

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

# کتاب الکترونیکی کوتاه و کاربردی از Nmap برای تست نفوذ

تهیه شده توسط

احسان نیک آور

عضو تیم Esecurity.ir

## مقدمه

با عرض سلام و ادب خدمت کلیه دوستان عزیز، این کتاب به عنوان یک راهنمای کوچک ولی کاربردی برای آشنایی هر چه بهتر و استفاده مناسب از ابزار کاربردی Nmap است.

در این کتاب، همانند کتب دیگر ما از نصب ابزار Nmap بر روی ویندوز یا لینوکس و ... شروع نخواهیم کرد. چرا که در کتاب های مشابه این امر توضیح داده شده است. البته این ابزار در سیستم عامل کالی لینوکس موجود است و ما از این سیستم عامل استفاده می کنیم.

این کتاب مرجعی سریع برای علاقمندان به امنیت شبکه و تست نفوذ می باشد که با زبانی ساده و به صورت کوتاه تهیه شده است که استفاده از آن آسان باشد و وقت زیادی از شما نگیرد.

این کتاب در هفت بخش تهیه شده است که در هر بخش مطالب کاربردی جهت استفاده از ابزار قدرتمند Nmap مطرح شده است.

پس پیشنهاد می کنیم تا انتهای این کتاب با ما همراه باشید.

هر کتاب و مطلبی قطعا کامل نیست و دارای نواقصی می باشد. به همین منظور هر گونه انتقاد، پیشنهاد و نظرات شما دوستان گرامی که این مطلب را مطالعه می نمایند، راه گشای ما برای تهیه کتاب ها و مطالب بعدی خواهد بود.

لذا کلیه از شما خواهشمند هستیم تا نظرات خود را به ایمیل [info@esecurity.ir](mailto:info@esecurity.ir) با موضوع Nmap ارسال نمایید.

بسیار ممنون می شوم که اگر این کتاب را مفید دانستید، آن را با دوستان خود به اشتراک بگذارید تا از این کتاب استفاده نمایند.

احسان نیک آور

## بخش اول

### Nmap در چه بخشی از تست نفوذ کاربرد دارد؟

مطابق با استاندارد شرکت Eccouncil که یکی از شرکت های بزرگ در زمینه امنیت شبکه و اطلاعات می باشد، مراحل تست نفوذ و یا اصطلاحاً Hacking Phase به پنج مرحله تقسیم می شود.

این پنج مراحل عبارتند از:

- جمع آوری اطلاعات
- اسکن یا پویش (که شامل اسکن شبکه، پورت و آسیب پذیری می باشد)
- به دست آوردن دسترسی اولیه
- ارتقاء و نگه داری دسترسی
- پاک کردن ردپا

ابزار قدرتمند Nmap در مراحل اول و دوم بسیار کاربرد دارد ولی کاربرد اصلی آن که شناخته شدن Nmap بر این اساس است، مرحله دوم یا اسکن می باشد.

در این کتاب هم ما بر روی مرحله اسکن با استفاده از Nmap تمرکز خواهیم داشت.

همانطور که اشاره شد، مرحله اسکن شامل اسکن شبکه، پورت و آسیب پذیری می باشد.

در اسکن شبکه، بازه یک شبکه و رنج آدرس های IP شناسایی می شوند.

در اسکن پورت، پورت های باز بر روی سیستم ها و سرویس های موجود بر روی آن ها شناسایی می گردد.

در اسکن آسیب پذیری، آسیب پذیری موجود بر روی سیستم مورد ارزیابی قرار خواهد گرفت.

## بخش دوم

### تعریف هدف برای Nmap

در اولین مرحله برای آشنایی با Nmap ما نیاز به تعریف هدف خود داریم که در واقع آدرس سیستم مورد نظر است. نحوه تعریف هدف به اشکال زیر امکان پذیر است:

#### **nmap 10.0.0.1**

در اولین و ساده ترین حالت، آدرس IP سیستم هدف را بعد از عبارت Nmap قرار می دهیم.

#### **nmap 10.0.0.1,2,3**

حالت دیگر جدا سازی آدرس ها با علامت کاما می باشد. (در صورت پشت سر هم بودن آدرس ها)

#### **nmap 10.0.0.1-100**

مشخص کردن بازه ای از آدرس ها که از ۱ تا ۱۰۰ در این مثال است.

#### **nmap 10.0.0.0/24**

مشخص کردن یک بازه ای از شبکه که به صورت Subnet مشخص شده است. در این مثال آدرس های ۱۰,۰,۰,۱ تا آدرس ۱۰,۰,۰,۲۵۴ هدف ما می باشد.

#### **nmap -iL list.txt**

در این مثال با استفاده از سوییچ -iL یک فایل که حاوی آدرس های IP می باشد، مورد نظر می باشد.

#### **nmap 10.0.0.0/24 --exclude 10.0.0.12**

اگر قصد داشته باشید که از یک بازه آدرس IP یک آدرس خاص را استثناء نمایید بعد از تعریف بازه آدرس از عبارت --excloude استفاده نموده و آدرس مورد نظر که نباید اسکن شود را وارد می کنید.

#### **nmap 10.0.0.0/24 --excludefile list.txt**

اگر قصد دارید تا بازه ای از آدرس ها را استثناء نمایید از دستور --excludefile در ادامه معرفی آدرس استفاده نموده و بعد از این عبارت، لیست حاوی آدرس ها را معرفی می نمایید.

