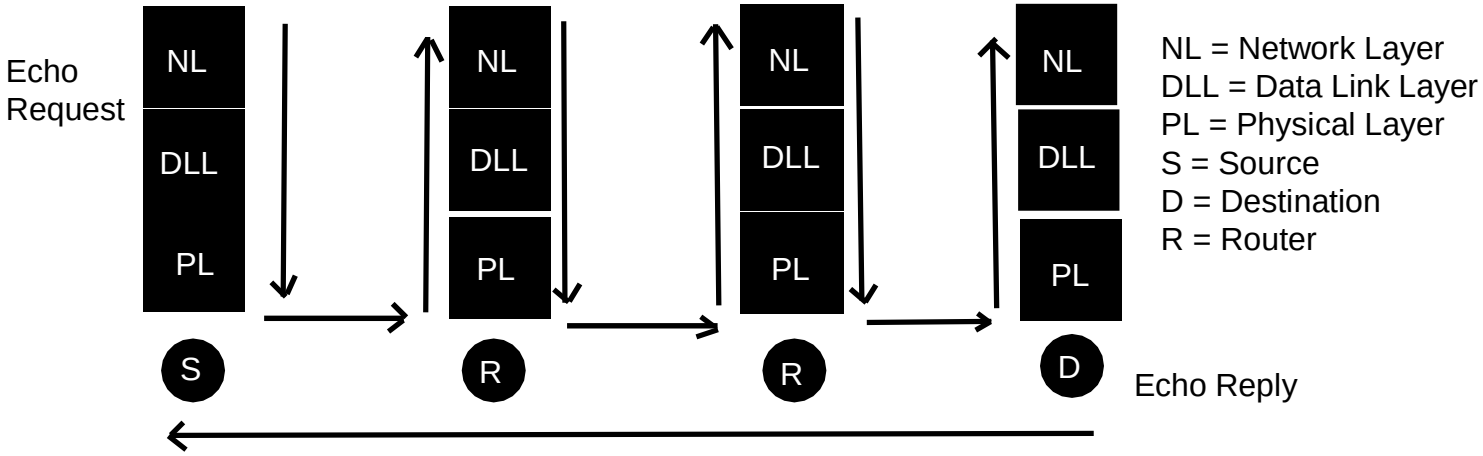
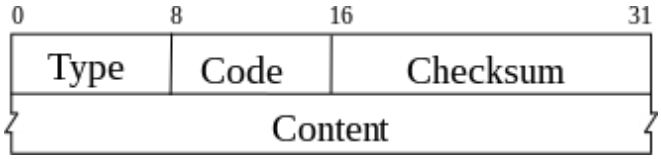
Ping Nedir ve Nasıl Çalışır

Bu yazımda Bilgisiyar dünyasının en eski programlarından birisi olan, ICMP protokolü altında çalışan Ping(packet internet network groper) programını yazıya alacağım. Network veya Siber güvenlik alanında çalışan insanların bunu öğrendikleri zaman ilk sordukları soru neden böyle basit bir programa ihtiyaç var, neden Bu durum IP protokolünden ayrı, IP protokolünde olsaydı daha iyi olmaz mıydı gibi sorular soruyorlar. Bu soruların cevabını daha iyi vakıf olabilmek için OSI katmanlarını ve ICMP protokolüne bakmamız gerekiyor fakat sizlere ufacık kısa bilgi vermek gerekirse, Ping programının çalışma durumunu anlamak için, IP protokolü bir data transferi için kullanılırken, ICMP protokolü aslında yönlendiriciler ve internete bağlı diğer bilgisiyarlar için, özellikle yönlendirme hakkında, ulaşılabilirlik hakkında, bilgi alışverişinde bulunmak için tasarlanmıştır.

