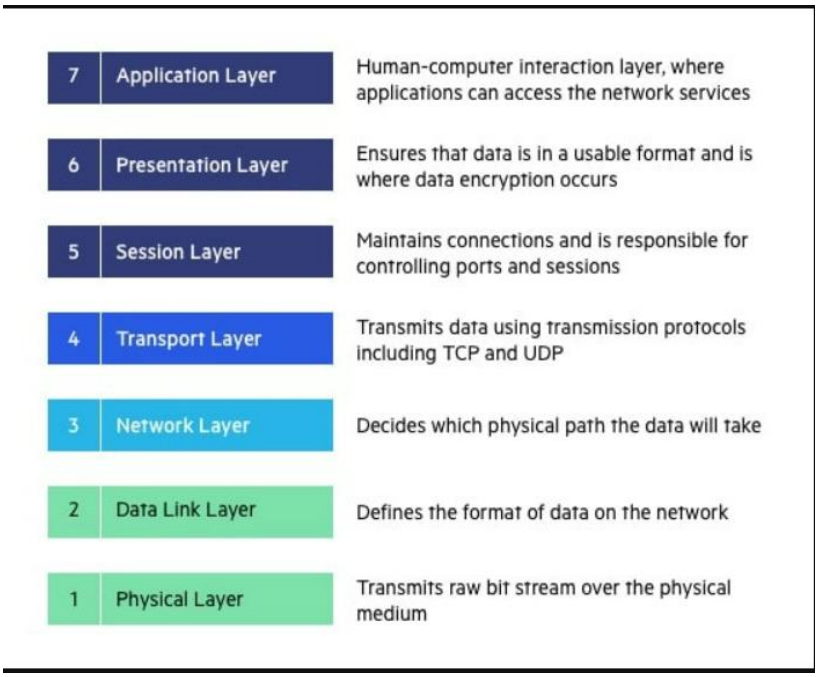
Networking Task

Task1:

OSI Model Nedir ve Nasıl İhtiyaç Duyulmuştur?

Önceden ağlar bilgisayar donanımı üreten kuruluşlara özgüydü. Bu olayda sadece kendi donanımlarına bağlanmasına izin vericek şekilde ayarlanmıştı. Şirketler ise maliyeti düşürmek ve haberleşmeyi arttırmak için ağlarını birleştirme ihtiyacı duyuyorlardı fakat bu şekilde çok mümkün olmuyordu. 1983'lerin başında ISO (International Organization for Standardizition) OSI (Open System Interconnection) modelini geliştirdi. Bu model herhangi donanıma göre değişiklik göstermiyordu. Belirli kalıplar çerçevesinde şekillenen kurallarlardan oluşuyordu. Üreticilerde buna göre kendi yazılım ve donanımlarını OSI standartlarına göre ayarlamaya başlattılar. OSI genel olarak ağ kullanıcılarının nasıl haberleşeceğine dair kurallardır. Ağ bileşenlerinin nasıl haberleştiklerini ve gönderilen bilginin hedefte nasıl görüntüleneceğini gibi bilgileri tanımlar. Farklı donanımların nasıl etkileşime gireceğini tanımlar. OSI modeli her bir katmanın bir üst katmana hizmet vermesi amacına dayanan ve birbirleriyle iletişimi ilişkili olan yedi farklı katmandan oluşan bir modeldir.



OSI katmanları

En üstten başlayarak açıklayacağım

7) Application Layer (Uygulama katmanı):

Uygulama katmanı son kullanıcı yani insanların bilgisayarla etkileşime girdiği yerdir. Bu web browser email sunucuları olabilir. Bu katmanda gelen veya gönderilen datalar anlamlı şekilde kullanıcıya gösterilir. HTTP, SMTP, FTP ,DNS bu katmanın protokollerindendir.