#### **nmap -6 IPv6**

تا به این جا آدرس های IPv4 مد نظر ما بود. در صورتی که قصد دارید تا آدرس های IPv6 را اسکن نمایید می توانید مطابق مثال بالا عمل نمایید.

## بخش سوم

### شناسایی سیستم های روشن در شبکه و اسکن با ICMP

یکی از موارد استفاده ابزار Nmap شناسایی سیستم های روشن در شبکه است که اصطلاحاً به آن Check for Live System یا Host Discovery گفته می شود.

برای این منظور می توان از دستور زیر استفاده نمود.

#### nmap -sn IP

در این دستور به جای عبارت IP می توان از حالات مختلفی که در بخش اول به آن اشاره کرد استفاده نمود. تا از سیستم های روشن درون شبکه اطلاع حاصل نمود.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sn 10.0.0.0/24

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 15:56 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.50
Host is up (0.00025s latency).
MAC Address: 00:0C:29:9F:C4:EC (VMware)
Nmap scan report for 10.0.0.200
Host is up (0.00028s latency).
MAC Address: 00:0C:29:73:9E:96 (VMware)
Nmap scan report for 10.0.0.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.09 seconds
root@kali:~#

```

روش دیگری که برای شناسایی سیستم های روشن از آن استفاده می شود تکنیک Ping Sweep است. در این روش یک بسته ICMP حاوی ECHO Request به آدرس مورد نظر ارسال شده و در صورت بازگشت یک جواب ECHO Reply، سیستم هدف روشن در نظر گرفته می شود.



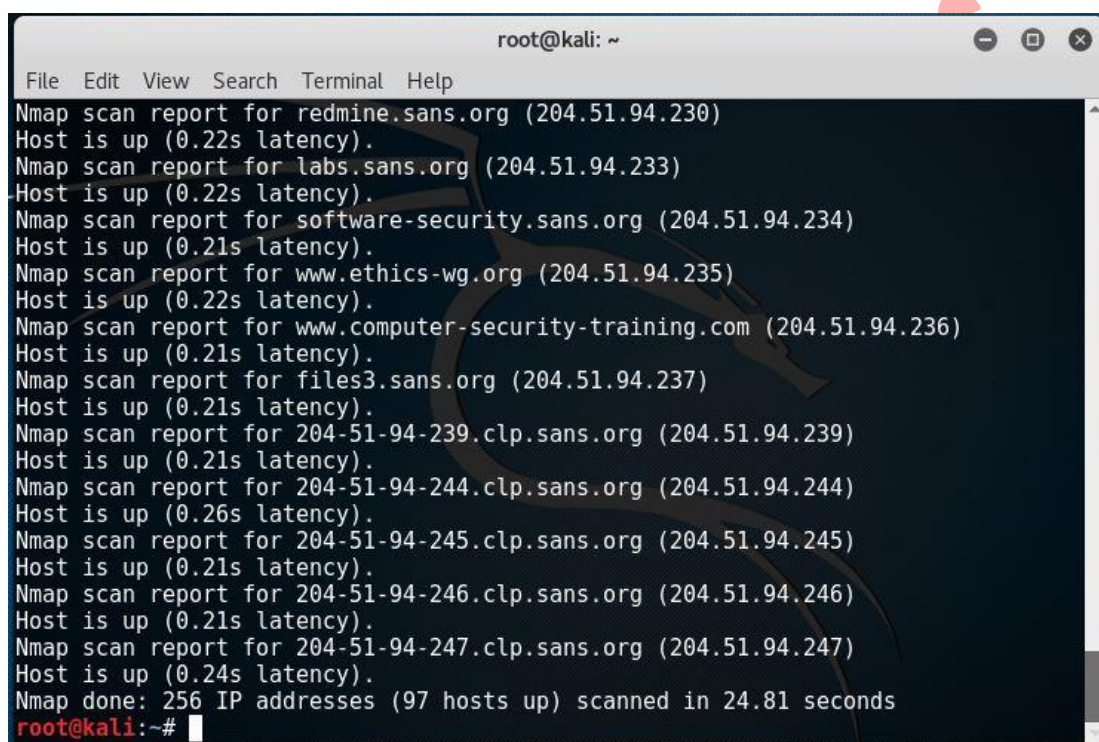
از دستور زیر برای اسکن به روش Ping Sweep استفاده می گردد.

### **nmap -sP 10.0.0.0/24**

در دستور بالا Subnet مورد نظر اسکن شده و در صورت روشن بودن هر سیستم، گزارش آن نمایش داده می شود. خروجی این دستور مشابه سوییچ -sn می باشد.

همچنین شما می توانید به جای آدرس IP از نام هاست نیز استفاده نمایید.

### **Nmap -sP eseternity.ir/24**