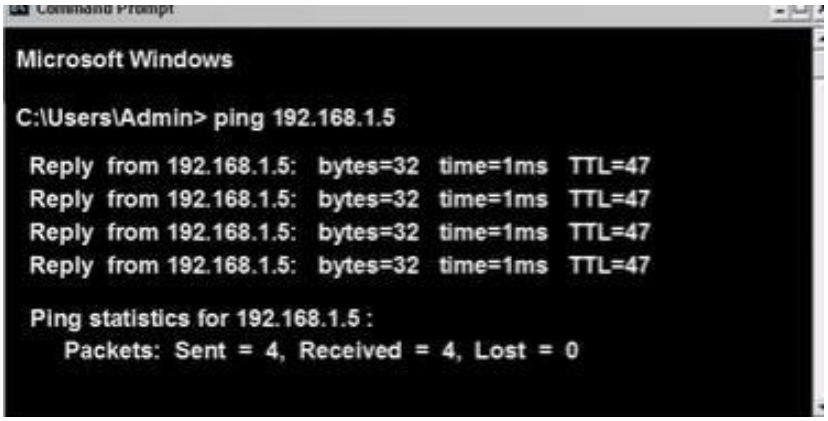
Ping, ağ bağlantısı gibi sorunlarını gidermek için kullanabileceğiniz basit bir araçtır. Yerel alan ağında bağlı olup olmadığınızı, internete bağlı olup olmadığınızı, ağ birimi kartınızı düzgün çalışıp çalışmadığını, ve ayrıca ad çözümleme gibi DNS sorunlarını test etmek içinde kullanılır. veya Siber güvenlik alanında mülakatlarda herkese cevap verdiği şekilde söylemek gerekirse, Karşı taraftaki bilgisiyarın veya Serverın ayakta olup olmadığını sağlayan program. Ping programın çalışma prensibi ilk olarak diyagram üzerinden göstermek gerekirse, aşağıdaki şekile bakabiliriz.



Yukarıdaki diyagrama bakacak olursak. Network Layer katmanında çıkan Echo request paketi, Routerlar üzerinden geçerek Destination IP adresine ulaşıyor ve aynı şekilde Destination IP adresinden, Source IP adresine Echo Reply packeti yollanıyor, bu bizim bildiğimiz ping atmak deyiminin arka tarafta gerçekleştiği durumdur. Tabii ki de bu tanımlar Network dünyasında farklı, Bunun için ICMP protokolün headerlarına bakmamız gerekirse



Echo request olarak göndermek istediğim paket, ICMP protokolünde bulunan headerlardaki code kısmındaki karşılığı 8 olarak ifade edilir. Dönen Echo reply packet'inde ise cevap 0 koduyla ifade edilir. Bu kodların ne anlam ifade ettiğini anlamak için sizi https://www.ibm.com/docs/en/qsip/7.4?topic=applications-icmp-type-code-ids adresini incelemenizi öneriyorum çünkü her zaman doğru bir ping kullanımı gerçekleşmeyebilir. Belkide karşı taraftaki bilgisiyar kapalı veya Local ağımızda bir sorun olabilir. bu sorunların bazılarını terminal üzerinden size göstermeye çalıştım. sizlere ilk önce yukarıdaki gösterdiğim olayın, terminal üzerinde gerçekleşen durumunu göstereceğim. Terminal açıyorum ve şu komutu girip entera basıyorum.



Yukarıdaki resmi, arka tarafta olan durum ile izah etmek gerekirse. Bilgisiyarımız tarafından, karşı taraftaki Bilgisiyar veya Servera default olarak 4 tane veri paketi gönderildi ve karşı taraftanda bize 4 veri paketi geldi. bu bizim yukarıda öğrendiğimiz echo request- echo reply durumunun tam karşılığıdır. ve paket başlıklarına bakacak olursak

