**Evaluation Only. Created with Aspose.Words. Copyright 2003-2024 Aspose Pty Ltd.**

**به نام خدا**

**نرم افزار Nmap**

**درس:** امنیت و شبکه

**استاد:**

سرکار خانم سالم

**دانشجو:** مهدی رمضانی

**انمپ** )به انگ[لیسی(](https://fa.wikipedia.org/wiki/%D8%B2%D8%A8%D8%A7%D9%86_%D8%A7%D9%86%DA%AF%D9%84%DB%8C%D8%B3%DB%8C) )Nmap :برگرفته از حروف اول (**N**etwork **Map**perیک پویشگر امنیتی است که در ابتدا به دست گردن لیو[ن )با اسم](https://fa.wikipedia.org/wiki/%D8%B2%D8%A8%D8%A7%D9%86_%D8%A7%D9%86%DA%AF%D9%84%DB%8C%D8%B3%DB%8C) مستعار فیودور واسکوویچ( نوشته شده و برای کشف م[یزبانها](https://fa.wikipedia.org/wiki/%D9%85%DB%8C%D8%B2%D8%A8%D8%A7%D9%86_(%D8%B4%D8%A8%DA%A9%D9%87)) و[خدمتگزاران در](https://fa.wikipedia.org/wiki/%D8%AE%D8%AF%D9%85%D8%A7%D8%AA_%D9%88%D8%A8) یک ش[بکه رایانهای](https://fa.wikipedia.org/wiki/%D8%B4%D8%A8%DA%A9%D9%87_%D8%B1%D8%A7%DB%8C%D8%A7%D9%86%D9%87%E2%80%8C%D8%A7%DB%8C) 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](https://fa.wikipedia.org/wiki/%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84) تشخیص دهد .

انمپ روی لینوکس، و[یندوز، س](https://fa.wikipedia.org/wiki/%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2)[ولاریس،](https://fa.wikipedia.org/wiki/%D8%B3%D9%88%D9%84%D8%A7%D8%B1%DB%8C%D8%B3_(%D8%B3%DB%8C%D8%B3%D8%AA%D9%85%E2%80%8C%D8%B9%D8%A7%D9%85%D9%84)) HP-UXو نسخههای مختلف [بی اس دی(](https://fa.wikipedia.org/wiki/%D8%A8%DB%8C_%D8%A7%D8%B3_%D8%AF%DB%8C) شامل م[ک اواس ایکس](https://fa.wikipedia.org/wiki/%D9%85%DA%A9_%D8%A7%D9%88%D8%A7%D8%B3_%D8%AF%D9%87) )[و](https://fa.wikipedia.org/wiki/%D9%85%DA%A9_%D8%A7%D9%88%D8%A7%D8%B3_%D8%AF%D9%87) همچنین آمیگا اواس و SGI IRIX اجرا میشود. رایجترین سکوی اجرای انمپ، لی[نوکس](https://fa.wikipedia.org/wiki/%D9%84%DB%8C%D9%86%D9%88%DA%A9%D8%B3) [است که](https://fa.wikipedia.org/wiki/%D9%84%DB%8C%D9%86%D9%88%DA%A9%D8%B3) ویندوز با اختلاف کمی آن را دنبال میکند .

