Telnet - nc Bağlantı Kurma ve Yakalama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu yazıda telnet'in oluşturduğu bağlantı talebini netcat yakalayacaktır ve böylece makinelerin birbirleriyle konuşmalarını kendi makinemizde simule etmiş olacağız.

Makine I	Makine II	
telnet	nc	

> telnet 127.0.0.1 32500	> nc -l 32500	// Not: Önce nc çalıştırılmalıdır.
		// Çünkü telnet bağlandığında
		// nc çalışır halde olmazsa
		// ve sonra çalıştırılırsa bağlantıyı
		// çoktan kaçırmış olacaktır.

telnet ile loopback adresimizin 32500ncü portuna bağlanıyoruz. nc ile de 32500ncü portumuzu dinliyoruz. Böylece telnet bağlantı talebi yolladığında nc bağlantıyı alacaktır ve iletişim başlayacaktır.

Makine I	Makine II
Trying 127.0.0.1... Connected to 127.0.0.1. Escape character is '^]'.	

Bu aşamada Makine I 'den göndereceğimiz veri Makine II ye yansıyacaktır.

Makine I	Makine II
Trying 127.0.0.1... Connected to 127.0.0.1. Escape character is '^]'.	
merhaba	merhaba
deneme	deneme

Dolayısıyıyla Makine I 'den satır satır http header'larını girerek karşı tarafa http talebinde bulunabiliriz.

Not: Paket göndermek görüldüğü üzere elle string girmek ve karşı tarafın string'leri almasından ibaret bir şeydir.

Kaynak: Yaz Tatili 2014 / Tubitak / YTE Eğitimleri / Linux temelleri.docx