DoS Attack

يعني ايه DoS Attack (Denial of Service)؟

- دلوقتي يا معلم انت في موقع مثلا الموقع محطوط علي سيرفر السيرفر ده بيكون معمول انو يستقبل عدد معين من الطلبات طب افرض احنا قعدنا نعمل عليه طلبات كتير؟ كدا هيحصل حرمان من الخدمه والموقع مش هيستحمل وهيقع ومش هيفتح لفتره معينه حسب قوة الاتاك وهيرجع تاني
- يعني مثلا لو عندك شباك تذاكر الموظف اللي واقف عالشباك معاه 5000 تذكره جه واحد غني قاله يا باشا انا هاخد ال 5000 تذكره دول هيروح مديهمله اللي وراه هيجي يشتري واحده الموظف هيقولو مفيش والله وبكدا الشخص اللي ورا الراجل الغني ده اتحرم من انه يدخل الماتش او الفيلم , بالظبط هو ده ال DoS Attack

“Pasted image 20250118172626.png” could not be found.

ايه الفرق بين ال DoS وال DDoS؟

1. DoS Attack

- المصدر: الهجوم بيجي من جهاز واحد بس
- الطريقة: بيتم إرسال عدد كبير من الطلبات من جهاز واحد بغرض شل حركة السيرفر أو الشبكة ومنعهم من تقديم الخدمة للمستخدمين الآخرين
- الهدف: تعطيل السيرفر بشكل مؤقت أو دائم بحيث ميقدرش يستجيب لطلبات المستخدمين الجدد
- السهولة: الهجمات دي أسهل في التنفيذ مقارنة بـ DDoS لأنها بتعتمد على جهاز واحد فقط
- الحماية: ممكن الدفاع عنها باستخدام جدران نارية أو تقنيات لتصفية البيانات

2. DDoS Attack

- المصدر: الهجوم بيجي من عدد كبير جدًا من الأجهزة المنتشرة في أماكن مختلفة، ودي الأجهزة غالبًا بتكون مخترقة أو متحكم فيها عن بعد (مثل الروبوتات - Bots) في شبكة تسمى Botnet
- الطريقة: الهجوم بيتم من خلال إرسال عدد هائل جدًا من الطلبات إلى السيرفر من خلال مجموعة ضخمة من الأجهزة (عدة مصادر)، وبالتالي يصعب تحديد مصدر الهجوم أو تصفيته
- الهدف: تعطيل السيرفر أو الشبكة بطريقة مشابهة لـ DoS، لكن باستخدام قوة أكبر، لأن الهجوم بييجي من مصادر متعددة مما بيصعب التعامل معاه

- السهولة: DDoS أكثر تعقيدًا وصعوبة في الحماية لأنه معتمد على عدد كبير من الأجهزة، وبالتالي الدفاع عنه بيكون أصعب
- الحماية: محتاجة حلول أكثر تعقيدًا زي أنظمة التصفية المتقدمة، أو استخدام شبكات CDN (Content Delivery Network) لتوزيع التحميل

طريقة عمل ال DoS Attack؟

Ping

- انا هنا بعمل طلبات بينج عادي جدا علي الموقع بس بعمله بكتره بحيث العدد يكون كبير فا السيرفر ميقدرش يستحمل
- فالعادي بنكتب `ping scanme.nmap.org` بس ايه رأيك لو خليت طلبات ال Ping دي اكتر من طلب فالثانيه الواحده
- هنا انا بختار عدد الطلبات فالثانيه `-c
- هنا انا بختار عدد الثواني بين كل طلب والتاني `-i
- `ping scanme.nmap.org -i .001` هنا معني الكوماند انه يعمل 1000 طلب علي الموقع كل ثانيه

hping3

- الhping3 دي اداه موجوده فاللينكس متقدمه اكتر من الping العادي
- دي بقي بتقدر تعملي طلبات بينج اكتر واسرع من ال Ping العادي عن طريق شويه كوماندات كدا

1. fast => بتبعت 10 طلبات فالثانيه
2. faster => بتبعت 100 طلب فالثانيه
3. flood => دي بقي اللي بتستخدم في الاتاك وبتبعت طلبات كتير جدا فالثانيه الواحده

sudo نكون فالروت او نستخدم hping3 خلي بالك لازم عشان نستخدم

“Pasted image 20250118172943.png” could not be found.