**ویژگیها**

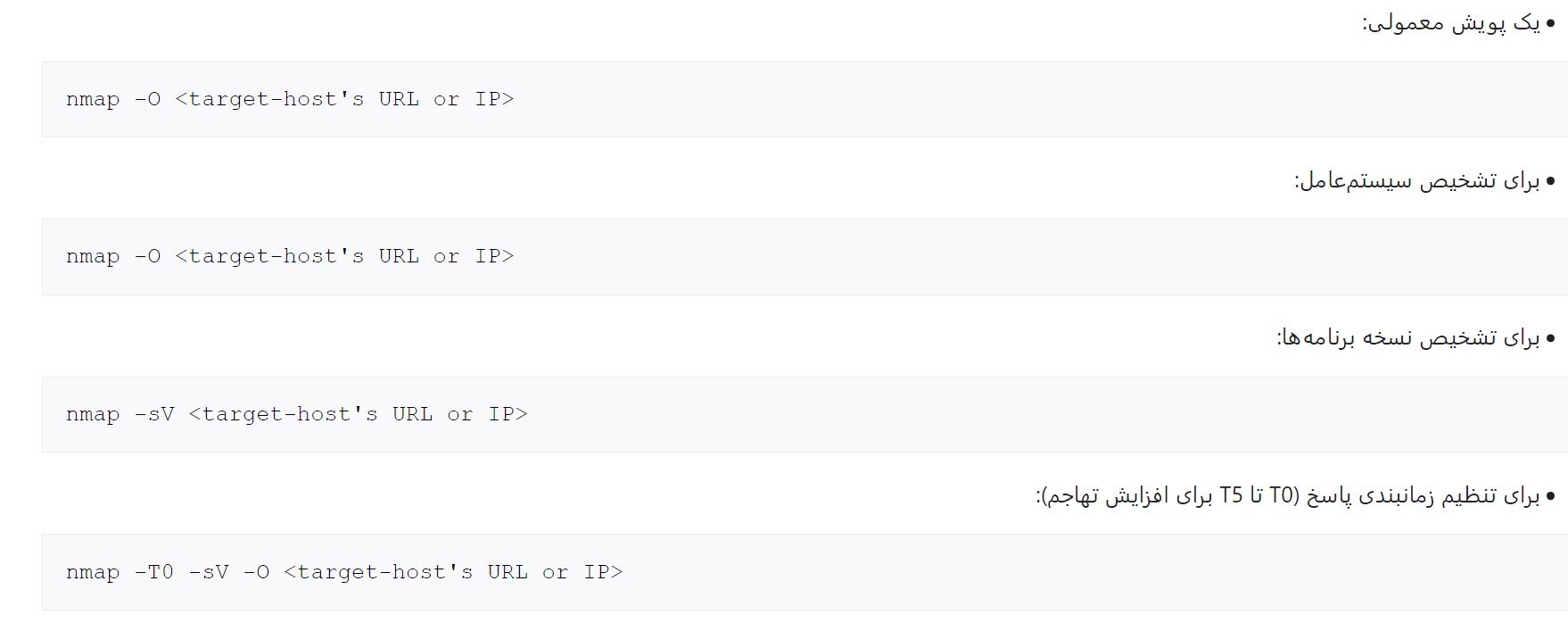
از ویژگی های انمپ میتوان موارد زیر را نام برد :

* کشف میزبان - تشخیص میزبانها در شبکه) بر اساس پاسخ به پینگ (Ping) یا بازبودن پورت خاص(
* پو[یش پورتها](https://fa.wikipedia.org/wiki/%D9%BE%D9%88%DB%8C%D8%B4_%D9%BE%D9%88%D8%B1%D8%AA%E2%80%8C%D9%87%D8%A7)
* تشخیص نسخه برنامه ها 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، ا](https://fa.wikipedia.org/wiki/%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87_%D9%86%D8%A7%D9%85_%D8%AF%D8%A7%D9%85%D9%86%D9%87)طلاعات قطعات، و [آدرس مک](https://fa.wikipedia.org/wiki/%D8%A2%D8%AF%D8%B1%D8%B3_MAC) 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 سیس](https://fa.wikipedia.org/wiki/%D8%AA%D8%B3%D8%AA_%D9%86%D9%81%D9%88%D8%B0%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C)تم.
* لیست گیری شبکه، نگاشت، نگهداری و مدیریت منابع شبکه.
* بررسی امنیت شبکه با کشف سرویسهای جدید پیشبینی نشده.