```

root@kali: ~
File Edit View Search Terminal Help
Nmap scan report for redmine.sans.org (204.51.94.230)
Host is up (0.22s latency).
Nmap scan report for labs.sans.org (204.51.94.233)
Host is up (0.22s latency).
Nmap scan report for software-security.sans.org (204.51.94.234)
Host is up (0.21s latency).
Nmap scan report for www.ethics-wg.org (204.51.94.235)
Host is up (0.22s latency).
Nmap scan report for www.computer-security-training.com (204.51.94.236)
Host is up (0.21s latency).
Nmap scan report for files3.sans.org (204.51.94.237)
Host is up (0.21s latency).
Nmap scan report for 204-51-94-239.clp.sans.org (204.51.94.239)
Host is up (0.21s latency).
Nmap scan report for 204-51-94-244.clp.sans.org (204.51.94.244)
Host is up (0.26s latency).
Nmap scan report for 204-51-94-245.clp.sans.org (204.51.94.245)
Host is up (0.21s latency).
Nmap scan report for 204-51-94-246.clp.sans.org (204.51.94.246)
Host is up (0.21s latency).
Nmap scan report for 204-51-94-247.clp.sans.org (204.51.94.247)
Host is up (0.24s latency).
Nmap done: 256 IP addresses (97 hosts up) scanned in 24.81 seconds
root@kali:~#

```

تصویر بالا بخشی از خروجی دستور Nmap -sP sans.org/24 می باشد.

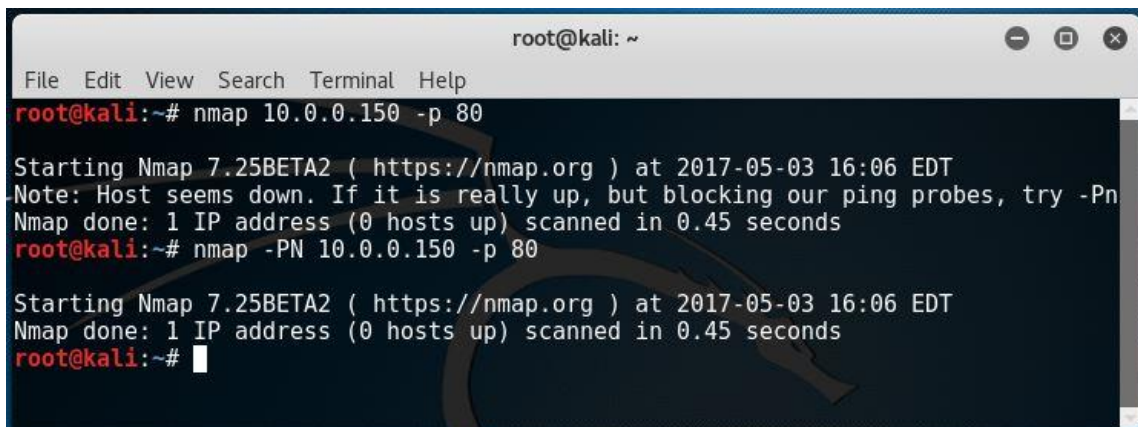
**نکته:** چون Nmap ابتدا Host Discovery انجام می دهد اگر فایروال بسته های ICMP را مسدود کرده باشد اسکن پورت انجام نمی شود. (در این حالت باید از سوییچ -PN استفاده گردد تا عملیات Host Discovery صورت نگیرد.)

### **Nmap -PN 10.0.0.10 -p 80 ➔ No Ping**

در دستور بالا با استفاده از سوییچ -PN عملیات Host Discovery صورت نمی گیرد تنها پورت ۸۰ از آدرس مورد نظر اسکن می شود. (به مبحث اسکن پورت در ادامه پرداخته می شود.)

## نکته

ابزار Nmap به حروف کوچک و بزرگ حساس می باشد.



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap 10.0.0.150 -p 80

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:06 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
root@kali:~# nmap -PN 10.0.0.150 -p 80

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:06 EDT
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
root@kali:~#

```

در تصویر بالا اولین بار دستور بدون **-PN** تست شد که در خروجی ملاحظه می نمایید که به ما می گوید:

"به نظر می رسد که هاست خاموش باشد اگر مطمئن هستید که این هاست فعال است اما توسط

فایروال، بسته های **Ping** و **ICMP** مسدود شده است، با سوییچ **-PN** تست را انجام دهید."

در دومین مرتبه که انجام شد با سوییچ **-PN** تست انجام شد که مشخص گردید هاست وجود ندارد و یا خاموش است.

بنابراین اگر سیستم هدف روشن باشد و توسط فایروال، بسته های **ICMP** مسدود شده باشد، اگر دستورات **Nmap** را بدون **-PN** وارد کنیم، ممکن است پاسخ تست دچار چالش شده و باعث نتیجه نادرست گردد.

نکته:

در **Nmap** تفاوتی میان **-Pn** و **-PN** و **-PO** وجود ندارد.



## بخش چهارم

### اسکن پورت

در ساختار شبکه، دو نوع پورت وجود دارد که شامل پورت سخت افزاری و نرم افزاری یا مجازی می باشد. پورت های سخت افزاری شامل پورت USB، PS/2، Serial، و VGA از این دست می باشد. به طور کلی پورت های سخت افزاری به صورت فیزیکی قابل رویت بوده و تعداد آنها محدود می باشد.

پورت های نرم افزاری یا مجازی بر خلاف پورت های سخت افزاری قابل مشاهده نیستند و تعداد آنها از یک تا ۶۵۵۳۵ می باشد. البته این تعداد هم برای TCP و هم برای UDP می باشد. این پورت ها به سه دسته تقسیم بندی می شوند.

۱-۱۰۲۴ پورت های مربوط به سرویس های خاص شبکه که به آن ها پورت های شناخته شده یا Well-known ports نیز گفته می شود.

۴۹۱۵۱-۱۰۲۵ پورت های تصادفی یا رندوم نامیده می شوند و زمانی که قصد برقراری ارتباط به طور مثال وب در شبکه را داریم. پورتهای که در مقصد باز می شود ۸۰ بوده و پورت باز شده سمت ما از این دسته می باشد. به این دسته از پورت ها Registered ports نیز گفته می شود.

۴۹۱۵۲-۶۵۵۳۵ این پورت ها که آزاد نامیده می شوند، بیشتر در برنامه نویسی کاربرد دارند. به این دسته از پورت ها Dynamic or private ports گفته می شود.

