به نام کیمیاگر عالم

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

امنیت شبکه

عنوان

تمرین دوم – فعالیت اول – مرحله شناسایی حملات سایبری

مدرس

دکتر سیاوش خرسندی

دانشجو

امیرحسین بابائیان

۴۰۱۱۳۱۰۰۲

ترم پاییز ۰۲-۰۱

گروه معماری کامپیوتر و شبکه های کامپیوتری

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

فهرست

بخش الف – مفاهیم

مفاهیم Footprinting، Scanning و Enumeration

مرحله شناسایی	نوع اطلاعاتی که به دست می آید
Footprinting	اطلاعات کلی که به صورت پابلیک در سایت ها و سامانه های مختلف وجود دارد و با ساده ترین اقدامات به دست می آید مانند محل یک شرکت یا اطلاعات داخل سایت مجموعه، تصاویر عمومی و وبلاگ کارمندان از سایت هایی مانند netcraft می توان برای پیدا کردن اطلاعات جامع یک وب سایت استفاده کرد. توضیحات کتاب : ▪ Network information ▪ Operating system information ▪ Organization information, such as CEO and employee information, office information, and contact numbers and e-mail ▪ Network blocks ▪ Network services ▪ Application and web application data and configuration information ▪ System architecture ▪ Intrusion detection and prevention systems ▪ Employee names ▪ Work experience
Scanning	اطلاعات شبکه ای به دست می آوریم از طریق اقداماتی که انجام داده می شود که برای مثال می توان بررسی کرد که چه هاست ها یا ip هایی و چه پورت هایی باز است و چه موارد قابل حلمه ای وجود دارد. توضیحات کتاب: ▪ IP addresses and open/closed ports on live hosts ▪ Information on the operating system(s) and the system architecture ▪ Services or processes running on hosts
Enumeration	دقیق تر شدن اقدامات مربوط به دو بخش قبلی من جمله اینکه اطلاعات جزئی تری از سیستم عامل، محل ذخیره سازی داده ها و ... را بدست می اوریم. توضیحات کتاب: ▪ Network resources and shares ▪ Users and groups ▪ Routing tables

▪ Auditing and service settings ▪ Machine names ▪ Applications and banners ▪ SNMP and DNS details	

انواع اسکن ها

نوع اسکن	هدف
Port Scanning	پیدا کردن پورت های باز سیستم، سیستم عامل و اطلاعات مربوط به ورژن های داخل یک هاست از جمله مواردی است که توسط این اسکن بدست می آید.
Network Scanning	هدف از نتورک اسکنینگ بدست آوردن اطلاعات مربوط به شبکه تارگت می باشد به صورتی که نحوه تعاملات، ساختار شبکه، وجود دستگاه های مختلف نظیر IDS ها و ... را بدست اوریم.
Vulnerability Scanning	مشکلات امنیتی مربوط به اطلاعات بدست آمده در گام port scanning را پیدا میکنیم، برای مثال در یک نسخه خاص از wordpress چه دسترسی هایی وجود دارد که اگر هاست پیدا شده دارای این نسخه از wordpress باشد می توانیم استفاده کنیم.

بخش ب – فعالیت عملی

در این گزارش از کتاب CEH Lab v11 استفاده شده است.

Footprinting

ب۱. تشریح لیست آزمایش ها

Footprinting با عنوان اطلاعات و جمع آوری اطلاعات ترجمه شده است.

لیست آزمایشات و ابزارها عبارتند از:

- جمع آوری اطلاعات از طریق موتور های جستجو
  - تکنیک های سرچ پیشرفته در گوگل
  - جمع آوری اطلاعات از طریق موتور های جستجوی ویدیو
  - جمع آوری اطلاعات از طریق موتور های جتسجوی FTP
  - جمع آوری اطلاعات از طریق موتور های جستجوی اینترنت اشیا
- جمع آوری اطلاعات از طریق وب سرویس ها
  - اطلاعات دامنه ها و شرکت ها
  - اطلاعات شخصی از طریق سایت های مربوطه
  - بدست آوردن لیست ایمیل
  - جمع آوری اطلاعات از طریق جستجو در دارک و دیپ وب
  - یافتن سیستم عامل تارگت به صورت passive
- جمع آوری اطلاعات از طریق شبکه های اجتماعی
  - جمع اوری اطلاعات از طریق لینکدین و چنین سایت هایی
  - جمع آوری اطلاعات از طریق سایت های کاریابی مانند followerwork و جابجینجا
- جمع آوری اطلاعات یک سایت
  - جمع آوری اطلاعات از طریق ping
  - جمع آوری اطلاعات از طریق website informer
  - جمع اوری داده ها از طریق ابزارهای Web Data Extractor، HTTrack و CeWL
- جمع آوری اطلاعات از طریق ایمیل
  - جمع آوری داده ها از طریق ابزار eMailTrackerPro
- جمع آوری اطلاعات از طریق whois

- بدست آورده اطلاعات از طریق سایت whois
- جمع آوری اطلاعات از طریق DNS
  - جمع آوری اطلاعات از طریق دستور nslookup
  - جمع آوری اطلاعات با استفاده از DNSRecon
- جمع آوری اطلات شبکه
  - پیدا کردن محدوده شبکه
  - استفاده از دستور های traceroute و tracert
  - استفاده از ابزار Path Analyzer Pro
- جمع آوری اطلاعات با ابزارهای مختلف
  - ابزار Recon-ng
  - ابزار Maltego
  - ابزار OSRFramework
  - ابزار FOCA
  - ابزار BillCipher
  - ابزار OSINT FrameWork

ب ۲. آزمایش شماره شش (Whois Lookup)

به روایت تصویر:

ورود به سایت whois.domaintools.com و وارد کردن amirhosseinbabaeayan.ir در بخش جستجو

اطلاعات Domain Profile که شامل ip، ip location و تعدادی اطلاعات دیگر نیز می باشد در تصویر آورده شده است:

Domain Profile

IP Address	135.181.126.180 - 475 other sites hosted on this server
IP Location	- Uusimaa - Helsinki - Hetzner Online Gmbh
ASN	AS24940 HETZNER-AS, DE (registered Jun 03, 2002)
Hosting History	6 changes on 3 unique name servers over 5 years

اطلاعات website در تصویر ذیل آورده شده است

Website

Website Title	Amir Hossein Babaeayan
Response Code	200
Terms	27 (Unique: 23, Linked: 7)
Images	10 (Alt tags missing: 0)
Links	13 (Internal: 5, Outbound: 8)

لازم به ذکر است این عملیات بسیار ساده است و برای انجام آن به اینترنت نیاز است.

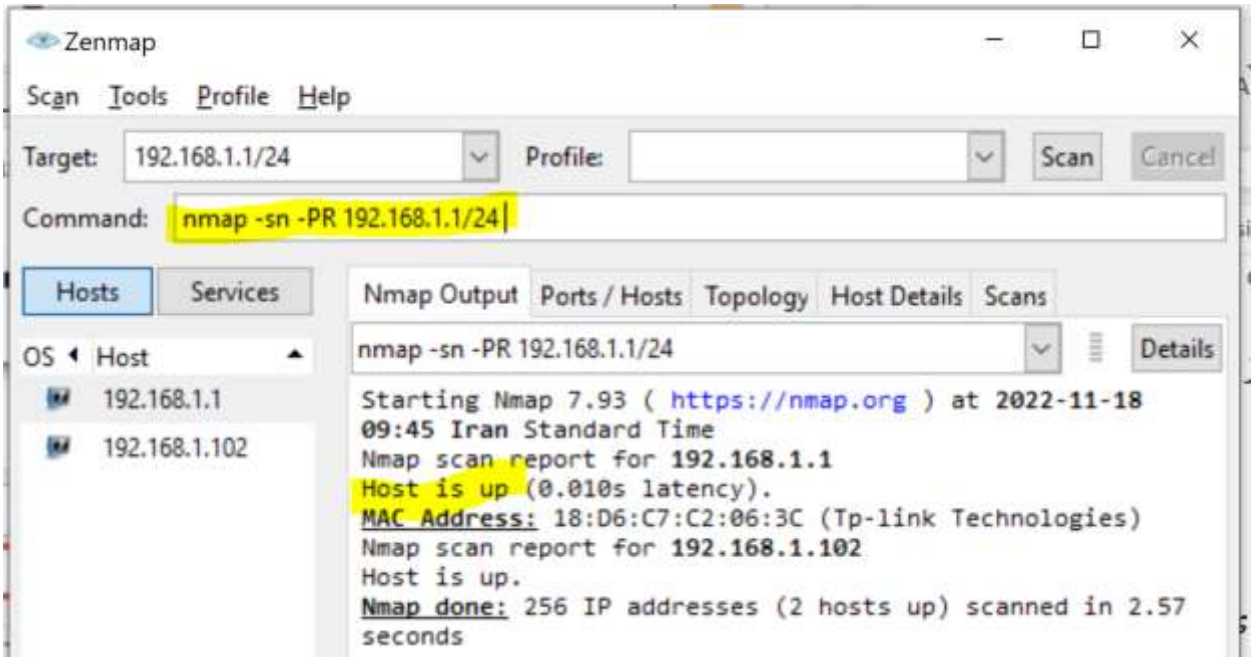
Scanning

مرجع مورد استفاده کتاب ورژن یازدهم CEH Lab است که نسبت به نسخه ای که در فایل تمرین ذکر نشده است دارای تفاوت می باشد از این رو بر اساس اطلاعات بدست آمده در این بخش از nmap استفاده کرده ام.

