TCP ATÖLYESİ

ATÖLYENİN HEDEFİ:

Bu atölyede TCP paketinin nasıl alındığını öğreneceksiniz.

ATÖLYENİN AMACI:

Transmission Control Protocol (TCP), TCP/IP‘nin ilk kısmıdır. Telnet, FTP ve BGP gibi bazı yönlendirme protokolleri gibi bağlantı odaklı hizmetlerin ve protokollerin ağlar üzerinden çalışmasını sağlar

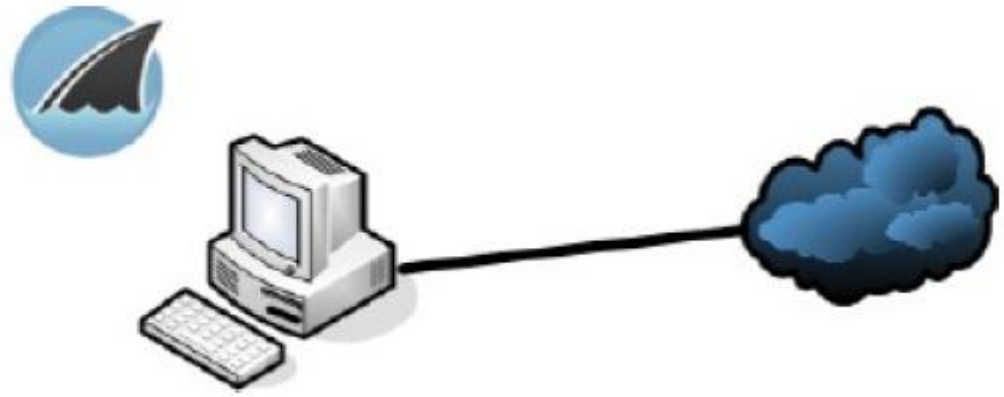
ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda da aynı kolaylıkla çalıştırabilirsiniz.

Bir Telnet/SSH istemcisi olan Putty'yi kurun. Putty'yi https://putty.org/ adresinden indirebilirsiniz. Putty, Telnet'i kullanmayı çok daha kolay hale getirir çünkü çoğu istemci yazılımı Telnet’i varsayılan olarak devre dışı bırakıyor.

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.

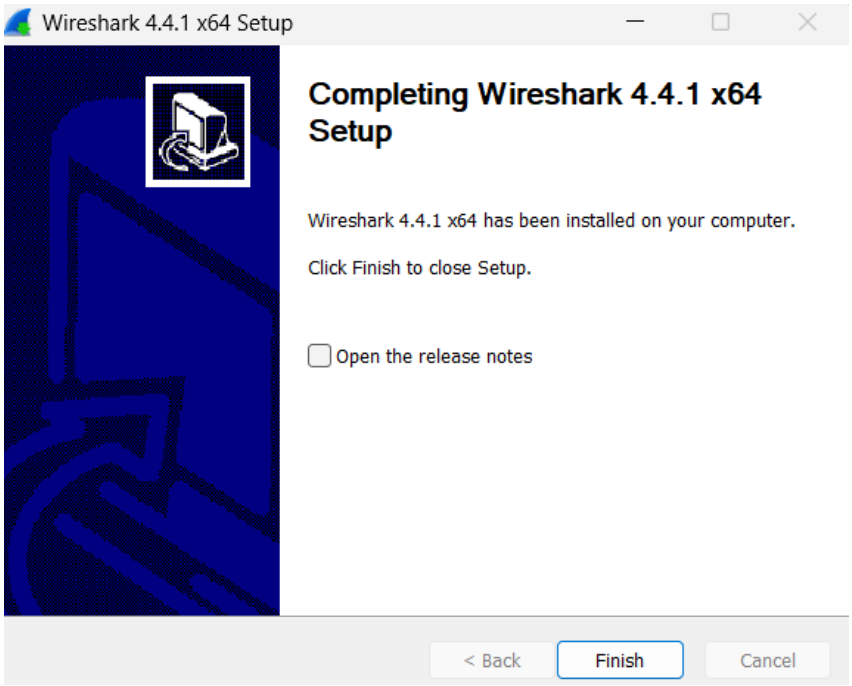


ATÖLYE ANLATIMI:

Adım 1:

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

Wireshark kurulduğunda aşağıdaki ekranı göreceğiz:



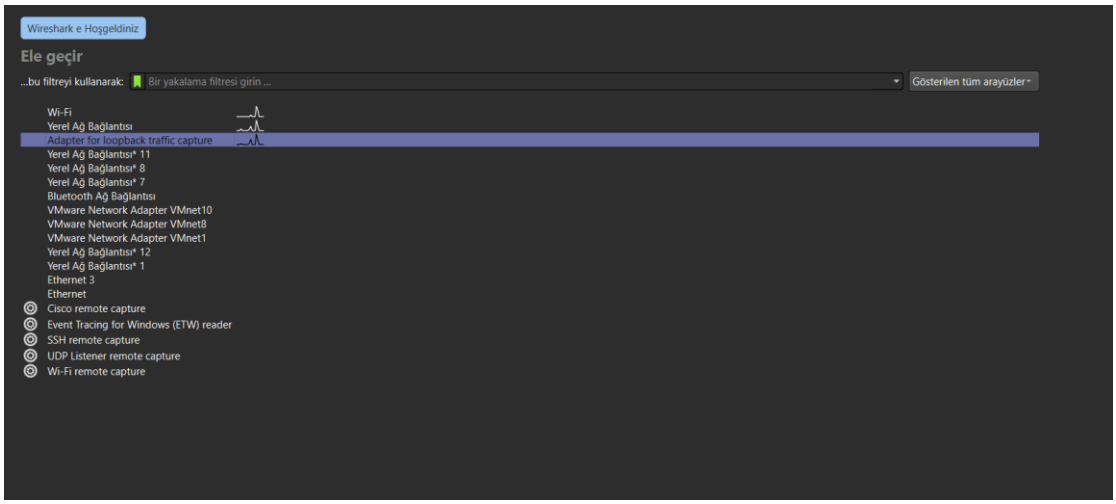
Adım 2:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html Adresinden bilgisayarımıza uygun olan kurulum dosyasını indirelim.

İndirme işlemi sonunda aşağıdaki ekranla karşılaşacağız:

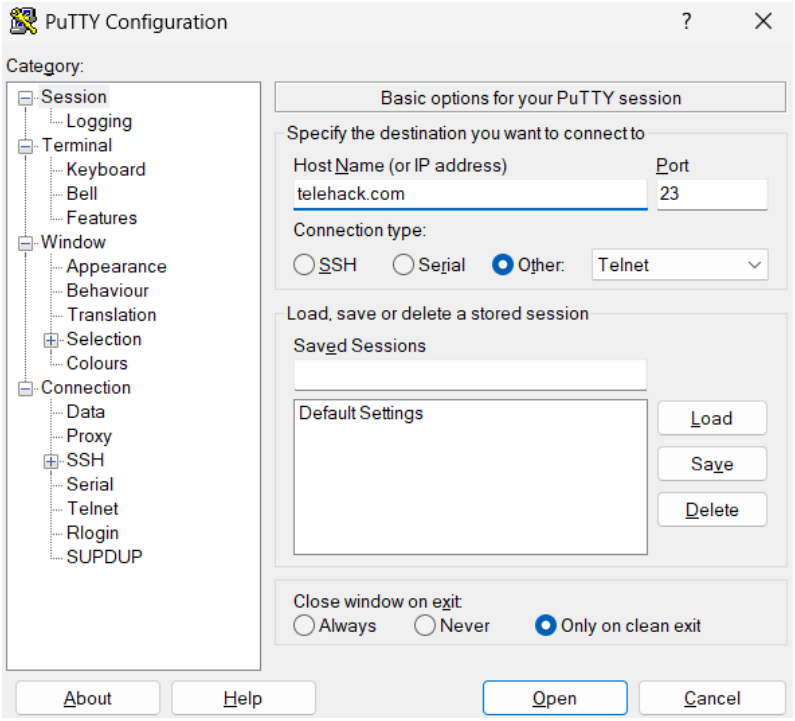
Adım 3:

wireshark'ı açalım ve sniff etmek istediğimiz bağlantıyı seçelim. Ben “yerel ağ bağlantısı”nı seçtim.



