أساسيات Nmap

تعلّم فحص الشبكات واكتشاف المنافذ في أقل من ١٥ دقيقة

أمن سيبراني · تحليل شبكات · دليل تعليمي مبسّط

Network Mapper

```
$ nmap -sV scanme.nmap.org
```

شنو هي أداة Nmap؟

التعريف والفكرة الأساسية

Nmap (اختصار Network Mapper) أداة مجانية ومفتوحة المصدر تُستخدم لفحص الشبكات: تكتشف الأجهزة المتصلة، وتحدد المفتوحة، وتتعرّف على الخدمات وأنظمة التشغيل التي تعمل عليها.

مجانية ومفتوحة المصدر

متاحة للجميع منذ عام 1997

تعمل على كل الأنظمة

لينكس، ويندوز، وماك

معيار عالمي

تُستخدم في اختبار الاختراق وإدارة الشبكات

```
$ nmap scanme.nmap.org

Starting Nmap ...

Host is up (0.045s latency).

PORT     STATE  SERVICE

22/tcp   open   ssh

80/tcp   open   http

443/tcp  open   https

3306/tcp closed mysql

Nmap done: 1 IP address scanned
```

شنو تكدر تسوي بيها؟

أربع قدرات أساسية

اكتشاف الأجهزة

معرفة أي الأجهزة متصلة وفعّالة على الشبكة (Host Discovery)

فحص المنافذ

تحديد المنافذ المفتوحة والمغلقة على كل جهاز (Port Scanning)

كشف الخدمات والإصدارات

معرفة الخدمة العاملة على المنفذ ونسختها (Service & Version)

كشف نظام التشغيل

تخمين نظام تشغيل الجهاز الهدف (OS Detection)

كيف تشتغل Nmap؟

فكرة العمل بأربع خطوات

1

إرسال الحزم

ترسل Nmap حزم بيانات (packets) إلى الجهاز الهدف على منافذ مختلفة

2

استقبال الردود

الجهاز الهدف يرد على كل حزمة حسب حالة المنفذ

3

تحليل الردود

تحلّل Nmap نوع الرد لتحدد إن كان المنفذ مفتوح أو مغلق أو مُصفّى

4

عرض النتائج

تعرض تقريراً بالمنافذ والخدمات وأنظمة التشغيل المكتشفة

تثبيت Nmap

حسب نظام التشغيل

لينكس (Debian / Ubuntu)

```
$ sudo apt install nmap
```

ماك (عبر Homebrew)

```
$ brew install nmap
```

ويندوز

حمّل المثبّت الرسمي من الموقع nmap.org ثم شغّله (يتضمن الواجهة الرسومية Zenmap)

تحقق من التثبيت بالأمر nmap --version

بنية الأمر الأساسية

كيف تكتب أمر Nmap

```
$ nmap [options] [target]
```

nmap
الأمر الأساسي

يشغّل الأداة

options
الخيارات

تحدد نوع الفحص، مثل sV- أو p- اختيارية)

target
الهدف

عنوان IP أو اسم موقع أو نطاق عناوين

أمثلة على الهدف:

```
192.168.1.1
scanme.nmap.org
192.168.1.0/24
```

حالات المنافذ

ماذا تعني نتيجة كل منفذ؟

مفتوح

`open`

يوجد تطبيق يستقبل الاتصالات على هذا المنفذ — نقطة دخول محتملة

مغلق

`closed`

المنفذ يستجيب لكن لا يوجد تطبيق يستمع حالياً

مُصفّى

`filtered`

جدار حماية أو فلتر يمنع Nmap من تحديد حالة المنفذ

أنواع الفحص الأساسية

الجزء 1من — 2الشرح والمثال وسبب الاستخدام لكل أمر

فحص TCP SYN — يرسل حزمة SYN بدون إكمال الاتصال الثلاثي الثلاثي مع المنفذ

ليش نستخدمها: أسرع وأخفى من الفحص الكامل، وهو الفحص الافتراضي عند توفر صلاحية root

```
$ nmap -sS 192.168.1.1
```

فحص TCP كامل — يكمل الاتصال الثلاثي (3-way handshake) مع كل منفذ

ليش نستخدمها: يشتغل بدون صلاحيات خاصة، بديل عملي لـ -sS إذا ما عندك root

```
$ nmap -sT 192.168.1.1
```

فحص منافذ UDP — يفحص خدمات مهمة مثل DNS و SNMP و DHCP

ليش نستخدمها: ضروري لأن أغلب الفحوصات تركّز بس على TCP وتفوّت ثغرات UDP

```
$ nmap -sU 192.168.1.1
```

