## **Network Scanning 3**

## **Nmap Scripts**

- طبعا ما عرفنا نستخدم ال nmap وعرفنا هيا بتعمل ايه والكوماندات بتاعتها عاوزين بقي نعمل حاجه عملية
- المnmap فيها scripts جاهزه ممكن تعملها ف الterminal عشان تحاول انها تعمل attack على السيرفر

ملحوظه : الscripts دي ضعيفه ومن الطبيعي انها متجبلكش اي نتيجه

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 يجبلي 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

هذا انا بقولو الخدمه اللي على البورت 21 اللي هيا ال ftp يعني وطبعا بعرف هيا مفتوحه و لا لأ من خلال الscan وبعد كدا
 بقولو نفذلي كل السكريبتات الخاصه بالftp عشان يجبلي اي معلومه تفيدني

-sS	الـ Stealth Scan (الفحص الخفي) بيعمل فحص SYN من غير ما يكمل الـ TCP handshake، فبيبقى أقل ظهورًا في اللوجات.
-S	الـSource ودي ممكن استخدمها عشان استعمل ip مش حقيقي من جوا نفس الشبكه بتاعت السير فر عشان او هم ال firewall اني من نفس الشبكه عادي

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

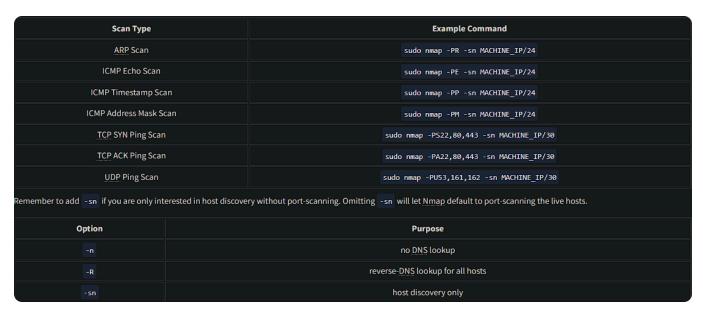
-sU	الـ UDP Scan بيفحص المنافذ الـ UDP، وده مهم عشان تعرف الخدمات اللي شغالة على بروتوكولات زي DNS,
	SNMP, DHCP

-sA	الـ ACK Scan بيشوف إذا كان في جدار ناري (Firewall) بيحجب المنافذ ولا لأ عن طريق إرسال حزم ACK.

-sV	إصدار	الـ Service Version Detection بيحاول يجيب إصدار الخدمات اللي شغالة على المنافذ، زي معرفة .Apache, SSH, FTP	
-0	على الجهاز .	الـ OS Detection بيحاول يحدد نوع نظام التشغيل اللي شغال .	
-A	يعمل	الـ Aggressive Scan بيجمع كذا حاجة في مرة واحدة: بيكشف نظام التشغيل، وإصدارات الخدمات، ويا traceroute	
-p	. p 1-100	الـ Port Selection بيحدد بورت معين أو مجموعة بورتات للفحص، زي -80,443 و -0	
-p-	خدمة شغالة.	الـ Full Port Scan بيفحص كل المنافذ (65535 بورت) عشان يجيب أي .	
-Pn	ICMP P	الـ No Ping بيخلي (nmap ما يعملش فحص Ping قبل الفحص، وده مفيد لو الجهاز بيمنع الـ ing	
-n	الـ No DNS Resolution بيخلي nmap ما يحاولش يجيب اسم الجهاز (hostname) من الـ IP، وده بيخلّي الفحص أسرع.		
-T[0-	سرع). [5-	الـ Timing Options بتحدد سرعة القحص من 10 (أبطأ) لـ T5 (أب	
-F	، وده أسرع	الـ Fast Scan بيفحص المنافذ المشهورة بس بدل كل الـ 65535 بورت:	
top		الـ Top Used Ports بيفحص أشهر المثافذ استخدامًا، زي100 top-ports لفحص أكتر 100 بورت استخدامًا.	
 scrip		الـ NSE Scripts بتستخدم سكريبتات جاهزة في nmap لفحص أعمق، زي script=vuln عشان يجيب الثغرات.	
scr	ript=vuln	الـ Vulnerability Scan بيعمل فحص للثغرات المعروفة على الجهاز المستهدف.	