6)Presentition Layer(Sunu Katmanı)

Bu katmanın en önemli görevi gönderilen bilginin bilgisayarın anlayacağı hale çevirilimesidir. Bu vesileyle farklı programlar birbirlerinin verisini kullanabilir hale gelir. Sunum katmanı uygulama katmanına verileri yollar daha sonra bu katmanda verinin yapısı biçimi ile ilgili düzenlemeler yapılır verinin formatı belirlenir. Ayrıca verinin şifrelenmesi, açılması, sıkıştırılması da bu katmanda yapılır.
GIF, JPEG, TIFF, EBCDIC, ASCII bu katmanda çalışır.

5)Session Layer(Oturum Katmanı)

Oturum katmanında iki bilgisayardaki uygulama arasındaki bağlantının yapılması, kullanılması ve bitilmesi işlemleri yapılır. Bir bilgisayar birden fazla bilgisayarlarla aynı anda iletişim içinde olduğunda, gerektiğinde doğru bilgisayarla konuşabilmesini sağlar. Named Pipes ve Sockets gibi protokoller bu katmanda çalışır.

4)Transport Layer(Taşıma Katmanı)

Bu katmanda üst katmanlardan gelen veriler ağ paketlerine böler. TCP, UDP protokolleri bu katmanda çalışır. Bu protokoller hata kontrolü gibi görevleri de yerine getirir. Veriler segment halinde taşınır. Eğer paketler istenilen şekilde ulaşmazsa tekrar request yapar.

3)Network Layer(Ağ Katmanı)

Ağ katmanı veri paketlerinin farklı bir ağa gönderileceği zaman gerekli yönlendiricilerin kullanım bilgisinin eklendiği katmandır. Bu katmanda veriler paket olarak taşınır. Ağ katmanında en ekonomik yoldan verinin iletimi sağlanmaya çalışılır. Routerlar aracılığıyla veri yönlendirilir. IP protokolü bu katmanda çalışır.

2)Data Link Katmanı

Bu katman fiziksel katmana ulaşmak ve kullanmak ile ilgili kuralları belirler. Bu katmanda Ethernet veya Token Ring olarak bilinen erişim yöntemleri çalışır. Burdan veriler fiziksel katmana gönderilir. Bu aşamada veriler belli parçalara bölünür. Bu bölünmüş parçalara kendi headırını ekler ve frame ismini alır. Buradaki işlemlerin büyük bölümü ağ kartı içinde gerçekleşir. Veri bağlantı katmanı ağ üzerindeki diğer bilgisayarları tanımlama kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir. MAC adresleri burada verilere eklenir ve fiziksel katmana gönderilir. Aynı şekilde karşı makinede decapsulation yaparken bunları kullanır. Burdan da LLC ‘ye taşınır (Logical

Link Control) burada protokole özel portlar oluşturulur. Böylece source ve destination aynı portlardan iletişime geçebilir. LLC ayrıca flow controlüde gerçekleştirir.

1) Physical Layer (Fiziksel Katman)

   Bu katmanda verinin kablo üzerinde iletimi için veriyi hazırlar. Veriler bit olarak iletilir. Verilerin nasıl ışık radyo ve elektrik sinyaline çevrileceğini ve aktarılacağını tanımlar. Hublar bu katmanda çalışır.

Ne Tür Saldırılar Yapılabilir?

