Network Scanning 2

Port Scanning

Ports

- البورت ده عامل زي الشباك تخيل معايا لو حرامي عاوز يدخل بيت اول حاجه هيبص عليها هيا الشبابيك وهيشوف لو هي مقفوله كويس ولا لأ طب هي مصنوعه بخامه كويسه ولا لأ عشان لو خامتها قديمه هيعرف يفتحها انما لو جديده هتبقي صعب وتكاد تكون مستحيل
- فا بالظبط البورت عامل زي الشباك
- كل بورت بيقدم خدمة معينه تعالي اعرفك علي شويه منهم او اهمهم

🔷 البورتات الشائعة (Well-Known Ports: 0-1023)

Port	الخدمة (Service)	الوصف
20	FTP (Data Transfer)	نقل البيانات عبر FTP
21	FTP (Command Control)	التحكم في الاتصال بالـ FTP
22	SSH (Secure Shell)	اتصال آمن بالأنظمة البعيدة
23	Telnet	بروتوكول اتصال قديم للتحكم في الأجهزة عن بعد (غير مشفر)
25	SMTP (Simple Mail Transfer Protocol)	إرسال البريد الإلكتروني
53	DNS (Domain Name System)	تحويل أسماء النطاقات إلى IP والعكس
67/68	DHCP (Dynamic Host Configuration Protocol)	توزيع عناوين IP للأجهزة على الشبكة
69	TFTP (Trivial FTP)	بروتوكول نقل ملفات بسيط بدون مصادقة
80	HTTP (Hypertext Transfer Protocol)	تصفح الإنترنت بدون تشفير
110	POP3 (Post Office Protocol 3)	استلام البريد الإلكتروني من السيرفر
123	NTP (Network Time Protocol)	مزامنة الوقت بين الأجهزة
143	IMAP (Internet Message Access Protocol)	استلام البريد الإلكتروني مع إمكانية التحكم في الرسائل على السيرفر

Port	الخدمة (Service)	الوصف
161/162	SNMP (Simple Network Management Protocol)	إدارة الأجهزة على الشبكة ومراقبتها
179	BGP (Border Gateway Protocol)	بروتوكول توجيه الإنترنت بين الـ ISPs
389	LDAP (Lightweight Directory Access Protocol)	إدارة قواعد بيانات المستخدمين (مثل Active Directory)
443	HTTPS (HTTP Secure)	تصفح الإنترنت بتشفير SSL/TLS
445	SMB (Server Message Block)	مشاركة الملفات والطابعات في شبكات ويندوز
500	IKE (Internet Key Exchange)	جزء من الـ IPSec لتأمين الاتصالات
514	Syslog	إرسال سجلات النظام إلى سيرفر لوجات
636	LDAPS (LDAP Secure)	نسخة مشفرة من LDAP
989/990	FTPS (FTP Secure)	نسخة مشفرة من FTP

🔷 البورتات المسجلة (Registered Ports: 1024-49151)

(تستخدمها التطبيقات والخدمات المختلفة)

Port	الخدمة (Service)	الوصف
1080	SOCKS Proxy	بروكسي يستخدم لتوجيه الاتصال
1433	MSSQL (Microsoft SQL Server)	قاعدة بيانات SQL من مايكروسوفت
1521	Oracle Database	قاعدة بيانات أوراكل
1723	PPTP (Point-to-Point Tunneling Protocol)	بروتوكول VPN قديم
1883	MQTT (Message Queue Telemetry Transport)	بروتوكول إنترنت الأشياء IoT
3306	MySQL Database	قاعدة بيانات MySQL
3389	RDP (Remote Desktop Protocol)	التحكم في سطح مكتب ويندوز عن بعد
5060/5061	SIP (Session Initiation Protocol)	بروتوكول VoIP للاتصالات الصوتية

- لو الserviceاللي شغاله علي البورت ده قديمه ممكن ناخد اسمها والاصدار ونبحث عنها ف جوجل او exploit-db او cve details واشوف استغلالها بيكون ازاي
- اي IP فالعالم بيكون عليه 65535 ودا عدد الportsالكلي

- ممكن تلاقي حالة الport :

1. open => معني كدا اني الخدمه مفتوحه عادي
2. closed => معناها اني الخدمه دي مقفوله
3. filtered => هنا الخدمه حالتها مش متحدده سواء هيا مفتوحه ولا مقفوله وغالبا بتكون ممنوعه كدا بسبب اني الفايروال هو اللي بيمنعها

---

nmap (Network Mapper)

- ذكرنا قبل كدا اني ال nmap من اكتر الادوات الشائعه فالعالم من حيث ال network scan ان لم تكن الشائعه

اوامر الnmap

1. لو عاوز افحص البورتات المفتوحه علي ip معين

```
nmap <ip/domain/subdmoain
```

```
nmap google.com
```

“Pasted image 20250131162235.png” could not be found.

- لو تلاحظ هنا في تلت خدمات مفتوحين smtp ودي بتاعت ارسال الايميلات و http و https بتوع خدمات الويب لأني جوجل اصلا موقع واي موقع لازم تلاقي بروتوكول ال http مفتوح
- فا انا لما الاقي http مفتوح فا انا هعرف اني ده موقع ويب
- خلي بالك ال Nmap مش بتفحص كل البورتات هيا بتفحص اشهر 1000 بورت بس طب لو عاوزينها تفحص كل البورتات

2. فحص جميع البورتات

```
nmap -p- google.com
```

or

```
nmap -p 1-65535 google.com
```

3. فحص بورت معين

```
nmap -p 21 google.com
```

```
nmap -p 21,22,80,443 google.com
```

“Pasted image 20250131162843.png” could not be found.

هنا بعد ما عرفنا الversion بتاع service معين ممكن نبحث عنه علي جوجل ونشوف الثغرات اللي فيه

مواقع scan زي الnmap كدا ممكن تساعدك

1. shodan.io
2. search.censys.io

FTP (File Transfer Protocol)

- ال ftp دا بروتوكول بيستخدم عشان لو عاوز ترفع ملفات علي السيرفر او هتنقل ملفات بين سيرفر وسيرفر تاني
- ال ftp هنتعرف انهارده علي ثغرتين مهمين فيه بس الاول خليني اعرفك ازاي اكونكت بالftp بتاع السيرفر

```
<ftp <ip
```

1. Anonymous Login

- الثغره دي عباره عن لما تيجي تكونكت بftp server وقالك دخل اليوزر والباس وجربت anonymous فالاتنين فا دي تعتبر ثغره

.Pasted image 20250131163509.png” could not be found“

- هنا انا دخلت فاليوزر anonymous والباس نفس الكلام خلاص عرفت اكونكت بالسيرفر ودي ثغره المفروض تبلغها للموقع او صاحب ال ip يعني

2. No Rate Limit

- دلوقتي لما تكونكت بسيرفر ftp بيقولك يوزر وبتدخله عادي لو جيت بقي تدخل الباس وقالك غلط تمام عادي جرب دوس enter تاني لو جبلك اني الباس غلط تاني ومع تالت مره جبلك تاني جبلك غلط وجيت ف رابع مره قالك دخل الباسورد تاني دا معناه اني في ثغره no rate limit عشان مفيش حدود علي ادخال الباسورد انما ف الطبيعي بيكون ليك محاوله واحده او تلاته بس لو عديت التلاته وقالك دخل الباسورد لرابع مره فا كدا دي ثغره

.Pasted image 20250131164105.png” could not be found“