أنواع الفحص الأساسية

الجزء 2من — 2الشرح والمثال وسبب الاستخدام لكل أمر

اكتشاف الأجهزة الحية فقط على الشبكة بدون فحص أي منفذ (Ping Scan)

ليش نستخدمها: خطوة أولى سريعة لمعرفة شنو موجود بالشبكة قبل الفحص التفصيلي

```
$ nmap -sn 192.168.1.0/24
```

يكشف اسم وإصدار الخدمة الشغالة على كل منفذ مفتوح

ليش نستخدمها: يساعدك تعرف إذا كان الإصدار قديم وفيه ثغرة أمنية معروفة

```
$ nmap -sV 192.168.1.1
```

يحاول تخمين نظام التشغيل عبر تحليل استجابة الحزم للجهاز الهدف

ليش نستخدمها: يفيدك تفهم بيئة الهدف وتختار الفحوصات المناسبة للمرحلة الجاية

```
$ nmap -O 192.168.1.1
```

أنماط التوقيت (Timing Templates)

من الأبطأ والأكثر تخفياً إلى الأسرع — من T0 إلى T5

`-T0`	Paranoid — الأبطأ على الإطلاق، تخفٍّ شبه كامل من أنظمة كشف التسلل IDS
`-T1`	Sneaky — بطيء ومتخفٍّ، مناسب لتجاوز أنظمة المراقبة الحساسة
`-T2`	Polite — بطيء ومهذب، يقلل الحمل على الشبكة والجهاز الهدف
`-T3`	Normal — الافتراضي في Nmap، توازن جيد بين السرعة والتخفي
`-T4`	Aggressive — سريع، مناسب للشبكات المستقرة والفحص المحلي
`-T5`	Insane — الأسرع، دقة أقل واحتمال فقدان بعض النتائج

محرك السكربتات NSE

— Nmap Scripting Engine يوسّع القدرات عبر --script

الاكتشاف (Discovery)

سكربتات تجمع تفاصيل إضافية عن الهدف مثل أسماء الأجهزة والمشاركات والخدمات المتاحة

فحص الثغرات (Vuln)

تبحث عن ثغرات أمنية معروفة (CVEs) في الخدمات الشغالة على الجهاز الهدف

المصادقة (Auth / Brute)

تختبر كلمات المرور الضعيفة عبر هجمات القوة العمياء Brute-force على الخدمات

الآمنة (Safe)

سكربتات لا تؤثر على الهدف، مناسبة للفحص الأولي غير المؤذي بدون مخاطر

تجاوز الجدران النارية وأنظمة الحماية

الجزء 1من — 2تقنيات للتخفي وتفادي كشف IDS/Firewall

تجزئة الحزمة — (f-)يقسّم حزم TCPلأجزاء IPأصغر بدل حزمة وحدة كبيرة

ليش نستخدمها: يتخطى بعض جدران الحماية وأنظمة IDS البسيطة اللي تفحص كل حزمة لحالها

```
$ nmap -f 192.168.1.1
```

فحص وهمي — (D-)يرسل الفحص مع عناوين IPوهمية إضافية جنب عنوانك الحقيقي

ليش نستخدمها: يصعّب على الهدف تحديد مين الفاحص الحقيقي بين كل العناوين المرسلة

```
$ nmap -D RND:5 192.168.1.1
```

إبطاء التوقيت — (T0-)يبطّئ إرسال الحزم لأقصى درجة، فحص وحدة كل عدة دقائق

ليش نستخدمها: يقلل احتمال تنبيه أنظمة كشف التسلل IDSاللي تراقب معدل الحزم

```
$ nmap -T0 192.168.1.1
```

تجاوز الجدران النارية وأنظمة الحماية

الجزء 2من — 2تقنيات للتخفي وتفادي كشف IDS/Firewall

تزييف عنوان MAC (--spoof-mac) — يغيّر عنوان الجهاز الظاهر بعنوان عشوائي أو مخصص أثناء الفحص

ليش نستخدمها : يخفي هوية جهازك الحقيقية على الشبكة المحلية أثناء تنفيذ الفحص

```
$ nmap --spoof-mac 0 192.168.1.1
```

الفحص الأعمى (-sI Idle Scan) — يستخدم جهاز وسيط "Zombie" خامل لتنفيذ الفحص نيابة عنك

ليش نستخدمها : يخفي هويتك تماماً لأن الهدف يشوف بس عنوان الـ zombie، مو عنوانك

```
$ nmap -sI zombie_ip target_ip
```

أوامر شائعة وعملية

الجزء 1من — 2الشرح والمثال وسبب الاستخدام لكل أمر

```
$ nmap 192.168.1.1
```

فحص سريع لجهاز واحد بالإعدادات الافتراضية)أشهر 1000 منفذ(

ليش نستخدمها :أفضل نقطة بداية لأي هدف جديد قبل التعمق أكثر بخيارات إضافية

```
$ nmap -p 80,443 192.168.1.1
```

