

تحليل الشبكة باستخدام أداة tcpdump

1 المقدمة:

Kali على (Network Traffic) لمراقبة وتحليل حركة مرور الشبكة tcpdump في هذا المشروع، قمنا باستخدام أداة 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
- lo أو eth0 واجهة الشبكة

الأوامر المستخدمة:

eth0: الأمر لتشغيل مراقبة الشبكة عبر الواجهة

```
sudo tcpdump -i eth0
```

Google DNS مع (ping) الأمر لتجربة الاتصال

```
ping 8.8.8.8
```

eth0 بلل lo شيء، جرب الأمر مع tcpdump أحياناً إذا لم تلتقط *

```
sudo tcpdump -i lo
```

```
(kali@kali)-[~]
$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:57:28.065652 IP 10.0.2.15 > dns.google: ICMP echo request, id 6123, seq 1,
length 64
21:57:28.068758 IP 10.0.2.15.58906 > 10.0.2.3.domain: 16619+ PTR? 8.8.8.8.in-
addr.arpa. (38)
21:57:28.124812 IP 10.0.2.3.domain > 10.0.2.15.58906: 16619 1/0/0 PTR dns.goo
gle. (62)
21:57:28.125351 IP 10.0.2.15.55312 > 10.0.2.3.domain: 15747+ PTR? 15.2.0.10.i
n-addr.arpa. (40)
21:57:28.151138 IP dns.google > 10.0.2.15: ICMP echo reply, id 6123, seq 1, l
length 64
21:57:28.234237 IP 10.0.2.3.domain > 10.0.2.15.55312: 15747 NXDomain* 0/1/0 (
)
21:57:28.241373 IP 10.0.2.15.52857 > 10.0.2.3.domain: 63930+ PTR? 3.2.0.10.in
addr.arpa. (39)
21:57:28.402480 IP 10.0.2.3.domain > 10.0.2.15.52857: 63930 NXDomain* 0/1/0 (
)
21:57:29.067516 IP 10.0.2.15 > dns.google: ICMP echo request, id 6123, seq 2,
length 64
21:57:29.152726 IP dns.google > 10.0.2.15: ICMP echo reply, id 6123, seq 2, l
length 64
21:57:30.070994 IP 10.0.2.15 > dns.google: ICMP echo request, id 6123, seq 3,
length 64
21:57:30.151159 IP dns.google > 10.0.2.15: ICMP echo reply, id 6123, seq 3, l
```

```
(kali@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=85.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=85.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=80.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=80.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=255 time=415 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=255 time=106 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=255 time=95.1 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=255 time=102 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=255 time=102 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=255 time=96.0 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=255 time=74.0 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=255 time=93.8 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=255 time=71.8 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=255 time=70.3 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=255 time=88.5 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=255 time=90.9 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=255 time=70.3 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=255 time=72.2 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=255 time=70.5 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=255 time=80.8 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=255 time=80.7 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=255 time=79.7 ms
```

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.

6 الخاتمة:

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

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