

WIRESHARK İLE NETWORK ANALİZ

YUNUS BÖLÜKBAŞ

İÇİNDEKİLER

BÖLÜM 1: SANAL NETWORK LABORATUVARLARINA GENEL BAKIŞ	1
CISCO Packet Tracer Yazılımına Bakış	7
Graphical Network Simulator (GNS) Yazılımına Bakış	9
eNSP Yazılımına Bakış	10
Neler Öğrendik?	11
BÖLÜM 2: GNS3 İLE SANAL AĞ ORTAMININ KURULMASI	13
GNS3 ile Sanal Laboratuvar Kurulumu	15
Minimum Sistem Gereksinimleri	15
Windows İşletim Sisteminde GNS Kurulumu	16
Mac OS X İşletim Sisteminde GNS Kurulumu	18
GNS'de IOS Yükleme Süreci	18
CISCO Switch/Router Temel Ayarlar	25
Cihazın (Switch/Router) Portlarına IP Ataması	26
VLAN Nedir ve Nasıl Oluşturulur?	26
Telnet Yapılandırması	28
DHCP Servisinin Yapılandırılması	29
Switch Mac Adres Tablosunun İncelenmesi	30
Neler Öğrendik?	30
BÖLÜM 3: İŞLETİM SİSTEMİ SANALLAŞTIRMA YAZILIMINA BAKIŞ	33
Microsoft Hyper-V Kurulumu	36
Yeni Bir Sanal Makine Oluşturma Süreci	38
VMware Workstation – Yeni Sanal Makine Oluşturma	47
Neler Öğrendik?	52

BÖLÜM 4: TEMEL NETWORK BİLGİSİ	53
Temel Network Bilgisi	54
OSI Katmanının Ortaya Çıkış Süreci	56
OSI Katmanlarına Bakış	56
Network Topolojileri	58
Bus Topoloji	58
Star Topoloji	59
Ring Topoloji	59
Temel Network Cihazları	59
REPEATER	59
HUB	60
Switch	61
Router	61
Firewall (Güvenlik Duvarı)	62
Yayın Türleri	62
Unicast (Tek Yöne Yayın)	62
Broadcast (Yayın Adresi)	63
Multicast (Çok Yöne Yayın)	63
IP Adresleri	64
IP (Internet Protocol) Sınıfları	64
A Sınıfı IP Adresleri	64
B Sınıfı IP Adresleri	64
C Sınıfı IP Adresleri	64
D Sınıfı IP Adresleri	65
E Sınıfı IP Adresleri	65
İlk okteti 240 – 254 arasında olan IP adresleridir.	65
Private (Özel) IP Adresleri	65
Neler Öğrendik?	65

BÖLÜM 5: PAKET ANALİZİ NEDİR? WIRESHARK PROGRAMININ GENEL ÖZELLİKLERİ 67

Paket Analizi Nedir?	68
Paket Analiz Yazılımı Seçim Süreci	69
WireShark Programının Kurulumu	70
WinPCAP Paket Yakalama Kütüphanesi	70
Merhaba Wireshark	73
İlk Paketimizi Yakalayalım	74
Wireshark Özelleştirme Seçenekleri	81
Paketlerin İşaretlenmesi	84
Yakalanan Paketler İçinden Arama Yapma	85
Yakalanan Paketlerin Kaydedilmesi	85
Yakalanan Paketlerin Dışa Aktarılması (Exporting)	87
Yakalanan Paketlere Ait Zaman Bilgisi	87
WireShark Paket Filtreleme İfadeleri	88
Kıyaslama Operatörlerinin Kullanımı	90
Mantıksal Operatörlerin Kullanımı	91
Protokol Analizine Merhaba	92
TCP 3 WAY Handshake	92
FTP Protokolü	95
DNS Protokolü	97
HTTP Protokolü	98
ARP Protokolü	99
DHCP Protokolü	100
DHCP Discover	101
Telnet Protokolü	103
CDP Protokolü	107
SSH Protokolü	108
ICMP Protokolü	109
STP Protokolü	112
Neler Öğrendik?	113

BÖLÜM 6: WIRESHARK GELİŞMİŞ ÖZELLİKLER	115
GeolP Veri Tabanı ile Konum Tespit	116
Protokol İstatistikleri	120
Endpoint (Uç Nokta) Bilgileri	121
Summary (Özet) Bilgisi	123
Conversation (Konuşma) Penceresi	124
IO Grafikleri	125
Neler Öğrendik?	126
BÖLÜM 7: ÖRNEK OLAYLAR	129
TCP Port Tarama Tespiti	130
FTP Login Saldırısı	133
ARP Taraması	137
Hedef Bilgisayara Ait İşletim Sistemi Tespit	138
GET Metodu Üzerinden Gelen Veriler	141
SYN Flood Atağının Tespiti	142
SQL Injection Saldırısının Tespiti	148
MSN Messenger Hizmetindeki Mesajların Takibi	151
MAC Flooding Tespiti	153
Multicast Yayınların İncelenmesi	157
UPD Protokolü Üzerinden Gelen Verilerin Doğruluğunun Kontrol Edilmesi	165
Resim Dosyalarını Yakalama ve Dışarı Aktarma	169
Neler Öğrendik?	171
SON SÖZ	171

1

SANAL NETWORK LABORATUVARLARINA GENEL BAKIŞ

BU BÖLÜMDE

CISCO Packet Tracer Yazılımına Bakış	7
Graphical Network Simulator (GNS) Yazılımına Bakış	9
eNSP Yazılımına Bakış	10
Neler Öğrendik?	11

Bu bölümde, öncelikle bilgisayarlar kendi aralarında neden haberleşmeye ihtiyaç duyuyor ve bilgisayar ağı nedir, bunları açıklayarak işe başlayalım.