همانند تعریف آدرس IP که در بخش های قبل به آن اشاره شد، تعریف پورت برای ابزار Nmap هم دارای حالات مختلفی است که در این بخش به آن اشاره می شود.

### Nmap -p 80

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -Pn 10.0.0.200 -p 80

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:16 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00036s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
root@kali:~#
```

اولین و ساده ترین روش تعریف پورت به صورت بالا می باشد که با سوییچ -p و مشخص نمودن شماره پورت می باشد.

### Nmap -p 80,443,445-450,3389

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 80,443,445-450,3389 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:18 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00091s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
445/tcp    open  microsoft-ds
446/tcp   closed ddm-rdb
447/tcp   closed ddm-dfm
448/tcp   closed ddm-ssl
449/tcp   closed as-servermap
450/tcp   closed tserver
3389/tcp  closed ms-wbt-server
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
root@kali:~#

```

روش بعدی تعریف چندین پورت می باشد که با استفاده از کاما جداسازی می شود. البته می توان شماره پورت های پشت سرهم را به صورت ۴۴۵-۴۵۰ تعریف کرد.

### Nmap -p http,https,ftp

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p http,https,ftp 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:19 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00063s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   closed https
8008/tcp  closed http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
root@kali:~#

```

روش دیگر استفاده از نام پروتکل یا سرویس است که مانند مثال بالا تعریف می شود.

**Nmap -p T:80,443 U:53,123**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p T:80,443 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:21 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00038s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
root@kali:~# nmap -sU -p U:53 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:21 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00041s latency).
PORT      STATE SERVICE
53/udp    open  domain
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
root@kali:~#

```

همانطور در همین بخش به آن اشاره شد، پورت نرم افزاری وجود دارد که در واقع ۶۵۵۳۵ پورت TCP و ۶۵۵۳۵ پورت UDP می باشد. برای تعریف هر پورت TCP به عنوان مثال از عبارت T:80، ابتدا عبارت T و پس از آن شماره پورت قرار داده می شود.

**نکته**

لازم به ذکر است اگر از عبارت U برای تعریف پورت UDP استفاده نمایید، باید از سویچ -sU استفاده کرد تا UDP Scan انجام شود.

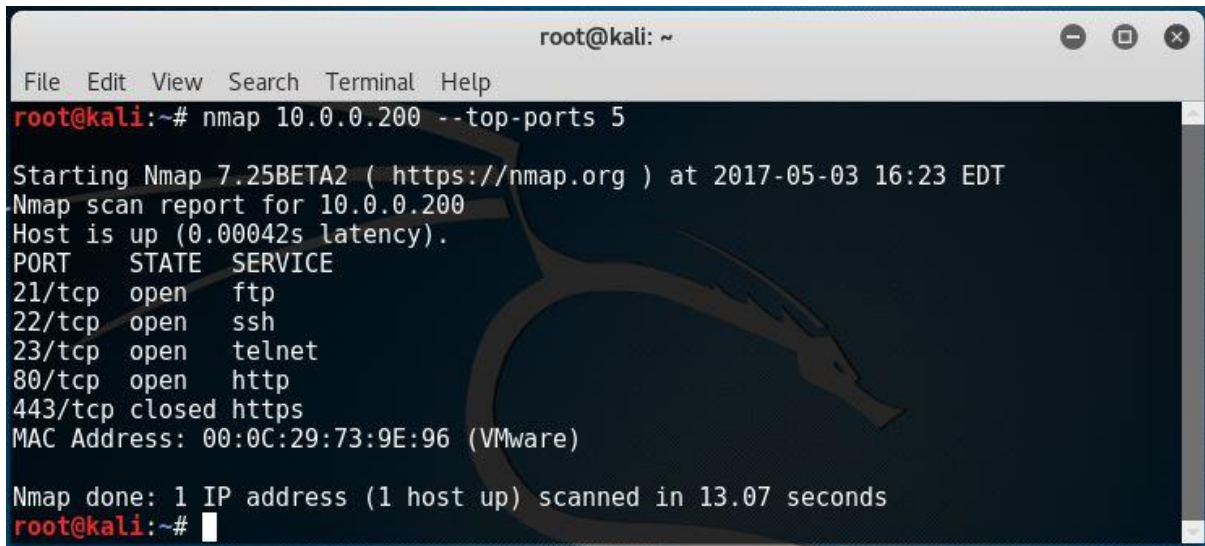
در حالت پیش فرض اسکن به صورت TCP Scan انجام می شود.

**Nmap -p -1024 → {1-1024}**

در مثال بالا در صورتی که از خط تیره (-) استفاده شود و در ادامه آن شماره ای وارد شود، کل پورت ها تا عدد مورد نظر اسکن خواهد شد. در مثال بالا ۱۰۲۴ پورت اسکن می گردد.

