

DDoS سيناريو محاكاة هجوم

1. **إعداد الخادم المحلي**:

- Linux أو Windows قم بإعداد خادم محلي باستخدام نظام تشغيل مثل
- Nginx أو Apache تأكد من تثبيت خدمات الويب مثل

2. **DDoS تنفيذ هجوم**:

- لمحاكاة الهجوم (HOIC (High Orbit Ion Cannon أو LOIC (Low Orbit Ion Cannon استخدم أدوات مثل
- قم بتوجيه عدد كبير من الطلبات إلى الخادم المحلي في وقت قصير لمحاكاة الهجوم

DDoS تقنيات التخفيف من هجمات

1. **Firewalls استخدام جدران الحماية**:

- قم بتكوين جدار حماية لتصفية حركة المرور غير المرغوب فيها
- المشبوهة IP استخدم قواعد لتحديد وحظر عناوين

2. **IPS (Intrusion Prevention System) وأنظمة منع التسلل (IDS) استخدام أنظمة كشف التسلل**:

- قم بتثبيت وتكوين أنظمة كشف ومنع التسلل لمراقبة حركة المرور واكتشاف الأنشطة المشبوهة
- قم بإعداد قواعد لتحديد وحظر الهجمات المحتملة

3. **DDoS استخدام خدمات الحماية من**:

- Akamai أو Cloudflare المقدمة من مزودي الخدمة مثل DDoS استخدم خدمات الحماية من
- هذه الخدمات توفر حماية متقدمة وتقوم بتصفية حركة المرور الضارة قبل وصولها إلى الخادم

4. **Load Balancing توزيع الحمل**:

- استخدم تقنيات توزيع الحمل لتوزيع حركة المرور على عدة خوادم
- هذا يساعد في تقليل الضغط على خادم واحد ويزيد من تحمل النظام للهجمات

5. **Rate Limiting تحديد معدل الطلبات**:

- قم بتحديد عدد الطلبات التي يمكن أن يستقبلها الخادم في فترة زمنية معينة
- هذا يساعد في تقليل تأثير الهجمات التي تعتمد على إرسال عدد كبير من الطلبات في وقت قصير

الخلاصة

واستخدام تقنيات التخفيف المناسبة، يمكنك حماية الأنظمة والخوادم من هذه DDoS من خلال فهم كيفية تنفيذ هجمات

الهجمات.