Bilgisayar ağları; ağ üzerindeki bilgisayarların ve diğer cihazların (yazıcı, dosya sunucusu vb.) kablo ya da kablosuz sinyaller marifetiyle birbirine bağlanarak oluşturmuş olduğu yapıdır.

Bilgisayar ağlarına kaynak paylaşımı, güvenlik, iletişim ile dosya ve bilgi paylaşımı sebeplerinden ötürü ihtiyaç duyulur. Şimdi beraber bu kavramların üzerinden geçelim.



Kaynak Paylaşımı:

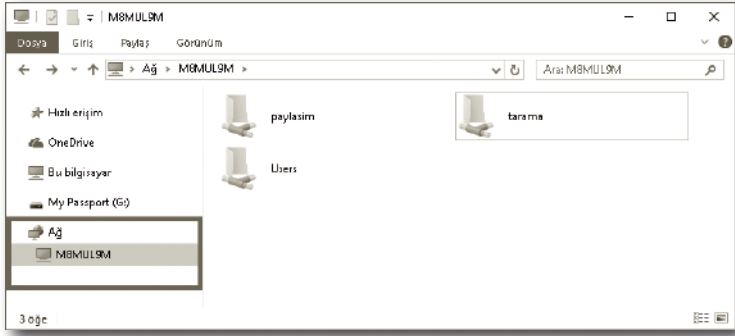
Her cihaz network (ağ) ve sistem yöneticisi tarafından üzerinde yapılan ön tanımlı ayarlar ile ağ ortamında çalışır. Örneğin iş yerinde yapılan iş gereği her bir odadaki personelin yazıcıdan çıktı alması gerekiyorsa her bir odaya yazıcı almak maliyetli bir süreçtir. Bunun yerine merkez bir noktada ağa bağlı bir yazıcı oluşturularak kaynak paylaşımı sağlanabilir. Tahmin edeceğimiz üzere, bu şekilde büyük maliyetler altına girmeden bilgisayar ağları marifetiyle çözüm üretilmiş olur.

Ayrıca ağa bağlı profesyonel bir yazıcı, sistem yöneticisinin yazıcı başına gitmeden yazıcıya IP adresi kullanarak erişebilir ve birçok durumları gözlemleyebilir. (Toner duurmaları, anlık çıktı gönderen kişi bilgileri, tarama dosyalarının tanımlanması gibi.) Bu durumda yönetim açısından da kolaylık söz konusu olmaktadır.

Güvenlik:

Ağ ortamındaki kaynaklar bilmesi gerekenler prensibine göre yapılandırılarak; herhangi bir dosya veya yetkiyi, bilgisayar kullanıcısının görev ve sorumlulukları kapsamında ve yetkisi düzeyinde bir ortama erişimini sağlayacak mekanizma olduğunu söyleyelim. Böylelikle ağ ortamındaki her dosya ve bilgiye herkes yetkisi düzeyinde eriştiğinden dolayı ağın güvenlik özelliği kullanılmış olur.

Örneğin Windows 7, 8, 8.1, 10 işletim sistemlerinden birini kullanarak yine bu işletim sistemlerinden birini kullanan kişiyle şifreli erişime sahip dosya paylaşımı yapmanız mümkündür. Yani illa ki ortamda sunucu rolüne sahip bir cihazın olmasına gerek yoktur. Küçük çaplı ağlarda bu yöntem ile dosya ve bilgi paylaşımı yapılmaktadır. Veya herkesin erişimine açık dosya paylaşımı yapmanız yine mümkün. Aşağıdaki resimde M8MUL9M isimli bilgisayar tarafından paylaşımında olan dosyalar görüntüleniyor.



İletişim:

Bilgisayarlar arası iletişim, bilgisayar kullanıcılarının gereksiniminden dolayı ortaya çıkmakta. Basit bir örnekle konuyu açıklayacak olursak: apartmandaki arkadaşıyla online (*çevrimiçi*) bir oyun oynamak isteyen bilgisayar kullanıcısı mutlaka arkadaşıyla aynı bilgisayar ağına dahil olması ya da kendi aralarında küçük çaplı bir yerel alan ağı oluşturmak zorundadır ki aralarında iletişim sağlayabilsinler. Aksi halde aynı ağda olamadıkları için iletişim gerçekleşmeyecek iletişim sağlanmadığı için oyun oynayamayacaklar. Kısaca bilgisayarlar ya da cihazlar arasındaki iletişim ihtiyacı, sizin de katılacağınız üzere kullanıcı gereksinimlerinden ortaya çıkıyor.