**Nmap --top-ports 5 → 80,23,443,21,22**

نوع دیگری از تعریف پورت، اسکن پورت های پر کاربرد یا top ports است. در این مثال با سوییچ --top-ports و قرار دادن عبارت ۵ بعد از آن، پنج پورت پرکاربرد اسکن می شود که این پورت ها ۸۰،۲۳،۴۴۳،۲۱،۲۲ می باشند.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap 10.0.0.200 --top-ports 5  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:23 EDT  
Nmap scan report for 10.0.0.200  
Host is up (0.00042s latency).  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
80/tcp    open  http  
443/tcp   closed https  
MAC Address: 00:0C:29:73:9E:96 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds  
root@kali:~#
```



## بخش پنجم

### دستورات پر کاربرد در Nmap

پس از تعریف آدرس IP و پورت، برخی از سویچ های پر کاربرد در Nmap وجود دارد که در تست نفوذ هم کاربردی می باشد.

#### Nmap -sV → Verbose

این دستور باعث می شود که اطلاعات بیشتری در مورد سرویس ارائه شود. به عنوان مثال اگر پورتنی باز باشد و از این سویچ استفاده شود، اطلاعات بیشتری در مورد پورت و سرویسی که بر روی آن قرار دارد، داده می شود. در تصویر زیر تفاوت بین خروجی Nmap بدون -sV و با این سویچ را مشاهده می نمایید.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 80 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:39 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00039s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
root@kali:~# nmap -p 80 -sV 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:39 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00036s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:73:9E:96 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.79 seconds
root@kali:~#

```

## Nmap -O → OS Detection

برای شناسایی سیستم عامل هدف می توان از سویچ -O استفاده کرد.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -O 10.0.0.200 -p 80

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:44 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00037s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.00 seconds
root@kali:~#

```

## Nmap -O --osscan-guess

اگر روش قبلی برای شناسایی سیستم عامل پاسخ گو نبود، از روش حدس سیستم عامل استفاده می شود که مطابق مثال عمل می شود.

## Nmap -F → Fast Scan (top 100 ports)

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -F 10.0.0.200

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:46 EDT
Nmap scan report for 10.0.0.200
Host is up (0.0017s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
root@kali:~#

```

سوییچ دیگر -F می باشد که اصطلاحاً اسکن سریع می باشد و ۱۰۰ پورت پرکاربرد را اسکن می کند.

**Nmap -A → Aggressive Scan = -sV , -sC , -O**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 10.0.0.200 -p 80

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:49 EDT
Nmap scan report for 10.0.0.200
Host is up (0.0029s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
|_ vulscan: scip VulDB - http://www.scip.ch/en/?vuldb:
|_ No findings

|_ MITRE CVE - http://cve.mitre.org:
|_ No findings

|_ OSVDB - http://www.osvdb.org:
|_ No findings

|_ SecurityFocus - http://www.securityfocus.com/bid/:
|_ No findings

|_ SecurityTracker - http://www.securitytracker.com:
|_ No findings

|_ IBM X-Force - http://xforce.iss.net:
|_ No findings

|_ Exploit-DB - http://www.exploit-db.com:
|_ [18329] Apache Struts2 <= 2.3.1 Multiple Vulnerabilities

|_ OpenVAS (Nessus) - http://www.openvas.org:
|_ [100858] Apache 'mod_proxy_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability

MAC Address: 00:0C:29:73:9E:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT    ADDRESS
1   2.89 ms 10.0.0.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.51 seconds

```

سوییچ بعد -A یا Aggressive می باشد که تلفیقی از سوییچ های -sV، -sC و -O می باشد که -sC شامل اعمال اسکریپت های پیش فرض می باشد. این مورد و همچنین چگونگی شناسایی top ports در سمینار آموزشی Nmap که در سایت Esecurity.ir وجود دارد، توضیح داده شده است.

برای مشاهده جزئیات فیلم سمینار Nmap به لینک زیر مراجعه نمایید. لازم به ذکر است این سمینار به صورت رایگان برای اعضای مدرسه امنیت برگزار گردید.

همچنین شما که این کتاب را مطالعه می نمایید می توانید این بسته آموزشی را با تخفیف بسیار ویژه تهیه نمایید. برای اطلاعات بیشتر و خرید فیلم کامل آموزشی سمینار Nmap به لینک زیر مراجعه نمایید.

**سمینار آموزشی Nmap**



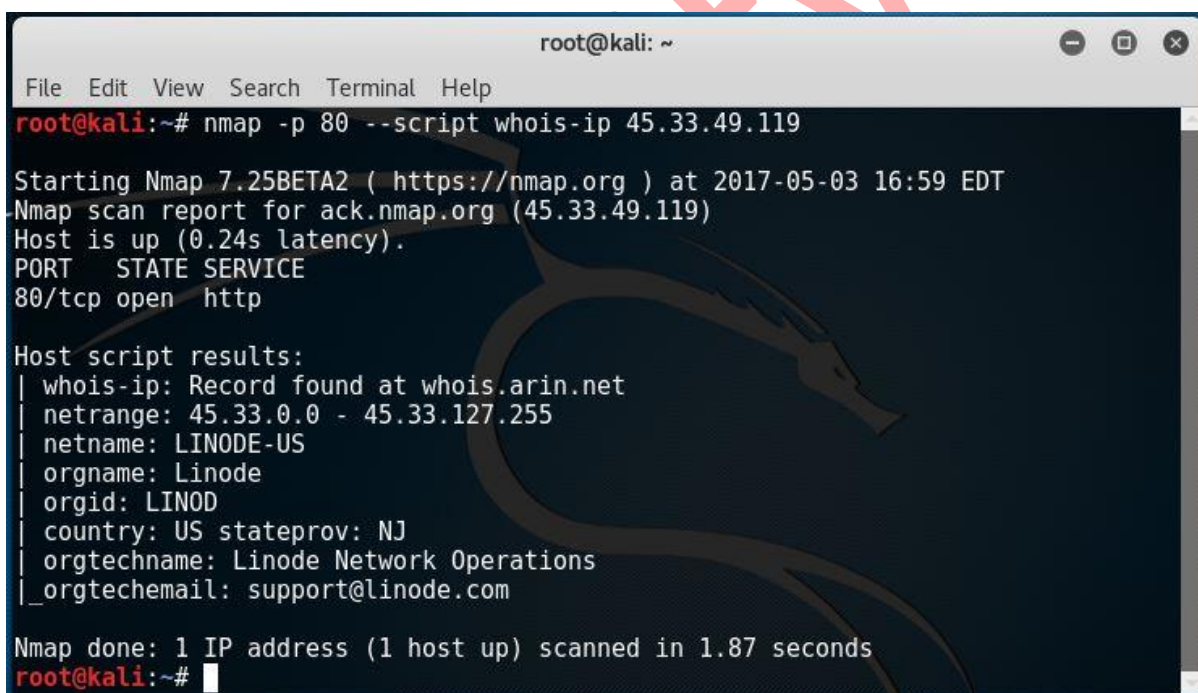
## بخش ششم

### اسکریپت های Nmap

علاوه بر مواردی که به آن اشاره نمودیم، Nmap دارای یک موتور اسکریپتی هم می باشد. در واقع Nmap دارای اسکریپت هایی می باشد که کارهای خاصی را انجام می دهند. تعداد زیادی اسکریپت در Nmap وجود دارد که در کالی لینوکس در مسیر `/usr/share/nmap/scripts` قرار دارند.

برای مشاهده اسکریپت های موجود باید وارد مسیر ذکر شده، شوید. همچنین برای استفاده از یک اسکریپت در Nmap از سوییچ `--script` استفاده شده و پس از آن نام اسکریپت مورد نظر قرار داده می شود. مثال زیر نمونه ای از استفاده یک اسکریپت در Nmap می باشد.

**nmap -p 80 --script whois-ip 20.0.0.1**



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 80 --script whois-ip 45.33.49.119

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 16:59 EDT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.24s latency).
PORT      STATE SERVICE
80/tcp    open  http

Host script results:
| whois-ip: Record found at whois.arin.net
| netrange: 45.33.0.0 - 45.33.127.255
| netname: LINODE-US
| orgname: Linode
| orgid: LINOD
| country: US stateprov: NJ
| orgtechname: Linode Network Operations
|_orgtechemail: support@linode.com

Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
root@kali:~#
  
