

تحدي الاسبوع 6

1. إعداد الخادم المحلي:

- قمت بتثبيت Apache على الخادم المحلي ليكون هدفًا للهجوم. تأكدت من أن الخادم يعمل بشكل صحيح ويستجيب للطلبات على الشبكة المحلية.

2. اختيار أداة الهجوم:

- اخترت أداة LOIC (Low Orbit Ion Cannon) لتنفيذ هجوم DDoS. LOIC هي أداة مفتوحة المصدر تُستخدم لمحاكاة هجمات حجب الخدمة عن طريق إغراق الخادم بحركة مرور كبيرة.

3. تنفيذ هجوم DDoS:

- قمت بإعداد LOIC على جهاز منفصل في الشبكة. أدخلت عنوان ال IP الخاص بالخادم المحلي الذي يستضيف Apache كهدف للهجوم.

- اخترت نوع الهجوم المناسب (TCP, UDP, HTTP) وبدأت في إرسال حزم البيانات إلى الخادم. الهدف كان إغراق الخادم بحركة مرور زائدة لإبطاء أو إيقاف استجابته للطلبات الشرعية.

- أثناء الهجوم، لاحظت زيادة كبيرة في استخدام الموارد على الخادم (مثل CPU و RAM) وانخفاض في معدل استجابة الخادم.

4. تطبيق تقنيات الحماية:

- تصفية حركة المرور باستخدام iptables:

- بدأت بتحديد عناوين IP التي تولد حركة مرور ضارة باستخدام أداة مراقبة الشبكة.

- استخدمت الأمر التالي في iptables لحظر حركة المرور القادمة من هذه العناوين:

```
sudo iptables -A INPUT -s <Malicious_IP> -j DROP
```

- تحديد معدلات الطلبات (Rate Limiting):

- قمت بتعديل إعدادات Apache لتقليل عدد الطلبات المسموح بها من نفس العنوان في فترة زمنية محددة باستخدام وحدة mod_evasive. أضفت القواعد التالية إلى ملف إعدادات Apache:

```
<IfModule mod_evasive20.c>
```

```
DOSHashTableSize 3097
```

```
DOSPageCount 2
```

```
DOSSiteCount 50
```

```
DOSPageInterval 1
```

```
DOSSiteInterval 1
```

```
DOSBlockingPeriod 10
```

```
</IfModule/>
```

- استخدام Load Balancer (في حال توفره):

- في بيئة الإنتاج، يمكنني إضافة Load Balancer لتوزيع حركة المرور على عدة خوادم، مما يساعد في تخفيف تأثير الهجوم.

5. مراقبة وتقييم الأداء:

- بعد تطبيق تقنيات الحماية، راقبت أداء الخادم باستخدام أدوات مثل top و htop و netstat.

- لاحظت تحسناً ملحوظاً في استجابة الخادم بعد تطبيق الفلاتر وتحديد معدلات الطلبات. الخادم استمر في الاستجابة للطلبات الشرعية حتى أثناء الهجوم.