Lan Tricks Yazılımları ve Kullanımları

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

IP NEDİR?

* (İ)nternet (P)rotocol kelimesinin kısa yazılması ip'yi olusturur. IP adresi 131.107.2.101 örnek adresinde olduğu gibi 4 bölümden oluşan bir adrestir. Nokta ile bir diğerinden ayrılan bu bölümlerin herbiri O ile 255 arasında bir değer alabilir. Peki, bir bilgisayar IP adresini nasıl alır? Bunun iki yolu var: Ya siz bu adresi elle girersiniz, ya da bir bilgisayar belli bir adres havuzundan aldığı adresleri diğer bilgisayarlara dağıtır. Adresleri elle girmenin en büyük sakıncası adreslerin, subnet mask değerinin ve default gateway gibi diğer bazı bilgilerin yanlış girilebilmesidir. Eğer ağınızdaki bilgisayar sayısı 5-10'u aşıyorsa adresleri elle girmek pek akıllıca değildir. IP adreslerini otomatik olarak dağıtmanın bir yolu vardır ve bu yolun adı Dinamik Bilgisayar Konfigürasyonu Protokolüdür. (Dynamic Host Configuration Protocol, DHCP) Bu protokol ile bir bilgisayar DHCP sunucu (server) olarak tanımlanır ve IP adres dağıtımı bu sunucu üzerinden yapılır.

DHCP sunucu üzerinde bir IP adres havuzu tanımlıdır (örneğin, 220.107.2.100 ile 220.107.2.200 arası gibi)

Bu yazımızda 6 adet programı tanıtacağız.Bu programlar ve download linkleri aşağıdaki gibi :

1-LanSpy :
http://lantricks.com/download/lanspy_setup.exe

2-LanShut Down :

http://lantricks.com/download/lanshutdown_setup.exe

3-LanWhois :
http://lantricks.com/download/lanwhois_setup.exe

4-LanCalculator :
http://lantricks.com/download/lancalculator_setup.exe

5-Look@Lan - Look@Host :
http://www.lookatlan.com/download/LALSetup.exe

6-Medas VNS :
http://www.lookatlan.com/download/MedasVNSSetup.exe

1) LanSpy

Önce program ile kendi bilgisayarımızı taratmayı anlatalım. Program açılınca sol üstteki (+) simgesine tıklıyoruz. 'Add' sekmesine giriyoruz. Get my ip seçeneği ile kendi ip'mizi oraya alıyoruz. OK'leyip anasayfaya dönüyoruz. Yandaki 'go' tuşuna basıyoruz (è) yada kısayoll tuşu olarak f-3'e basınız.

Karşımıza bir çok şey geldi.Şimdi bunların bazılarını tanıyalım :

DNS Name : Windows kurarken yazdığımız şirket adı bilgisi çıkar. Mesela ben şirket adına xx A.Ş. yazmıştım karşıma o çıktı.
MAC : Donanımsal mac adresinizdir. Bilgisayarınızın tc kimlik no'su gibi düşünebiliriz.
Workgroup : Bilgisayarınızın dahil olduğu çalışma grubudur. Çoğunlukla ev kullanıcılarında workgroup yada ev ağı gibi isimlere sahiptir.

Remote time of day :

0 – Time of day : Siz ip'ye tarama yaptığınızda bilgisayarın mevcut tarih ve saatidir.
0 – System Loaded : Tarama yapılan bilgisayarın ne zaman açıldığını gösterir. Mesela ben sabah 9'da açtım ordaki bilgi 09.45.12 şeklinde.

Disks : Sistemde kullanılan diskleri gösterir. Muhtemelen A,B,C,D,E bilgileri olacaktır. Tabi siz farklı bir isim atamadıysanız.
Transports : Çoğunlukla netbios device'yi bulacaktır. Device\\NetbiosSmb şeklinde bilgi sunulacaktır. Transport adres , network adres , number of VCS gibi bilgileri bu kısımdan alabilirsiniz.
Network Adapters : Network iletişim donanımlarının bilgilerini içerir. Çoğunlukla modem bilgisini bu kısımdan alabilirsiniz. Bu sayede karşı bilgisayarın ttnet hesabına ve modemine telnet üzerinden yada superscan gibi programlar ile giriş yapabilirsiniz. Bu bilgi bize giriş yapmak istediğimizde sorulan user name – passport'u bulmamızda yardımcı olacaktır. Default olarak bırakılan modem şifreleri ile kolayca karşı modeme gireriz.