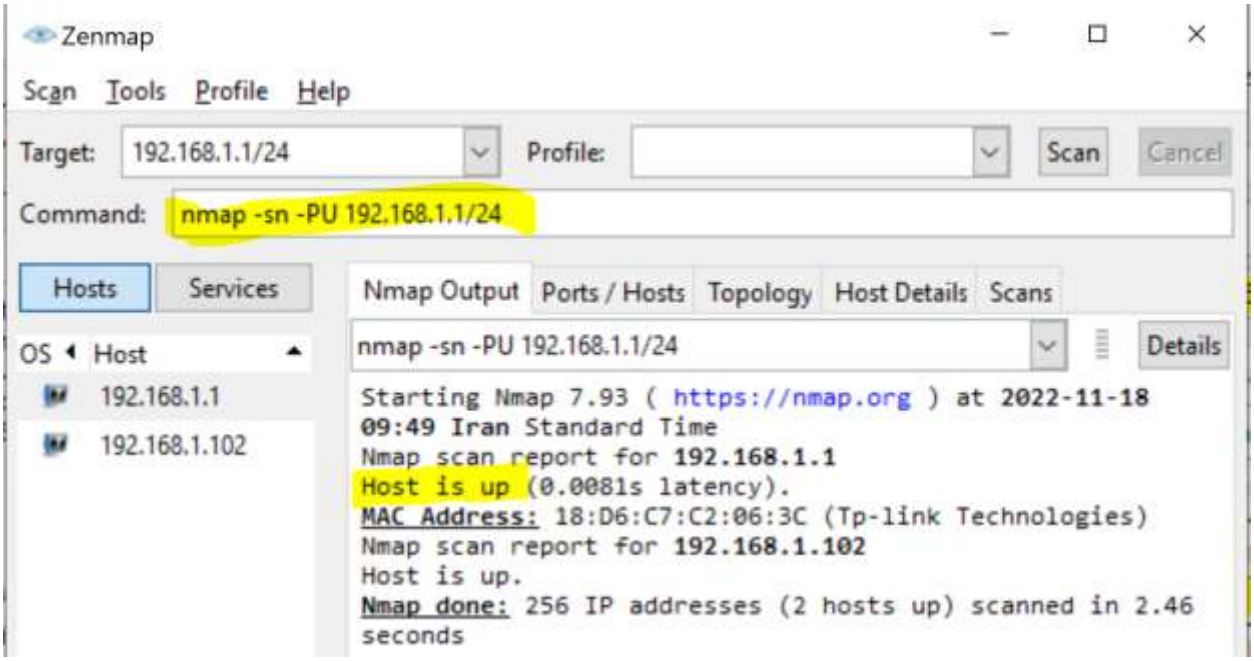
ب ۳. استفاده از nmap

بخش ۱,۱

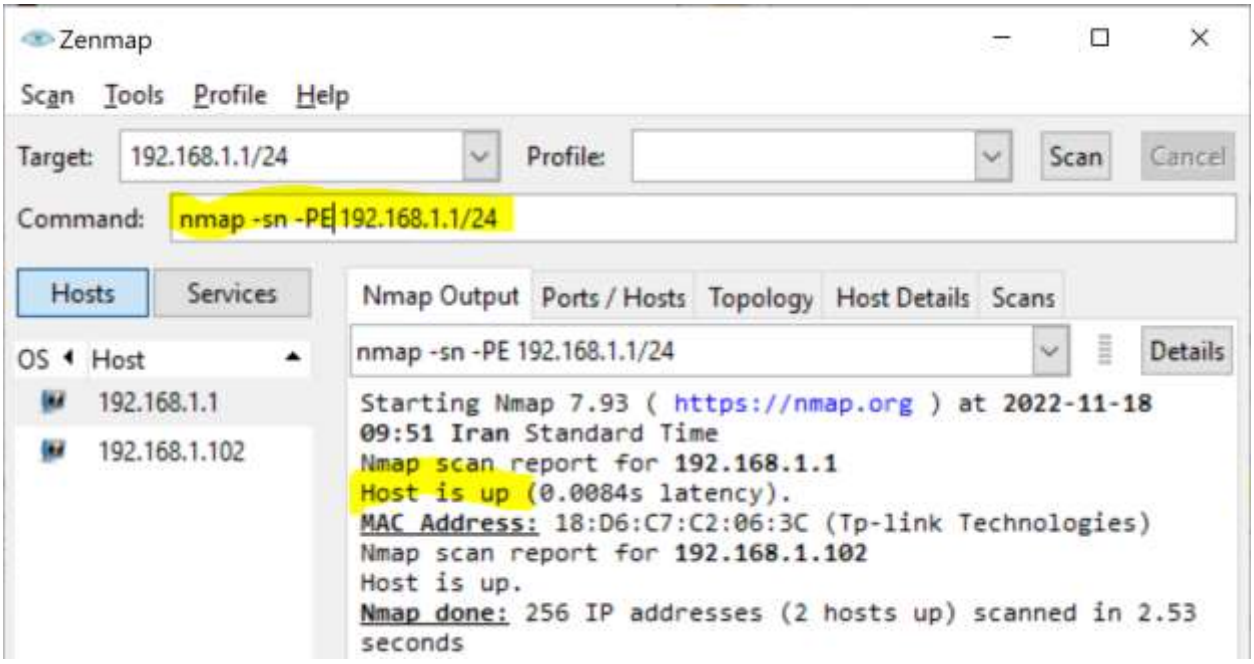
اسکن با سوییچ PR- یک اسکن ARP ping



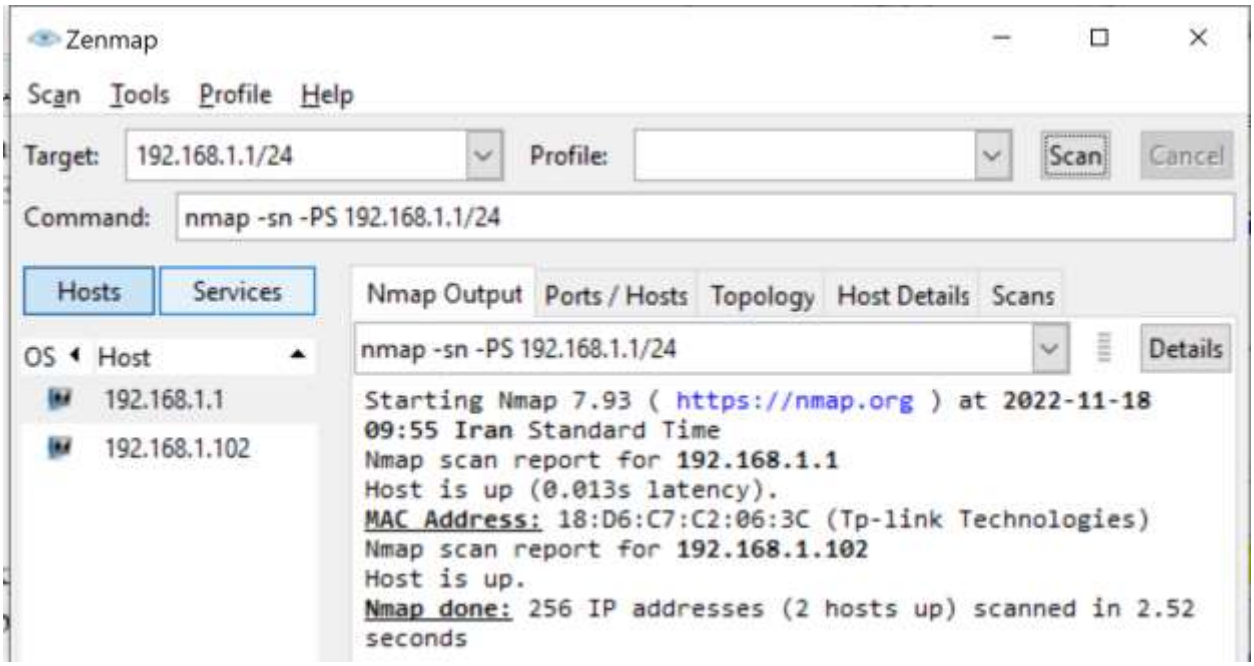
اسکن با سوییچ PU- یک اسکن UDP ping



اسکن با سوییچ PE- یک اسکن ICMP ECHO ping

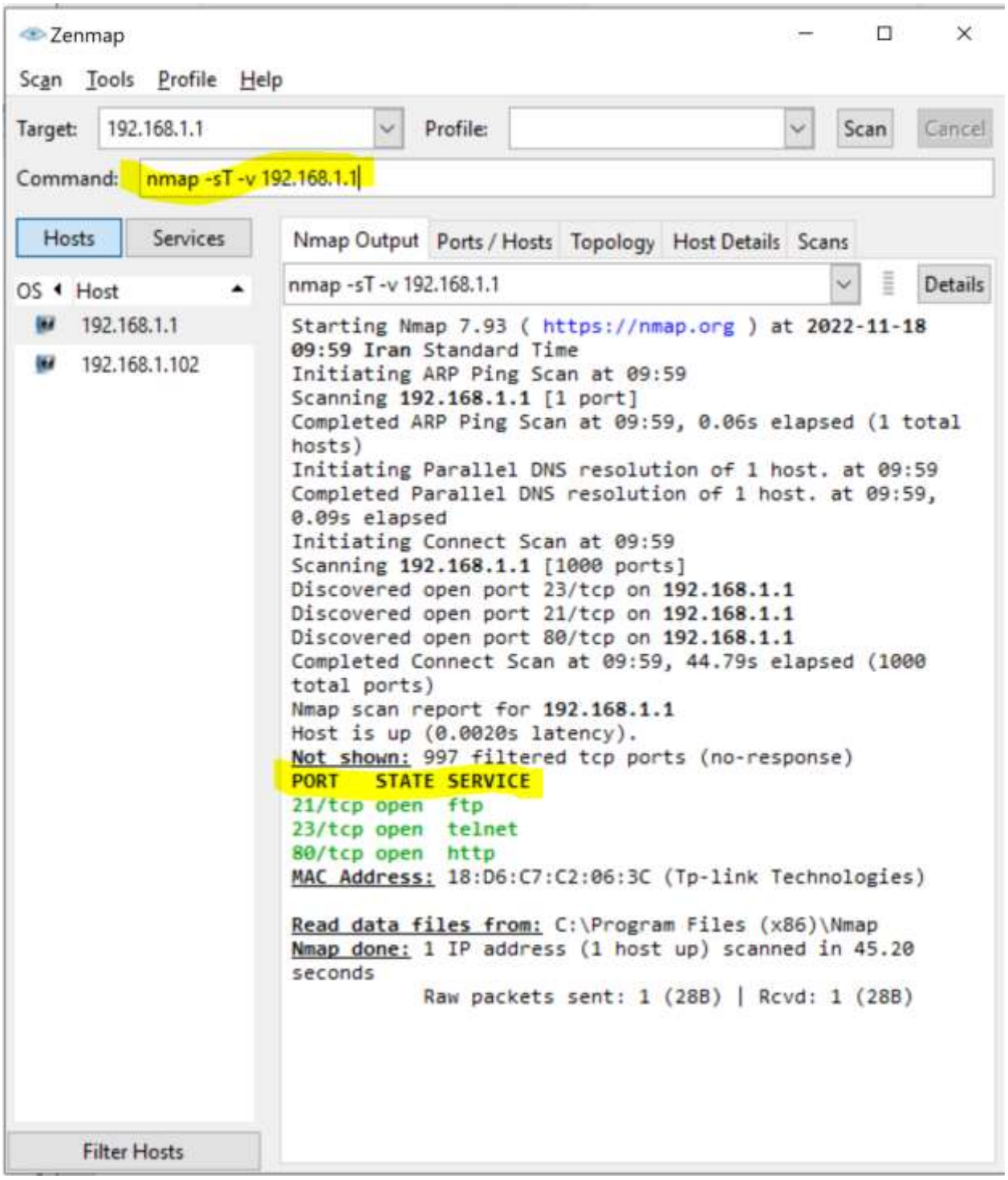


اسکن با سوییچ PS- یک اسکن که در واقع صرفا یک SYN خالی به تارگت ارسال میکند.