**دستورهای پایه:**



**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.**

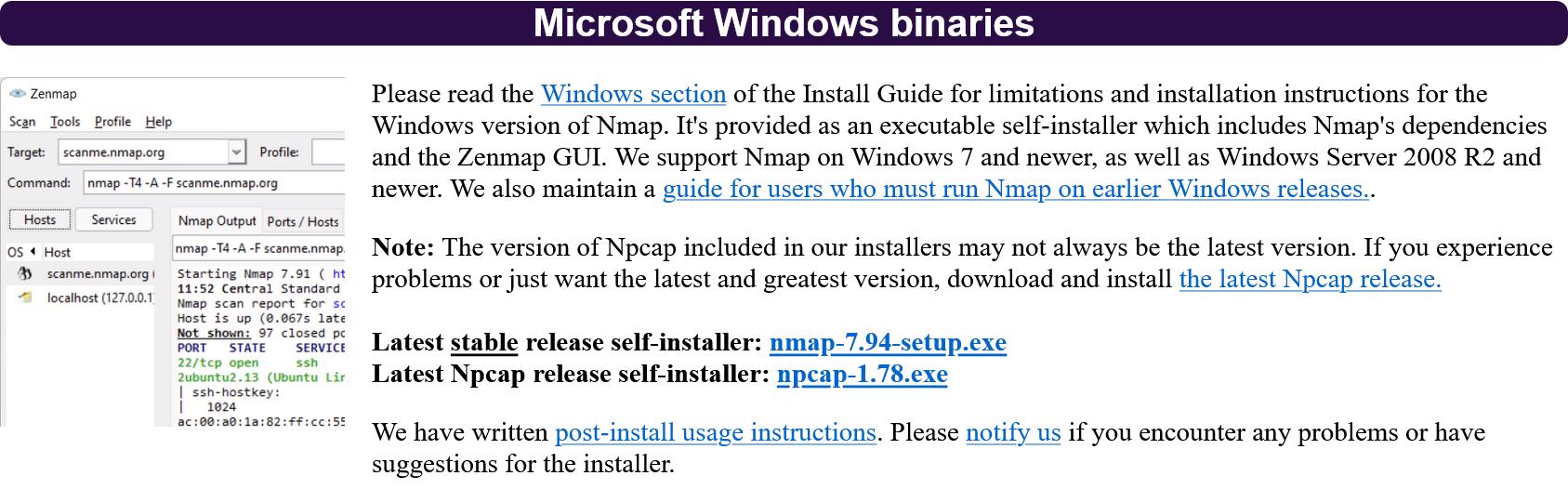
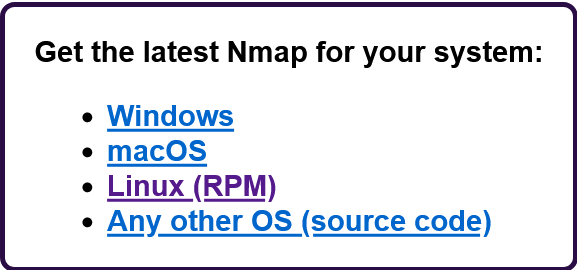
**cmd-2**

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

**نحوه نصب برنامه:**

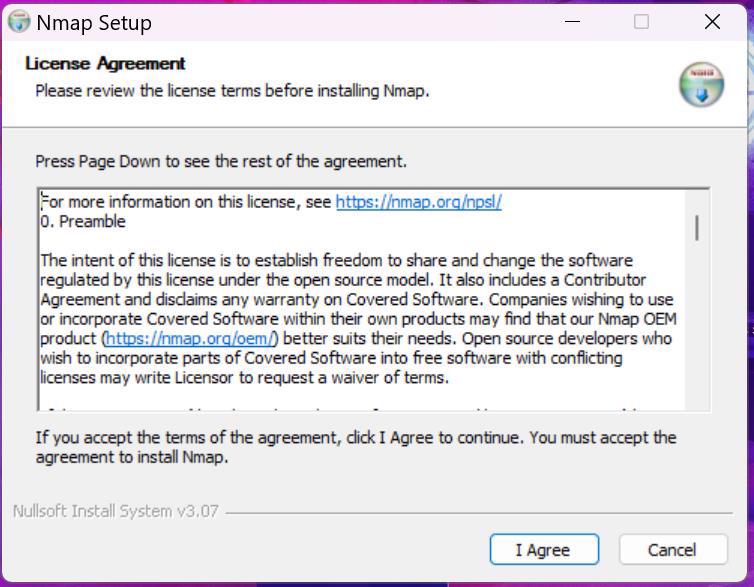
[**nmap**](https://nmap.org/download) **1- ورود به وبسایت**