يفحص منفذين محددين بس 80)و (443بدل كل المنافذ

ليش نستخدمها :يوفر وقت لما تكون تعرف مسبقاً وين تدور بالضبط على الهدف

```
$ nmap -sV 192.168.1.1
```

يكشف الخدمات وإصداراتها على المنافذ المفتوحة

ليش نستخدمها :يساعد بتحديد الثغرات المرتبطة بإصدار معين من الخدمة

أوامر شائعة وعملية

الجزء 2من — 2الشرح والمثال وسبب الاستخدام لكل أمر

```
$ nmap -A 192.168.1.1
```

فحص شامل يجمع كشف الخدمة ونظام التشغيل والسكربتات ومسار الشبكة (traceroute)

ليش نستخدمها :يعطيك صورة كاملة بأمر وحد، بس أبطأ وأوضح للهدف من الفحوصات البسيطة

```
$ nmap -sn 192.168.1.0/24
```

اكتشاف كل الأجهزة الحية على شبكة كاملة بدون فحص أي منفذ

ليش نستخدمها :مفيد لعمل خريطة سريعة لكل الأجهزة المتصلة قبل التعمق بأي جهاز

التجربة العملية — الجزء 1: فحوصات أساسية

نفّذ هذه الأوامر خطوة بخطوة على جهازك أو شبكة تجريبية مصرّح بفحصها

الخطوة 1: اكتشف الأجهزة الحيّة على الشبكة قبل البدء بأي فحص تفصيلي

```
$ nmap -sn 192.168.1.0/24
```

الخطوة 2: نفّذ أول فحص بسيط على جهاز واحد بالإعدادات الافتراضية

```
$ nmap 192.168.1.1
```

الخطوة 3: افحص منافذ محددة بدل الفحص الكامل لتوفير الوقت

```
$ nmap -p 22,80,443 192.168.1.1
```

الخطوة 4: جرّب فحص SYN الخفي (يحتاج صلاحية root/sudo)

```
$ nmap -sS 192.168.1.1
```

الخطوة 5: اكتشف إصدارات الخدمات الشغالة على المنافذ المفتوحة

```
$ nmap -sV 192.168.1.1
```

التجربة العملية — الجزء 2: فحوصات متقدمة

أكمل باقي الخطوات لتغطية اكتشاف النظام والسكربتات وحفظ النتائج

الخطوة 6: حاول اكتشاف نظام التشغيل المستخدم على الجهاز الهدف

```
$ nmap -O 192.168.1.1
```

الخطوة 7: نفّذ فحصاً شاملاً يجمع اكتشاف الخدمة ونظام التشغيل والسكربتات

```
$ nmap -A 192.168.1.1
```

الخطوة 8: شغّل سكربتات NSE للبحث عن ثغرات معروفة على الهدف

```
$ nmap --script vuln 192.168.1.1
```

الخطوة 9: افحص كل المنافذ الـ 65535 بسرعة أعلى باستخدام T4-

```
$ nmap -T4 -p- 192.168.1.1
```

الخطوة 10: احفظ نتيجة الفحص بصيغة نصية لمراجعتها لاحقاً

```
$ nmap -oN result.txt 192.168.1.1
```

الاستخدام الأخلاقي والقانوني

نقطة مهمة جداً قبل ما تبدأ

فحص أنظمة لا تملكها أو بدون إذن مكتوب قد يُعدّ جريمة يعاقب عليها القانون في معظم الدول.

مسموح

- فحص أجهزتك وشبكتك الخاصة
- بيئات تدريب مخصصة مثل scanme.nmap.org
- اختبار اختراق بعقد وإذن رسمي
- مختبرات افتراضية للتعلّم

ممنوع

- فحص مواقع أو خوادم لا تملكها
- شبكات الشركات أو الجهات دون تصريح
- الشبكات العامة أو شبكات الآخرين
- أي استخدام بنية الإضرار أو التطفّل

الخلاصة

- Nmapأداة أساسية لفحص الشبكات واكتشاف الأجهزة والمنافذ والخدمات
- البنية بسيطة + nmap :الخيارات +الهدف، وتتحكم بالفحص عبر خيارات مثل -sV -Pn
- افهم حالات المنافذ :مفتوح، مغلق، ومُصفّى — كل حالة تعني شيئاً مختلفاً
- استخدمها بمسؤولية :افحص فقط ما تملكه أو بإذن رسمي

ابدأ بالتجربة على scanme.nmap.org — وتذكّر دائماً الاستخدام الأخلاقي.