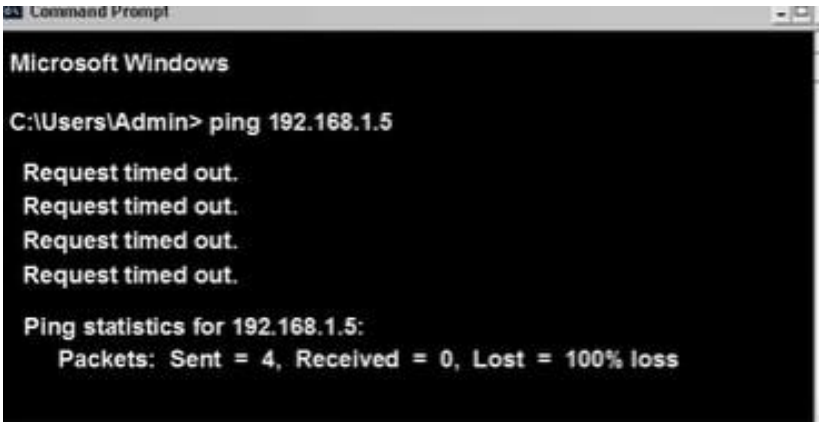
Reply from 192.168.1.5 ----> *Paketin geldiği ip adresini temsil eder*

bytes= 32 -----> *paketin boyutunu temsil eder*

time=1ms------> *Paketini gidip, gelme süresini belirtir.*

TTL= *time to live,paket kaybı olmasın durumunda, network dünyasında trafik yapmasını engeller.(Traceroute konusunda anlatıldı).*

Ancak başka bir örnekte aynı IP adresine ping atarsak

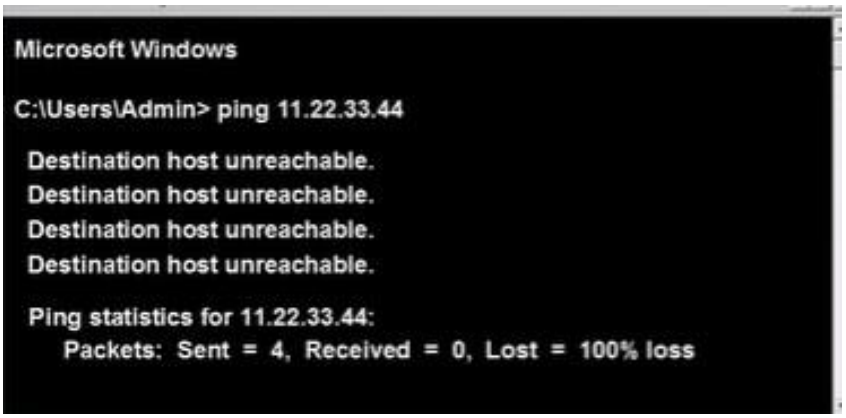


ve bu sefer yukarıda olduğu gibi terminalimizde bir yazı görürsek, bu sunucunun yanıt vermediği anlamına gelir. böyle bir durumda oluşabilecek senaryoları sıralamak gerekirse, karşı taraftaki sunucunun kapalı olduğunu, Firewall tarafından engellendiğini veya ICMP protokolüne cevap vermediğini düşünebilirsiniz.

şimdi bir başka örnek, bir hostname ping atalım.

default olarak gönderdiğimiz 4 veri paketinden sadece hedefe 2 veri paketini ulaştığını görüyoruz, buna paket kaybı denir, ve birkaç nedenden dolayı paket kayıpları meydana gelebilir. Ağ tıkanıklığı olduğu anlamına gelebilir, Bir ağda çok fazla trafik varsa ve bu trafiği kaldıramıyorsa, veri paketleri düşecektir. Bozuk kablolar, kötü kablolama, kötü bir ağ kartı ya da kötü bir modem gibi nedenlerden kaynaklanıyor olabilir.