Dosya ve Bilgi Paylaşımı:

Bu özellik dağıtık dosya sistemi yapısı olarak adlandırılan ağ özelliğidir. Dosya ve bilgi paylaşımı özelliği sayesinde aynı ağdaki cihazlar, herhangi bir bilgisayarda bulunan dosya ve bilgiye konum bağımsız erişme yetisine sahiptir.

2

GNS3 İLE SANAL AĞ ORTAMININ KURULMASI

BU BÖLÜMDE

GNS3 ile Sanal Laboratuvar Kurulumu	15
Windows İşletim Sisteminde GNS Kurulumu	16
Mac OS X İşletim Sisteminde GNS Kurulumu	18
GNS'de IOS Yükleme Süreci	18
CISCO Switch/Router Temel Ayarlar	25
VLAN Nedir ve Nasıl Oluşturulur?	26
Telnet Yapılandırması	28
DHCP Servisinin Yapılandırılması	29
Switch Mac Adres Tablosunun İncelenmesi	30
Neler Öğrendik?	30

GNS nedir? diyerek bölümümüze bir adım atalım ve sonrasında neden GNS kullanmalıyız? sorusunun cevaplarını birlikte arayalım.

GNS, Graphical Network Simulator (Görsel Ağ Simülatörü) kelimelerinin baş harflerinin kısaltmasından oluşmuş olup, karmaşık network simülasyonları oluşturup test etmeye olanak veren profesyonel bir network simülatör yazılımdır.

Eğer router, switch gibi cihazlara doğrudan sahip değilseniz ki birçok okurumuzun bunlara sahip olduğunu düşünmüyorum, bu yazılım vasıtasıyla gerçek dünyadaki network ortamlarını, bilgisayar ortamında simüle edebilecek ve fiziksel cihazlar olmadan çalışmalarını gerçekleştirebileceğiz. Bizlere bu süreç içerisinde gerekli olan iki şey vardır. Bunlardan ilki yazılımın kendisi, diğeri ise Cisco ya da Juniper network ürünlerine ait IOS'lara sahip olmaktır. GNS açık kaynak kodlu ve ücretsiz bir yazılımdır ayrıca birçok platformda kullanılabilir. (Windows, MacOSx, Linux)

Önceki bölümde bahsetmiş olmamıza rağmen neden GNS kullanmalıyız tekrar hatırlatmak isterim. Aslında GNS'in birçok platformda çalışıyor olması, bilgisayarımızda kurulu bulunan sanal makineler ile iletişime geçebilmesi, hatta ve hatta fiziksel makinemiz ile de konuşabilmesi, verdiği tepkilerin tıpkı fiziksel cihazların verdiği tepkilere benzer olması ve ücretsiz olması hasebiyle eğitimimiz boyunca GNS'i kullanıyor olacağız.

Ancak şunu da belirtmeliyim ki güçlü donanım özelliklerine sahip bir bilgisayarınız yoksa GNS bilgisayarınızın donanımlarını büyük oranda kullanacağından bilgisayarınızda yavaşlamalar ile karşılaşabileceğinizi de ayrıca hatırlatmak isterim.

NOT

IOS (Internetwork Operating System); Network cihazları içerisinde yüklü olan ve bir nevi bu cihazların işletim sistemi olan yazılımdır. IOS olmadan network cihazı hiçbir şey ifade etmez çünkü yönetilemezdir. IOS, network yöneticilerine çeşitli komutları icra edebileceği CLI ekranı üzerinden müdahalede bulunabileceği bir ara yüz sağlar. Nasıl ki bilgisayar donanımı tek başına bir şey ifade etmiyor ise network cihazları içinde aslında benzer şey söz konusudur.

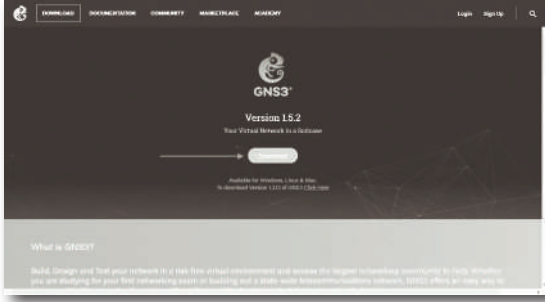
Birçok kursiyer network cihazlarının programlanması safhasında genellikle Cisco Packet Tracer yazılımını kullanır. Ancak Cisco Packet Tracer profesyonel ve uzman seviyedeki kişilere hitap edememektedir. Çünkü desteklediği CLI komutları bakımından GNS'e göre kısıtlıdır ve dış ortam ile iletişim kuramaz.

O halde bu kadar güzel özelliklerinden bahsettiğimiz GNS yazılımını indirmek için neden bekliyoruz? GNS'i indirebilmek için <http://www.gns3.com> web adresini ziyaret ederek Download menüsünü kullanabilirsiniz.

Yukarıda belirttiğim özelliklerin dışında GNS3 tarafından desteklenen özellikler:

- » Karmaşık network topolojileri oluşturmayı,

- » Wireshark ile paket analizi,
- » PuTTY ile CLI (Command Line Interface) üzerinden komut yazımı,



İPUCU

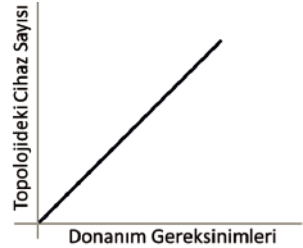
PuTTY; Server ya da Network cihazlarına Telnet, SSH, Console vasıtasıyla bağlanmamızı sağlayan indir-çalıştır bir programdır. PuTTY bağlantı aşamasında GUI'ye sahip iken, sisteme giriş yapıldıktan sonra UNIX komutları kullanılmaktadır.

