

به نام خدا

نرم افزار Nmap

درس:

امنیت و شبکه

استاد:

سرکار خانم سالم

دانشجو:

مهدی رضانی

ان‌مپ (به [انگلیسی](#)) (Nmap): برگرفته از حروف اول (Network Mapper) یک پویشگر امنیتی است که در ابتدا به دست گردن لیون (با اسم مستعار فیودور واسکوویچ) نوشته شده و برای کشف [میزبان‌ها](#) و [خدمتگزاران](#) در یک [شبکه رایانه‌ای](#) و در نتیجه ایجاد یک «نگاشت» از شبکه، استفاده می‌شود. برای این منظور ان‌مپ بسته‌های دستکاری شده را به سمت هدف می‌فرستد و سپس پاسخ آن‌ها را تحلیل می‌کند.

برخلاف بسیاری از پویشگرهای ساده پورت (port scanner) که فقط با یک نرخ ارسال ثابت که از قبل تعیین شده بسته‌ها را ارسال می‌کنند، ان‌مپ شرایط شبکه (نوسانات تأخیر، ازدحام شبکه، تداخل هدف در پویش) را نیز در نظر می‌گیرد. همچنین با در دست داشتن جامعه کاربری بزرگی که بازخورد می‌دهند و در تکامل امکانات آن شرکت می‌کنند، ان‌مپ قادر به توسعه بیش از پیش قابلیت‌های اکتشافی‌اش خارج از محدوده فقط فهم باز و بسته بودن پورت یا در دسترس بودن میزبان بوده است؛ ان‌مپ قادر است سیستم عامل هدف، نام و نسخه خدمات (services)، مدت زمان تخمینی در دسترس بودن (uptime)، نوع دستگاه و حضور [فایروال](#) را تشخیص دهد.

ان‌مپ روی لینوکس، [ویندوز](#)، [سولاریس](#)، HP-UX و نسخه‌های مختلف [بی‌اس‌دی](#) شامل [مک اواس ایکس](#) (و همچنین آمیگا اواس و SGI IRIX اجرا می‌شود. رایج‌ترین سکوی اجرای ان‌مپ، [لینوکس](#) است که ویندوز با اختلاف کمی آن را دنبال می‌کند.

ویژگی‌ها

از ویژگی‌های ان‌مپ می‌توان موارد زیر را نام برد:

- کشف میزبان - تشخیص میزبان‌ها در شبکه (بر اساس پاسخ به پینگ (Ping) یا بازبودن پورت خاص)
- [پویش پورت‌ها](#)
- تشخیص نسخه برنامه‌ها و خدمات
- تشخیص سیستم عامل
- تعامل به شکل اسکریپتی با هدف - با استفاده از موتور اسکریپت ان‌مپ (Nmap Scripting Engine) و زبان لوا، می‌توان پرس‌وجوهای سفارشی ساخت.

علاوه بر موارد بالا، ان‌مپ اطلاعات بیشتری از اهداف شامل برگردان نام [دی‌ان‌اس](#)، اطلاعات قطعات، و [آدرس مک](#) را فراهم سازد. موارد استفاده از ان‌مپ:

- بررسی امنیت شبکه یک دستگاه با کشف اتصالات شبکه‌اس که می‌تواند به آن وصل شود.
- کشف پورت‌باز روی هدف قبل از [تست نفوذپذیری](#) سیستم.
- لیست گیری شبکه، نگاشت، نگهداری و مدیریت منابع شبکه.
- بررسی امنیت شبکه با کشف سرویس‌های جدید پیش‌بینی نشده.

دستورهای پایه:

• یک پویش معمولی:

```
nmap -O <target-host's URL or IP>
```

• برای تشخیص سیستم عامل:

```
nmap -O <target-host's URL or IP>
```

• برای تشخیص نسخه برنامه ها:

```
nmap -sV <target-host's URL or IP>
```

• برای تنظیم زمانبندی پاسخ (T0 تا T5 برای افزایش تهاجم):

```
nmap -T0 -sV -O <target-host's URL or IP>
```

نسخه های برنامه:

دارای دو نسخه می باشد:

1-نسخه گرافیکی

این نسخه که به آن zenmap نیز گفته میشود در سیستم عامل ویندوز قابل نصب می باشد.

cmd-2

این نسخه در ویندوز همزمان با نصب نسخه گرافیکی به صورت خودکار نصب میشود

نحوہ نصب پرنامہ:

1- ورود به وبسایت nmap

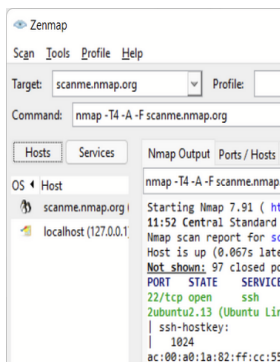
2- انتخاب سیستم عامل

3- دائلود نسخه مورد نظر

Get the latest Nmap for your system:

- Windows
- macOS
- Linux (RPM)
- Any other OS (source code)

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

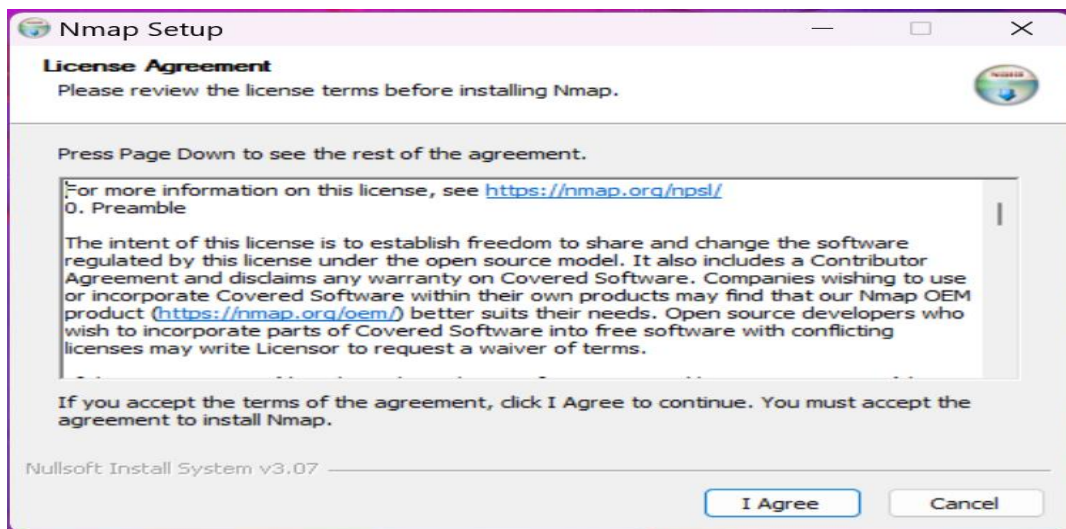
Latest stable release self-installer: [nmap-7.94-setup.exe](#)

Latest Npcap release self-installer: [npcap-1.78.exe](#)

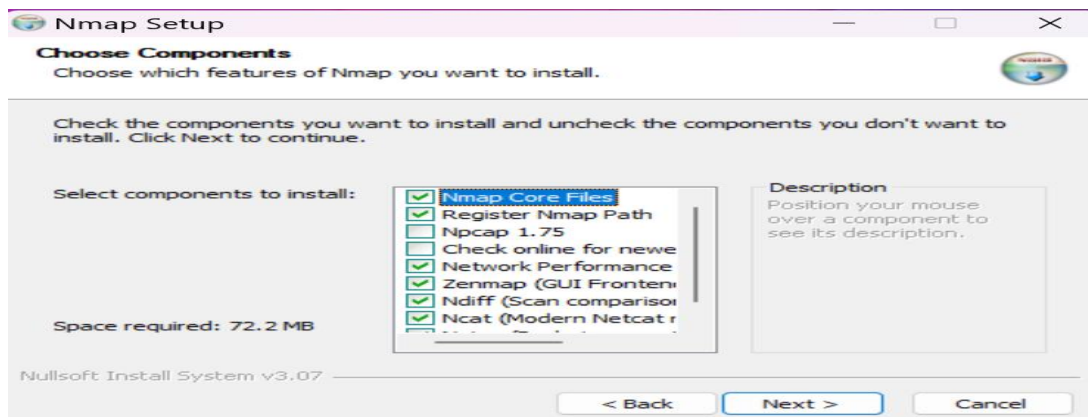
We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

نصب در ویندوز:

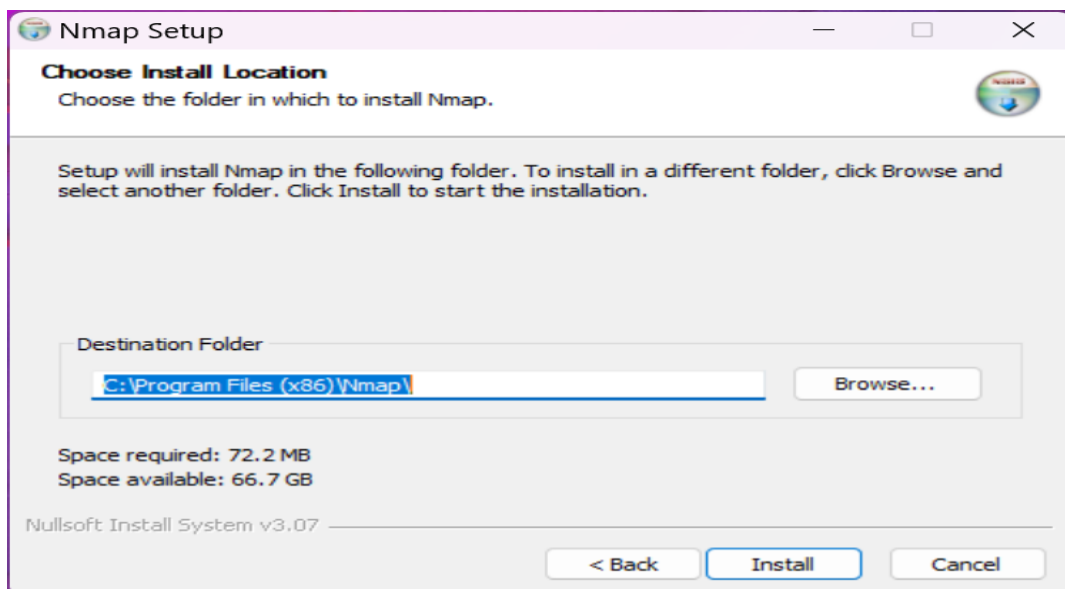
-1



-2



-3



نصب در لینوکس:

در لینوکس با استفاده از دو روش میتوان نرم افزار را نصب کرد:

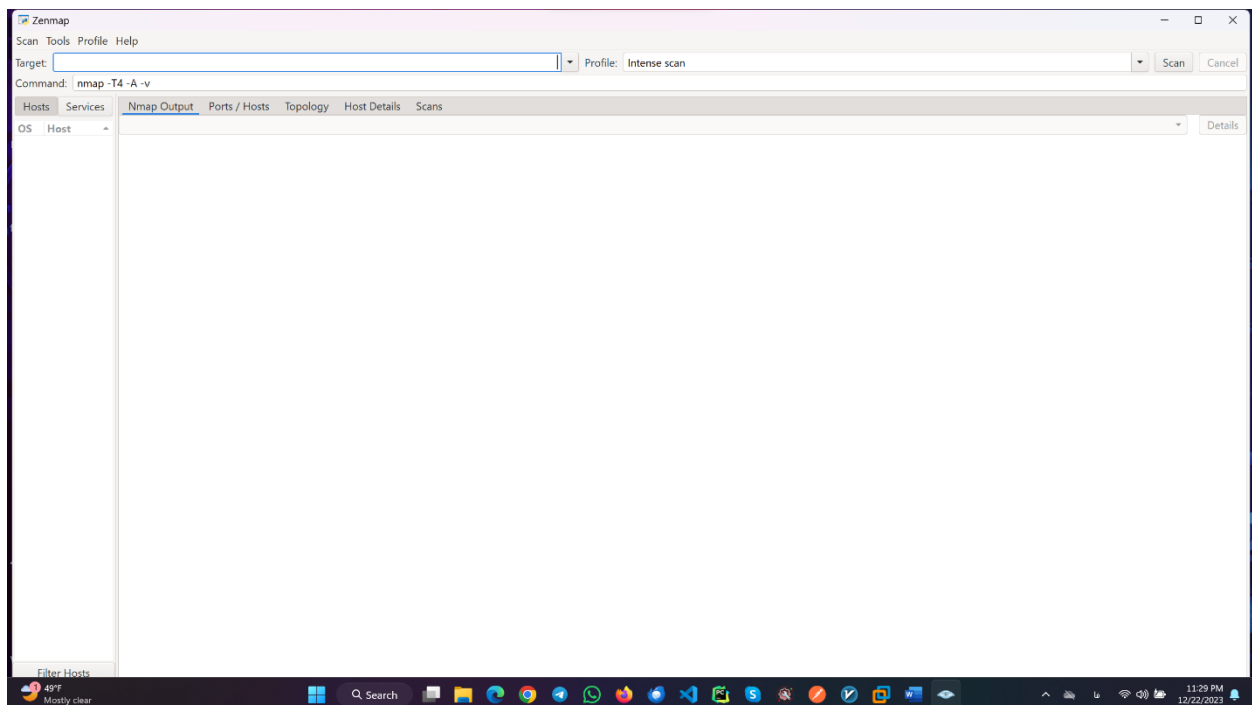
1-دانلود فایل نصبی نرم افزار و استفاده از نرم افزار های گرافیکی در لینوکس و نصب برنامه

2-با استفاده از ترمینال لینوکس:

```
Sudo apt install nmap
```

با استفاده از این دستور،نصب میشود.