Başka bir senaryoda aynı hostname ping atarsanız



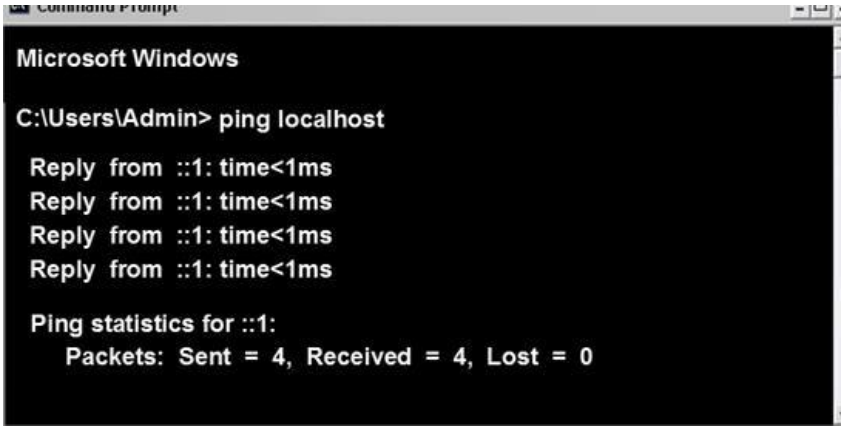
ve terminalinizde böyle komut görürseniz, bu hedefe giden yolun bulunamadığı anlamına gelir. Bunun olmasının nedenleri, bir yönlendiricinin verileri hedefe nasıl yönlendiriceğine dair herhangi bir bilgisi olmadığı, uzak sunucunun kapalı olduğu veya bilgisiyarınızı bir ağa bağlı olmadığı anlamına gelebilir.

Öyleyse herkesin başına gelmiş bir senaryo düşünelim. birinin bana bilgisiyarlarıyla herhangi bir web sayfasına erişemediğ için internet bağlantısı olmadığını söylediğini varsayalım ki bu oldukça yaygın bir sorundur.

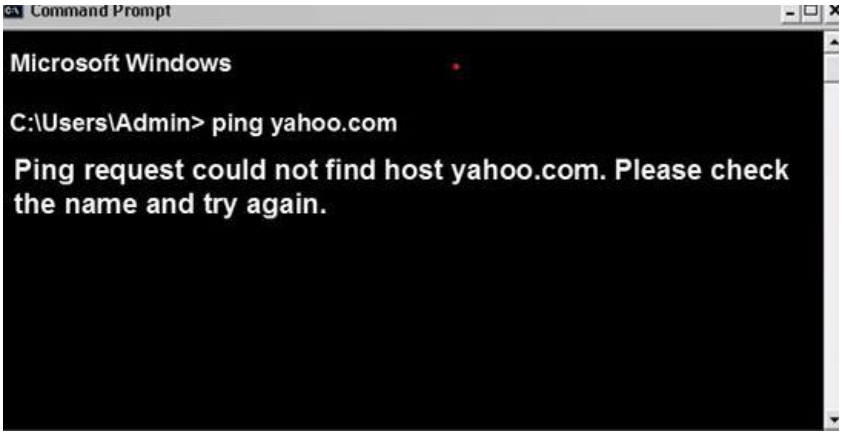
Yaptığım ilk şey, bilgisiyarın başına oturup, Ping yardımcı programını kullanarak internete bağlı olup olmadığımı görmek olacaktır. Komut istemi açar

herhangi bir web sitesi alan adına ping atardım, bu örnek yahoo.com alan adını kullandım. bunu böyle yapmamanı nedeni, DNS ile ilgili alan ad çözümleme sorunlarını test ediyor oluşum ve ayrıca yahoo.com Ip adresi bilmememde bu etkenlerin arasında diyebilirim. Yahoo.com adresinden başarılı bir yanıt aldığımda. İnternet servis sağlayacısı dahil olmak üzere, kabloları, ağ kartı,yönlendirici, modem gibi tüm donanımların doğru bir şekilde çalıştığını anlarım. Artık sorunun, donanım tarafında değilde yazılım tarafında olduğunu teyit ettim. İnternet tarayıcılarında veya bir güvenlik duvarı sorunu olabilir.