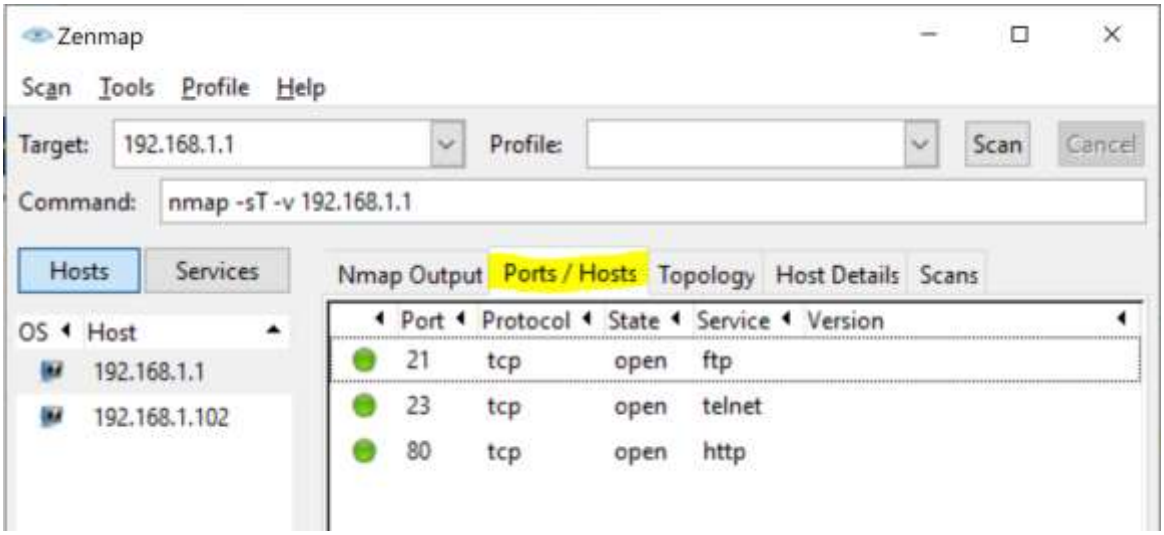


بخش ۲,۳

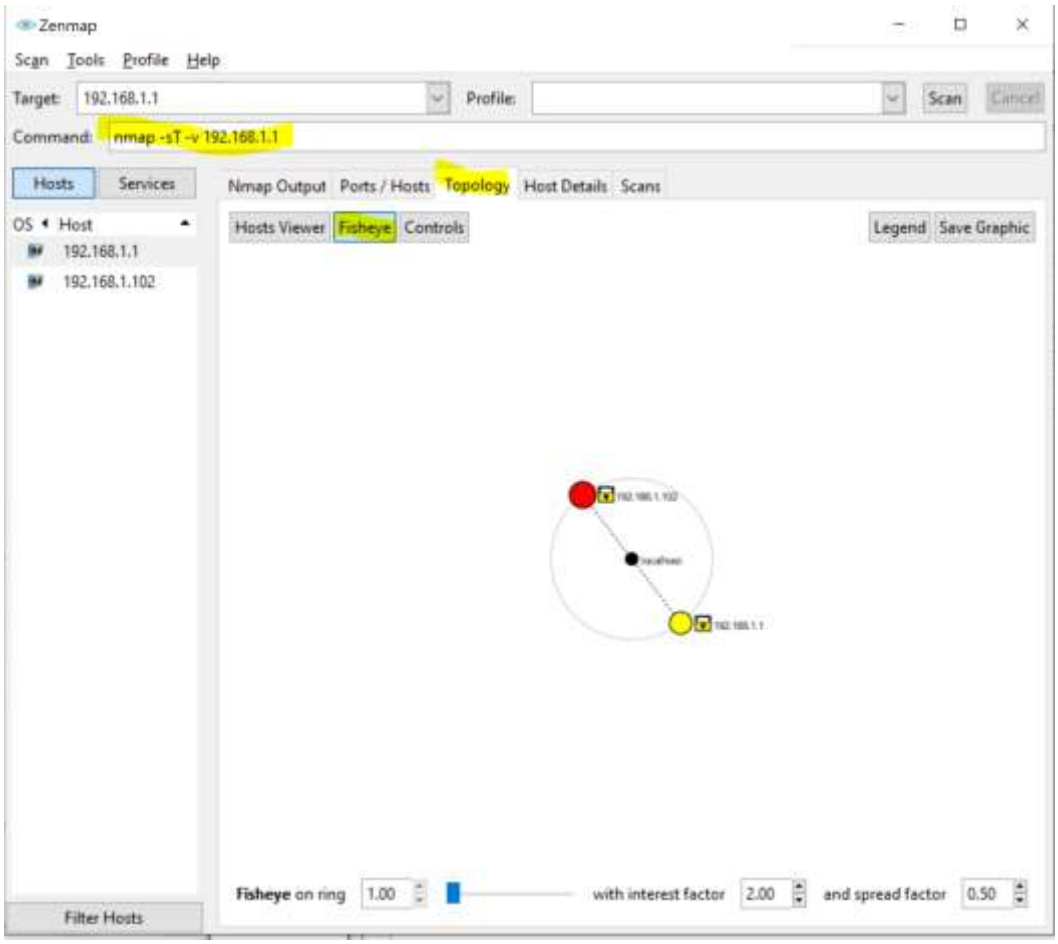
پیدا کردن پورت های باز تارگت



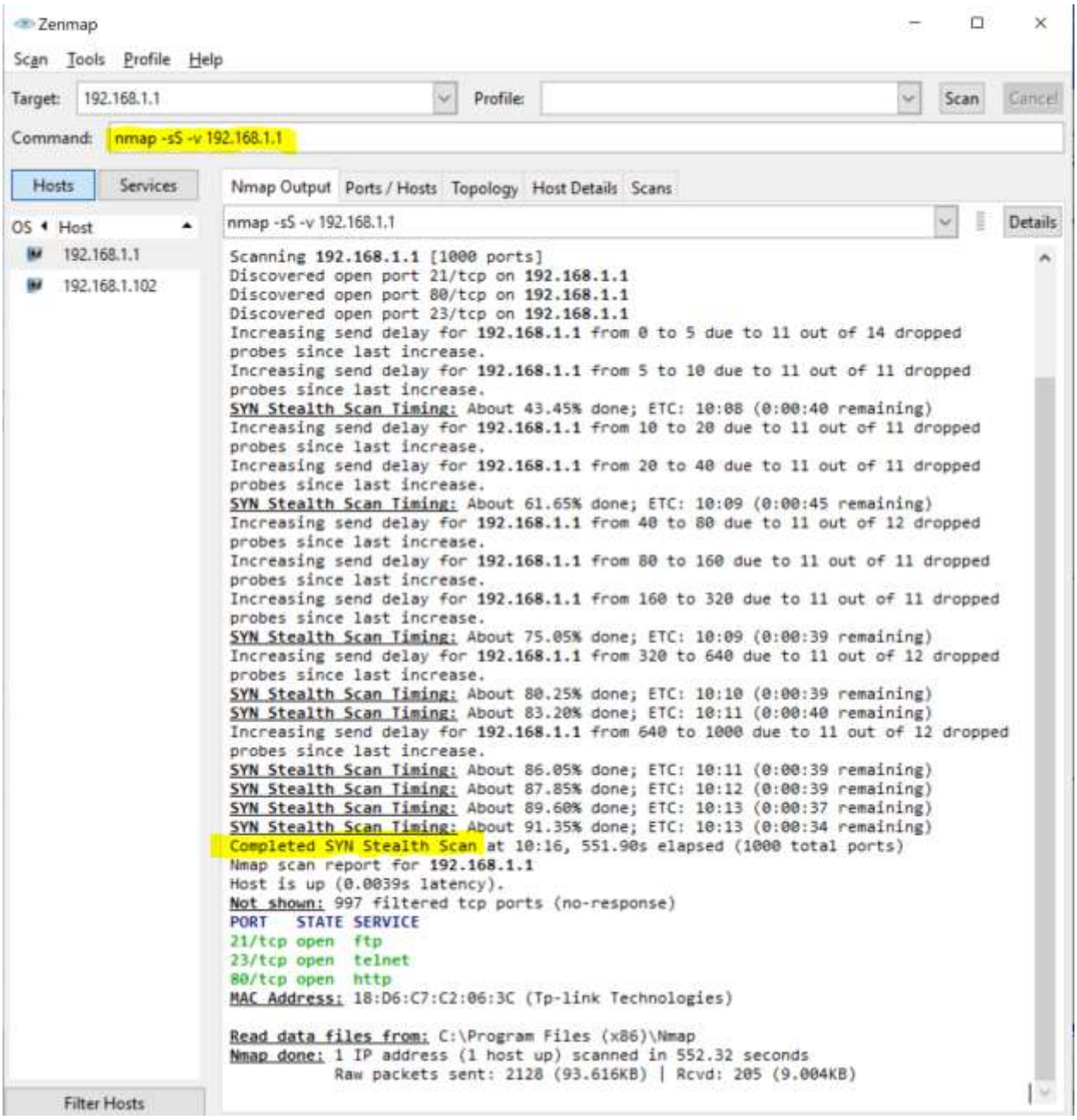
اطلاعات بخش Ports/Hosts



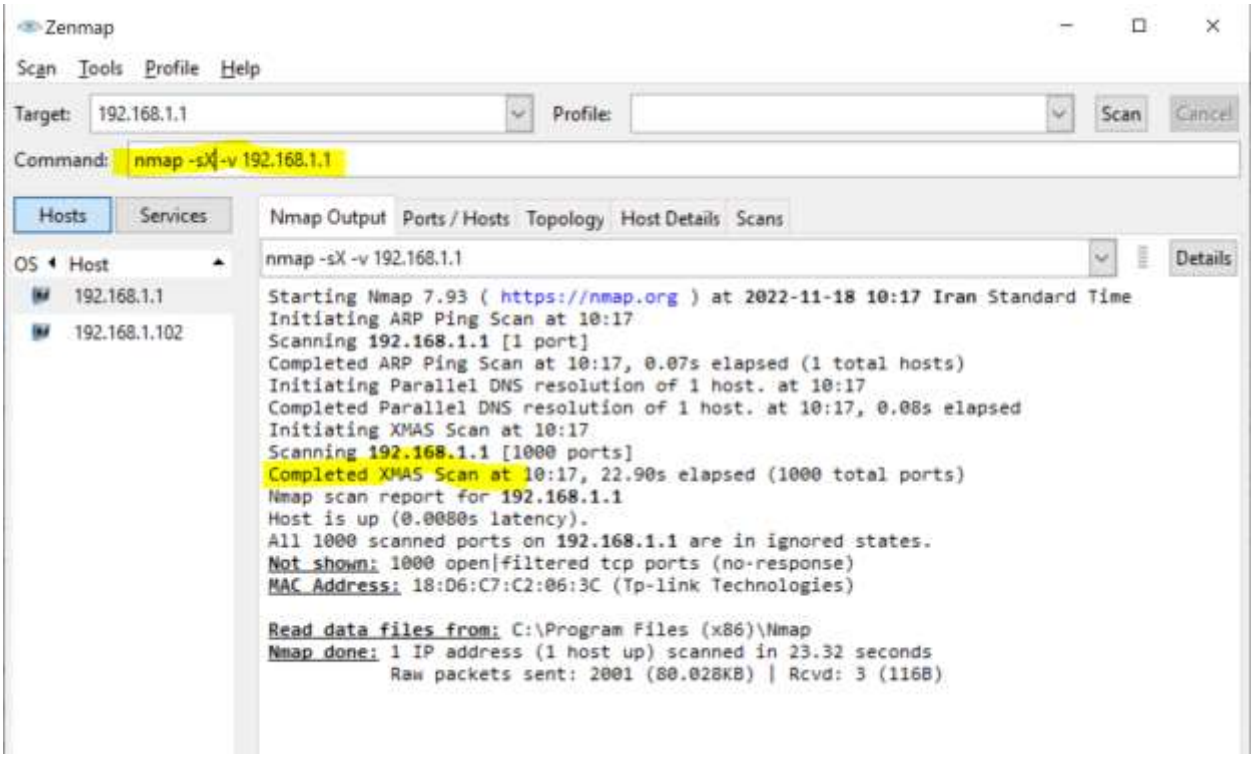