تصاویر محیط برنامه در ویندوز:



Target:

در این قسمت آیپی یا ادرس دامین سرور یا وبسایتی که مورد نظر است وارد میشود.

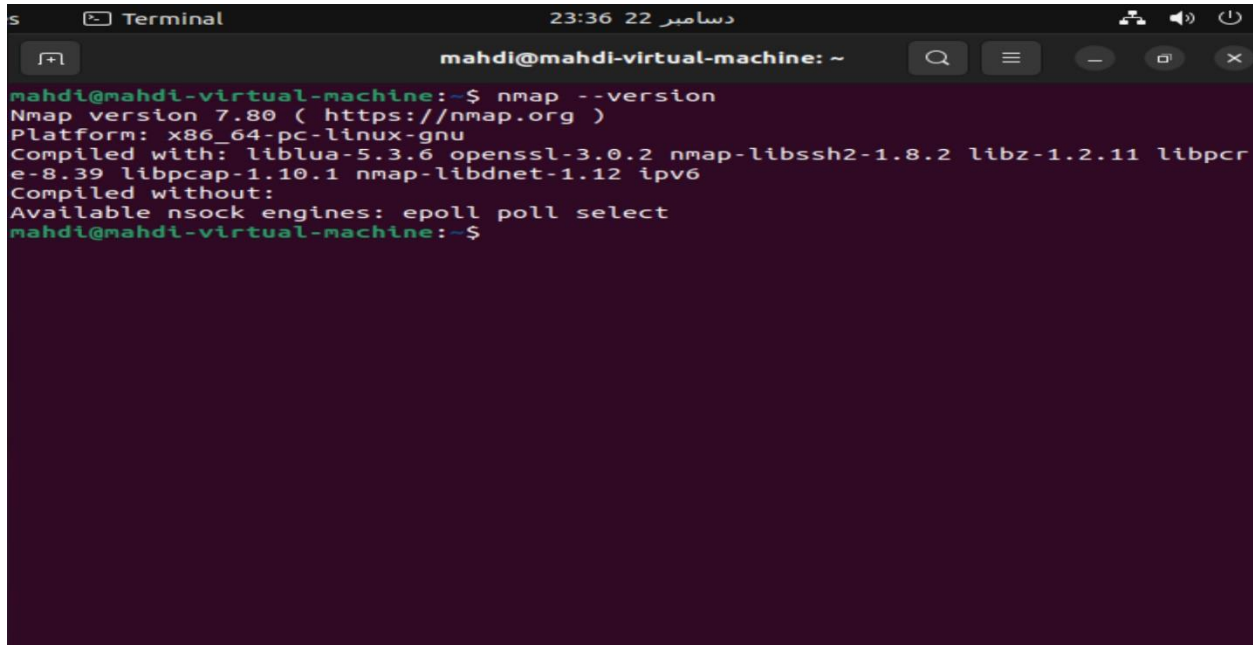
Command:

در این قسمت کامند مورد نظر برای حمله به تارگت وارد میشود.

Profile:

در این قسمت کامند های آماده و سریعی که بیشتر مورد استفاده قرار میگیرد به صورت آماده موجود می باشد.

تصاویر محیط در لینوکس:



```
s Terminal 23:36 22 دسامبر
mahdi@mahdi-virtual-machine: ~
mahdi@mahdi-virtual-machine:~$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.2 nmap-libssh2-1.8.2 libz-1.2.11 libpcr
e-8.39 libpcap-1.10.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
mahdi@mahdi-virtual-machine:~$
```

Nmap چیست؟

انمپ یا Nmap یک اسکنر بسیار قدرتمند و یک نقشه بردار که به منظور کاوش بررسی امنیتی شبکه به کار می رود است. انمپ یک ابزار open source یا به اصطلاح متن باز می باشد که برای اسکن و جستجوی آسیب پذیری ها مورد استفاده امنیت کاران و هکرها قرار میگیرد. این ابزار اولین بار توسط گردن لیون نوشته شده و توسعه یافته است و در سه نسخه ویندوز , لینوکس و مک به صورت کامندی و گرافیکی ارائه شده و به صورت رایگان و متن باز در اختیار عموم قرار گرفته است که در کالی لینوکس و دیگر سیستم عامل های امنیتی به صورت پیشفرض وجود دارد.

