

Network Scanning 3

Nmap Scripts

- طبعا ما عرفنا نستخدم ال nmap وعرفنا هيا بتعمل ايه والكوماندات بتاعتها عاوزين بقي نعمل حاجة عملية
- ال nmap فيها scripts جاهزه ممكن تعملها ف ال terminal عشان تحاول انها تعمل attack علي السيرفر
- ملحوظة : ال scripts دي ضعيفه ومن الطبيعي انها متجلكش اي نتيجة
`nmap 90.84.187.113 --script vuln`
- دا سكريبت بيعرفني ايه الخدمات اللي فيها ثغرات
`nmap 90.84.187.113 --script brute`
- سكريبت بيعمل brute علي كلمات السر ف خدمه معينه انا محددهالو عشان يجيلي اليوزر والباس بتاعه
`nmap 90.84.187.113 --script exploit`
- سكريبت بيحاول انو يستغل الثغرات اللي اكتشفت
- طب دلوقتي انا عاوز اعمل اعمل attack علي خدمه معينه او اركز عليها
`*nmap 90.84.187.113 -p21 --script=ftp`
- هنا انا بقولو الخدمه اللي علي البورت 21 اللي هيا ال ftp يعني وطبعا بعرف هيا مفتوحه ولا لا من خلال ال scan وبعد كدا بقولو نفذلي كل السكريبتات الخاصه بال ftp عشان يجيلي اي معلومه تفيدني

-sS	ال Stealth Scan (الفحص الخفي) بيعمل فحص SYN من غير ما يكمل ال TCP handshake ، فبيبقى أقل ظهورًا في اللوجات.
-S	ال Source ودي ممكن استخدمها عشان استعمل ip مش حقيقي من جوا نفس الشبكة بتاعت السيرفر عشان اوهم ال firewall اني من نفس الشبكة عادي

-sT	ال TCP Connect Scan بيستخدم اتصال TCP كامل ، وده أبطأ لكنه بيكشف كل المنافذ اللي مفتوحة.
-----	--

-sU	ال UDP Scan بيفحص المنافذ ال UDP ، وده مهم عشان تعرف الخدمات اللي شغالة على بروتوكولات زي DNS, SNMP, DHCP .
-----	--

-sA	ال ACK Scan بيشفوف إذا كان في جدار ناري (Firewall) بيحجب المنافذ ولا لا عن طريق إرسال حزم ACK.
-----	---

-sV	الـ Service Version Detection يحاول يجيب إصدار الخدمات اللي شغالة على المنافذ، زي معرفة إصدار Apache, SSH, FTP.
-----	---

-O	الـ OS Detection يحاول يحدد نوع نظام التشغيل اللي شغال على الجهاز.
----	--

-A	الـ Aggressive Scan بيجمع كذا حاجة في مرة واحدة: بيكشف نظام التشغيل، وإصدارات الخدمات، ويعمل traceroute .
----	---

-p	الـ Port Selection بيحدد بورت معين أو مجموعة بورتات للفحص، زي -p 80,443 أو -p 1-1000.
----	---

-p-	الـ Full Port Scan بيفحص كل المنافذ (65535 بورت) عشان يجيب أي خدمة شغالة.
-----	---

-Pn	الـ No Ping بيخلي nmap ما يعملش فحص Ping قبل الفحص ، وده مفيد لو الجهاز يمنع الـ ICMP Ping .
-----	--

-n	الـ No DNS Resolution بيخلي nmap ما يحاولش يجيب اسم الجهاز (hostname) من الـ IP ، وده بيخلي الفحص أسرع.
----	--

-T[0-5]	الـ Timing Options بتحدد سرعة الفحص من T0 (أبطأ) لـ T5 (أسرع).
---------	--

-F	الـ Fast Scan بيفحص المنافذ المشهورة بس بدل كل الـ 65535 بورت، وده أسرع.
----	--