script=ftp- anon (anonymous Login Scan Ji بيشوف لو الدير فر عرضة لهجوم FTP Anonymous Login Scan Ji (anonymous Login ) script=ftp- bounce FTP Bounce (Attack Check Ji بيضوف لو الدير فر عرضة لهجوم FTP Bounce Attack Check Ji بيخليك تستغل الـ FTP Bounce (الي بيخليك تستغل الـ FTP Bounce (الي بيخليك تستغل الـ Save Output (Normal Format) اللهجوم Save Output (XML Format) اللهجوم (معيد)  -OX		
الى بيخليك تستغل الـ FTP Bounce عيشوف لو السير فر عرضة لهجوم FTP Bounce Attack Check اللي بيخليك تستغل الـ FTP Bounce عيشوف لو السير فر عرضة لهجوم.  -ON result.txt \$\text{Save Output (Normal Format)} \]  -OX		
اللي بيخليك تستغل الـ FTP كـ وسيط الهجوم.  -ON result.txt الهجوم Save Output (Normal Format) المحدود	anon	
اللي بيخليك تستغل الـ Save Output (Normal Format) بيخفظ نتاج الفحص في ملف نصى عادي.  -OX الله Save Output (XML Format) بيحفظ النتائج بصيغة قابلة للبحث باستخدام Save Output (Grepable Format) بيحفظ النتائج بصيغة قابلة للبحث باستخدام grep  -OA output (Normal, XML, Grepable) بيحفظ النتائج بكل الصيغ (Verbose Mode المنافذ المفتولة بعض المنافذ المفتولة النهاية المنافذ المفتولة النهاية ويبكرن مفيد أو عايز تتابع الفحص بالتفصيلV ويبكرن مفيد أو عايز تتابع الفحص بالتفصيلV (المورت مفتوح أو مفتق، مفيد أنهم إذاي map بيحدد والمورث المفتولة المفتولة المفتولة المفتولة المفتولة المفتولة Open (Open Ports Only المفتولة Open		ETD Downer with the Author ETD Downer Attack Check II
الـ Save Output (XML Format) بيدفظ النتائج بصيغة قابلة للبحث باستخدام المورث. Save Output (Grepable Format) بيدفظ النتائج بصيغة قابلة للبحث باستخدام Save Output (Grepable Format) . grep  -OA output  -OA output  -OA output  -OA output  -V  -V  -V  -V  -V  -V  -V  -V  -V  -		
الـ Save Output (XML Format) بيدفظ النتائج بصيغة قابلة للبحث باستخدام Save Output (Grepable Format) بيدفظ النتائج بصيغة قابلة للبحث باستخدام . grep  - OA output . ويعفظ النتائج بصيغة قابلة للبحث باستخدام . grep  - OA output . بيدفظ النتائج بكل الصيغ ( Normal , XML , Grepable ) مع بعض . All Output Formats المحتال التنبية بكل الصيغ ( Verbose Mode ) مع بعض . الله النقصيل اكثر من - v وبيكون مفيد لو عايز تتابع الفحص بالتفصيل .  - V . بيعرض سبب اعتبار البورث مفتوح أو مفلق، مفيد لفيم از اي reason المفتودة بس وبيتجاهل المفتودة .		
- OG الـ Save Output (Grepable Format) بيخفظ النتائج بصيغة قابلة للبحث باستخدام Save Output (Grepable Format) . grep - OA output . وبيكون مغيد ( Normal, XML, Grepable ) مع بعض. All Output Formats الـ Verbose Mode بيخلي الفحص يظهر تفاصيل أكثر من - v وبيكون مفيد لو عايز تتابع الفحص بالتفصيل . Extra Verbose Mode الـ Port State Reason بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم ازاي nmap بيحدد ومعادل المعتولة المفتوحة بس وبيتجاهل المغتولة . Open المعتولة .	-oN result.txt .	الـ (Save Output (Normal Format بيحفظ نتانج الفحص في ملف نصي عادي
الـ Save Output (Grepable Format) بيحفظ النتيج بصيغة قابلة للبحث باستخدام grep . grep . وربيكون مفيد لو عايز تتابع الفحص بلاتفصيل. المع بعض. ( Normal, XML, Grepable ) مع بعض. All Output Formats اللهابة . و Verbose Mode النتيجة بكل الصيغ ( Verbose Mode النتيجة بكل الفحص يظهر تفاصيل اكتر لحظيًا بدل ما يستنى لحد النهابة . و اللهابة . اللهابة . اللهابة . اللهابة . المعامل اكتر من وبيكون مفيد لو عايز تتابع الفحص بالتفصيل . و اللهابة . و اللهابة . اللهابة . و اللهابة . و اللهابة . اللهابة . و اللها	-oX	الـ (Save Output (XML Format بيحفظ النتائج بصيغة XML، مفيد لو هتعالج البيانات