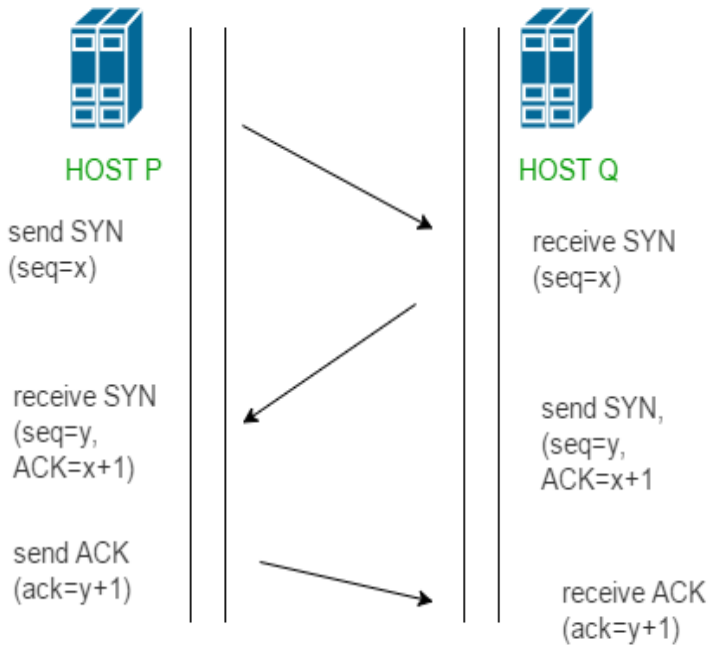
Katmanlara göre farklı saldırı vektörleri vardır. Genelde çoğu saldırı application layerde gerçekleşir çünkü kullanıcı burada ağ ile etkileşime girer. Örnek vericek olursak SQL injection, XSS, phisihng gibi ataklar burada gerçekleşir. Kullanıcı arayüzü olduğu için kullanıcı manipüle edilmeye çalışılır. Input alanlarında Javascript veya SQL dilinin bazı özel karakterleri encoding edilmediyse burada zafiyetler ortaya çıkabilir. Ayrıca DNS çalışma prensibiyle alakalı local DNS sunucusunun cache'nde saklanan IP adreslerine sızılarak DNS Poisoning saldırısı gerçekleşebilir. Presentation layer da da bunların yanı sıra Ddos saldırıları olabilir. Session Layer de Man in the middle attack yapılabilir. Session layerde bilgisayarların portlar vb gibi alanlarla birbirine bağladığından MAN IN THE MİDDLE Attackla kullanıcıların birbiriyle konuşurken araya girilip mesajları decoding edilip okunabilir. Bu katmanda ayrıca Cookie exploitleri oluşabilir. Kullanıcının kullandığı cookiler çalınıp authentication zaafiyeti oluşabilir. Transport Layer'da ise SYN flood , TCP session attack gibi ataklar yer alabilir. Burada SYN flood bir çeşit Ddos saldırı çeşididir. Buradaki amaç Server kaynaklarını kullanarak Serverın kullanımını engellemek burada hep başlangıç olarak gönderilen SYN paketi gönderiliyor. Ardından server SYN/ACK 3lü sıkışma kuralına göre gönderiyor fakat hacker ip spoofing yapıp onun cliente ulaşmasını engelliyor server da orada onaylanmadığı için SYN/ACK paketlerini gödermeye devam ediyor. Bütün uygun portlara gönderilen bu paketler en sonunda yoğun bir trafik oluşturuyor. Session attack da bu Application layer da daha fazla kullanılmakla birlikte Transport katmanında da TCP üzerinde kullanılıyor. Network Layerda ise IP spoofing, ICMP attack, packet sniffing gibi saldırlılar gerçekleştirilebilir. Burda IP spoofing hackerın kendini gizlemesi için kullanılır. Gelen istekler kullanıcıdan geliyomuş gibi servera yollanır oysaki Hacker kullanıcının adresini kullandığı için işlemleri belli olmaz. Tüm IP paketleri paketin gövdesinden önce gelen ve kaynak adresi de dahil olmak üzere önemli yönlendirme bilgilerini içeren bir başlık içerir. Normal bir pakette kaynak IP adresi paketi gönderenin adresidir. Paket sahteyse kaynak adres sahte olacaktır. ICMP de DDOS attack türüdür. Burada kullanıcıya pingler yollanarak serverın trafiği arttırılır.

Task 2:

TCP/IP nedir?