Herkes GNS3 yazılımını indirmişti diye düşünerek GNS3'ün kurulumuna geçebiliriz. Kurulum süreci oldukça kısa olsa da bu süre zarfında birçok yeni kavramı göreceğiniz için dikkatinizi en üst seviyeye çıkarsanız iyi olur.

GNS3 İLE SANAL LABORATUVAR KURULUMU

MINIMUM SİSTEM GEREKSİNİMLERİ

GNS3 programının kurulumu için gerekli olan minimum donanım gereksinimleri resmi web sayfasında bulunmakla birlikte, yapılacak çalışma ile alakalı olarak donanım gereksinimleri değişiklik gösterebilir. Örneğin; birkaç CISCO router ile topoloji kurularak çalışma yapılacaksa düşük düzeyde bir PC yeterli olabilirken, sanal makineler ile çok sayıda router ve switch kullanılarak bir test ortamı yapılacaksa ihtiyaç duyulacak donanım gereksinimleri de doğru orantılı olarak artış gösterir.



Minimum Gereksinimler

OS	Windows 7 ve sonrası, Mavericks ve sonrası, Linux dağıtımları
CPU	Çift çekirdek ya da fazlası
RAM	4 GB
HDD	1 GB

4

TEMEL NETWORK BİLGİSİ

BU BÖLÜMDE

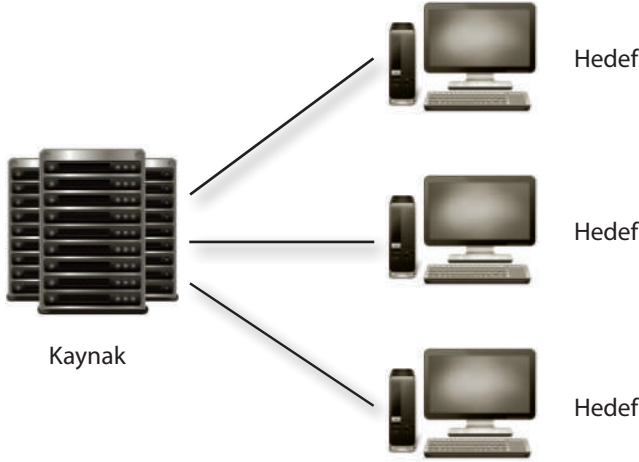
Temel Network Bilgisi	54
OSI Katmanının Ortaya Çıkış Süreci	56
Network Topolojileri	58
Temel Network Cihazları	59
Yayın Türleri	62
Ip Adresleri	64
IP (Internet Protocol) Sınıfları	64
Private (Özel) IP Adresleri	65
Neler Öğrendik?	65

Wireshark programını kullanarak network analizine başlamadan önce temel network bilgisine sahip olmamız, programda yakaladığımız paketlerin anlamlandırılması açısından önem arz etmektedir.

Temel network bilgisine hakim olmanız aslında günümüzde bilgisayar ağlarının girmedığı bir nokta kalmadığı düşünüldüğünde en azından temel network mantığını biliyor olmak sizlere sadece bu kitap kapsamında değil birçok alanda da yardımcı olacaktır.

TEMEL NETWORK BİLGİSİ

Yavaş yavaş kavramlar ile işe yola koyulmaya başlayalım. Kavramları anladıktan sonra ilerleyen bölümlerde Wireshark programı ile analiz aşamasına geçtiğimizde konuları kolaylıkla kavrayacaksınız. Bu yüzden bu bölümde yer alan hususları dikkatlice okumanızın yararlı olacağını düşünüyorum. Kaynakların etkin ve verimli şekilde kullanılabilmesi ile belirlenen cihazların kendi aralarında bilgi alış verişi yapıp, haberleşebilmesini sağlayan yapıya **Network (Ağ)** denir. Network ortamında **source (kaynak)** ve **destination (hedef)** vardır.



Yukarıdaki resimde bir kaynak birden fazla hedef bulunmakta ise de bu durumun tam tersi de söz konusu olabilir.

Kaynak ve hedeften bahsettiğimize göre artık network'ün de bileşenleri bulunduğunu söyleyebilir ve bu bileşenleri inceleyerek yolumuza devam edebiliriz.

Bilgi (Information):

Bir dizi işlem sonucunda belli bir amaç için üretilmiş olan ve bir noktadan başka bir noktaya iletilmek istenen metin, ses, video, resim vb. ifade eder.

Kaynak (Source)

Ağ ortamında bilginin üreticisi olup, üretilen bilginin kablolar, kablosuz sinyaller vasıtasıyla hedefe gönderilmesini sağlayan birimdir. Üretilen bilginin hedefe güvenli bir şekilde gidebilmesi için bilgi şifrelenmiş ya da şifrelenmemiş olarak

gönderilebilmektedir. Bu yapılan işin mahiyetine göre değişkenlik gösterebilir. Şifrelenmiş olarak gönderilen bilginin hedef tarafından çözülebilmesi için benzer şifreleme algoritmalarının hedefte de çalışıyor olması gerektiği unutulmamalıdır.