```

در این مثال از اسکریپت `whois-ip` برای استخراج اطلاعات Whois مربوط به IP ۲۰,۰,۰,۱ استفاده می شود.

در این نوع از اسکریپت ها برای جلوگیری از اسکن پورت های پیش فرض از سوییچ `-p` و شماره پورت ۸۰ استفاده می شود.

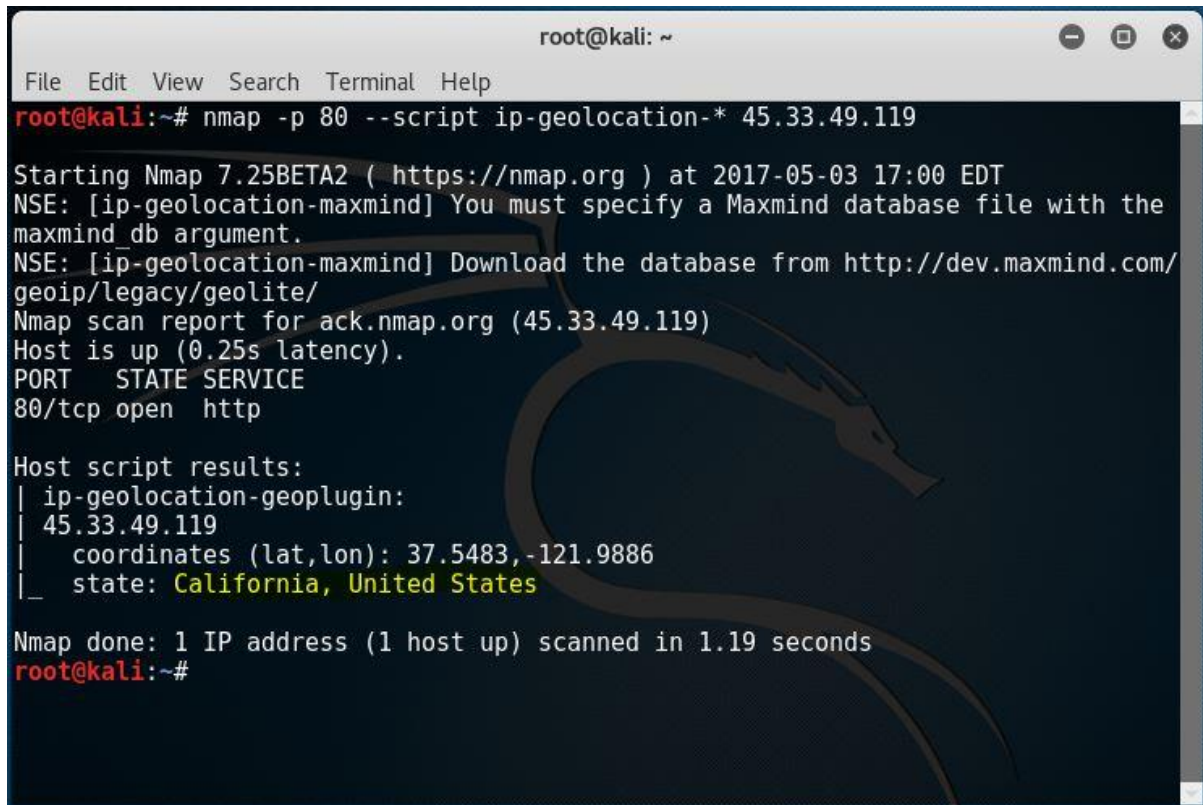


## نمونه های دیگری از اسکریپت های Nmap

**nmap -p 80 --script whois-domain esecurity.ir**

اسکریپت بالا اطلاعات Whois مربوط به دامین مورد نظر را به شما می دهد.