TCP/IP TCP (Transmission Control Protocol) ve IP (Internet Protocol) protokollerinin birleştirilmesiyle oluşturulan verilerin aktarılmadan önce nasıl paketleneceğini, bu paketlerin nasıl taşınacağını, nasıl adresleneceği ve hedef tarafından nasıl çözümlenerek alınacağını kontrol eden veri iletim protokolüdür. TCP ve IP iki ayrı internet protokolüdür. Veri gönderimi sırasında bir kaynak üzerinden bir hedefe gönderilen paketlerin yönlendirilmesinden IP sorumludur. IP söz konusu olduğunda gönderilen verinin içeriği önemli değildir. IP verinin gönderileceği adresin belirlenmesini sağlar. Aynı şekilde gönderilen verinin alıcı tarafından kabul edilip edilmeyeceğini doğrulamak IP'nin görevleri arasında yer almaz. Bu doğrulama işlemi bir üst katman olan TCP'nin görevidir. TCP verinin karşıya iletilmesinden sorumludur. Sistem bir mesaj yolladığında tamamını birden gönderseydi ve yolda bir sıkıntı yaşansaydı, bu durumda mesajın yeniden gönderilmesi gerekirdi. TCP/IP ile ise her mesaj paketlere ayrılır. Yollanan paket grupları, hedef uçta yeniden bir araya gelir. Ayrıca, TCP/IP iletişim görevlerini farklı katmanlara böler. Her katmanın farklı bir görevi bulunur. Veriler, alınmadan önce dört ayrı katmana uğrar. Daha sonra TCP/IP, verileri yeniden bir araya getirmek için bu katmanlardan ters sırayla geçer. Bir ağa bağlı cihazlar arasında iletilen veriler, bu katmanlardan geçerek kaynaktan hedefe ulaşır.

THREEWAY HANDSHAKE 3'LÜ EL SIKIŞMA



Üçlü el sıkışma öncelikle güvenliği sağlar yani karşı tarafa paket gidip gitmediğini karşı tarafın gönderdiği mesaj sonucunda anlayıp ona göre veriyi göndermeye başlar yukarıda gördüğümüz şekilde Host P SYN ile bir segment gönderir ve sunucuyu istemcinin iletişime başlaması gerektiği ve sıra numarasının ne olması gerektiği konusunda bilgilendirir. Sonrasında Host Q SYN-ACK sinyali seti ile müşteri isteğine yanıt verir. ACK, alınan segmentin yanıtını belirtmenize yardımcı olur ve SYN segmentlerle başlayabilmesi gereken sıra numarasını belirtir.En sonda ise hostlar yanıtını kabul eder ve ikisi de kararlı bir bağlantı oluşturur ve gerçek veri aktarım sürecini başlatır.

UDP nedir?

UDP(User Datagram Protocol) TCP/IP protokol takımının iki aktarım katmanı protokolünden bir tanesidir. UDP genellikle kayıp toleransı yüksek olan video, resim tarzı dosyaların gönderilmesinde kullanılır. Buradaki bağlantı connectionless dir. Yani TCP deki gibi verinin ulaşıp ulaşmadığı kontrol edilmez. UDP de mesaj takibi bağlantı sıralaması gibi durumlar bulunmza sadece ana hedef göndermektir karşı tarafın alıp alamaması da problem değildir. TCP de kaybolan paketler yeniden gönderilirken UDP de öyle bir sorumluluk yoktur. İkiside hata kontolü yapar fakat UDP'de bu işlem çok ayrıntılı değildir en son temel bir checksum yapar. UDP broadcasti destekler fakat TCP'de bu gerçekleşmez.

TCP FLAGLARI

SYN	Bağlantıyı kurmak için gönderilen ilk pakettir.Sıra numarasını senkronize etmek için kullanılır
ACK	Bağlantının başarılı bir şekilde gerçekleştiğini söylemek için kullanılır. Eğer acknowledgement alanı geçerli bir numaraysa set edilir. SYN no bir artırılarak karşı tarafa gönderlilir.
FIN	Eğer gönderilecek başka paket yoksa bağlantının durdurulması için kullanılır.
RST	TCP bağlantısında herhangi bir sorun çıktığında veya istenilen paket gelmediğinde gönderilir.