--top-ports	الـ Top Used Ports بيفحص أشهر المنافذ استخدامًا ، زي --top-ports 100 لفحص أكثر 100 بورت استخدامًا .
-------------	--

--script	الـ NSE Scripts بتستخدم سكريبتات جاهزة في nmap لفحص أعمق، زي --script=vuln عشان يجيب الثغرات.
----------	---

--script=vuln	الـ Vulnerability Scan بيعمل فحص للثغرات المعروفة على الجهاز المستهدف.
---------------	---

<pre>--script=ftp-anon</pre>	FTP Anonymous Login Scan الـ FTP بيشوف لو الـ FTP بيسمح بتسجيل الدخول كمجهول (anonymous login).
------------------------------	--

<pre>--script=ftp-bounce</pre>	FTP Bounce Attack Check الـ FTP بيشوف لو السيرفر عرضة لهجوم FTP Bounce اللي بيخليك تستغل الـ FTP كـ وسيط للهجوم.
--------------------------------	--

<pre>-oN result.txt</pre>	Save Output (Normal Format) الـ بيحفظ نتائج الفحص في ملف نصي عادي.
---------------------------	---

<pre>-oX result.xml</pre>	Save Output (XML Format) الـ بيحفظ النتائج بصيغة XML ، مفيد لو هتعالج البيانات برمجياً.
---------------------------	---

<pre>-oG result.gnmap</pre>	Save Output (Grepable Format) الـ بيحفظ النتائج بصيغة قابلة للبحث باستخدام grep .
-----------------------------	---

<pre>-oA output</pre>	All Output Formats الـ بيحفظ النتيجة بكل الصيغ (Normal, XML, Grepable) مع بعض.
-----------------------	---

<pre>-v</pre>	Verbose Mode الـ بيخلي الفحص يظهر تفاصيل أكثر لحظياً بدل ما يستنى لحد النهاية.
---------------	---

<pre>-vv</pre>	Extra Verbose Mode الـ بيعرض تفاصيل أكثر من -v وبيكون مفيد لو عايز تتابع الفحص بالتفصيل.
----------------	--

<pre>--reason</pre>	Port State Reason الـ بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي nmmap بيحدد حالة البورت.
---------------------	--

<pre>--open</pre>	Open Ports Only الـ بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.
-------------------	---

<pre>-d</pre>	Debug Mode الـ بيشغل وضع التصحيح عشان تشوف كل خطوة في الفحص.
---------------	---

<pre>-6</pre>	IPv6 Scan الـ ييفحص الأجهزة اللي شغالة بـ IPv6 بدل IPv4 .
---------------	--

"Pasted image 20250207105613.png" could not be found.

Scan Type	Example Command
ARP Scan	<code>sudo nmap -PR -sn MACHINE_IP/24</code>
ICMP Echo Scan	<code>sudo nmap -PE -sn MACHINE_IP/24</code>
ICMP Timestamp Scan	<code>sudo nmap -PP -sn MACHINE_IP/24</code>
ICMP Address Mask Scan	<code>sudo nmap -PM -sn MACHINE_IP/24</code>
TCP SYN Ping Scan	<code>sudo nmap -PS22,80,443 -sn MACHINE_IP/30</code>
TCP ACK Ping Scan	<code>sudo nmap -PA22,80,443 -sn MACHINE_IP/30</code>
UDP Ping Scan	<code>sudo nmap -PU53,161,162 -sn MACHINE_IP/30</code>
Remember to add <code>-sn</code> if you are only interested in host discovery without port-scanning. Omitting <code>-sn</code> will let Nmap default to port-scanning the live hosts.	
Option	Purpose
<code>-n</code>	no DNS lookup
<code>-R</code>	reverse-DNS lookup for all hosts
<code>-sn</code>	host discovery only

<https://www.stationx.net/nmap-cheat-sheet/>

<https://www.geeksforgeeks.org/nmap-cheat-sheet/>