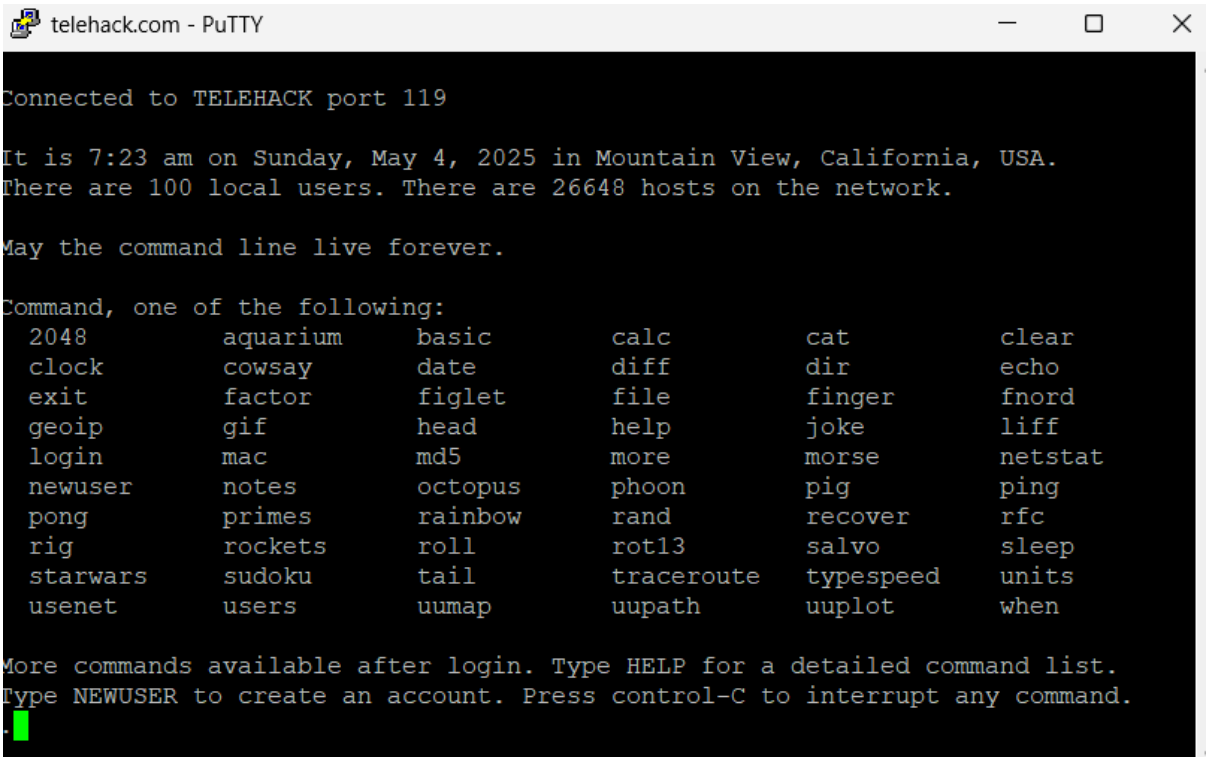
Adım 4:

Putty’i açarak host name kısmına telehack.com yazıp 23 portunu seçip Other diyerek Telnet’i seçelim.



