Network Basics 1

What's IP

- اول حاجه دا اختصار لكلمة Internet Protocol
- دا بالظبط بيكون عنوانك فالشبكه وكل يوزر فالشبكه بيكون ليه ip خاص بيه مختلف عن التاني
- بيتكون من 4 اجزاء من 1-255

- 192.168.1.1
- 176.16.13.199

Ports

- كل جهاز بيكون فيه بورتات مفتوحه البورتات دي بتكون بتقدم خدمة معينه
- تخيل معايا لو انت روحت مصلحه حكوميه فا هتلاقي كل شباك مثلا دا بتاع الفيزا ودا بتاع الجوازات ودا بتاع الضرايب فا هنا كل شباك بيقدملي خدمه معينه الports نفس الكلام برضو كل port بيكون شغال عليه service معينه ومش شرط كل البورتات تكون مفتوحه يعني
- كل ip بيكون عليه 65535 بورت ومش شرط كلهم يكونو شغالين
- طب احنا as a pentester افرض مثلا انت لو ف مصلحه حكوميه لقيت شباك وموظف قاعد عليه بس مش واخد باله وبيكلم زميله مثلا وفي فلوس محطوطه فا انت ممكن تسرق الفلوس دي من غير ما الموظف ياخد باله طب ليه حصل كدا؟ عشان الموظف اللي قاعد مكنش عامل حمايه بشكل كافي انو يمنع اي عملية سرقه
- بالظبط نفس المثال اللي فات ده فال pentest لو لقيت خدمه ضعيفه ساعتها اقدر استغلها واهكر الشبكه

مراحل تهكير الشبكه من خلال الservice اللي شغاله

1. ببدأ اعمل scanning واشوف البورتات المفتوحه
2. بشوف انهي services شغاله علي البورتات دي بالظبط

3. اعرف الاصدار بتاعها (عشان لو اصدر الخدمه قديم ممكن استغلها)
4. ببدأ استغل الservice الضعيفه دي

انواع حالات البورتات

---

1. Opened => يعني الخدمه شغاله
2. Closed => يعني الخدمه مقفوله
3. Filtered => معني كدا اني طلبات الشبكه الموجهة للخدمه دي بيتم حظرها وغالبا بيكون من الفايروال

Domain Name

- تخيل معايا كدا لو مكنش في اختراع ال contacts ومتضطر انك تحفظ ارقام صحابك وأهلك كلهم فا طبعا الموضوع هيكون صعب.....بس ايه علاقة الكلام ده بال Domain
- مبدأيا ال Domain ده بيتكون من حاجتين `Website Name + Top-level Domain`

Website Name

1. Google
2. Facebook
3. Instgram

Top-level Domain

4. .com => للشركات او للاستخدام العام
5. .org => للمنظمات
6. .net => للشبكات او مقدمي الخدمات
7. .edu => للمؤسسات التعليميه
8. .gov => للجهات الحكوميه

(بس دول الاشهر Top-level Domains دول مش ال)

Ex.

- google.com
- x.com

- rednexus.org
- facebook.com

- خلي بالك كل Domain لازم يكون ليه IP واحد
- انما ال IP ممكن يهندل اكتر من Domain

DNS Server

- حد هيقولي طب وايه علاقة المثال اللي قولتلو فوق بتاع الارقم بال DNS
- اقولك ماهو اصلا اي ويب سايت بيكون عباره عن IP مش اسم كدا زي مانت فاكر وال IP دا بتاع السيرفر اللي عليه الموقع
- طب هل انا هفضل احفظ بقي كل IP بتاع اي موقع انا عاوزه؟ اقولك لأماهو ال DNS هيحل المشكله دي
- احنا لما نعوز نفتح google.com مثلا فا هنروح نكتب فالبراوزر google.com فهيروح الطلب بتاعي مبعوت لل DNS يشوفلي google.com ده ال IP بتاعه ايه وبيبعتهولي والجهاز بتاعي يبعت للسيرفر فا الموقع يفتح

دا شكل ال Table اللي بيكون ف ال DNS

"Pasted image 20250109162244.png" could not be found.

"Pasted image 20250109162300.png" could not be found.