بخش Topology



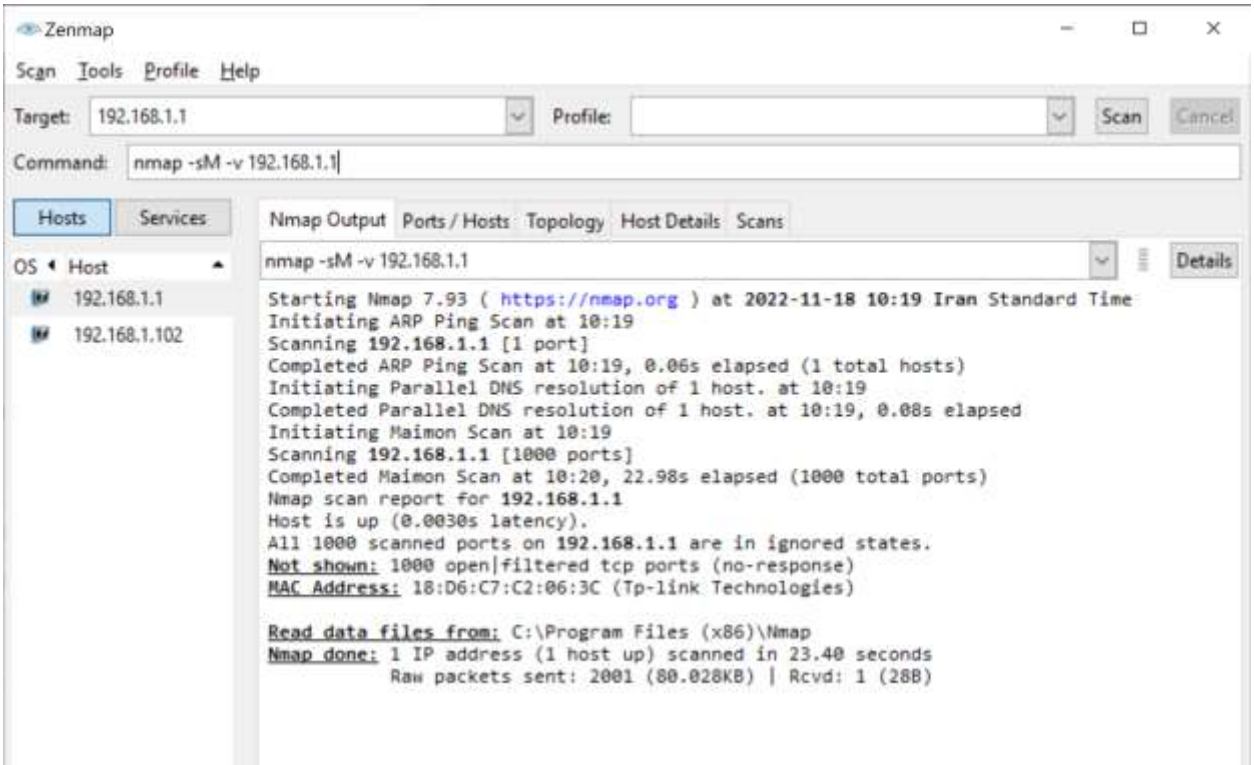
اسکن با سوئیچ sS- که به یک 3way handshake ناقص انجام میدهد.



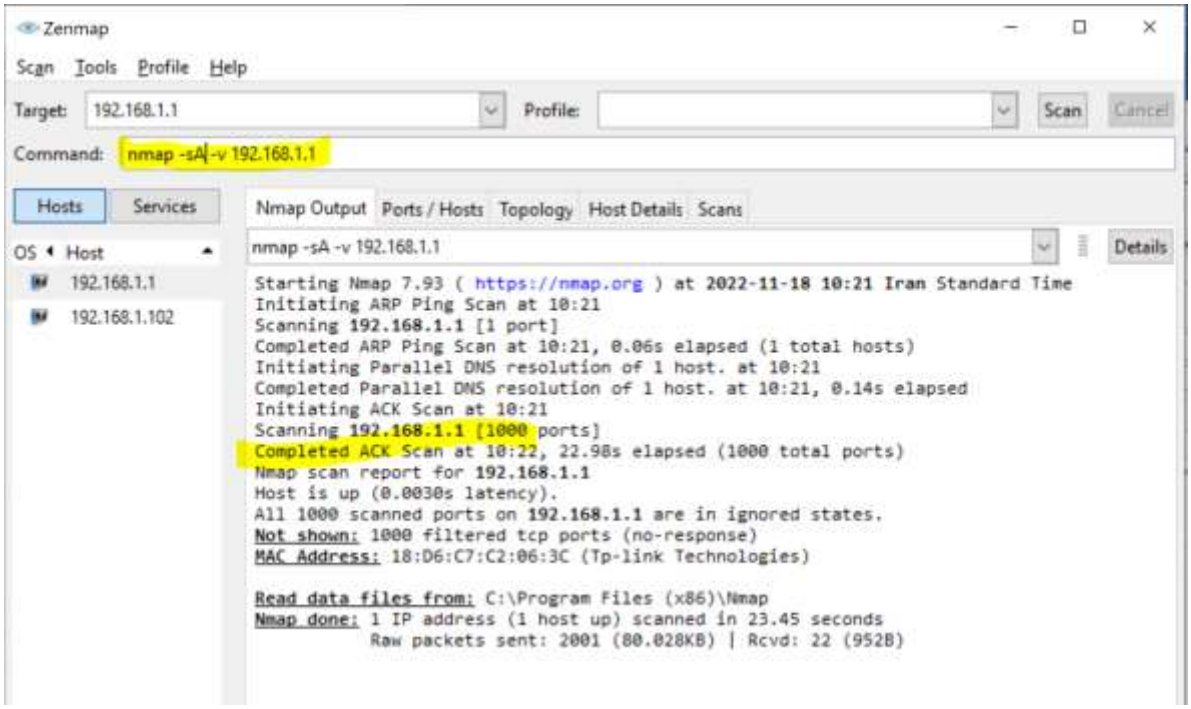
اسکن با سوئیچ sX- که ارسال پکت ها با فعال نمودن فلگ های مختلف انجام می شود.