**2- انتخاب سیستم عامل 3- دانلود نسخه مورد نظر**

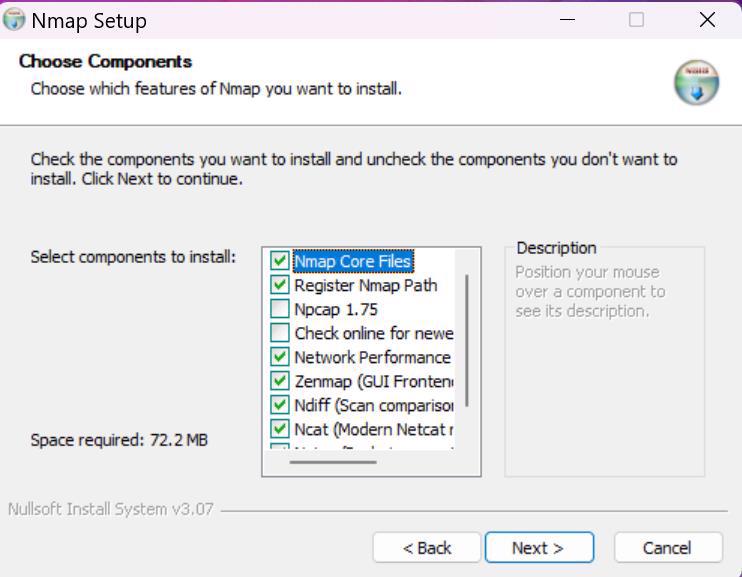


**نصب در ویندوز:**

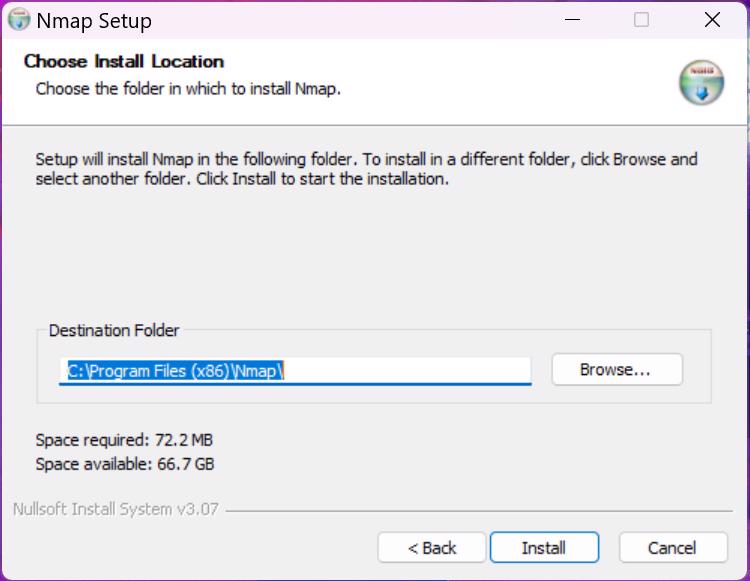