SYN SCAN Nedir?

SYN scan, portların açık olup olmadığını kontrol etmek için kullanılan bir metottur. Yukarıda da bahsettiğim zaafiyette olduğu gibi tam bağlantı kurmadan hangi portların açık olduğunu anlamak için kullanılır. TCP/IP bağlantısında olduğu gibi üçlü el sıkışma ypar gibi burada önce SYN paketleri portlara gönderilir. Sunucu herhangi bir porttan ACK veya SYN/ACK yanıtı verirse o portun açık olduğu anlaşılır. Ardından hacker RST sıfırlama isteği gönderir. Eğer sunucu RST paketi yollarsa o portun kapalı olduğu ortaya çıkar.

ACK SCAN Nedir ?

Ana bilgisayarın herhangi bir filtreleme yöntemi tarafında korunup korunmadığıno anlamak için yapılır. Bu yöntemde rastgele sıra numarasına sahip ACK paketi gönderir. Yanıt olmazsa portun filtrelendiği anlamına gelir. Eğer RST yanıtı gelirse portun kapalı olduğu anlamına gelir.

FIN SCAN Nedir ?

Fın scan fın flagı portlara gönderilerek yapılır. Sunucuda bağlantı olmadğı için hangi bağlantıyı sonlandıracağını bilmez ve cevap vermezse o portun açık olduğu anlamına gelir. RST cevabı döndürürse port kapalıdır.

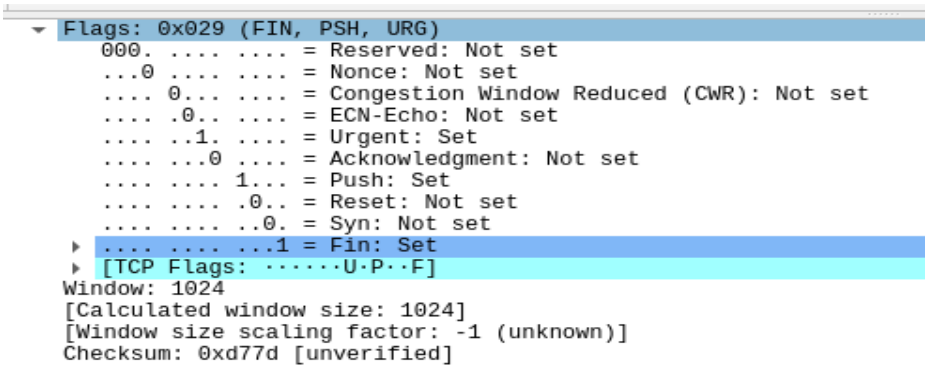
RST SCAN nedir ?

Burada bağlantı noktası kapalı ancak karşıda aktif bir bilgisayar olduğu öğrenilir.

Xmas nedir ?

Xmas flagları kullanarak TCP üzerinden yapılan bir saldırı türüdür.

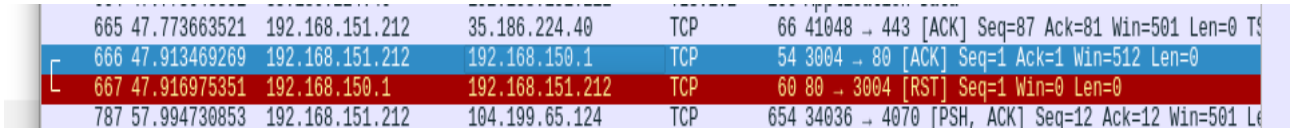
Önceden hazırlanmış FIN, Push ve urgent flagları aktif edilip yollanır. Normalde bu flagların aynı anda olması mümkün değildir. Bu paketlerin cevabıı farklı işletim sistemlerinde farklı tepki gösterir. Nmap -sX ile denedik aşağıda görüldüğü üzere bahsettiğimiz flaglar set edildi. Bu şekilden dolayı christimas tree attack da deniyor.