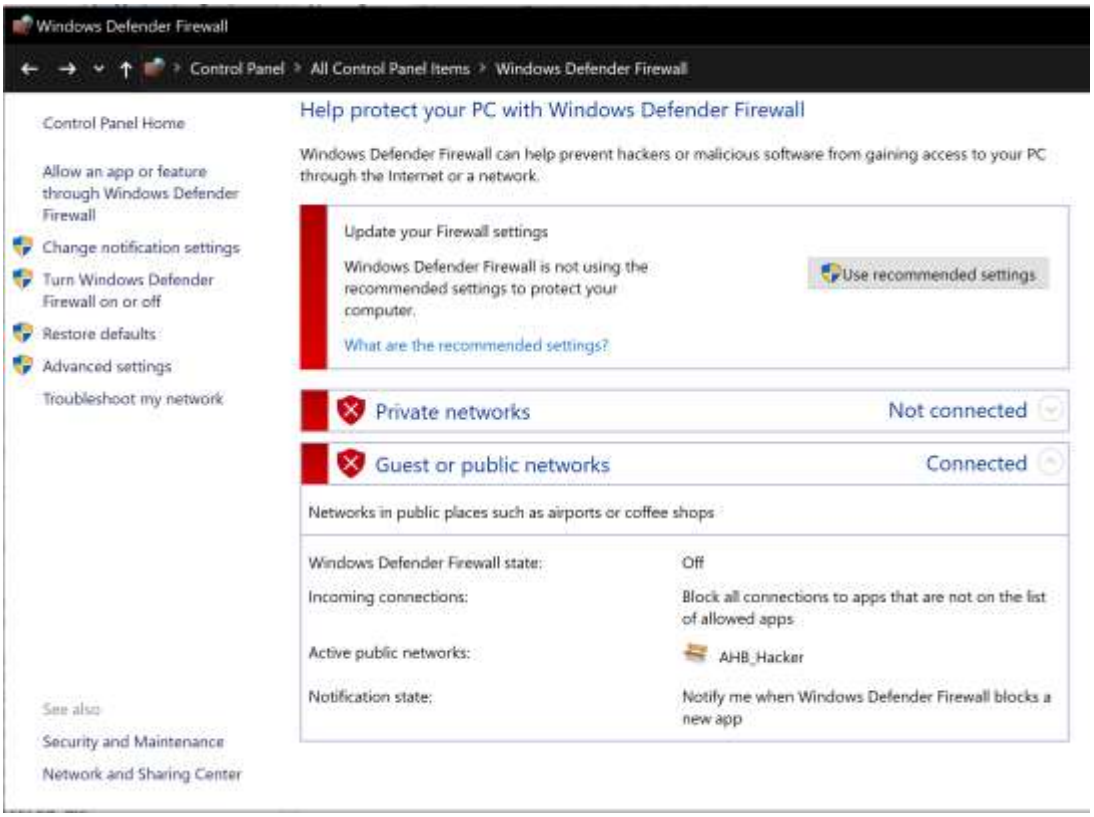
اسکن با سوئیچ sM-



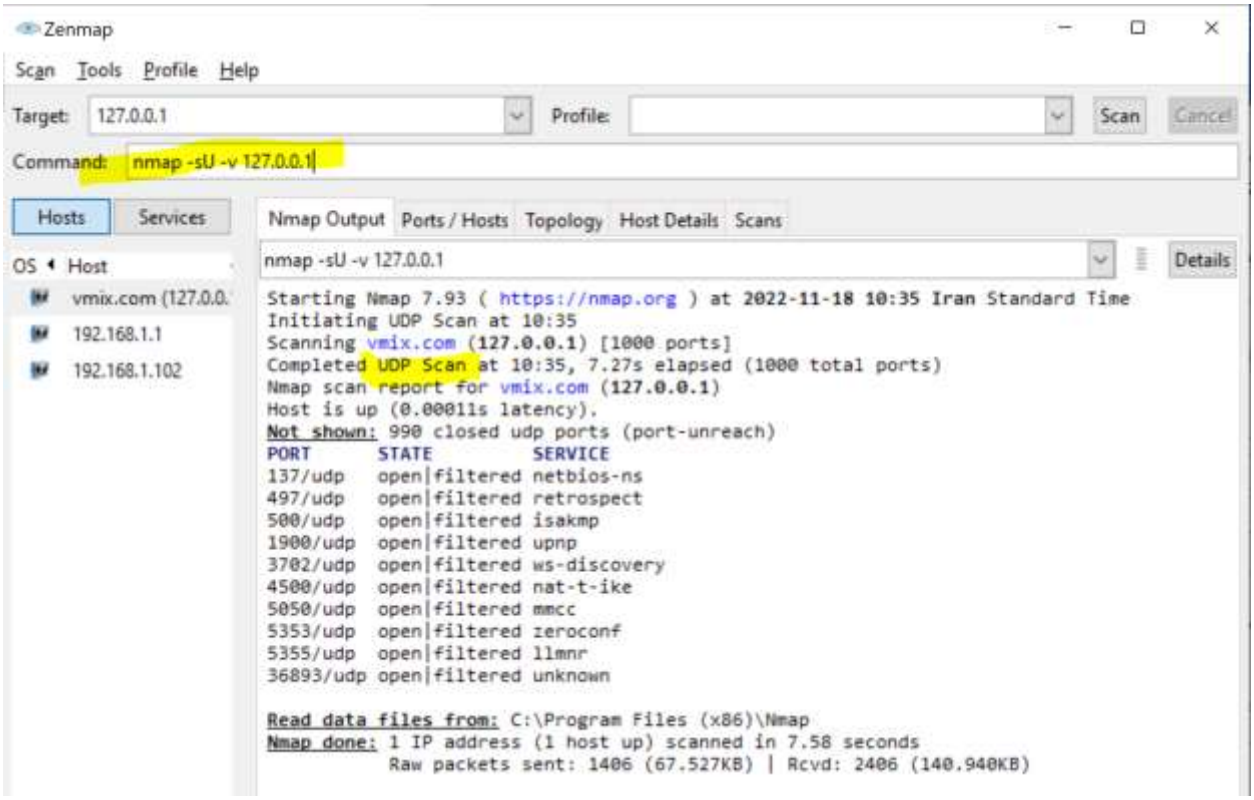
اسکن با سوئیچ sA- ارسال ACK



حال فایروال سیستم را خاموش میکنیم

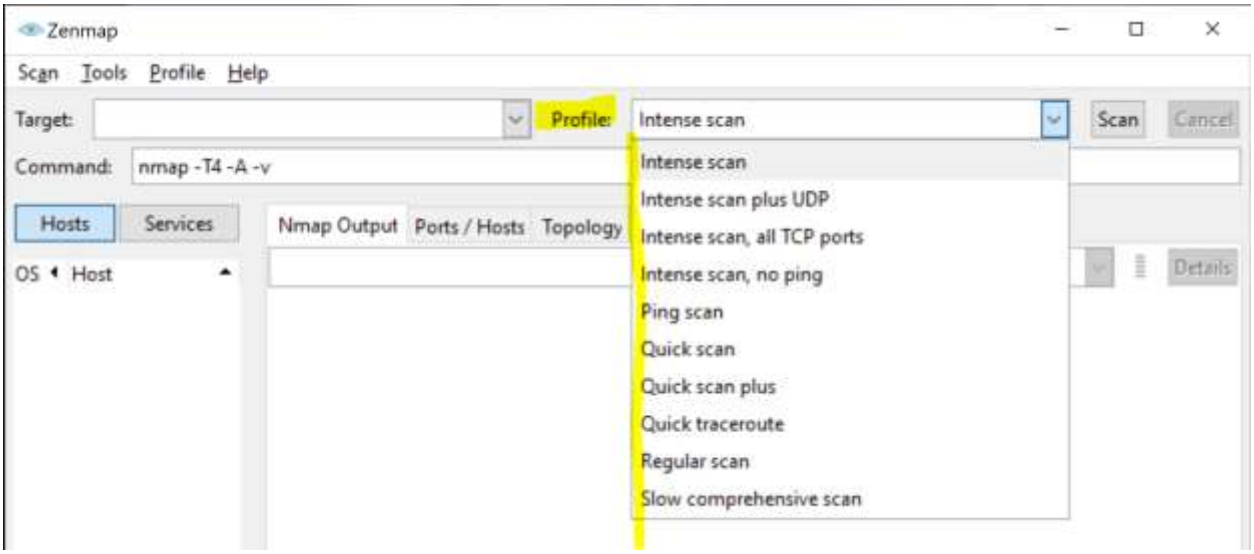


سپس با سوئیچ sU- اسکن UDP روی پورت ها انجام می دهیم



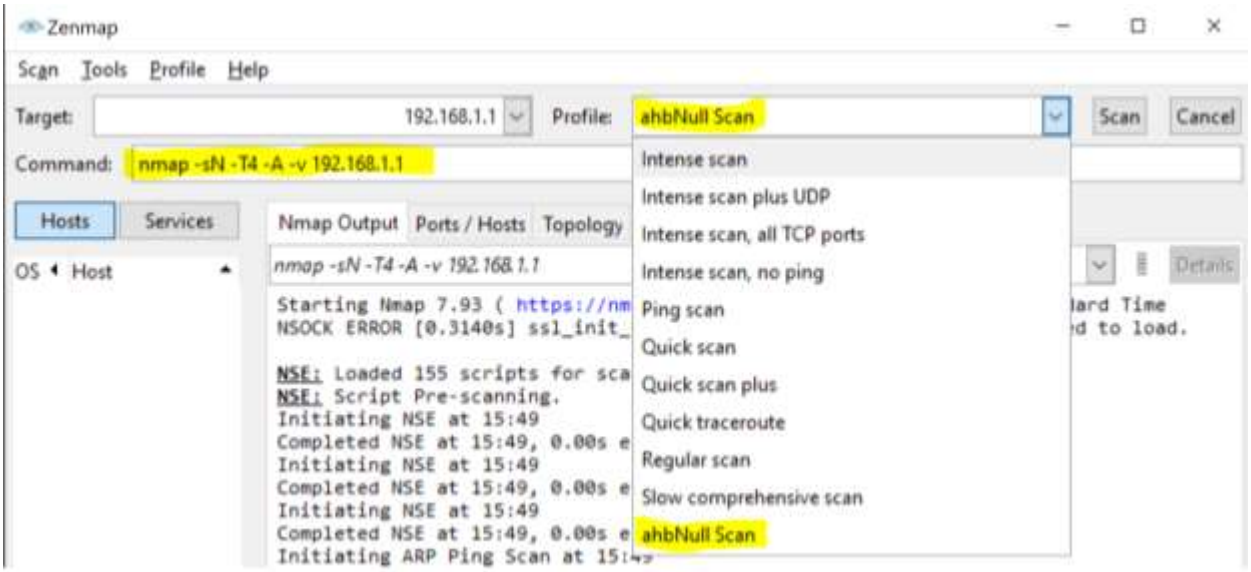
ساخت یک پروفایل در nmap

در تصویر زیر پروفایل های موجود را می توانید ببینید