**-1**



**-2**



**-3**



**نصب در لینوکس:**

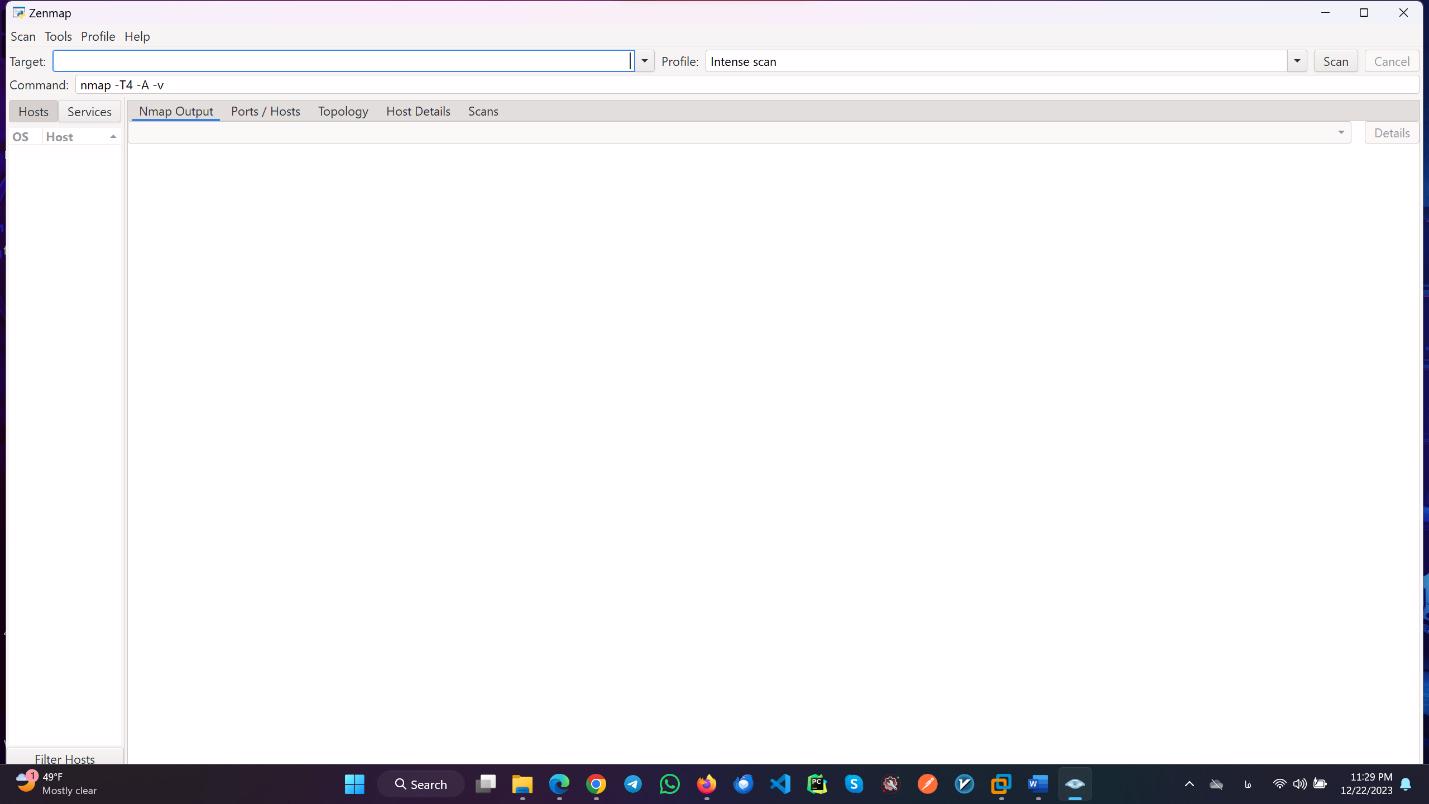
**در لینوکس با استفاده از دو روش میتوان نرم افزار را نصب کرد:**