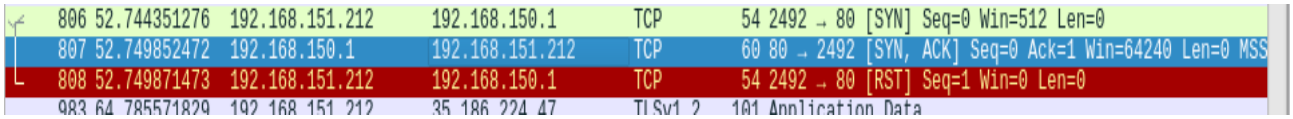


Oluşturulan paket bütün portlara yollanır. Portlar açıksa paketler yok sayılır. Portlar kapalıysa RST geri yollanır.

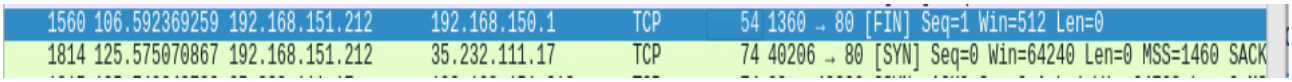
HPİNG ile modem cevapları incelenmesi

Hping üzerinden bahsedilen 80,443,8888 portlarına SYN ACK FIN ve RST flaglarını aktig edip yolladım. 80 portunda SYN ACK için RST flagı döndürdü bunun anlamıda o portun kapalı olduğu anlamına gelir. FIN ve RST yolladığımda TCP üzerinden cevap alamadım

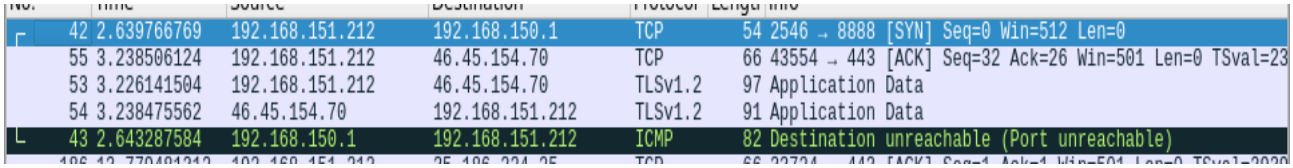




Yukarudaki resimde görüldüğü üzere SYN isteği attığımda SYN ACK cevabını vermiş ardından benim ıp adresinden RST flagı ile bir paket yollanmış.



Yukarıda FIN flagını set edip attığım istek gözüküyor fakat cevap gelmedi. Cevap gelmediği için o portun kapalı olduğunu anlıyoruz eğer RST döndürseydi FIN scanda port açık anlamına gelirdi.



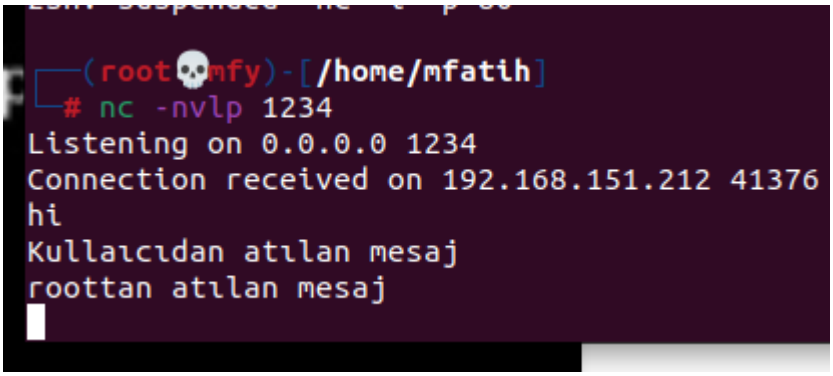
Yukarıdaki resimde 8888 portuna SYN flagını set edip attığımda ICMP protokoluyle portun ulaşılamayacağı anlamını içeren mesaj gönderdi. Aynısı ACK içinde oldu.