**nmap -p 80 --script ip-geolocation-\* IP**



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -p 80 --script ip-geolocation-* 45.33.49.119  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:00 EDT  
NSE: [ip-geolocation-maxmind] You must specify a Maxmind database file with the  
maxmind_db argument.  
NSE: [ip-geolocation-maxmind] Download the database from http://dev.maxmind.com/  
geoip/legacy/geolite/  
Nmap scan report for ack.nmap.org (45.33.49.119)  
Host is up (0.25s latency).  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Host script results:  
| ip-geolocation-geoplugin:  
| 45.33.49.119  
|   coordinates (lat,lon): 37.5483,-121.9886  
|_  state: California, United States  
  
Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds  
root@kali:~#
```

با استفاده از اسکریپت بالا، موقعیت جغرافیایی یک آدرس IP شناسایی می گردد.

**nmap -p 80 --script whois-ip 193.70.88.144**

اسکریپت بالا همانطور که اشاره شد برای Whois آدرس IP استفاده می شود.

## nmap -p80 --script dns-brute nmap.org

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p80 --script dns-brute sans.org

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:06 EDT
Nmap scan report for sans.org (204.51.94.202)
Host is up (0.23s latency).
rDNS record for 204.51.94.202: mail.sans.org
PORT      STATE SERVICE
80/tcp    open  http

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   admin.sans.org - 204.51.94.215
|   www.sans.org - 204.51.94.202
|   www2.sans.org - 66.35.59.202
|   oracle.sans.org - 10.10.10.10
|   mail.sans.org - 204.51.94.202
|   mail2.sans.org - 66.35.59.44
|   sip.sans.org - 52.113.65.139
|_

Nmap done: 1 IP address (1 host up) scanned in 20.40 seconds
root@kali:~#

```

اسکرپت بالا برای پیدا کردن دامین های زیر مجموعه سایت nmap.org استفاده می شود که شما می توانید به جای این سایت، سایت مورد نظر خود را قرار دهید.

## nmap -p80 --script http-waf-detect esecurity.ir

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p80 --script http-waf-detect esecurity.ir

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:08 EDT
Nmap scan report for esecurity.ir (193.70.88.144)
Host is up (0.11s latency).
rDNS record for 193.70.88.144: 144.ip-193-70-88.eu
PORT      STATE SERVICE
80/tcp    open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_ esecurity.ir:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
root@kali:~#

```

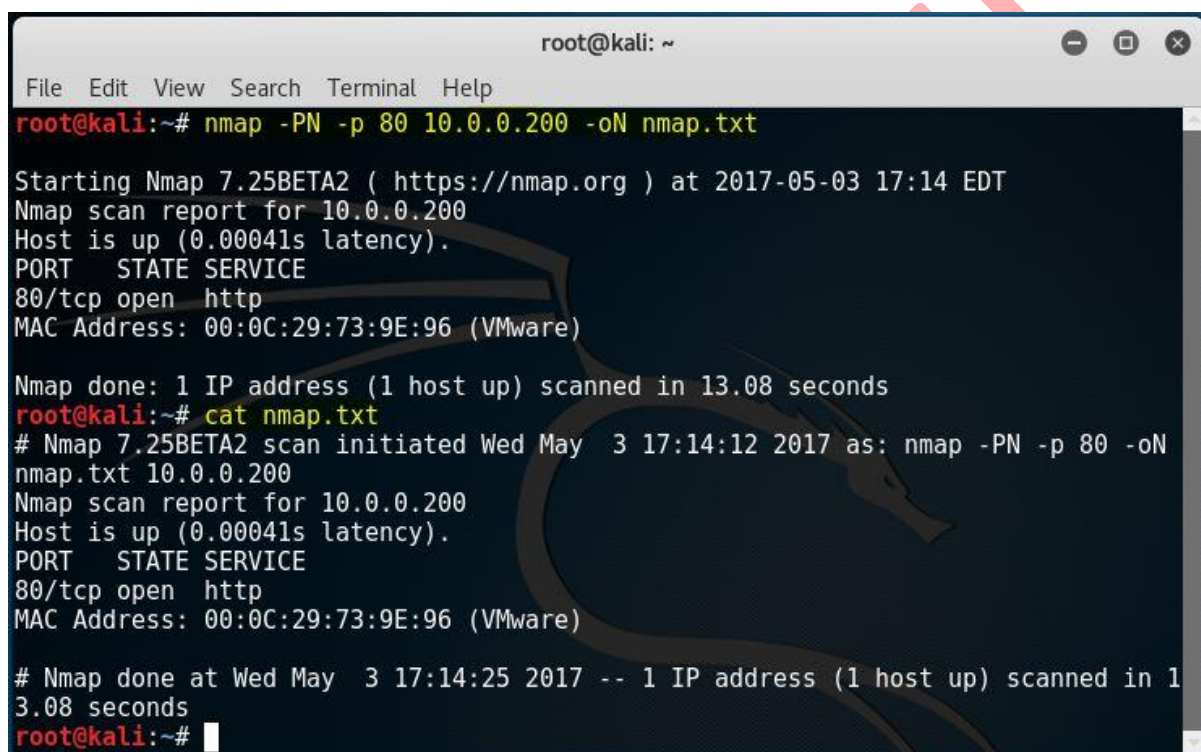
از اسکرپت بالا برای شناسایی فایروال تحت وب یا Web Application Firewall یک وب سایت استفاده می شود.

## بخش هفتم

### انواع خروجی ها در Nmap

پس از اینکه با سوییچ های مختلف و نحوه معرفی آدرس و پورت در Nmap آشنا شدید، هم اکنون باید اطلاعات به دست آمده را در قالب یک خروجی ذخیره نمود تا در آینده به توان از آن استفاده نمود. در این بخش با انواع خروجی ها و کاربرد آن آشنا خواهیم شد.

#### -oN → Nmap File(Text file)



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PN -p 80 10.0.0.200 -oN nmap.txt
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:14 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00041s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
root@kali:~# cat nmap.txt
# Nmap 7.25BETA2 scan initiated Wed May 3 17:14:12 2017 as: nmap -PN -p 80 -oN
nmap.txt 10.0.0.200
Nmap scan report for 10.0.0.200
Host is up (0.00041s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

# Nmap done at Wed May 3 17:14:25 2017 -- 1 IP address (1 host up) scanned in 1
3.08 seconds
root@kali:~#