* Bu bilgilerin detaylarına bakarsanız False ve True gibi bilgiler görürsünüz. Bunlar

enabled açıklaması için verilmiştir. Eğer true ise şu an o device enabled yani aktif durumdadır.

WAN MİNİSPORT (IP) başlığı altından Ip adresini – Dns host ismini – Ip ağ maskesini – Ip gateway gibi bilgileri bulabilirsiniz.

USERS : Bilgisayarınızda sahip olduğunuz kullancı adlarıdır. Her zaman administrator ve sizin hesabınızın bilgileri bulunur. Buna ek olarak Windows dahilinde gelen ASPNet , Guest , HelpAsistant gibi user'larda bulunur. Bunların size bir zararı yoktur ve normal şartlarda user listesinde göremezsiniz. İptal edemezsiniz.

SHARED RESOURCES : Bizim için en önemli bölümlerden biridir. Bilgisayarınızın paylaşım alanlarını gösterir. Admin , C ve D olmak üzere 3 tane paylaşım alanını kendi bilgisayarınıza tarama yapınca mutlaka görürsünüz. Bu konuda endişelenmenize gerek yoktur. Bunların yanında kilit işareti olmalıdır. Birini seçip sağ tıkladıktan sonra open diyerek içeriğini görebilirsiniz.

Yada herhangi bir browser penceresine \ ip adresiniz \admin$ yazarak en basitinden Windows klasörlerine ulaşırsınız. Bunu \c$ yada \d$ şeklinde çoğaltabilirsiniz.

SERVİCES / PROCESSES : Sistemde çalışmakta olan durdurulmuş yada iptal edilmiş servislere ait bilgiler bulunur.Başlat menüsünden çalıştır'a SC yazarak entera basarsanız çalışmakta olan servisleri görebilirsiniz.

* Servisleri yönetmek için Başlat/Çalıştır'a services.msc yazmanız yeterlidir.

Şimdilik anlatacağımız program özellikleri bunlar. Biz bu taramayı kendi ip'miz üzerinde yaptık. İp seçme kısmına istediğiniz kişinin ip'sini yazarak tarama yapabilirsiniz. Bilgisayarına yada shared folders'ına girmek için browser penceresine \ kişininip'si \ admin$ yada \ c$ gibi komutları deneyebilirsiniz.

Program üstünde bilgisayar adına sağ tıklayınca open seçeneği ile klasörlere girebilirsiniz. Open as seçeneği ile kişinin bilgisayarını FTP , Telnet , WWWServer olarak görebilirsiniz. Telnet'i seçince firewall'ınız uyarı verecektir bu yüzden ona izin veriniz.

Sağ tıklayınca ShutDown seçeneği ile o bilgisayarı anında kapatabilirsiniz. Bunun için; aynı ağ üzerinde olmanız ve LanShutDown programı gereklidir. O programıda sırası gelince anlatacağız.

2-LANSHUTDOWN

LanSpy ile entegre çalışan bir programdır. Zaten kurulmadığı takdirde lanspy'de ip no'ya sağ tıklayıp shutdown dediğinizde bu program olmadığı için hata alacaksınız. Programı dağıtan resmi sitesinde Windows 2000/XP/2003 için geçerli olduğu yazıyor. Windows

XP'nin ServicePack1'de sorunsuz çalışıyor ancak Service Pack2 yüklenmiş versiyonlarında etki göstermiyor.

Program açılınca sol tarafta çıkan ip'ler yapımcılar tarafından default olarak eklenmiştir. Onlara takılmayınız zaten hepsinin offline olduğunu görebilirsiniz.
Üst menüden 5.sırada olan 'add computer in list' şeçeneğine giriyoruz. Girdiğimiz ip'ye 5 çeşit işlem yapabiliyoruz. Bunlar sırasıyla 'Lock' , 'Log off' , 'Hibernate' , 'Reboot' ve 'ShutDown'dur. Türkçe olarak yazarsak 'Kitle' , 'Oturumu kapat' , Uyku moduna al' 'Yeniden başlat' ve 'Kapat'.