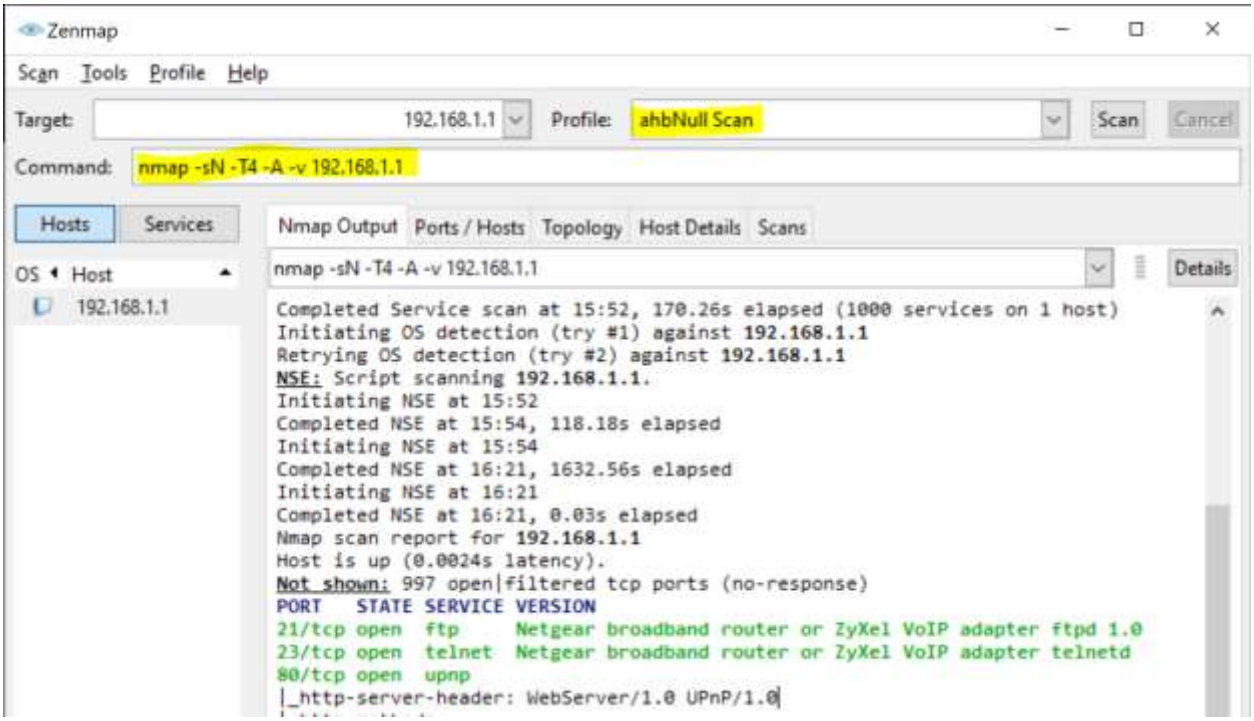


حال می خواهیم یک پروفایل جدید اضافه کنیم، از بالا profile را انتخاب میکنیم و سپس گزینه اضافه کردن یک پروفایل جدید را می زنیم، در صفحه جدید ابتدا یک نام دلخواه برای پروفایل مورد نظر انتخاب کنیم ahb Null Scan انتخاب من است.

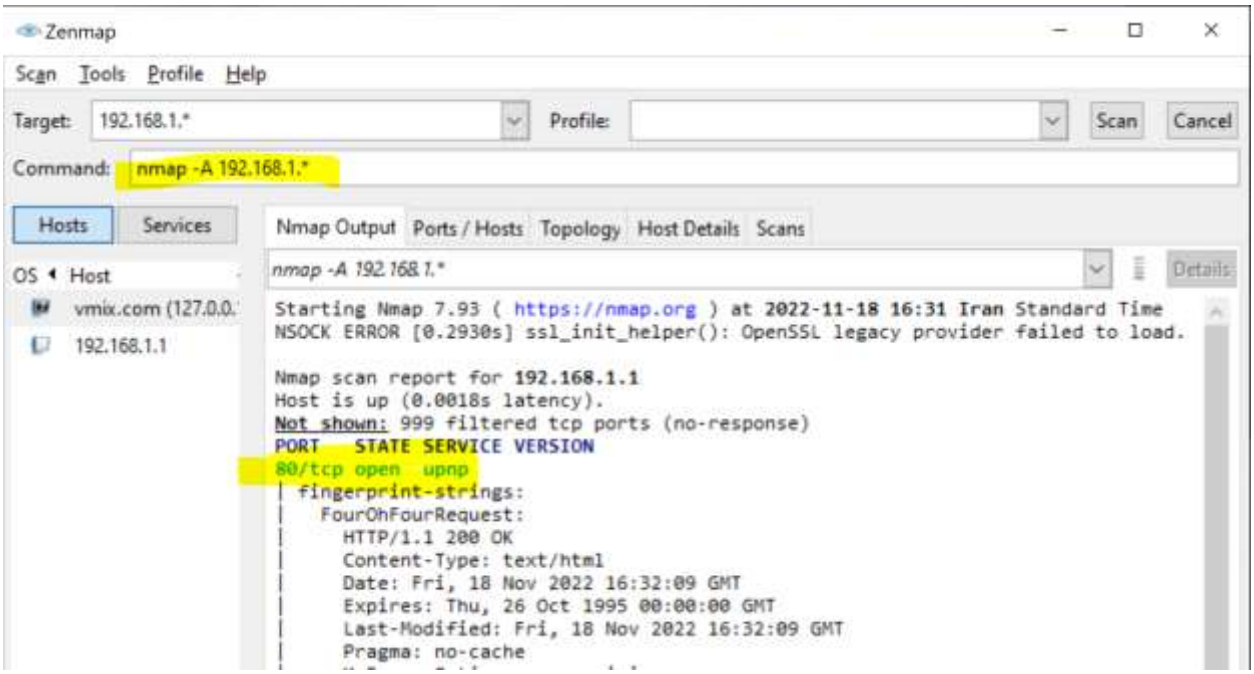
حال فعالیت های مورد نیاز را تعریف نموده و saved changes را میزنیم که پروفایل به بخش پروفایل ها افزوده می شود.