Zenmap چیست؟

zenmapنسخه گرافیکی ابزار nmap می باشد و برای شروع کار و آموزش nmap بهتر است که از zenmap استفاده کنیم به دلیل اینکه ساده تر است و دستورات را برای شما در فهرستی قرار داده است اما فراموش نکنید که nmap حرفه ای تر عمل می کند و دست ما را بازتر نگاه می کند.

دستورها و کامندهای کار با Nmap

1- اسکن اولیه Nmap در برابر IP یا میزبان

nmap 1.1.1.1

در حال حاضر، اگر می خواهید یک نام میزبان را اسکن کنید، به سادگی IP را برای میزبان جایگزین کنید، همانطور که در زیر مشاهده می کنید:

nmap cloudflare.com

این نوع اسکن های اولیه برای آشنایی و شروع اولین مراحل [Nmap](#) بسیار مناسب است

2- اسکن پورت های خاص و یا اسکن کل محدوده پورت ها در یک سرور محلی و یا سرور ریموت

nmap -p 1-65535 localhost

در این مثال، تمام پورت های 65535 را برای رایانه محلی خود اسکن کردیم Nmap. قادر به اسکن تمام پورت های موجود است، اما شما می توانید پورت های خاص را نیز اسکن کنید که نتایج سریعتری را گزارش می دهند. مثال زیر را ببینید:

nmap -p 80,443 8.8.8.8

3- اسکن چندین آدرس IP

به منظور اسکن چندین آدرس IP بایکدیگر از دستور زیر میتوان استفاده کرد:

nmap 1.1.1.1 8.8.8.8

شما همچنین می توانید آدرس های متوالی را اسکن کنید:

nmap -p 1.1.1.1,2,3,4

این موارد 1.1.1.1، 1.1.1.2، 1.1.1.3 و 1.1.1.4 را اسکن می کند.

4- اسکن محدوده های IP

می توانید Nmap برای اسکن کل محدوده IP CIDR استفاده کنید، مثلا:

nmap -p 8.8.8.0/28

دستور زیر 14 محدوده IP متوالی را از 8.8.8.1 تا 8.8.8.14 اسکن می کند:

nmap 8.8.8.1-14

شما حتی می توانید از کلمات کلیدی برای جستجو کل محدوده IP کلاس C در دستورات nmap استفاده کنید، مثلا:

nmap 8.8.8.*

این 256 IP را از 8.8.8.1 تا 8.8.8.256 اسکن می کند. اگر نیاز به حذف بعضی از IP های خاص از اسکن دامنه IP را داشتید، می توانید از گزینه "exclude-" استفاده کنید، همانطور که در زیر مشاهده می کنید:

nmap -p 8.8.8.* --exclude 8.8.8.1

5- پورت های محبوب را به وسیله دستور nmap اسکن کنید

با استفاده از پارامتر "top-ports" همراه با یک عدد خاص، می توانید پورت های معمولی X به بالا را برای آن میزبان اسکن کنید، همانطور که می بینیم:

nmap --top-ports 20 192.168.1.106

عدد 20 را جایگزین کنید، مانند مثال زیر:

```
[root@securitytrails:~]nmap --top-ports 20 localhost
Starting Nmap 6.40 ( http://nmap.org ) at 2018-10-01 10:02 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000016s latency).
Other addresses for localhost (not scanned): 127.0.0.1
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    filtered http
110/tcp   closed pop3
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
143/tcp   closed imap
```

443/tcp filtered https
445/tcp closed microsoft-ds
993/tcp closed imaps
995/tcp closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy

-6 اسکن میزبان ها و آدرس های IP از طریق خواندن یک فایل متنی

دستور nmap برای خواندن فایل هایی که حاوی کل IP ها و میزبان هاست بسیار مناسب است. فرض کنید شما یک فایل list.txt ایجاد می کنید که حاوی این دستور ها است:

192.168.1.106 cloudflare.com microsoft.com securitytrails.com

پارامتر "-iL" به شما اجازه می دهد که آن فایل را بخوانید و تمام آن میزبان ها را اسکن کنید:

nmap -iL list.tx

nmap -iL /root/Desktop/targets.txt

-7 نتایج اسکن Nmap خود را به شکل یک فایل ذخیره کنید

از سوی دیگر، در مثال زیر ما از یک پرونده دسترسی خواندن یا reading نخواهیم داشت، اما استخراج / ذخیره نتایج به یک فایل متنی با دستور زیر امکان پذیر میباشد:

nmap -oN output.txt securitytrails.com

Nmap توانایی استخراج فایل ها را به فرمت XML نیز دارد، مثال را ببینید:

nmap -oX output.xml securitytrails.com

-8 غیر فعال کردن رزولوشن نام DNS

اگر شما نیاز به کم کردن سرعت اسکن خود دارید، می توانید همیشه برای تمام اسکن های خود disable reverse DNS resolution انتخاب کنید. فقط کافیست پارامتر “-n” را اضافه کنید.

```
[root@securitytrails:~]nmap -p 80 -n 8.8.8.8 Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:15 -03 Nmap scan report for 8.8.8.8 Host is up (0.014s latency). PORT STATE SERVICE 80/tcp filtered http
```

تفاوت نتیجه را با normal DNS-resolution مشاهده کنید:

```
[root@securitytrails:~]nmap -p 80 8.8.8.8 Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:15 -03 Nmap scan report for google-public-dns-a.google.com (8.8.8.8) Host is up (0.014s latency). PORT STATE SERVICE 80/tcp filtered http
```

9-تشخیص سریع سیستم عامل و سرویس ها

با استفاده از پارامتر “-A” شما می توانید نوع سیستم عامل و سرویس را تشخیص دهید و در عین حال این دستور را با “-T4” برای اجرای سریع تر ترکیب کنید. مثال:

```
nmap -A -T4 cloudflare.com
```

خروجی که برای این مثال دریافت میکنیم:

```
[root@securitytrails:~]nmap -A -T4 cloudflare.com

Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 08:57 -03
Nmap scan report for cloudflare.com (198.41.214.162)
Host is up (0.022s latency).
Other addresses for cloudflare.com (not scanned): 198.41.215.162 2400:cb00:2048:1::c629:d7a2 2400:cb00:2048:1::c629:d6a2
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Cloudflare nginx
|_ http-server-header:
|   cloudflare
|   cloudflare-nginx
|_ http-title: Did not follow redirect to https://www.cloudflare.com/
443/tcp   open  ssl/https    cloudflare
|_ fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Server: cloudflare
|     Date: Mon, 01 Oct 2018 11:58:15 GMT
|     Content-Type: text/html
|     Content-Length: 167
|     Connection: close
|     CF-RAY: 462ec1a4696267c1-EZE
|     <html>
|     <head><title>403 Forbidden</title></head>
|     <body bgcolor="white">
|     <center><h1>403 Forbidden</h1></center>
|     <hr><center>cloudflare</center>
|     </body>
|     </html>
```

10- تشخیص نسخه سرویس daemon/

تشخیص نسخه سرویس daemon/ را می توان با استفاده از پارامترهای -SV انجام داد

nmap -sV localhost

همانطور که می بینید پاسخ سیستم به شکل زیر خواهد بود:

```
[root@securitytrails:~]nmap -sV localhost Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:28 -03 Nmap scan report for localhost (127.0.0.1) Host is up (0.000020s latency). Other addresses for localhost (not scanned): ::1 Not shown: 997 closed ports PORT STATE SERVICE VERSION 111/tcp open rpcbind 2-4 (RPC #100000) 631/tcp open ipp CUPS 2.2 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

11- اسکن با استفاده از پروتکل TCP یا UDP

یکی از ویژگی های منحصر به فرد نرم افزار اسکن شبکه Nmap این است که برای هر دو پروتکل های TCP و UDP کار می کند. و در حالی که اکثر سرویس ها فقط بر روی پروتکل TCP اجرا می شوند، همچنین می توانید از طریق اسکن کردن سرویس های مبتنی بر UDP ، مزیت بزرگی کسب کنید. خروجی اسکن استاندارد: TCP:

```
[root@securitytrails:~]nmap -sT 192.168.1.1 Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:33 -03 Nmap scan report for 192.168.1.1 Host is up (0.58s latency). Not shown: 995 closed ports PORT STATE SERVICE 80/tcp open http 1900/tcp open upnp 20005/tcp open btx 49152/tcp open unknown 49153/tcp open unknown Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```