JBu program zaten gayet basit bir program fazla anlatılacak bir yönü yok. Lan ağlarında ufak tefek şekilde eğlenebilirsiniz.

3-LanWhoİs

Evet işte lan serisinde en sevdiğim pratik programlardan biri budur.Whois sorgumuzu e-hack'e yapacağız.

Adres kısmına başına www koymadan domaini yazıyoruz (domain=alan adı) Yani sadece 'e-hack.org' yazıyoruz ve ilk sıradaki (?) şekline tıklıyoruz (F3'e de bassanız aynı işi görür)

Evet karşımıza gelen bilgileri inceliyoruz.

Registrant Name:volkan cinar
Registrant Street1:Ofis gevran caddesi 5/13
Registrant Postal Code:34000
Registrant Country:TR
Registrant Phone:+90.234567890
Registrant Phone Ext.:
Registrant FAX:+90.234567890
Registrant Email:fuzbing@yahoo.com
Name Server:NS1.PLAZMAWEB.NET
Name Server:NS2.PLAZMAWEB.NET

Bu program ile web sitelerinde çırpınmadan en hızlı ve doğru şekilde whois çekebilirsiniz.

Peki whois'in hacking'e faydası nedir?

* - Domain hackte bilinen yöntemlerden biride adminin mailini hacklemektir. Admin mailini buradan öğrenebilirsiniz.
* - Domain ip'sini öğrenebilirsiniz. Buna göre dos atack yapabilirsiniz.
* - Social enginnering konusunda bize gerekecek admin bilgileri olabilir onları temin edebilir ve güzel bir senaryo ile işi daha kolay halledebilirsiniz.
Vb. vb. Diğer programımıza geçelim.

4-LanCalculator

Bu programı anlatmadan önce Özgür Karataş'ın yazdığı şu yazıyı okumanızı öneririm :

IP ADRESİ

Daha önceki dökümanlarımızda network ve yapılarını basitçe tanımıştık. Bu networklar üzerinde bulunan istemci bilgisayarlar (client); birbirleri ile ethernet olarak bilinen ağ kartları ile iletişim kurarlar. Bu kullanılan ethernet kartlarının ayrı ayrı bir MAC adresi (donanım numarası) vardır. Bu ethernet kartları üretilirken verilen değişmez/eşşiz numaralardır.

IP adresi; bir bilgisayara kullanıcı tarafından atanmış olan 32 bitlik bilgidir. Bu bilgi genelde rakamlardan oluşur. Ipv4 ve Ipv6 olmak üzere iki çeşit IP adresi mevcuttur. Bu IP adresleri birbirlerinden nokta ile ayrılırlar ve her bir nokta ile ayrılmış bölüme oktet denir. IP adresleri her biri onlu sayı 0 ila 255 arası bir sayıdır. Bu sayede farklı yerlerde bulunan bilgisayarların birbirleri ile daha sağlıklı haberleşmesi sağlanır. Aynı zamanda bilgisayarların internet protokolu üzerinden çalışmasını sağlayan tanımlamalardır.

Örneğin; 194.27.200.20 IP adresi, dört oktetten oluşur ve her bir oktet 8 bit olarak (ondalık tabloya göre) hesaplanır.

NOT: IP adresleri her zaman Ipv4 standartlarına göre 4 oktetten oluşmaktadır. Ipv6'da bu değişiktir.

Desimal gösterim : 123. 45 . 35 .122
İkili Gösterim : 11001010. 00101010 . 00100101 . 11010010

IP adresleri ise kendi aralarında iki bölümden oluşurlar. Bu bölümlere NetID ve HostID adı verilir.

NetID:

Bilgisayarın bağlı bulunduğu ağı IP adresi üzerinde tanımlayan bölüme NetID denir.