```

با استفاده از دستور بالا، خروجی Nmap در قالب یک فایل متنی قرار می گیرد. در برخی از کتاب های آموزشی Nmap به این نوع خروجی Nmap File هم گفته می شود.



**-oX → XML File**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PN -p 80 10.0.0.200 -oX nmap.xml

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:17 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00044s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
root@kali:~# cat nmap.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xml" type="text/xsl"?>
<!-- Nmap 7.25BETA2 scan initiated Wed May 3 17:17:15 2017 as: nmap -PN -p 80 -oX nmap.xml 10.0.0.200 -->
<nmaprun scanner="nmap" args="nmap -PN -p 80 -oX nmap.xml 10.0.0.200" start="1493846235" starttime="Wed May 3 17:17:15 2017" version="7.25BETA2" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1" services="80"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1493846235" endtime="1493846248"><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="10.0.0.200" addrtype="ipv4"/>
<address addr="00:0C:29:73:9E:96" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
<ports><port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" method="table" conf="3"/></port>
</ports>
<times srtt="441" rttvar="3761" to="1000000"/>
</host>
<runstats><finished time="1493846248" timestr="Wed May 3 17:17:28 2017" elapsed="13.09" summary="Nmap done at Wed May 3 17:17:28 2017; 1 IP address (1 host up) scanned in 13.09 seconds" exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun>

```

نوع دیگری از خروجی که توسط Nmap پشتیبانی می گردد، XML است. که برای این نوع خروجی از سویچ بالا استفاده می شود.

**-oG → Grep support file**

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -PN -p 80 10.0.0.200 -oG nmap.gnmap  
  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:23 EDT  
Nmap scan report for 10.0.0.200  
Host is up (0.00040s latency).  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 00:0C:29:73:9E:96 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds  
root@kali:~# cat nmap.gnmap  
# Nmap 7.25BETA2 scan initiated Wed May 3 17:23:58 2017 as: nmap -PN -p 80 -oG  
nmap.gnmap 10.0.0.200  
Host: 10.0.0.200 ()      Status: Up  
Host: 10.0.0.200 ()      Ports: 80/open/tcp//http//  
# Nmap done at Wed May 3 17:24:11 2017 -- 1 IP address (1 host up) scanned in 1  
3.29 seconds  
root@kali:~#
```

خروجی دیگری که در Nmap از آن پشتیبانی می شود، Grepable است. این نوع خروجی برای زمانی مورد استفاده قرار می گیرد که قصد داشته باشید تا از خروجی Nmap برای دستور Grep استفاده نمایید. این دستور، خروجی Nmap را برای دستور Grep آماده می کند.

**-oA → All (NXG)**

این سوییچ هر سه خروجی بالا را به صورت یک جا ایجاد می نماید.

**-oS → Script Kids file ☺**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -PN -p 80 10.0.0.200 -oS nmap-s.txt

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-03 17:26 EDT
Nmap scan report for 10.0.0.200
Host is up (0.00043s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:73:9E:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
root@kali:~# cat nmap-s.txt

$start|ng NmAp 7.25B3t42 ( hTTps://nmap.org ) At 2017-05-03 17:26 3dT
Nmap $can report FOr 10.0.0.200
Ho$t |z Up (0.00043s latenCy).
PORT  $Tat3 S3RV!C3
80/tcp Open  http
M4C Addr3ss: 00:0c:29:73:9E:96 (Vmware)

Nmap d0n3: 1 |P addressz (1 h0sT up) $canned !n 13.12 $3c0ndS
root@kali:~#

```

این نوع خروجی بیشتر جنبه تفریحی دارد و خروجی را به صورت زبان هکرها ایجاد می نماید.

در پایان امیدوارم از کتاب الکترونیکی کوتاه و کاربردی از Nmap برای تست نفوذ استفاده لازم را برده باشید و اگر این کتاب را مفید دانستید، آن را با دوستان خود و علاقمندان به تست نفوذ به اشتراک بگذارید.

همچنین لازم به ذکر است در این کتاب به صورت کوتاه و کاربردی به برخی از توانمندی های نرم افزار قدرتمند Nmap پرداخته شد و این ابزار قابلیت های زیادیتری از آنچه در این کتاب به آن اشاره شد، را داراست.

**همواره موفق و سربلند باشید**