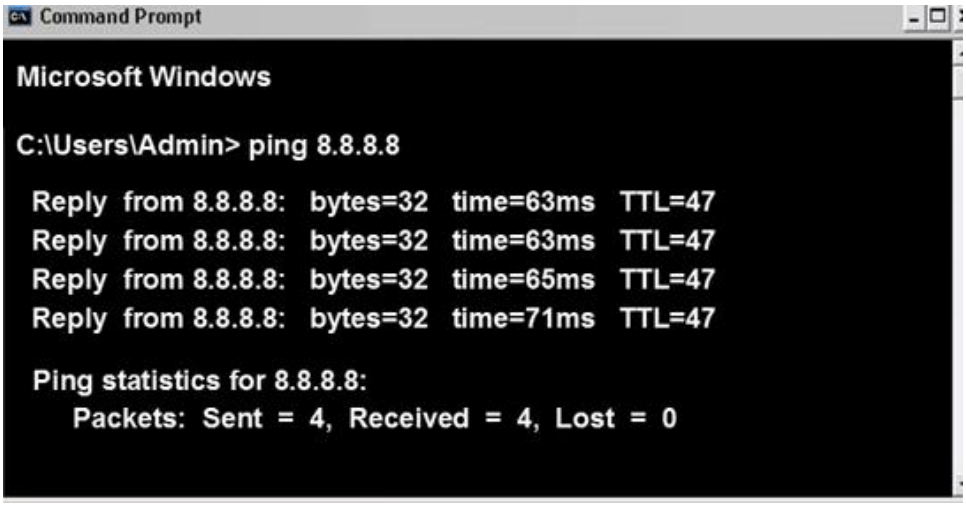
Bununla birlikte bazen internet bağlantısından ziyade Ağ kartı veya donanım cihazlarınızı test etmek isteyebilirsiniz. bunun için terminale gelip aşağıdaki komutu yazarsam



ve buradaki durumu izah etmek gerekirse, kendi local adresimize ping atma durumudur. Buna loopback(geri döngü) testi adı verilir. Loopback testi, test amacıyla bilgisiyarınıza sinyaller gönderme işlemidir. ayrıca aynı şekilde ping localhost yerine ping 127.0.0.1 adresinide yazabilirsiniz. Ping programı, DNS sorunlarını test etmek içinde kullanılabilir, eğer DNS'in nasıl çalıştığına aşina değilseniz,web sitemden buna ulaşabilirsiniz. kısaca DNS'i anlatmak gerekirse, Alan adlarını, IP adreslerine dönüştürme işlemi gerçekleştirir. Daha önce gördüğümüz gibi, IP adresi yerine "yahoo.com" alan adını ping atarak, ping testi yaptım. Ping başarılı olması durumu, tüm donanım cihazlarının sorunsuz bir şekilde çalıştığı teyit ettim. Ancak bazı durumlarda DNS, sağlıklı bir şekilde çalışmadığı durumlar söz konusu olabiliyor. Terminali açıp



yahoo.com adresine ping atmak istediğiniz zaman, böyle bir hata alıyorsanız. Bu DNS'in IP adresine erişemediği anlamına geliyor. Böyle bir durumda daha sağlıklı bir şekilde teyit edilmesi için Bir IP adresine ping atmayı denyebilirsinz. komut satırına gelip



Hatırlanması kolay olan, Google'ın 8.8.8.8 DNS sunucusuna ping atarak, sorunun DNS'den kaynaklandığına artık daha vakıfsınız. Dns sorunlarını çözmek için bir kaç yöntem deneyebilirsiniz. Komut satırını açıp "ipconfig /flushdns" yazarak önbelleğini temizleyebilirsiniz. Veya ağ kartı yapılandırmanızıdaki DNS ayarlarınızı kontrol etmek isteyebilirsiniz.

Bu yazımda size Ping programının, kısada olsa arka tarafta nasıl çalıştığını ve terminalde olan durumlarını anlatmaya çalıştım.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/