Network Basics 2

IP (Internet Protocol)

- ذكرنا قبل كدا فالدرس اللي قابله وقولنا اني ده بيكون عنوانك علي الشبكه
- خلي بالك ال IP علي جهاز بيكون نوعين هو public و private
- ال private ده اللي بيكون علي جهاز وخاص بالشبكه لو هتتواصل مع اي جهاز ف نفس الشبكه 192.168.1.50 حاجه زي كدا مثلا
- ال public بقي دا عنوانك علي الانترنت واللي الناس بيشوفوه زي 167.158.44.149
- بيتم تحويل ال ip من private ل public عن طريق ال NAT Protocol

IPv4

- نوع من الايبي بيتكون من اربع مقاطع وبيكون 32 بت زي مثلا 192.168.1.1

IPv6

- نوع من الايبي بيتكون من ست مقاطع وبيكون 128 بت وبيكون بنظام ال hexadecimal زي مثلا 2001:0db8:85a3:0000:0000:8a2e:0370:7334

الهجمات اللي ممكن تحصل علي ال IP

- IP Spoofing
- DDoS Attack

Switch

- دا جهاز بيكون متوصل بالراوتر وظيفته انو يربط اجهزة الشبكه ببعض وبيبعت الداتا للأجهزه عن طريق ال MAC Address
- في حاجه فالswitch اسمها VLAN يعني مثلا اعزل اكتر من جهاز متوصلين بالswitch افتراضيا واديهم ايبيهات افتراضيه كل الكلام ده مشروح ف جزء ال Network ف كورس ال +Security في ريبو تانيه علي نفس الاكونت باسم SecurityPlusTantawixEdition

الهجمات اللي ممكن تحصل علي ال Switch

1. Mac Flooding
2. VLAN Hopping

Router

- دا بقي الجهاز اللي بيتحكم ف الشبكه كلها وبيوزع ايبيهات ويوجه البيانات عن طريق ال IP

الهجمات اللي ممكن تحصل علي ال Router

1. Router Poisoning
2. DNS Spoofing
3. DoS/DDoS

Firewall

- دا جهاز حمايه للشبكه طبعا دا بيكون يا اما hardware او software
- طريقة عمل ال firewall انت بتعمله configuration او بتظبطه يعني انو لو لقي حاجه معينه يوقف الحاجه دي علاطول
- يعني مثلا انا لو هجيب حارس للبيت هقولو خلي بالك لو لقيت حد لابس ابيض ف اسود او حد تحركاته مريبه وواقف قدام البيت كدا مشيه من قدام البيت او امنعه

- بالظبط ال Firewall نفس الكلام بس خلي بالك اني ال Firewall بيبص علي ال header بتاع ال packets اللي بتتبعت انما هو مش بيبص علي المحتوي اللي جوا الباكيت دي (اللي بيبص علي المحتوي ده بيكون جهاز ال IPS وال IDS)

الهجمات اللي ممكن تحصل علي ال Firewall

1. Firewall Evasion
2. DoS on Firewall

"Pasted image 20250110170133.png" could not be found.

Access Point

- دا بيكون عامل زي ال switch بس دا بيكون wireless وفي منو wire برضو عادي بس بيدعم ال wireless connection

Active Directory

- في نسخة ويندوز زي ويندوز 10 و ويندوز 11 وكدا اسمها Windows Server
- النسخه دي بتكون خاصه للسيرفرات عشان تديرها وتتحكم فالشبكه وتدي الصلاحيات المناسبه لكل قسم
- فا الويندوز دي بيكون في software اسمه Active Directory ودا برنامج خاص بالويندوز سيرفر عشان انت كا Network Admin تتحكم فالصلاحيات لكل قسم يعني مثلا الفولدرات دي محدش يعرف يأكسس عليها الا القسم المختص بيها
- لو عرف ال attacker يستغل اي ثغره ف ال active directory هيعرف انو يخترق السيستم بالكامل لأنه أكسس علي كل حاجه ويقدر يعلي صلاحياته ويعمل حاجات بأنه يمسح ملفات او يسربها ويخرب ف كل حاجه حرفيا (Privilege Escalation)