Hedef (Destination)

Kaynak tarafından üretilen bilginin alıcısıdır. Hedef bir client olabileceği gibi server'da olabilir. Hedef aldığı bilgiyi değerlendirmeye tabi tutar ve bu değerlendirme sonucunda kaynağa geri dönüt (feedback) verir. Ancak her alınan bilgi sonucunda geri dönüt döndürülmez. (Telsiz haberleşmesinde olduğu gibi.) İletişim esnasında kaynak ve hedef süreç esnasında rol değişimi yapabilir.

Kaynak \longleftrightarrow Hedef

Ortam (Environment)

Ortam; kaynak tarafından üretilen bilginin hedefe ulaşırken kullanmış olduğu yolu ifade eder. Network ortamında hatırlayacak olursanız bilgi, kablo ve sinyaller vasıtasıyla gönderilir diye önceki bölümlerde belirtmiştik. Bilginin bozulmadan hedefe ulaşabilmesi için, ortam çok önemlidir. Örneğin çok gürültülü bir ortamda iletişim kurmak istediğiniz bir insana bağırsanız dahi sizi duymayabilir. Aynı şekilde ağ ortamında da elektriksel sinyaller vb. kaynaklı gürültülerin çok olması bilginin bozulmasına yol açabileceği unutulmamalıdır.

Protokol (Protocol)

Her oyunun bir kuralı olduğu gibi, iletişimin de belli kuralları vardır. Bu kurallar bütünü protokol olarak adlandırılır. Bilgisayarlar iletişime geçiyor dahi olsa aralarında istenen hizmetin çalışabilmesi için ilgili protokollerin çalışıyor olması gerekir. HTTP, FTP, SSH gibi protokoller günümüzde yaygın olarak kullanılan protokollerden bazılarıdır.



Aslında günümüzde bilgisayar sistemleri birbirleriyle iletişim kurarken ya da network cihazı üreticileri üretim yaparken bazı network modellerini baz alarak çalışmaktadır. OSI modeli bu modellerden yalnızca bir tanesidir. Bunun yanı sıra

6

WIRESHARK GELİŞMİŞ ÖZELLİKLER

BU BÖLÜMDE

GeoIP Veri Tabanı ile Konum Tespit	116
Protokol İstatistikleri	120
Endpoint (Uç Nokta) Bilgileri	121
Summary (Özet) Bilgisi	123
Conversation (Konuşma) Penceresi	124
IO Grafikleri	125
Neler Öğrendik?	126

Wireshark ücretsiz olmasına rağmen çok gelişmiş özelliklere sahiptir. Bu özellikler kullanıcılara özellikle analiz safhasında yardımcı olan özelliklerdir. Örneğin yakalanan paketlerin toplam boyutu ve ağdaki ortalama bant genişliği tüketimi nedir sorularını birkaç hamleyle ortaya çıkarabilirsiniz. Ya da ağda anlık bant genişliği tüketiminin grafiksel gösterimi gibi çeşitli gelişmiş özelliklerin nasıl kullanılacağını ele almaya başlayalım.

GEOLIP VERİ TABANI İLE KONUM TESPİT

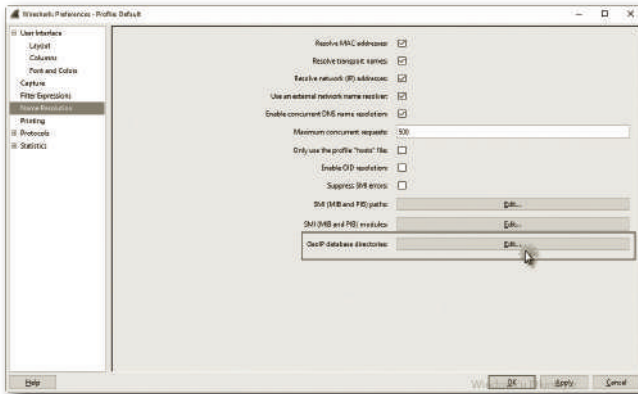
Benim en sevdiğim özelliklerden bir tanesi GeoIP veri tabanını kullanarak Wireshark üzerinden konum tespittir. Wireshark üzerinde çalışma yaparken web sayfalarının barındırıldığı hostların hangi ülkede bulunduğu ya da sisteme düzenlenen bir saldırının hangi IP adresi ve ülke üzerinden geldiği ile ilgili olarak kestirimde bulunabilmek için GeoIP veri tabanı kullanılır.

Ağınızda Wireshark hali hazırda açıksa tüm gelişmeler paket olarak kaydedilecektir. Bu paketlerin hangi konumlardan geldiği GeoIP veri tabanı ile ortaya çıkarılabilir. GeoIP veri tabanı dosyaları Wireshark'ta mevcutta olarak kurulu değildir. GeoIP veri tabanına ait dosyaları <http://dev.maxmind.com/geoip/legacy/geolite> web adresinden indirerek gerekli kurulumları yapmamız gerekir.