HostID:

Ağ içerisindeki bilgisayarların birbirinden ayrılmasını sağlayan IP Adresi değerine ise HostID denir.

IP Adresleri temel olarak A, B, C diye (standartlara göre) 3 sınıfa ayrılırlar.
A Sınıfı: 127 ağ ve 16,77,214 bilgisayar tanımlanabilir.
B Sınıfı: 16,383 ağ ve 65,534 bilgisayar tanımlanabilir.
C Sınıfı: 2,097,151 ağ ve 254 bilgisayar tanımlanabilir.

Bir network üzerinde bulunabilecek bilgisayar sayısı IP adresinin HostID alanına bağlıdır. HostID'in bit sayısı arttıkça ağın birleşeceği bilgisayar sayısı da artmaktadır. Bunlar dışında iki IP Sınıfı daha vardır;

D Sınıfı: Multicasting için kullanılır.
E Sınıfı: Gelecekte kullanmak üzere rezerve edilmiştir.

Network mühendisi; TCP/IP yazılımını bilgisayarlara yükleyerek, üzerinde bulunan her bir kartın IP adresini tanımlar.

Bir IP adresi 32 bit uzunluğundadır. Diğer bir deyişle 8 bitlik 4 kısımdan oluşmaktadır. Her bir kısım binary (ikili) olarak da ifade edileceğinden dolayı desimal olarak 0-255 arasında, ikili olarak da 0000000 ile 11111111 arasında değer almaktadır.

Sınıf İlk bölüm sayıları

A 1-126
B 128-191
C 192-223

Örneğin; 111.192.110.1 bir A sınıfı IP adresidir. 131.192.110.1 bir B sınıfı IP adresidir. 194.192.110.1 ise bir C sınıfı IP adresidir.

SUBNETTING NEDİR ?

Bir şirket düşünün ve bu şirketin çalışma gruplarına ayrıldığını düşünün. Bu şekilde ise her çalışma grubunun kendine ait bir IP Adresi olması gerekmektedir. İşte bu durumda bir adres alanını subnetlere bölmek için Subnet Mask olarak bilinen IP maskları (subnetting) kullanılır.

SUBNET MASK :

Subnet mask IP adresinin mask kısmını oluşturur. Böylece TCP/IP, Network adresi ile TCP/IP adresini birbirinden ayırır. Bu sayede NetID ve HostID bölümleri birbirinden ayırt edilir.

Subnet mask network sınıfına göre düzenlenir. Varsayım subnet değerleri:

Sınıf Adresi

A 255.0.0.0
B 255.255.0.0.
C 255.255.255.0

Özel Subnet Mask Oluşturmak :

NetID ve HostID değerlerinden oluşan IP adreslerinde; özel subnet maskları oluşturularak daha verimli bir network iletişimi sağlanabilir. Bu durumda network içerisindeki çalışma gruplarını da kısımlara ayırmak gereklidir. Öncelikle network üzerinde kaç tane subnet yaratılacak ona karar verilir.

CLASSLESS INTER DOMAIN ROUTING (CIDR)

CIDR, Internet için yeni bir adresleme yöntemidir. IP adreslerinin daha etkin kullanımını sağlar. CIDR'a duyulan gereksinimin ana nedeni IP adreslerinin tükenmesi yani yeni bağlantılar için gerek duyulan IP adresinin, adresleme sisteminden doyalı adres bulunamamasıdır.

Bu program ile ip numaranızı ve subnet mask no'nuzu yazarak bunlara ilgili hesaplanmış değerleri öğrenebilirsiniz.
Subnet mask no'sunu ip adresinizin ait olduğu sınıfı (A – B- C) şeklinde seçerek öğrenebilirsiniz.Genelde çoğu ip B class'a aittir.
---------- ----------
---------- ----------
Programımız ip adresi ve subnet mask'a bağlı olarak prefix – min ip – max ip – broadcast adress – hosts per network gibi değerlere ait bilgiler alabilirsiniz.Pek bir işinize yaramayan bu değerlerden ziyade yukardaki bilgileri okumanızı tavsiye ederim.