Load Balancer

- بيوزع الحمل او الطلبات اللي بتيجي علي السيرفرات بالتساوي عليهم
- دلوقتي كان ال attackers بيعملو هجمات علي المواقع زي ال DoS ودي اتاك بتمنع الموقع انه يشتغل

DoS Attack

- هجمات الحرمان من الخدمه الاتاكر هنا بيقعد يبعت ريكويستات كتير للسيرفر فا لما السيرفر يجيلو ريكويستات كتير مش هيقدر يتعامل مع كم الطلبات اللي بتجيلو ف الموقع يقع
- “Pasted image 20250110171128.png” could not be found.
- فا عشان اصحاب المواقع يحمو نفسهم من الاتاك دي عملو ايه؟.....قالو احنا حاطين سيرفرات لينا ف كل دوله يعني في دول معينه احنا حاطين فيها سيرفرات فا احنا هنجيب ال Load Balancer ده ويوزع الريكويستات بالتساوي علي السيرفرات
- يعني مثلا موقع معين عنده سيرفر ف امريكا وسيرفر ف فرنسا فا الاتاكر ممكن يعمل DoS علي السيرفر اللي ف امريكا والموقع يقع طب ايه رأيك لو جبنا Load Balancer وخلينا اني الطلبات تتوزع بين السيرفر اللي ف امريكا والسيرفر اللي ف فرنسا وساعتها بما اننا خففنا الحمل علي السيرفرات فا هيقدرو يتعاملو مع الطلبات دي عادي عشان قللناها وبكدا نكون منعنا ال DoS Attack

“Pasted image 20250110171105.png” could not be found.

DHCP Server (Dynamic Host Configuration Protocol)

- دا سيرفر مسؤول عن انو يدي ايبيهات للاجهزه تلقائيا
- انا دلوقتي لو حد جه يتصل بالشبكه يا اما يدي لنفسه ايبي من خلال اعدادات الجهاز بتاعه او يستخدم ال DHCP ده أنه يديك ايبي تلقائي

الهجمات اللي ممكن تحصل علي ال DHCP

- DHCP Starvation
- Rogue DHCP

3-Way Hanshake

الـ **Way Hanshake-3** هو عملية التهيئة الأساسية اللي بيستخدمها بروتوكول **TCP (Transmission Control Protocol)** لإنشاء اتصال موثوق بين جهازين (Client وServer) العملية دي بتضمن إن الجهازين جاهزين للإرسال والاستقبال قبل ما يبدأوا نقل البيانات

خطوات الـ Way Handshake-3

1. **SYN (Synchronization)**
   - الجهاز العميل (Client) بيبعت حزمة (Packet) اسمها **SYN** للسيرفر
   - الغرض منها طلب بدء الاتصال وتحديد رقم تسلسلي (Sequence Number) عشان يتابع البيانات اللي هتتبعت

   `Client → Server: SYN`
2. **SYN-ACK (Synchronization-Acknowledgment)**
   - السيرفر بيستلم الـ **SYN** وبيبعت رد باسم **SYN-ACK**
   - الـ SYN: السيرفر بيقول "أنا موافق نبدأ الاتصال"
   - الـ ACK: تأكيد استلام حزمة الـ SYN من العميل

   `Server → Client: SYN-ACK`
3. **ACK (Acknowledgment)**

- العميل بيبعت حزمة **ACK** للسيرفر لتأكيد استلام حزمة **SYN-ACK**
- كده الاتصال جاهز وموثوق، وبيبدأ نقل البيانات

`Client → Server: ACK`

“Pasted image 20250110172133.png” could not be found.