نتایج اسکن UDP با استفاده از پارامتر: “-SU”

```
[root@securitytrails:~]nmap -sU localhost Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 09:37 -03 Nmap scan report for localhost (127.0.0.1) Host is up (0.000021s latency). Other addresses for localhost (not scanned): ::1 Not shown: 997 closed ports PORT STATE SERVICE 68/udp open|filtered dhcpc 111/udp open rpcbind 5353/udp open|filtered zeroconf
```

12- تشخیص آسیب پذیری با استفاده از دستور: Nmap

یکی از بزرگترین ویژگی های Nmap ، که کمتر مدیران شبکه و سیستمها در مورد آن می دانند، چیزی است به نام Nmap Scripting Engine (NSE). این موتور اسکریپت اجازه می دهد تا کاربران از یک مجموعه اسکریپت از پیش تعیین شده استفاده کنند یا با استفاده از زبان برنامه نویسی Lua اسکریپت منحصر به فرد خودشان را بنویسند. استفاده

از NSE برای اسکن خودکار سیستم و آسیب پذیری بسیار مهم است. به عنوان مثال، اگر می خواهید تست آسیب پذیری کاملی را در برابر هدف خود انجام دهید، می توانید از این پارامتر ها استفاده کنید:

nmap -Pn -script vuln 192.168.1.105

مثال:

```
[root@securitytrails:~]nmap -Pn -script vuln 192.168.1.105 Starting Nmap 7.60 (
https://nmap.org ) at 2018-10-01 09:46 -03 Pre-scan script results: | broadcast-avahi-dos: |
Discovered hosts: | 224.0.0.251 | After NULL UDP avahi packet DoS (CVE-2011-1002). |
Hosts are all up (not vulnerable). Nmap scan report for 192.168.1.105 Host is up (0.00032s
latency). Not shown: 995 closed ports PORT STATE SERVICE 80/tcp open http |_http-
csrf: Couldn't find any CSRF vulnerabilities. |_http-dombased-xss: Couldn't find any
DOM based XSS. | http-slowloris-check: | VULNERABLE: | Slowloris DOS attack |
State: LIKELY VULNERABLE | IDs: CVE:CVE-2007-6750 | Slowloris tries to keep
many connections to the target web server open and hold | them open as long as possible. It
accomplishes this by opening connections to | the target web server and sending a partial
request. By doing so, it starves | the http server's resources causing Denial Of Service. | |
Disclosure date: 2009-09-17 | References: | http://hacker.org/slowloris/ |_
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 |_http-stored-xss:
Couldn't find any stored XSS vulnerabilities. |_http-vuln-cve2014-3704: ERROR: Script
execution failed (use -d to debug) 1900/tcp open upnp 20005/tcp open btx 49152/tcp open
unknown 49153/tcp open unknown
```

همانطور که می بینید، در این آزمایش آسیب پذیری ما قادر به شناسایی یک CVE حمله Slowloris DOS بودیم.

13- راه اندازی DOS با دستور Nmap

به نظر می رسد که تاریخ استفاده از Nmap هرگز به پایان نمی رسد و به لطف NSE حتی این امکان را به ما میدهد که ما حملات DOS را علیه تست های شبکه انجام دهیم. در مثال قبلی ما (# 12) ما متوجه شدیم که میزبان به حمله Slowloris آسیب پذیر بوده است و اکنون سعی خواهیم کرد تا با استفاده از یک حمله DOS در یک حلقه برای همیشه از این آسیب پذیری بهره برداری کنیم.

nmap 192.168.1.105 -max-parallelism 800 -Pn -script http-slowloris -script-args http-slowloris.runforever=true

14- راه اندازی حملات brute force

NSE واقعا شگفت انگیز است – شامل اسکریپت هایی از هر چیز که می توانید تصور کنید. سه نمونه دیگر از BFA را در مورد وردپرس، MSSQL و سرور FTP مشاهده می کنید:

حمله / brute force (خشونت آمیز) به وردپرس:

```
nmap -sV --script http-wordpress-brute --script-args  
'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-  
wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.105
```

حمله / brute force (خشونت آمیز) به MS-SQL:

```
nmap -p 1433 --script ms-sql-brute --script-args  
userdb=customuser.txt,passdb=custompass.txt 192.168.1.105
```

حمله / brute force (خشونت آمیز) به FTP:

```
nmap --script ftp-brute -p 21 192.168.1.105
```

15- تشخیص نقطه ضعف های مخرب MALWARE در میزبان های از راه دور (remote hosts) با دستور nmap

Nmap قادر به تشخیص نرم افزار های مخرب و backdoors با اجرای آزمایش های گسترده در سرویس های عمومی سیستم عامل مانند Idetd، Proftpd، Vsftpd، IRC، SMB و SMTP است. همچنین دارای یک ماژول برای نشان دادن کرم های مخرب در سرور های ریموت است و همچنین پایگاه های ایمن مرورگر گوگل و VirusTotal را نیز ادغام می کند.