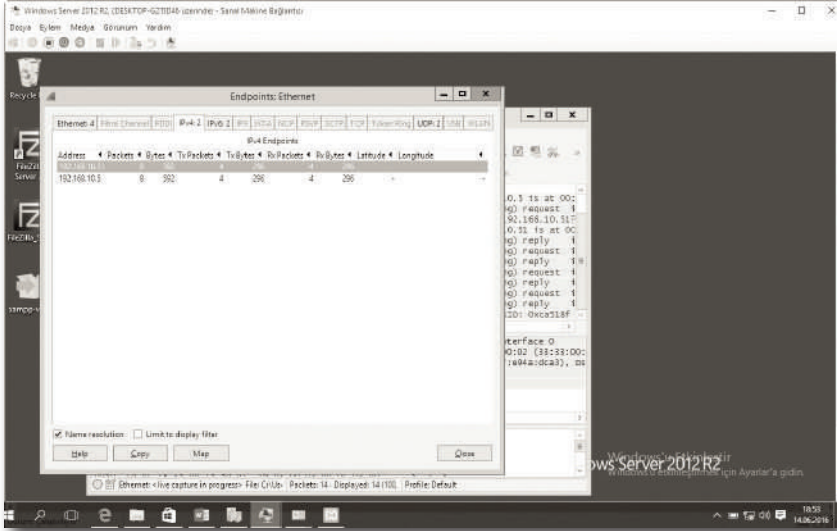
Downloads

Database	Download links				
	Binary / gzip	Binary / xz	CSV / gzip	CSV / zip	CSV / xz
GeoLite Country	Download	Gzip only	Zip only	Download	Zip only
GeoLite Country IPv6 ←	Download	Gzip only	Download	Gzip only	Gzip only
GeoLite City	Download	Download	Zip and xz only	Download	Download
GeoLite City IPv6 (Beta) ←	Download	Gzip only	Download	Gzip only	Gzip only
GeoLite ASN	Download	Gzip only	Zip only	Download	Zip only
GeoLite ASN IPv6 ←	Download	Gzip only	Zip only	Download	Zip only

GeoIP veritabanına ait dosyalar hem IPv4 hem de IPv6 için indirilebilmektedir. İndirilen dosyaları bir klasör içine çıkardıktan sonra dosya yolları gösterilmelidir. Öncelikle Edit>Preferences yolu izlenmelidir.



Öncelikle, indirmiş olduğumuz GeoIP Database dosyalarına ait dizinin bulunduğu konumu göstermemiz gerekiyor. (GeoIP Database Directories)



Endpoints penceresinde IPv4 sekmesi incelendiğinde, haberleşen cihazlara ait IP adresleri ve değişik parametreler görüntülenmektedir. Bu parametreleri ele alalım.

Address	Ağ ortamındaki bilgisayar gibi uç birim cihazlara ait IP adreslerini gösterir.
Packets	Gönderilen toplam paket sayısıdır.
Bytes	Gönderilen toplam byte değeridir.
Tx Packets	Gönderilen paket sayısıdır.
Tx Bytes	Gönderilen byte değeridir.
Rx Packets	Alınan paket sayısıdır.
Rx Bytes	Alınan byte değeridir.

Örneğimizde bir cihazdan başka bir bilgisayara ping atılmıştır. Ping komutu var sayılan da dört **echo request** paketi gönderir. Karşı taraftaki bilgisayarın aktif olması durumunda dört **echo reply** paketi ile dönüş yapılır. Resimden de görüleceği Tx packets değerinin 4 olduğu görülmektedir. Bu paketler **echo request** paketleridir. Aynı şekilde Rx packets değerinin de 4 olduğu görülmektedir. Bu paketler ise **echo reply** paketleridir.

Ayrıca latitude (*enlem*) ve longitude (*boylam*) değerlerinin olması halinde **Map** butonu vasıtasıyla IP adresine ait konumu gösterir harita açılır. Ancak harita üzerinde konum gösterilebilmesi için internet bağlantısı gerekmektedir.

ÖRNEK OLAYLAR

BU BÖLÜMDE

TCP Port Tarama Tespiti	130
FTP Login Saldırısı	133
ARP Taraması	137
Hedef Bilgisayara Ait İşletim Sistemi Tespit	138
GET Metodu Üzerinden Gelen Veriler	141
SYN Flood Atağının Tespiti	142
SQL Injection Saldırısının Tespiti	148
MSN Messenger Hizmetindeki Mesajların Takibi	151
Mac Flooding Tespiti	153
Multicast Yayınların İncelenmesi	157
UPD Protokolü Üzerinden Gelen Verilerin Doğruluğunun Kontrol Edilmesi	165
Resim Dosyalarını Yakalama ve Dışarı Aktarma	169
Neler Öğrendik?	171
Son Söz	171

Wireshark ile birçok şey yapabilirsiniz. Örneğin IP adresini bilmediğiniz bir cihazı ağa dahil ederek gönderdiği ARP paketlerini inceleyerek IP adresinin tespitini ya da yönettiğiniz bir ağda aşırı yavaşlama var ise gelen giden paketleri protokol (bittorent vb.) bazında ele alarak yavaşlığın sebebini tespit edebilirsiniz.