از پروفایل ساخته شده استفاده کردیم و یک اسکن Null انجام دادیم



استفاده از سوئیچ A-



Enumeration

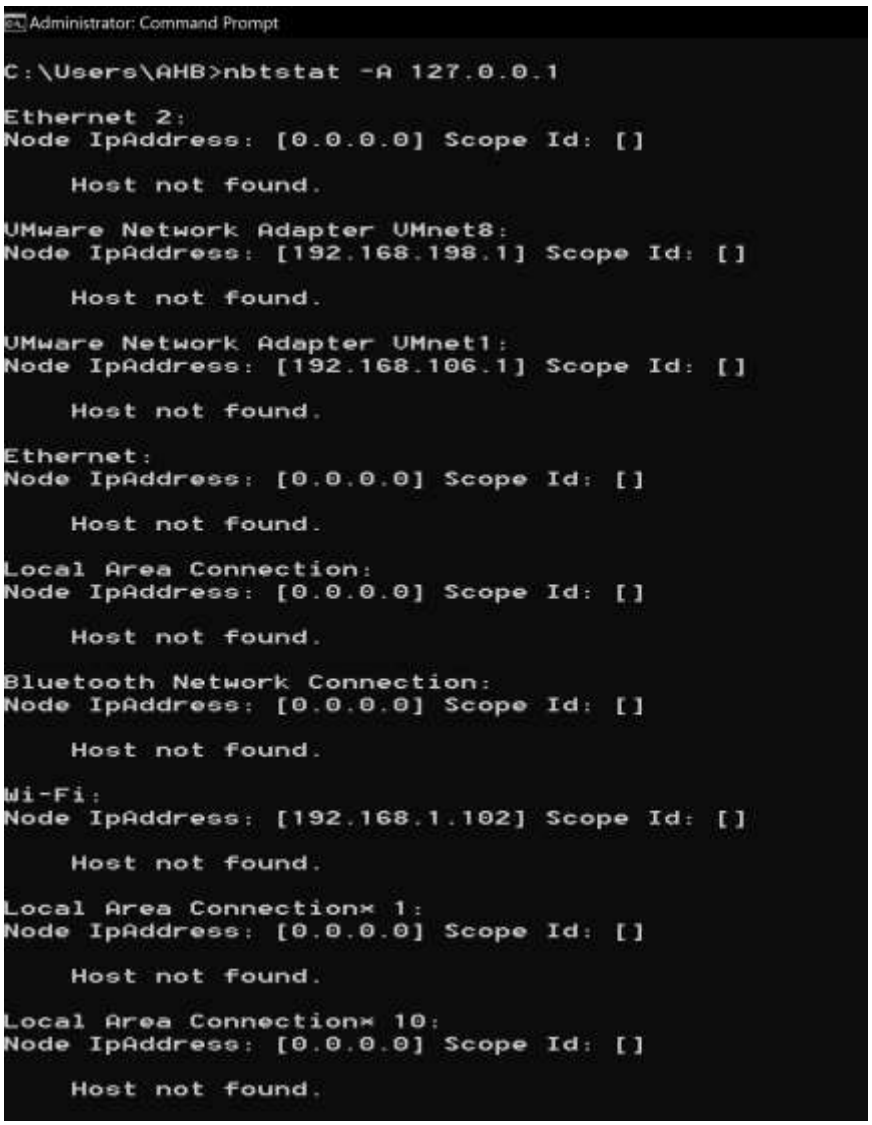
ب ۴. اسکنر های NetBios و SNMP

NetBios

این اسکن ها به ما اطلاعات مهمی از تارگت، نظیر لیستی از کامپیوتر های مرتبط با دامنه ip، آدرس MAC دیوایس شبکه، نام کامپیوتر، قوانین (پروتکل های موجود)،سرویس ها، کلمات عبور و .... را به ما میدهد.

