

يمكن إعداد سيناريو لمحاكاة هجوم حجب الخدمة الموزع (DDoS) على خادم محلي ومحاولة تخفيف الهجوم باستخدام تقنيات الحماية المتاحة. سأوضح لك خطوات إعداد هذا السيناريو وكيفية تنفيذ التقنيات المختلفة لتخفيف الهجوم.

1. إعداد البيئة التجريبية

1.1. إعداد الخادم المحلي

- قم بإعداد خادم محلي على جهاز افتراضي (مثل VirtualBox) أو على جهاز حقيقي.
- يمكنك استخدام نظام تشغيل مثل **Ubuntu Server** أو **Windows Server**.
- تأكد من تثبيت **خدمة ويب** (مثل Apache أو Nginx) على الخادم المحلي.

1.2. إعداد أدوات المحاكاة

- تحتاج إلى أدوات لمحاكاة هجوم DDoS من الأدوات الشائعة هي **LOIC (Low Orbit Ion Cannon)** أو **HOIC (High Orbit Ion Cannon)**. يمكنك استخدام أدوات أخرى مثل **Hping3** أو **Metasploit** للسيناريوهات أكثر تقدمًا.
- تأكد من استخدام أدوات في بيئة اختبارية فقط لضمان عدم الإضرار بالشبكات أو الأنظمة الأخرى.

2. تنفيذ هجوم DDoS

2.1. إعداد LOIC

- قم بتحميل وتثبيت **LOIC** من مصادر موثوقة.
- افتح LOIC ، وقم بإدخال عنوان IP الخاص بالخادم المحلي في الحقل المخصص.
- اختر نوع الهجوم (TCP/UDP/HTTP) وحدد عدد الطلبات (Requests) التي تريد إرسالها.
- انقر على "IMMA CHARGIN MAH LAZER" لبدء الهجوم.

2.2. تنفيذ الهجوم

- في **LOIC**، بعد بدء الهجوم، سيبدأ الخادم المحلي في تلقي كمية كبيرة من الطلبات التي قد تؤدي إلى تعطله.
- استخدم أدوات المراقبة مثل **Netstat** أو **iftop** على الخادم المحلي لمراقبة النشاط.

3. تخفيف الهجوم

3.1. استخدام جدار الحماية

- **iptables على Linux** :
 - يمكنك استخدام **iptables** لتصفية حركة المرور غير المرغوب فيها. على سبيل المثال، يمكنك تحديد حد لعدد الاتصالات الواردة من عنوان IP معين.

```
iptables -A INPUT -p tcp --dport 80 -m limit --limit 10/s -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j DROP
```

• Windows Firewall:

- قم بتكوين قواعد تصفية في Windows Firewall لتحديد حد للاتصالات.

3.2. استخدام أدوات مراقبة الشبكة

- استخدم أدوات مثل Wireshark لتحليل حركة المرور وتحديد مصدر الهجوم.
- استخدم Snort أو Suricata للكشف عن الأنماط غير الطبيعية في حركة المرور.

3.3. تحسين الخادم

- قم بتعديل إعدادات الخادم لتحسين الأداء، مثل زيادة عدد الاتصالات المتزامنة أو تحسين تكوين الذاكرة.
- استخدام CDN (شبكة توصيل المحتوى) لتوزيع الحمل وتحسين الأداء.

4. توثيق النتائج

4.1. التقاط صور أو تسجيل فيديو

- استخدم أدوات التقاط الشاشة مثل Snipping Tool أو OBS Studio لتوثيق الخطوات.
- سجل الفيديو الذي يوضح كيفية تنفيذ الهجوم وتخفيفه باستخدام التقنيات الموضحة.

4.2. كتابة تقرير

- أعد تقريرًا يتضمن شرحًا للخطوات التي تم تنفيذها، النتائج التي تم الحصول عليها، والتقنيات المستخدمة لتخفيف الهجوم.

ملحوظة مهمة:

تأكد من تنفيذ هذه الأنشطة فقط في بيئة آمنة ومخصصة للاختبار لضمان عدم تأثيرها على الشبكات أو الأنظمة الأخرى.