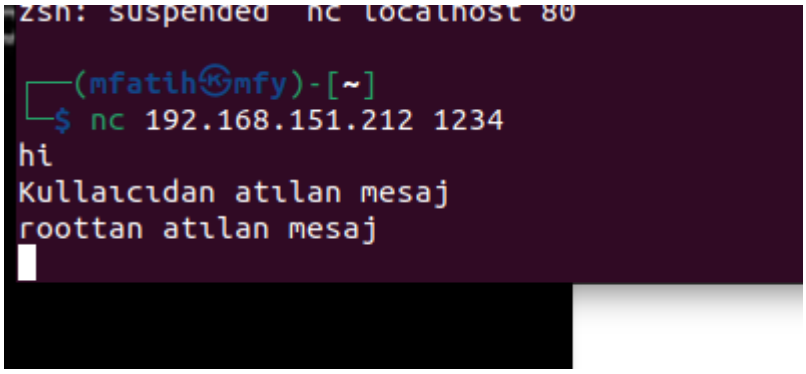
443 portunda da aynı şekilde SYN ve ACK flaglarında SYN için SYN-ACK mesajı döndü fakat source tarafından RST dönüp kapandı. ACK de destination RST yolladı portun kapalı olduğunu öğrendik.

NETCAT nedir?

Portlarda olan TCP UDP protokollerini kullanarak gerçekleşen verileri okuma ve yazma işlemlerini taramak için kullanılır. Netcat'in komut halini "nc" olarak kullanıyoruz. Bu komutun temel amacı networkler arasındaki veri okuma / yazma işlemlerine dair işlemlerdir.

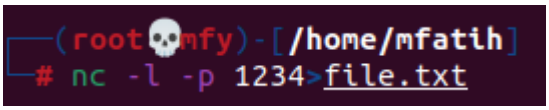
80 portunu dinlediğimde önceden bağlıdığım zaman port açık olduğu için Wireshark'ta SYN yollanıyor ayriyeten dönen SYN-ACK flagıyla ACK döndürüp kurulum tamamlanıyor.

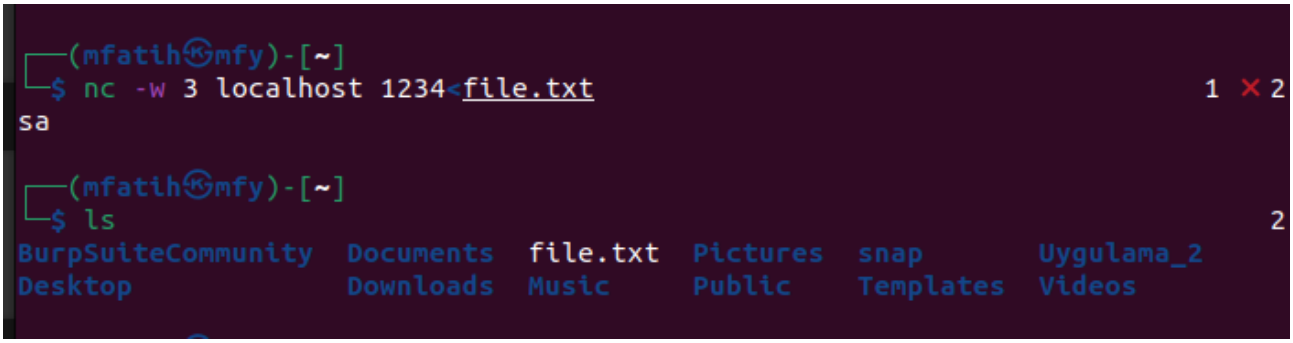




Yukarıda -n DNS'te resolve edilmemesi için numeric IP adresi kullanılıcak anlamına gelir. -v verbose ayrıntılı bilgi verilir. -l ile birlikte port dinlenmeye başlanır. -p kaynak bağlantı noktasını belirtmek için kullanılır.