رایج ترین اسکن مالوار های مخرب با استفاده از دستور nmap به شکل زیر انجام می شود:

```
nmap -sV --script=http-malware-host 192.168.1.105
```

یا با استفاده از تروجان چک: Google

```
nmap -p80 --script http-google-malware infectedsite.com
```

خروجی:

```
80/tcp open http |_http-google-malware.nse: Host is known for distributing malware.
```

16- نادیده گرفتن یک آیبی هنگام اسکن:

تصور کنید در شبکه ای هستیم که قصد داریم شبکه را اسکن کنیم اما میخواهیم زمانی که انمپ در حال اسکن شبکه است ایپی ادمین شبکه اسکن نشود تا امنیت خود را هم حفظ کنیم برای استفاده از این روش از دستور زیر استفاده میکنیم در اینجا فرض میکنیم ایپی ادمین 192.168.1.45 می باشد

```
nmap 192.1681.1/24 — exclude 192.168.1.45
```

17-اسکن ایپی ورژن 6:

```
nmap -6 ip_address_version6
```

18-اسکن مخفی:

```
Nmap -sU target
```

19-اسکن پورت:

```
Nmap -p 8201 target     one port scan
```

```
Nmap -p 22,8201 target     two port scan
```

```
Nmap -p 8201- 1040 target     range port scan
```

20-زمانبندی در nmap :

```
Nmap -T0 target     low speed scan
```

```
Nmap -T1 target     low speed scan
```


Nmap -T2 target low speed scan

Nmap -T3 target low speed scan normal scan -> default

Nmap -T4 target

Nmap -T5 target high speed scan

21-اسکن موازی:

تعداد عملیات های موازی در nmap

Nmap -main-parallelism 100 target

در لحظه 100 عملیات را بطور همزمان اجرا کن-سرعت بسیار بالا-صحت کم

Nmap -max-parallelism 100 target

از حداکثری 5 عملیات موازی را باهم انجام بده-سرعت کم-صحت بالا

22-تشخیص سیستم عامل:

Nmap -O target

23-عبور از فایروال:

Nmap -f target

بسته ها و درخواست را به بسته های 8 بایتی تبدیل کن

Nmap -mtu 8 target

به جای 8 خودمون میتونیم عدد بدیم که بسته های ما را به همان مقدار تقسیم کند و ارسال کند

24-اسکن پنهان(ارسال ریکوئست از سرویس های مختلف):

Nmap -D 8 target

عدد 8<- 8 سرویس ساختگی ایجاد میکند و درخواست ها را از آن سرویس ها استفاده میکند،و سرور اصلی بین آنها گم میشود و ردیابی سخت می شود

سوئیچ های nmap

- اطلاعاتی در رابطه با اسکن سیستم عامل جمع آوری می نماید.
- A-ردپا یا Fingerprint ی را در رابطه با پورت را خدمت شما ارائه میدهد.
- p-فقط یک پورت را بررسی می نماید.
- F-مخفف Fast می باشد و خیلی سریع 100 پورت اول (رایج) را بررسی و خدمت شما ارائه می دهد.
- sS-اقدام به اسکن TCP Syn مینماید.
- sT-گهگاهی sS-درست جواب کارما را میدهددر این مواقع بهتر است از این سوئیچ استفاده گردد.
- sA-اقدام به حمله TCP مینماید.
- sW-برای سرویس های ویندوزی کاربرد دارد.
- p-برای این که مشخص کنیم که دستور nmap تمامی پورت ها را چک نماید می توان از این دستور استفاده نمود.
- sC-برای اجرای اسکریپت های nmap استفاده می شود.

Nmap یکی از کامل ترین و دقیق ترین اسکنر پورت هاست که توسط متخصصین Infosec استفاده می شود. با استفاده از nmap، می توانید وظایف ساده اسکن پورت ها را انجام دهید یا از موتور قدرتمند اسکریپتش برای حملات DOS ، تشخیص مالواری ها و یا آزمایش های مخرب (brute force attack) در سرورهای محلی استفاده کنید.