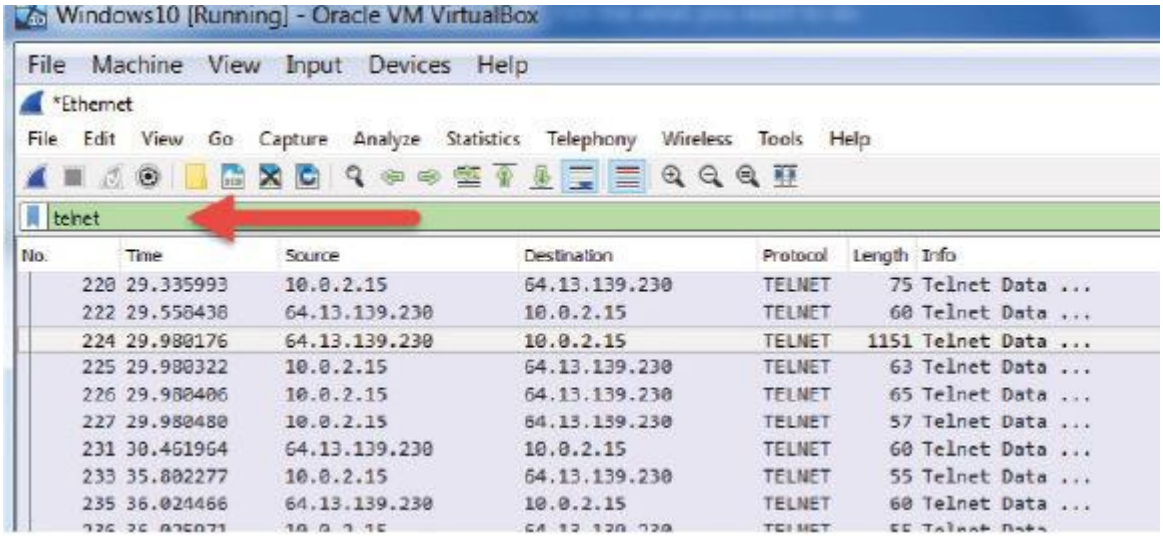
Adım 5:

Open yazısına basalım. Eğer aşağıdaki ekran çıkarsa başarılı olmuşuz demektir.



Adım 6:

Wiresharka geri dönerek filtre kısmına telnet yazalım. Ok işaretine basarak telnet paketlerini filtrelemiş oluruz.



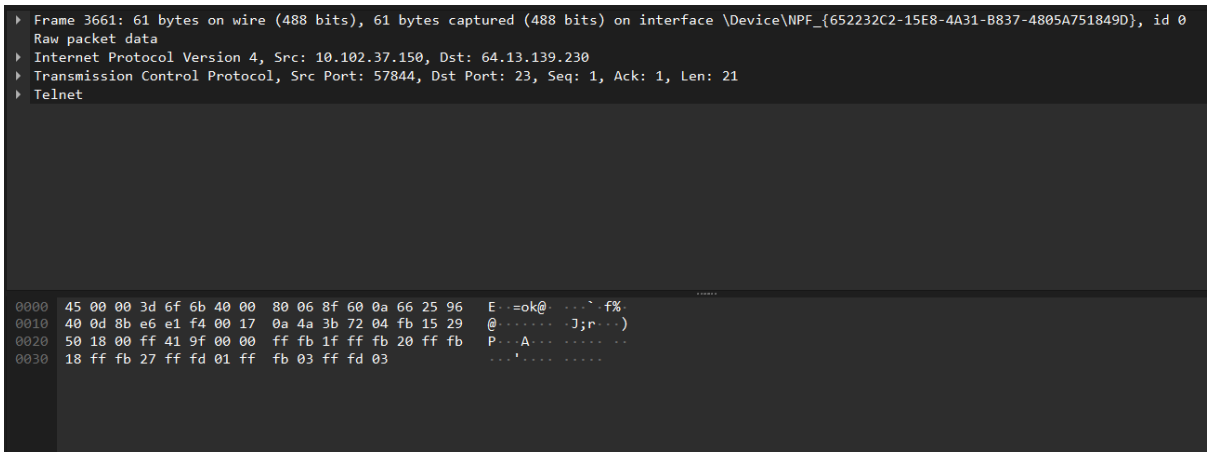
Adım 7:

Paketlerden birine tıklarsanız, daha fazla ayrıntıya inebilirsiniz. Lütfen

Telnet'in kullandığı 'TCP' yazdığına dikkat edin. Alanları aşağıdaki TCP paketinin

görüntüsüyle karşılaştırın. Kaç alanı görebileceğinize bakın.

Kaynak portunun 23 olduğunu görebilirsiniz, ki bu elbette Telnet'tir.



Adım 8:

TCP paket formatı aşağıda görüldüğü gibidir.

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

Adım 9:

Son olarak, Telnet'in oturumun içeriklerini şifrelemediğini unutmayın, böylece veri akışında neyin gönderildiğini kolayca görebilirsiniz. Wireshark'ın alt penceresinde, Telnet üzerinden gönderilen gerçek verileri bulacaksınız.