Netcat ile dosya transferi





Yukarıda görüldüğü üzere roottan normal kullanıcıya dosya gönderimini sağladık. > gonderici bu işaret ile göndermek istediği dsyayı belirtiyor. Alıcı ise -w ile timeout süresi ayarlıyor 3 sniye ardından port numarasını girip < küçüktür işaretiyle dosyayı indirir.

REVERSE SHELL ve BİND SHELL Nedir ?

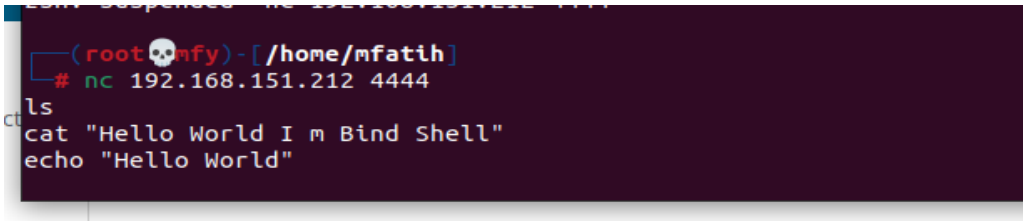
Bind Shell

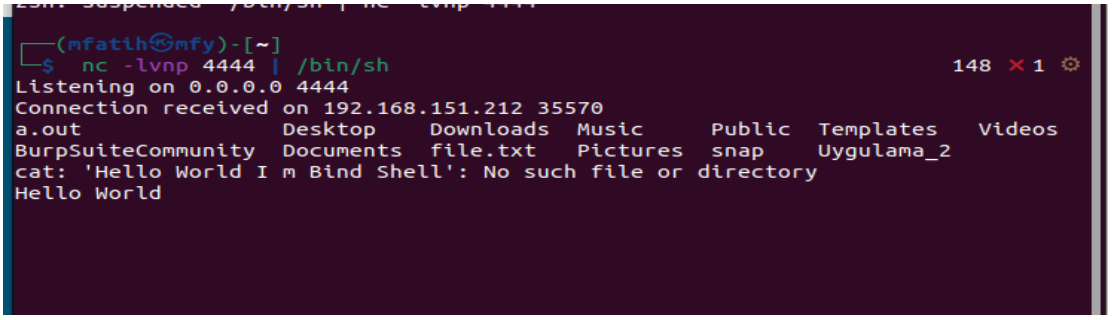
Hedef makinede açık olan bir porttan(bu son kullanıcının çalıştırmış olduğu zararlı bir uygulamaya bağlı olarak da olabilir) dinleyici açılarak kullanıcının shelline erişilen bir kabuk türüdür. Bu sayede saldırgan port üzerinden istediği shell işlemlerini gerçekleşitrebilir.

Reverse Shell

Hedef makinede çalıştırıldığında saldırganın bilgisayarının portlarına hedef makinenin bağlanmasıyla elde edilir. Bind shellin zıttı gibidir. Saldırgan bu sayede hedef bilgisayarda komut çalıştırma hakkına sahip olur.

Bind shell örneği





Yukarıdaki görsellerde saldırı gerçekleştirdiğimiz bilgisayardaki açık olan portu saldırganın kendisinin dinlemesini sağlıyoruz ardından o porta bağlanıp istediğimiz komutları saldırgan pcden gerçekleştirebiliyoruz

REVERSE SHELL ÖRNEĞİ

Aşağıdaki resimlerde de tam tersi clear yazdığım için gözükmüyor ama saldırgan bilgisayardan açık olan portu dinliyoruz ardından hedef bilgisayar o porta bağlanıp scrpiti çalıştırdığında reverse shell le erişim sağlayabiliyoruz.