CIDR (Classless Inter-Domain Routing)

- دا نظام لتقسيم عناوين الشبكه واحسن كفاءتها
- عشان احدد الشبكه بستخدم ال CIDR ده وبيكون عباره عن `192.168.1.0/24` `IP Address/Prefix`
- ال prefix بيعبر عن ال subnet mask
- من خلال ال CIDR و IP الشبكه اقدر احدد عدد الاجهزه اللي ممكن اوصلها وتاخد ip من الرينج ده طب ازاي؟
  `-(prefix-32)^2` => by this role `2`

ASN (Autonomous System Number)

- دا بيكون رقم تعريفي خاص بكل شركه وبيكون فالشركات الكبيره جدا بس الرقم ده بيعبر عن ال assests بتاعت الشركه اللي ممكن اعمل عليها pentest زي ال Apks , servers , domains , Ips واخد مكافئه علي الكلام ده لو لقيت ثغره معينه وبلغتهم بيها
- Ex: AS3303 For Swisscom LTD
- Ex: AS15169 For Google
- طبعا بيكون في ادوات بتديلها ال ASN بتعرفك ايه الحاجات اللي متاح تعمل عليها pentest

---

TCP & UDP

TCP (Transmission Control Protocol)

- بروتوكول يعتمد على الاتصال الموثوق (Reliable)، ويضمن تسليم البيانات بشكل صحيح وفي الترتيب الصحيح وبيكون امان بس مشكلته انو بطئ

أمثلة:

1. **HTTP/HTTPS**:
   - عند تصفح المواقع الإلكترونية.
   - يستخدم TCP لضمان تحميل صفحات الويب بشكل صحيح.
2. **FTP (File Transfer Protocol)**:
   - لتحميل ورفع الملفات.
   - يحتاج نقل الملفات لدقة وضمان عدم فقدان البيانات.
3. **SMTP/IMAP/POP3**:
   - لإرسال واستقبال الإيميلات.
   - البريد الإلكتروني يحتاج إلى تسليم موثوق للرسائل.
4. **SSH (Secure Shell)**:
   - للاتصال بالخوادم بشكل آمن.
   - يعتمد على الاتصال الموثوق والآمن.
5. **Database Communication**:
   - بروتوكولات زي MySQL أو PostgreSQL.
   - تحتاج اتصال دقيق وموثوق لنقل البيانات بين العميل والخادم.

UDP (User Datagram Protocol):

- بروتوكول غير موثوق (Unreliable) وأسرع، لأنه لا يضمن تسليم البيانات أو ترتيبها، ومناسب للتطبيقات اللي الأولوية فيها للسرعة ميزته انه سريع بس بيفقد packets

أمثلة:

1. **DNS (Domain Name System)**:
   - لتحويل أسماء النطاقات (مثل google.com) إلى عناوين IP.
   - يعتمد على UDP لأنه سريع وبيحتاج إرسال طلبات صغيرة.
2. **VoIP (Voice over IP)**:
   - مكالمات الصوت والفيديو عبر الإنترنت (مثل Skype أو Zoom).
   - يستخدم UDP لتقليل التأخير (latency) حتى لو فقدت بعض البيانات.
3. **Online Gaming**:
   - ألعاب الأونلاين زي PUBG أو Fortnite.
   - تحتاج نقل بيانات سريع حتى لو فقدت بعض الحزم (Packets).
4. **Streaming (Audio/Video)**:
   - بث الفيديو والصوت مثل YouTube وNetflix.
   - يعتمد على UDP لتقليل وقت التأخير.
5. **DHCP (Dynamic Host Configuration Protocol)**:

```
- لتوزيع عناوين IP على الأجهزة داخل الشبكة.
- يتم باستخدام UDP وسريع بسيط لأنه.
```

“Pasted image 20250109163537.png” could not be found.

“Pasted image 20250109163608.png” could not be found.

Protocols

- البروتوكول ده عباره عن مجموعه من الخوارزميات عشان يتم نقل الداتا بيها
- زي ال Http , ftp , ssh , smtp

SSL & TLS

- عرفنا البروتوكولات فوق بس خلي بالك اني في بروتوكولات ضعيفه من ناحية الامان
- خليني اقولك فكرة ال TLS وال SSL انو بيحطلك شهاده موثقه مفادها اني الموقع ده محمي من الاختراق وعليه بروتوكولات حمايه زي ال SSL او ال TLS (ال TLS وال SSL مشروحين بالتفصيل فكورس ال +Security ف ريبو عندي باسم SecurityPlusTantawixEdition لو عاوز تفهمهم اكتر)
- الSSL خاص بحماية ال HTTP فا بيبقي HTTPS , بس الattackers اكتشفو ثغره ف ال SSL اسمها SSL Strip ودي بتخلي الكونكشن يبقي http بدل https فا اتعمل منها شهادة اقوي واكتر امان اسمها TLS
- بيتم تشفير الداتا وبتتحط ف نفق مغلق عشان محدش يقدر يعمل Sniffing او يتجسس علي ال traffic بتاعي

“Pasted image 20250109164250.png” could not be found.