**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.

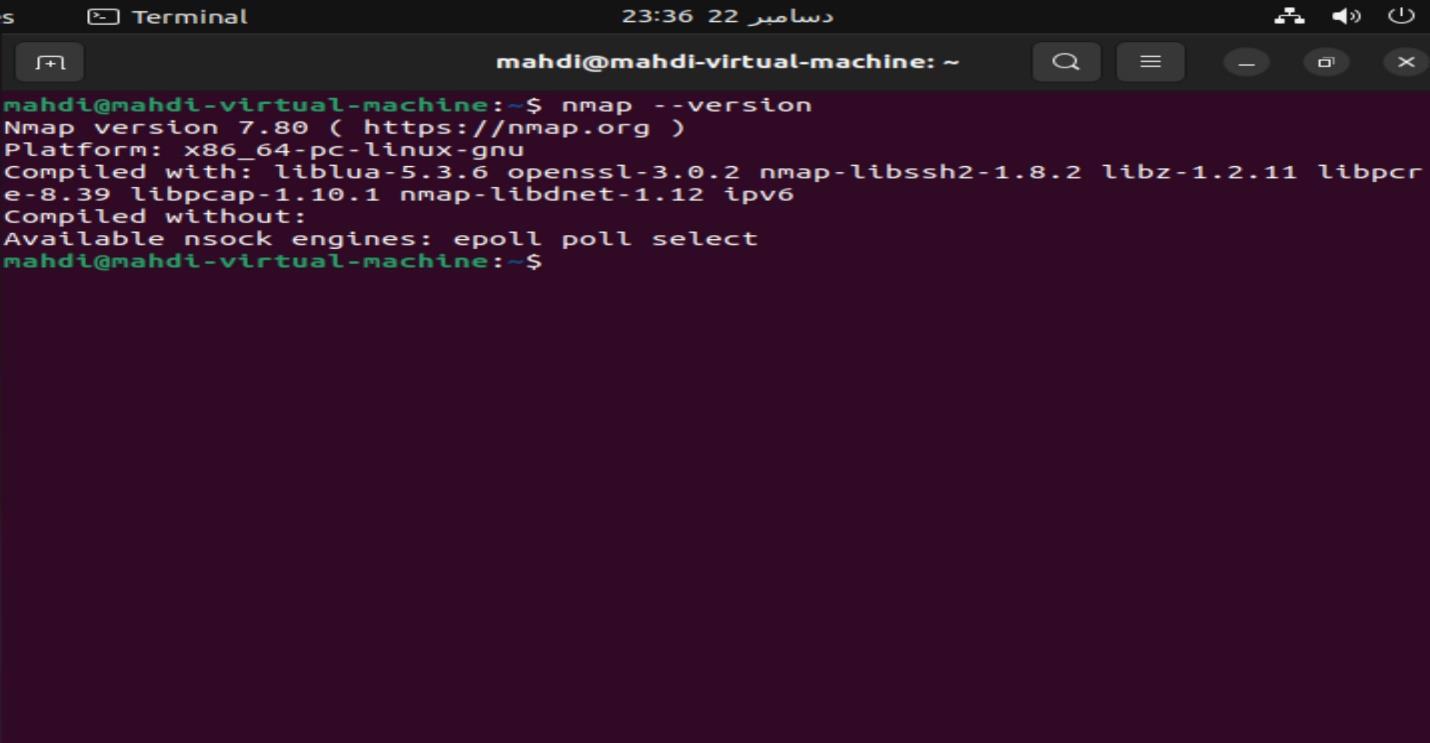
**Command:**

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 قزاز میگیرد به صورت آماده موجود می باشد.

**تصاویر محیط در لینوکس:**



**چیست؟Nmap**

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 اصطالح متن باز می باشد که برای اسکن و جستجوی اسیب 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.

**چیست؟Zenmap**

استفاده zenmap بهتر است که از nmap می باشد و برای شروع کار و اموزش nmap نسخه گرافیکی ابزارzenmap

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 ودست ما را بازتر نگه می کند.

**Nmap دستورها و کامندهای کار با**

**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  [Nmapبسیار](https://technet24.ir/tag/nmap) مناسب است

.

–**2اسکن 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**

**IP3اسکن چندین آدرس-**

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.

**IP4اسکن محدوده های-**

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 IP 256 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**

**-5پورت 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**

**-6اسکن میزبان ها و آدرس های IP ازطریق 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

* ایجاد می کنید که حاوی این دستورها استlist.txt

**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

**-7نتایج 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**

* نیز دارد، مثال را ببینید XML توانایی استخراج فایل ها را به فرمتNmap

**nmap -oX output.xml securitytrails.com**

[**DNS**](https://technet24.ir/implementing-windows-server-2019-domain-name-system-dns-%d8%a2%d9%85%d9%88%d8%b2%d8%b4-%d9%be%db%8c%d8%a7%d8%af%d9%87-%d8%b3%d8%a7%d8%b2%db%8c-dns-%d8%af%d8%b1-%d9%88%db%8c%d9%86%d8%af%d9%88%d8%b2-16939) 8غیرفعال کردن رزولوشن نام-

disable reverse DNS اگر شما نیاز به کم کردن سرعت اسکن خود دارید، می توانید همیشه برای تمام اسکن های خود