5-Look@Lan ve Look@Host

İlk olarak Look@Lan programını anlatacağız. Program açıldığında NewProfile diyerek yeni bir profil hazırlıyoruz. Speed'i ADSL olarak ayarlayın. Manually Specifiy Scan Range seçeneği ile scan edeceğimiz ip aralığını seçiyoruz. Burda aralığı bol tutmanın bi manası yok.Boşuna işlemi uzatmış oluruz.

Ben 88.240.159.1 ile 88.240.160.1 aralığını taratıyorum.

Tarama bitince önünüze bir network raporu gelecek. Bu rapordan online olan ip'leri görebileceksiniz. Hide seçeneği ile listeyi kapatıp ilk tarama sayfasına dönüyoruz. Bu listeden ip'lerin şuan online olup olmadığını – kullandıkları işletim sisteminin Windows olup olmadığını – çok nadirde olsa bazen bilgisayar adını – netbios adını – SNMP

durumunu görebiliriz.

Üst menüden hierarchical network wiev yapıyoruz. Bu sayede ip'lerin bizim taramamıza kaç saniyede yanıt verdiğini görebiliyoruz. Eğer taradığınız aralıkta kendi ip'niz varsa adsl hizmeti aldığınız yere ait bilgiler alabilirsiniz. Mesela ben ege bölgesinde yaşadığım için izmir'den hizmet alıyorum bu yüzden izm_t1_1-brs_t2.ttnet.net.tr ve 32 mlsn. Bilgisi karşıma geliyor. Bu sayede bağlantı çıkış hızımın gayet iyi olduğunu görebiliyorum. Bu listeden istediğim ip adresine sağ tıklayarak prof scan yapabiliyorum.Bu tarama daha detaylı oluyor.

Şimdi prof scan üstünde biraz duralım.

Bu scan seçeneği ile yaptığımız 4 ping testinin sonuçları görüntülenecektir.Mesela benim 4 ping sonuçlarım şöyle :

Ping 1 : 32ms
Ping 2 : 31ms
Ping 3 : 40ms
Ping 4 : 32ms

Hostname gibi bilgilerim arama sonucunda çıkmadı çünkü bunları 3.party programlarla saklamıştım daha önce.

Active services seçeneği altında açık portları görebilir ve bunlarla iletişime geçebiliriz. Benim sadece tek aktif olan portum 135 olarak çıktı.

Asıl sayfadan graphical ping seçeneği ile bu işlemi grafik üstünde görebiliriz.

İlk profil sayfamıza dönelim. Ordan bazı seçekleri birazda sizin kurcalamanıza bıraktım. EditPortScan services'e giriyoruz. Burdan port numaralarının ne işe yaradığını görebiliriz. Buraya yeni port numaraları ekleyerek onlarında taranmasını sağlayabiliriz. Port tanımlarını değiştirebiliriz.

Şimdide Look@Hot programını anlatalım. Bu programa ip numarası ekleyerek yeni taramalar yapabiliriz. Kendi bilgisayarınızı ekleyip denemenizi tavsiye ederim. Yeşil olanlar aktif olanlar,kırmızı olanlar. Bu program look@lan ile ortak çalıştığı için fazla anlatmaya gerek duymuyorum. Look@lan'ı iyi anlarsanız bu program zaten onun küçük bir parçası gibi.

6-MEDAS VNS

Program açıldığı zaman kendi bilgisayarınızı karşınızda göreceksiniz.

Program ile LanSpy'ın yaptığı çoğu işi yapabilirsiniz. Network interfacelerinizi görebilir, İp-

ICMP-TCP-UDP layerlarınız hakkında detaylı bilgileri görebilirsiniz.

Active connections seçeneğinden TCP ve UDP bağlantılarınızı ve bunların status bilgilerini görmeniz mümkün. Eğer established yazan bir status varsa buna süphe ile bakmanızı tavsiye ederim.

Routes bölümümden subnet mask'ınızı görebilirsiniz. Bilgisayarınızın ne kadar süredir açık olduğunu görebilirsiniz.

Sıkıldım, kısa kesiyorum, görüşmek üzere ((:

MUSTAFA SERHAT DÜNDAR