ICMP ATÖLYESİ

ATÖLYENİN HEDEFİ:

Bu atölyede ICMP paketinin nasıl alındığını öğreneceksiniz.

ATÖLYENİN AMACI:

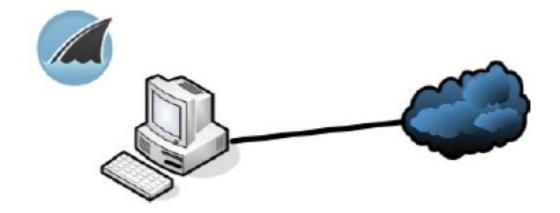
Internet Control Message Protocol (ICMP) ağ aygıtları tarafından güvenilirlik hakkında raporlama yapmak ve hata mesajları göndermek için kullanılır. ICMP, TCP/IP içindeki diğer protokollerin çoğundan farklıdır çünkü veri taşımak için kullanılmaz.

ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda da aynı kolaylıkla çalıştırabilirsiniz.

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.



ATÖLYE ANLATIMI:

Adım1:

https://www.wireshark.org/download.html Adresine giderek sisteminize uygun wireshark'ı indirin ve bilgisayarınıza kurun.

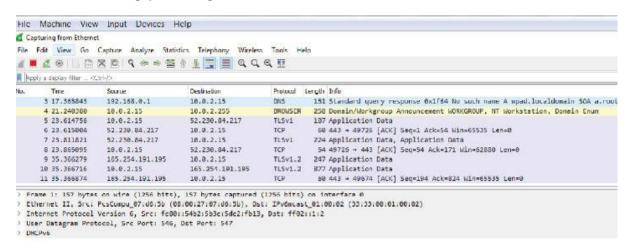
Adım2:

Wireshark'ı açarak yakalamak istediğimiz bağlantıyı seçelim. Ben "yerel ağ bağlantısı"nı seçtim.



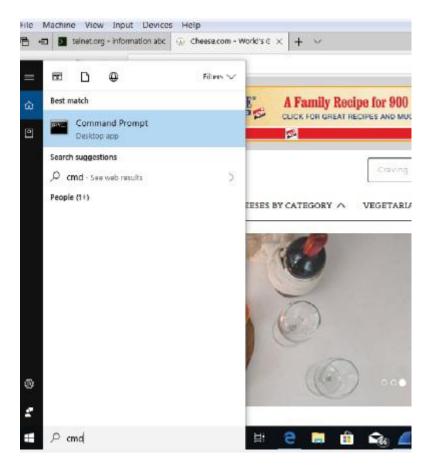
Adım 3:

Wireshark'ın trafiği yakaladığından emin olun.



Adım 4:

Arama çubuğuna 'cmd' yazarak bir komut satırı penceresi açın.



Adım 5:

cisco.com gibi genel bir URL'ye ping atın. Birçok site ICMP'yi engellemiştir. Bu yüzden bunu engellememiş bir websitesi bulun (veya ağınızdaki dahili bir makineye ping atın).

```
Microsoft Windows [Version 10.0.17134.228]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\paulw>ping cisco.com

Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=221ms TTL=237
Reply from 72.163.4.185: bytes=32 time=224ms TTL=237
Reply from 72.163.4.185: bytes=32 time=227ms TTL=237
Reply from 72.163.4.185: bytes=32 time=229ms TTL=237

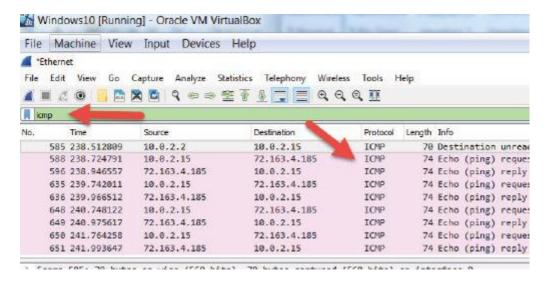
Ping statistics for 72.163.4.185:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 221ms, Maximum = 229ms, Average = 225ms

C:\Users\paulw>_
```

Adım 6:

Sonuçları daraltmak ve ICMP trafiğini kullanmak için Wireshark filtre çubuğunu kullanın. Yalnızca küçük harfle yazın.



Adım 7:

Ping'in ICMP echo isteği ve echo yanıt paketlerini kullandığını unutmayın. Yanıt süresini, uzunluğunu vb. bulun.

```
> Internet Protocol Version 4, Src: 72.163.4.185, Dst: 10.0.2.15

> Internet Control Message Protocol

    Type: 0 (Echo (ping) reply)
    Code: 0

    Checksum: 0x555a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)

    [Request frame: 280]
    [Response time: 221.766 ms]

> Data: 6162636465666768696.666666666707172737475767761...
    [Length: 32]
```

Adım 8:

Time To Live'i (TTL) IP başlığı altında bulun.

```
✓ Internet Protocol Version 4, Src: 72.163.4.185, Dst: 10.0.2.15
    8100 .... - Version: 4
    .... 0101 - Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x4dc4 (19908)

> Flags: 0x0000
    Time to live: 237
    Protocol: ICMP (1)
    Header checksum: 0x2692 [validation disabled]
    [Header checksum status: Unverified]
    Source: 72.163.4.185
```