الاسم: ليلى نزهان ثقل القحطاني
التخصص: الامن السيبراني

تحليل الشبكة باستخدام أداة tcpdump

1 المقدمة:

في هذا المشروع، قمنا باستخدام أدا **tcpdump** لمراقبة وتحليل حركة مرور الشبكة **(Network Traffic)** على **Kali Linux.**

تم إرسال طلبات **ICMP** عبر الأمر **ping** إلى عنوان خارجي، وتم التقاط الحزم باستخدام **tcpdump** لتحليل الاتصال.

الأدوات المستخدمة:

- **Kali Linux**
- أداة **tcpdump**
- الأمر **ping**
- واجهة الشبكة **eth0** أو **lo**

الأوامر المستخدمة:

الأمر لتشغيل مراقبة الشبكة عبر الواجهة **eth0:**

```
sudo tcpdump -i eth0
```

الأمر لتجربة الاتصال **(ping)** مع **Google DNS:**

```
ping 8.8.8.8
```

✳ أحيانًا إذا لم تلتقط **tcpdump** مع الأمر جرب شيء، بدل **eth0** **lo**

sudo tcpdump -i lo

الاسم: ليلى نزهان ثقل القحطاني
التخصص: الامن السيبراني

التحليل:

.(التابع لجوجل DNS إلى العنوان 8.8.8.8 (سيرفر ICMP من خلال النتائج، نلاحظ أن الجهاز قام بإرسال طلبات

قامت بالتقاط هذه الحزم وعرض تفاصيلها، مثل tcpdump أداة:

- **عنوان المصدر والوجهة**
- **البروتوكول (ICMP)**
- **الوقت الذي تم فيه الإرسال والاستقبال**

هذا يوضح قدرة tcpdump على مراقبة الاتصالات وتحليلها في الوقت الحقيقي.

الاسم: ليلى نزهان ثقل القحطاني
التخصص: الامن السيبراني

6 الخاتمة:

تعتبر من الأدوات الأساسية لتحليل الشبكة، وهي مفيدة جدًا في الأمن السيبراني ومجالات اختبار الاختراق. tcpdump أداة

توفر هذه الأداة إمكانية رؤية ما يحدث داخل الشبكة من حيث حركة الحزم والتواصل بين الأجهزة