* را اضافه کنید “-n” انتخاب کنید. فقط کافیست پارامترresolution

**[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**

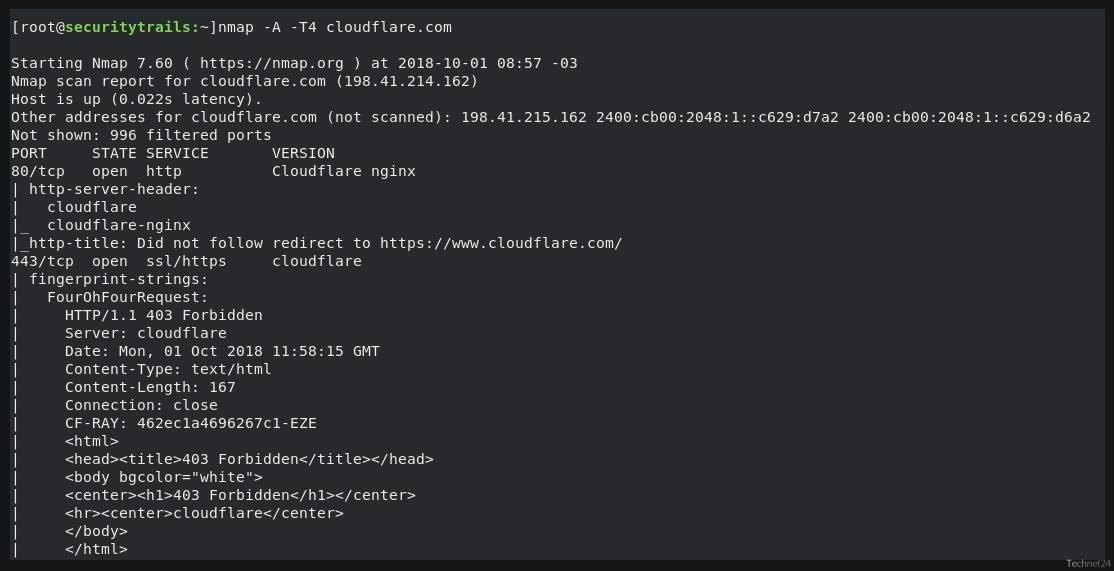
**-9تشخیص سریع سیستم عامل و سرویس ها**

با استفاده از پارامتر ”-A“ شما می توانید نوع سیستم عامل و سرویس را تشخیص دهید و در عین حال این دستور را با

* برای اجرای سریع تر ترکیب کنید. مثال“T4-”

**nmap -A -T4 cloudflare.com**

خروجی که برای این مثال دریافت میکنیم:



**/daemon10 -تشخیص نسخه سرویس**

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**

**UDP**[**ی**](https://technet24.ir/tag/tcpip)**ا**[TCP](https://technet24.ir/tag/tcpip) **11اسکن با استفاده از پروتکل-**

UDP و TCP این است که برای هر دو پروتکل های Nmap یکی از ویژگی های منحصر به فرد نرم افزار اسکن شبکه

کار می کند. و در حالی که اکثر سرویس ها فقط بر روی پروتکل TCP اجرا می شوند، همچنین می توانید از طریق اسکن

TCP:مزیت بزرگی کسب کنید .خروجی اسکن استاندارد ، UDPکردن سرویس های مبتنی بر

**[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**

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

**[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**

**Nmap:12تشخیص آسیب پذیری با استفاده از دستور-**

یکی از بزرگترین ویژگی هایNmap ، که کمتر مدیران شبکه و سیستمها در مورد آن می دانند، چیزی است به نام

این موتور اسکریپت اجازه می دهد تا کاربران از یک مجموعه اسکریپت از (NSE). یا“Nmap Scripting Engine

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://ha.ckers.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.

**Nmapبا دستور DOS 13راه اندازی-**

به نظر می رسد که تاریخ استفاده از Nmap هرگز به پایان نمیرسد و به لطف NSE حتی این امکان را به ما میدهد که ما

Slowloris را علیه تست های شبکه انجام دهیم.در مثال قبلی ما )# 12( ما متوجه شدیم که میزبان به حمله DOS حملات

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**

**brute force 14راه اندازی حملات-**

را BFA واقعا شگفت انگیز است – شامل اسکریپت هایی از هر چیز که می توانید تصور کنید. سه نمونه دیگر ازNSE

در مورد وردپرس، MSSQLو 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**

**MS-SQL**: خشونت آمیز( به ( **brute force /** حمله **nmap -p 1433 –script ms-sql-brute –script-args**

**userdb=customuser.txt,passdb=custompass.txt 192.168.1.105**

[**FTP**:](https://technet24.ir/solarwinds-serv-u-mft-server-13998) خشونت آمیز( به ( **brute force /** حمله

**nmap –script ftp-brute -p 21 192.168.1.105**

**-15تشخیص نقطه ضعف های مخرب MALWARE در میزبان های از راه**

**This document was truncated here because it was created in the Evaluation Mode.**