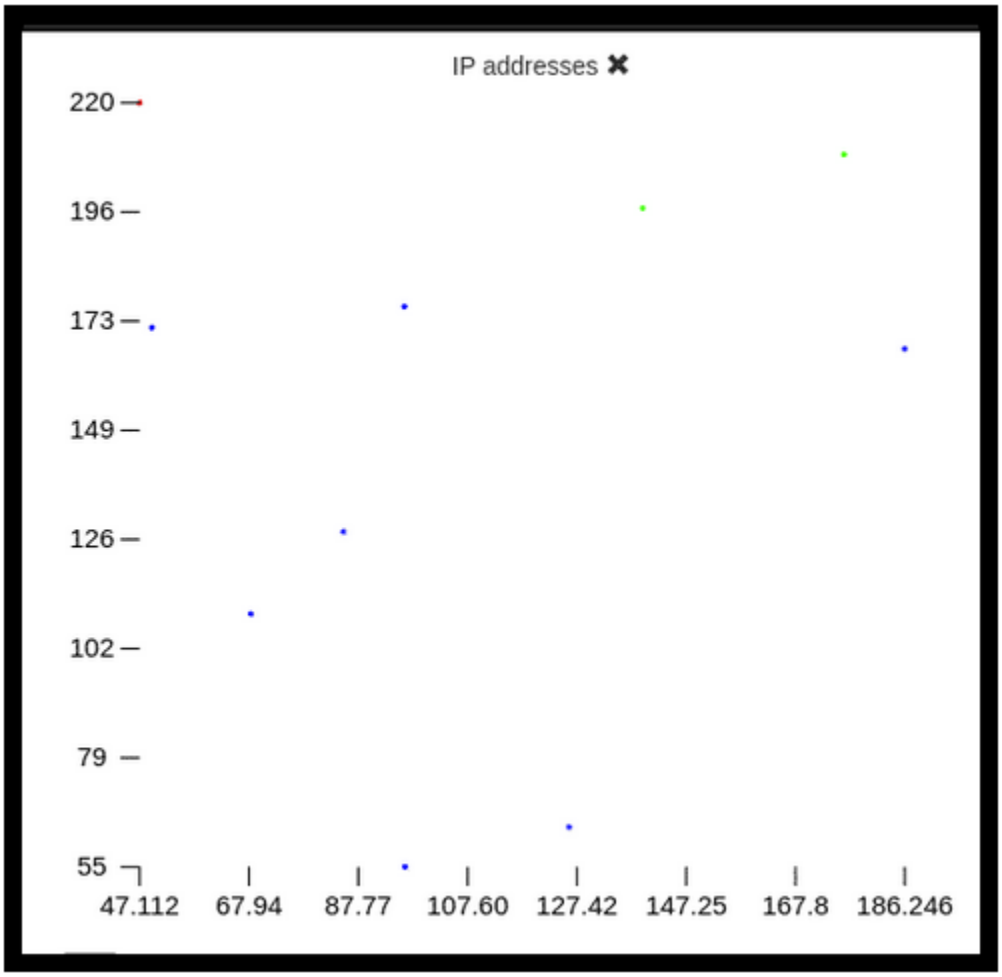
این مقدار کل نتایج موجود در پایگاه داده را از تمام اسکن ها (مجموع ما اکنون 10 است) خروجی می‌دهد.

```
(IVRE-install) root@box5:~/IVRE-install/scans# ivre scancli --count
10
(IVRE-install) root@box5:~/IVRE-install/scans#
```

با استفاده از ویژگی «Explore»، می‌توانیم برخی از نمودارهای IVRE را مشاهده کنیم. آی‌پی ها و پورت ها:



فضای آدرس ده آی‌پی در زیر آمده است:



بسته به نحوه انجام تحقیقات شما، یا غلظت فضای آدرس/IP ها (زمانی که تحقیق به یک زیرشبکه خاص نگاه می کند) یا یک نمودار پراکنده (هنگامی که به IP های یک شرکت فناوری بزرگ مانند گوگل نگاه می کنید) خواهید دید.

IVRE همچنین از رسم نمودارها به طور مستقیم با استفاده از matplotlib پشتیبانی می کند (ما باید نرم افزار را به تنهایی نصب کنیم که با استفاده از این دستور سریع انجام می شود: `pip install matplotlib`).

```
ivre plotdb --category ROUTABLE --2d
```

این دستور یک نمودار دو بعدی از نتایج دسته ROUTABLE رسم می کند.

می‌توانیم یک ممیزی DNS دامنه دیگر را با اجرای دستورِ زیر بررسی کنیم:

```
ivre auditdom facebook.com > fb.xml
```

این به ما یک خروجی XML به سبک Nmap می دهد که اطلاعات DNS را ارائه به نمایش می‌گذارد.

```
(IVRE-install) root@box5:~/IVRE-install# cat fb.xml
<?xml version="1.0"?>
<?xml-stylesheet href="file:///usr/local/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!DOCTYPE nmaprun PUBLIC "-//IDN nmap.org//DTD Nmap XML 1.04//EN" "https://svn.nmap.org/nmap/docs/nmap.dtd">
<?xml-stylesheet href="file:///usr/local/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- ivre auditdom 0.9.15 scan initiated 2020-07-12 12:10:31.498176 as: ivre auditdom facebook.com -->
<nmaprun scanner="ivre auditdom" args="ivre auditdom facebook.com" start="1594555831" startstr="2020-07-12 12:
0.9.15" xmloutputversion="1.04">
<scaninfo type="audit DNS domain" protocol="dig" numservices="1" services="53"/>
</nmaprun>
```

با اینکه ما این تست را برای شناساییِ فعال تنظیم کردیم، IVREبرای شناساییِ غیرفعال با استفاده از ابزارهایی مانند Zeek نیز مفید است .شما می توانید فایل لاگ خود را به IVRE متصل کنید و به طور مداوم داده ها را از لاگ ها به IVRE تغذیه کنید .اطلاعات بیشتر در مورد آن را می توان در اینجا یافت.

یکی دیگر از ویژگی های واقعا عالی IVRE توانایی اجرای "عامل" از راه دور است .با 'agents' (یا Workers) می توانید مینیمم ابزارهای لازم را اجرا کنید و نصب IVRE را با 'agent' از طریق rsync همگام‌سازی کنید .این در شرایطی مفید است که شما اسکن‌های بزرگی را اجرا می کنید و می‌خواهید یک شبکه توزیع‌شده از عوامل برای انجام اسکن بدون نیاز به نمونه IVRE میزبان شما برای اجرای هر گونه اسکن، خودش کار کند.

منابع:

i. https://securitytrails.com/blog/ivre
ii. https://www.irandnn.ir/mag/what-is-nmap/
iii. https://ivre.rocks/#about

پایان.