Bu bölümde ele alacağımız senaryolar gerçek hayatta karşılaşılabileceğiniz senaryolardır tabi ki de gerçek hayat senaryoları bu kadar değil. İhtiyaç durumunuzu, çalıştığınız alana göre Wireshark'a çeşitli şekillerde ihtiyaç duyacaksınız. Önemli olan temel analiz mantığını oturtmak ve network protokollerinin yapısını bilmekten geçiyor, gerisi ise teferruat.

Kemerlerinizi sıkı sıkı bağlayın bu bölümde Wireshark'la neler yapıldığını derinlemesine göreceğimiz uzun ve keyifli bir yolculuğa başlıyoruz.

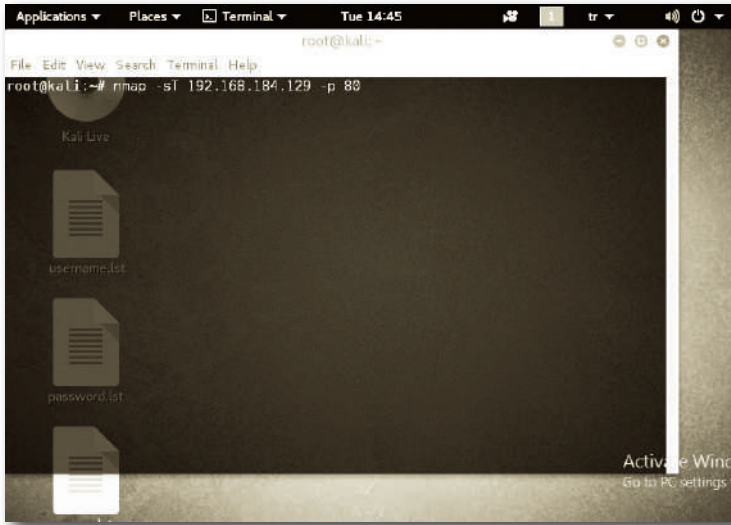
TCP PORT TARAMA TESPİTİ

Öncelikle port nedir ile işe başlayalım. Portlar bilgisayar yazılımlarının dışarı açılan kapı ve pencereleridir. Bu portlar üzerinden yazılım diğer bilgisayarlar ile konuşabilmektedir. Eee hal böyle olunca bilgisayar hacker'ları, saldırının ilk safhası olan bilgi toplama ile ağıımızdaki bilgisayarların hangi portlarının açık olduğunu tespit etmek için çeşitli faaliyetler yürütürler.

NOT

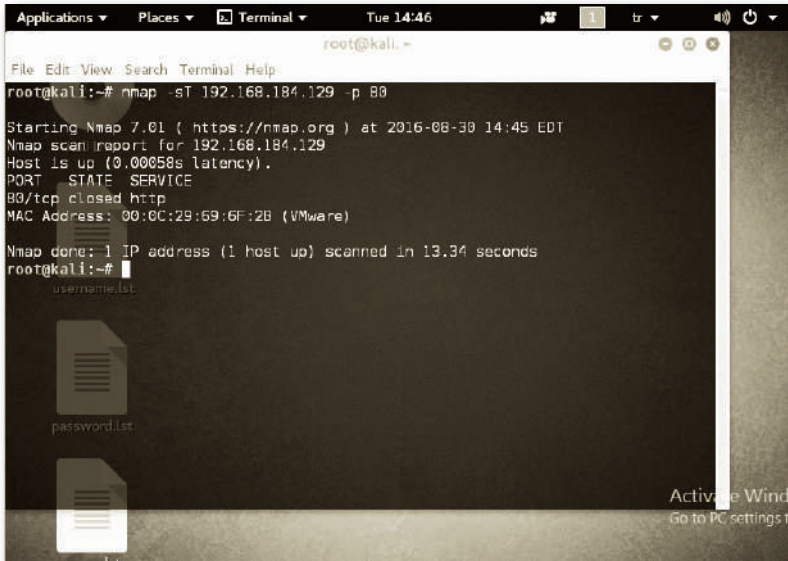
Portlar bir evin kapı ve pencerelerine benzetilebilir. Eve giriş çıkışlar kapı ve pencerelerden yapılırken, bilgisayar sistemlerinde de portlar bu işi yürütürler.

Port tarama faaliyetlerini Windows işletim sisteminde **Zenmap**, **Advanced Port Scanner** gibi araçlar ile gerçekleştirebileceğiniz gibi Kali Linux işletim sistemi içinde kurulu olarak gelen **nmap**, **metasploit** gibi araçlar ile de gerçekleştirebilirsiniz. O halde ne duruyoruz, başlayalım.