کامند nbtstat با سوئیچ های a- ، A- و c- در ویندوز مربوط به NetBios هستند، روی پورت های ۱۳۹ و ۱۳۸ TCP و ۱۳۷ UDP کار میکند.

اجرای دستور nbtstat -A 127.0.0.1 در تصویر :



SNMP

این اسکن ها به ما اطلاعاتی از لیست های اکانت کاربران و دستگاه های داخل سیستم تارگت به ما می دهند، به ما کمک میکند دیوایس هایی که در اطراف ما SNMP در آنها فعال است را بیابیم، با توجه به اینکه SNMP در بسیاری از دیوایس ها مانند روتر ها قابل دسترس است از این رو میتوانیم احتمال دسترسی بالاتری داشته باشیم.

SNMP روی پورت ۱۶۱ UDP قرار دارد،

ب. ۵ . آزمایش DNS Enumeration Using Zone Transfer و DNSSEC Zone Walking

آزمایش پنجم

Zone Transfer

در کالی لینوکس نسخه VBox دستور زیر را در حالت Super User میزنیم.

```
dig ns amirhosseinbabaeayan.ir
```

در تصویر میتوان خروجی را مشاهده کرد (بخش های مورد نیاز هایلایت شده است.)

```
└─# dig ns www.amirhosseinbabaeayan.ir

; <<>> DiG 9.18.4-2-Debian <<>> ns www.amirhosseinbabaeayan.ir
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20303
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.amirhosseinbabaeayan.ir.   IN      NS

;; ANSWER SECTION:
www.amirhosseinbabaeayan.ir. 14400 IN   CNAME   amirhosseinbabaeayan.ir.
amirhosseinbabaeayan.ir. 21600  IN      NS      dns2.talahost.com.
amirhosseinbabaeayan.ir. 21600  IN      NS      dns1.talahost.com.
amirhosseinbabaeayan.ir. 21600  IN      NS      dns3.talahost.com.
amirhosseinbabaeayan.ir. 21600  IN      NS      dns4.talahost.com.

;; Query time: 292 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Nov 18 12:57:13 EST 2022
;; MSG SIZE  rcvd: 158
```

سپس دستور مقابل را وارد میکنیم، بخشی از دستور را با استفاده از دستور قبلی به دست آورده ایم.

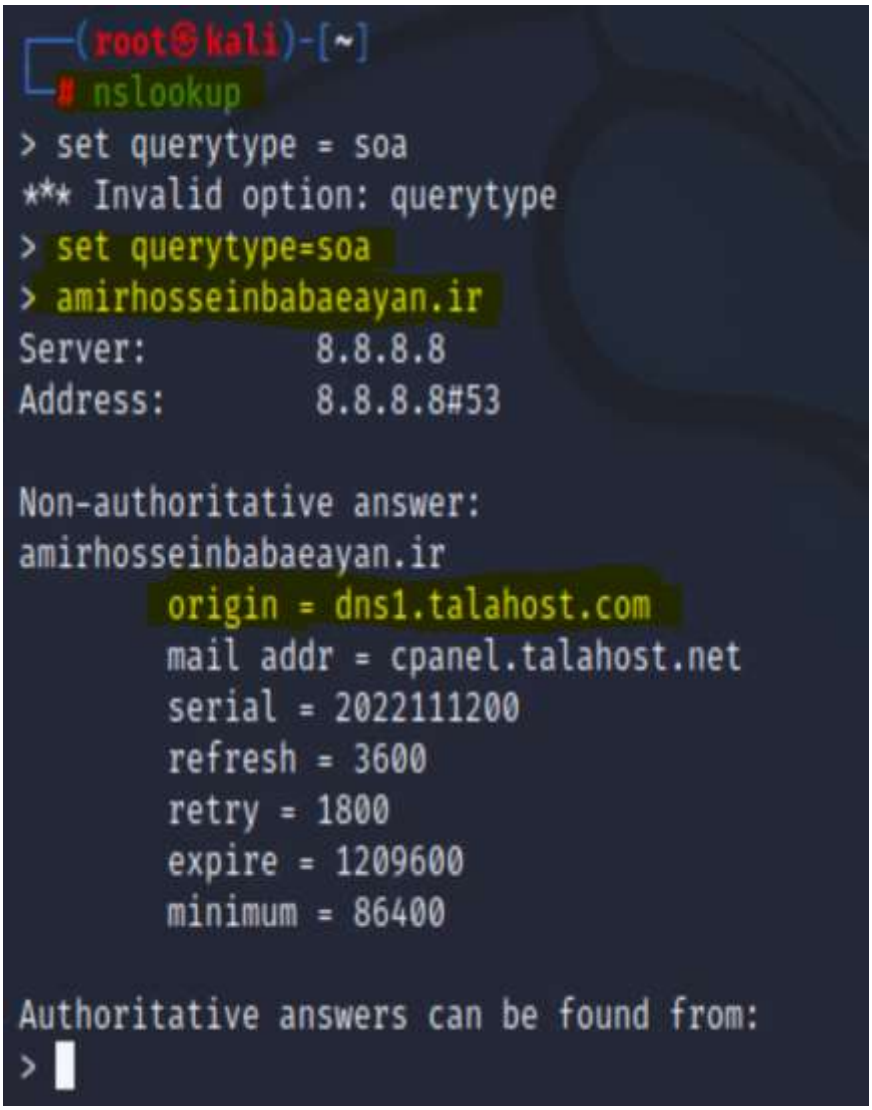
```
dig @dns2.talahost.com www.amirhosseinbabaeayan.ir axfr
```

```
┌──(root㉿kali)-[~]
└─# dig @dns2.talahost.com www.amirhosseinbabaeayan.ir axfr

; <<>> DiG 9.18.4-2-Debian <<>> @dns2.talahost.com www.amirhosseinbabaeayan.i
r axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

بر اساس آنجه در پاسخ دیدیم نتوانستیم اقدامی انجام بدهیم چرا که به Transfer faild مواجه شدیم.

حال در این گام از nslookup کمک میگیریم و querytype=soa قرار میدهیم.



در این گام کامند مقابل را تایپ میکنیم و خروجی را در تصویر میبینیم.

```
is -d dns1.talahost.com
```

```
> is -d dns1.talahost.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
is
        origin = ht-tldsecondary01.isnic.is
        mail addr = hostmaster.isnic.is
        serial = 1668795002
        refresh = 7200
        retry = 7200
        expire = 2419200
        minimum = 1800

Authoritative answers can be found from:
>
```

DNSSEC Zone Walking

```
┌──(root㉿kali)-[~]
└─# dnsrecon -d www.amirhosseinbabaeayan.ir -z
[*] std: Performing General Enumeration against: www.amirhosseinbabaeayan.ir.
..
[-] DNSSEC is not configured for www.amirhosseinbabaeayan.ir
[-] Exception "The DNS operation timed out." while resolving SOA record.
[-] Error while resolving SOA while using 213.217.60.172 as nameserver.
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.amirhosseinbabaeayan.ir
[*] Getting SOA record for www.amirhosseinbabaeayan.ir
[-] Exception "The DNS operation timed out." while resolving SOA record.
[-] Error while resolving SOA while using 213.217.60.172 as nameserver.
[-] This zone appears to be misconfigured, no SOA record found.
[*]       A www.amirhosseinbabaeayan.ir 135.181.126.180
[-] A timeout error occurred while performing the zone walk please make
[-] sure you can reach the target DNS Servers directly and requests
[-] are not being filtered. Increase the timeout to a higher number
[-] with --lifetime <time> option.
[+] 1 records found
```