- OA output مع بعض. ( Normal, XML, Grepable ) مع بعض. All Output Formats الديمة بكل الصيغ ( Normal, XML, Grepable ) مع بعض. All Output Formats الديمة و Verbose Mode الفحص يظهر تفاصيل أكثر لحظيًا بدل ما يستنى لحد النهاية VV بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لو عايز تتابع الفحص بالتفصيل. Port State Reason البورت. مفتوح أو مغلق، مفيد لفهم إزاي nmap بيحدد Peason ويبتجاهل المقفولة.	result.xml	
الـ Verbose Mode بيخلّي الفحص يظهر تفاصيل أكثر لحظيّا بدل ما يستنى لحد النهاية.  - V بيخلّي الفحص يظهر تفاصيل أكثر لحظيّا بدل ما يستنى لحد النهاية.  - VV بيعرض تفاصيل أكثر من - V وبيكون مفيد لو عايز تتابع الفحص بالتفصيل.  - Port State Reason بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي nmap بيحدد حومه البورت.  - Copen بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي Open Ports Only بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.	-oG	الـ (Save Output (Grepable Format بيحفظ النتائج بصيغة قابلة للبحث باستخدام
الـ Verbose Mode البيخلّي الفحص يظهر تفاصيل أكثر لحظيًا بدل ما يستنى لحد النهاية.  -v وبيكون مفيد لو عايز تتابع الفحص بالتفصيل.  -v وبيكون مفيد لو عايز تتابع الفحص بالتفصيل.  المفتوحة بس وبيتجاهل المقفولة.  open بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.	result.gnmap	
الـ Verbose Mode اليخلّي الفحص يظهر تفاصيل أكثر لحظيًا بدل ما يستنى لحد النهاية.  -vv المنافد النهاية الفحص بالتفصيل.  -vv وبيكون مفيد لو عايز تتابع الفحص بالتفصيل.  المستنى لحد النهاية البورت مفتوح أو مغلق، مفيد لفهم إزاي nmap بيحدد والمعالم المعتوحة بس وبيتجاهل المقفولة.  open المعتوحة بس وبيتجاهل المقفولة.		and the second and th
الـ Extra Verbose Mode بيعرض تفاصيل أكثر من ٧٠ وبيكون مفيد لو عايز تتابع الفحص بالتفصيل. ١٠٥ الـ Extra Verbose Mode بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي (nmap بيحدد المورث. Open Ports Only بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.	-oa output .osq	الله All Output Formats بيحفظ السيجة بعن الصبح ( Normat, XML, Grepable ) كل
الـ Port State Reason بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي nmap بيحدد حالة البورث. حالة البورث.  Open Ports Only بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.	ستنى لحد النهاية.	الـ Verbose Mode بيخلّي الفحص يظهر تفاصيل أكتر لحظيًا بدل ما يس
الـ Port State Reason بيعرض سبب اعتبار البورت مفتوح أو مغلق، مفيد لفهم إزاي nmap بيحدد حالة البورت. حالة البورت.  Open Ports Only بيعرض المنافذ المفتوحة بس وبيتجاهل المقفولة.		
reason	لفحص بالتفصيل.	الـ Extra Verbose Mode بيعرض تفاصيل أكثر من ٧-١ وبيكون مفيد لو عايز تتابع ا
الـ Debug Mode بيشغل وضع التصحيح عشان تشوف كل خطوة في الفحص.	اهل المقفولة.	الـ Open Ports Only بيعرض المنافذ المفتوحة بس وبيتج
الـ Debug Mode بيشغل وضع التصحيح عتمان تتموف كل خطوة في الفحص.	39	
	طوة في الفحص.	الـ Debug Mode بيشغل وصع النصحيح عشان نسوف كل ح
الـ IPv6 Scan بيفحص الأجهزة اللي شغالة بـ IPv6 بدل IPv4 بالـ IPv4 بالـ IPv4 الله IPv4 الله IPv4 الله IPv4 الله	-6 .IPv4 بدل IPv	الـ IPv6 Scan بيفحص الأجهزة اللي شغالة بـ 6

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



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

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