Kali linux içinde terminal'i açıp `nmap -sT 192.168.184.129 -p 80` yazarak taramayı başlatıyoruz. Buradaki komut parçacıklarını ve parametreleri öğrenelim:

Nmap	-> uygulamanın adı
-sT	-> TCP scanning
192.168.184.129	-> hedef bilgisayar
-p	-> port parametresi
80	-> 80 portunun taranacağını ifade etmektedir.



```

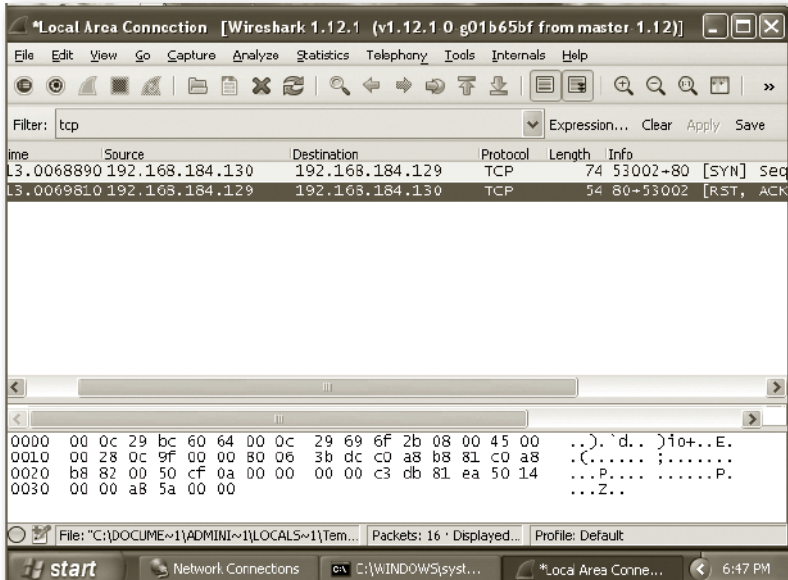
root@kali:~# nmap -sT 192.168.184.129 -p 80

Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-30 14:45 EDT
Nmap scan report for 192.168.184.129
Host is up (0.00058s latency).
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:0C:29:69:6F:2B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@kali:~#

```

Döner sonucu incelediğimizde TCP 80 portunun kapalı olduğunu, hedef bilgisayarın açık olduğunu, hedef bilgisayara ait MAC adresi gibi bilgileri görebiliyoruz. Şimdi de tarama esnasında Wireshark üzerinde neler olup bittiğine bakalım.



Time	Source	Destination	Protocol	Length	Info
13.0068890	192.168.184.130	192.168.184.129	TCP	74	53002→80 [SYN] Seq...
13.0069810	192.168.184.129	192.168.184.130	TCP	54	80→53002 [RST, ACK] Seq...

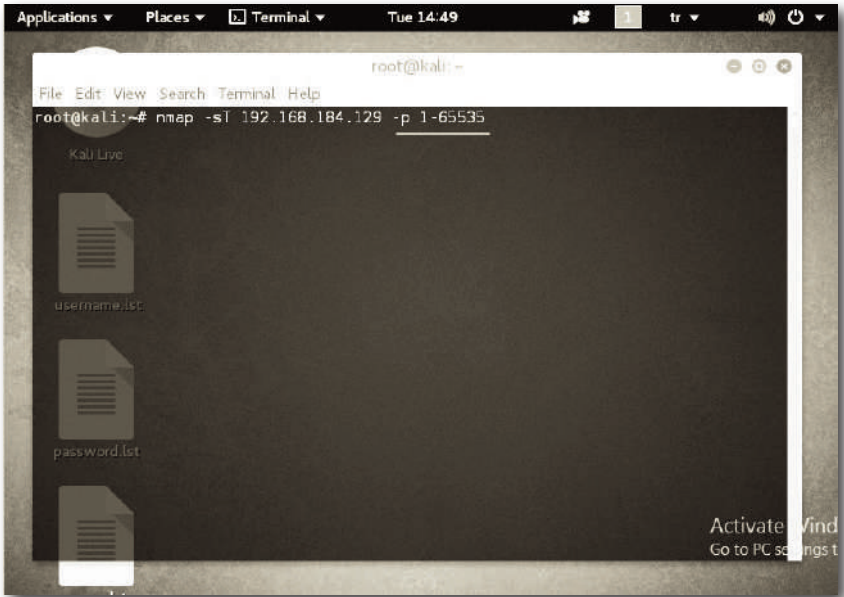
```

0000  00 0c 29 bc 60 64 00 0c 29 69 6f 2b 08 00 45 00  ..).`d.. )1+..E.
0010  00 28 0c 9f 00 00 80 06 3b dc c0 a8 b8 81 c0 a8  ..(.....;.....
0020  b8 82 00 50 cf 0a 00 00 00 00 c3 db 81 ea 50 14  ...P.....P.
0030  00 00 a8 5a 00 00  ..Z..

```

192.168.184.130 IP adresli bilgisayardan, 192.168.184.129 IP adresli bilgisayara TCP 3 way handshake amacıyla [SYN] paketinin gönderildiği görülmektedir. Ancak bir sonraki paket incelendiğinde 192.168.184.129 IP adresli bilgisayar RST, ACK paketleri ile dönüş yapıyor. Bu paketler ile dönüş yapılmasının nedeni oldukça basittir. Ya bağlantı kurulmak istenen port kapalıdır ya da firewall tarafından filtrelediği için [RST, ACK] paketleri ile dönüş yapılmıştır.

Bilgisayar hacker'ı spesifik bir portu taramak yerine, TCP kapsamındaki 65535 portu tarayarak hangilerinin açık olduğunun tespitini de yapmak isteyebilir.



Bu sefer Wireshark paket listesi penceresinde göreceğiniz ekran aşağıdaki gibi olacaktır.