VPS (Virtual Private Server)

- عباره عن PC افتراضي بيكون ليه مواصفات عاليه جدا سواء رام او بروسيسور او كارت شاشه وبسرعة نت عاليه جدا
- بيكون جزء من خادم فعلي (Physical Server) لكن له نظام تشغيل وموارد مخصصة زي RAM، CPU، ومساحة تخزين
- في منصات كتير بتقدر توفرلك VPS زي Segfault , Azure , Google

ليه نستخدم VPS؟

1. استضافة مواقع الإنترنت (Web Hosting):
   - لو عندك موقع ويب محتاج أداء أعلى من الاستضافة المشتركة (Shared Hosting)، فالـ VPS بيكون خيار ممتاز لأنه بيقدم موارد مخصصة
2. تجربة بيئات التطوير (Development Environments):
   - لو عايز تعمل بيئة تطوير واختبار لتطبيقاتك أو مشاريعك بدون الاعتماد على جهازك الشخصي
3. إدارة الخوادم:
   - تقدر تستخدم الـ VPS كخادم (Server) لتشغيل قواعد بيانات، خوادم بريد إلكتروني (Mail Servers)، أو حتى خوادم تطبيقات زي Node.js وDjango
4. التكلفة مقابل الأداء:
   - بيقدّم توازن ممتاز بين التكلفة والأداء. أرخص من شراء خادم فعلي (Dedicated Server) وأكتر كفاءة من الاستضافة المشتركة
5. إدارة سيرفر خاص بالألعاب (Gaming Servers):
   - لو عايز تستضيف ألعاب أونلاين زي Minecraft أو CS:GO، الـ VPS بيوفر بيئة مستقرة وقابلة للتعديل
6. تشغيل برامج مخصصة:
   - لو عندك تطبيقات أو سكربتات محتاجة تشغيل 24/7، زي بوتات (Bots)، أنظمة مراقبة، أو أتمتة
7. استعماله كـ VPN:
   - ممكن تستخدم الـ VPS كـ VPN لتأمين اتصالك بالإنترنت وحماية خصوصيتك
8. تحكم كامل (Full Root Access):
   - مع الـ VPS، عندك تحكم كامل في الخادم. تقدر تثبت أي نظام تشغيل، تعدل إعدادات الشبكة، أو تنزل البرامج اللي محتاجها
9. الأمان (Security):
   - مقارنة بالاستضافة المشتركة، الـ VPS بيقدم أمان أعلى لأن كل خادم افتراضي بيكون معزول عن الخوادم التانية
10. التوسع (Scalability):
    - لو مشروعك بيكبر وبتحتاج موارد أكتر، تقدر توسع موارد الـ VPS بسهولة بدون نقل بياناتك لخادم جديد

Virtualization

- الافتراضيه بشكل عام انك تقدر توفر حاجه بشكل افتراضي
- زي مثلا اني اسطب كالي وانا بستخدم ويندوز دلوقتي دا Virtual Machine
- اني بقدر اوفر للكالي دي مثلا مساحه فالمساحه اللي بوفرها دي مش مساحه فعليه بجد دي حاجه افتراضيه
- تقدر تعمل أكتر من سيرفر افتراضي على نفس السيرفر المادي لتوفير التكاليف واستغلال الموارد بشكل أفضل

.Pasted image 20250110172458.png” could not be found“

Virtualization Modes:

Bridge Mode:

- في الوضع ده، الجهاز الافتراضي (VM) بياخد عنوان IP مستقل من الشبكة المحلية، زي كأنه جهاز حقيقي متصل بالشبكة
- مثال: لو نظام Windows الأساسي عنده IP: `192.168.1.5`، الجهاز التخيلي (Linux) ممكن ياخد IP زي `192.168.1.6` أو أي IP في نفس النطاق `x.192.168.1`

NAT (Network Address Translation):

- في الوضع ده، الجهاز الافتراضي بياخد عنوان داخلي خاص ومترجم عن طريق الجهاز الأساسي
- يعني الجهاز التخيلي ما بيظهرش مباشرة للشبكة الخارجية وبيستخدم عنوان الجهاز الأساسي للاتصال.
- مثال: لو الجهاز الأساسي عنده IP: `192.168.1.5`، الجهاز التخيلي ممكن ياخد IP زي `192.168.45.1`، وهو IP داخلي مخصص من Virtualization Software

ليه نستخدم Virtualization؟

- توفير التكاليف، بدل ما تشتري أجهزة كتير
- سهولة تجربة أكتر من نظام تشغيل
- عزل بيئة العمل (Sandboxing) عشان تختبر البرامج بدون التأثير على النظام الأساسي