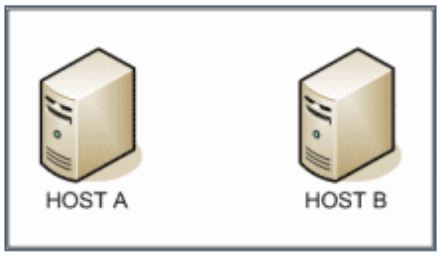
HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

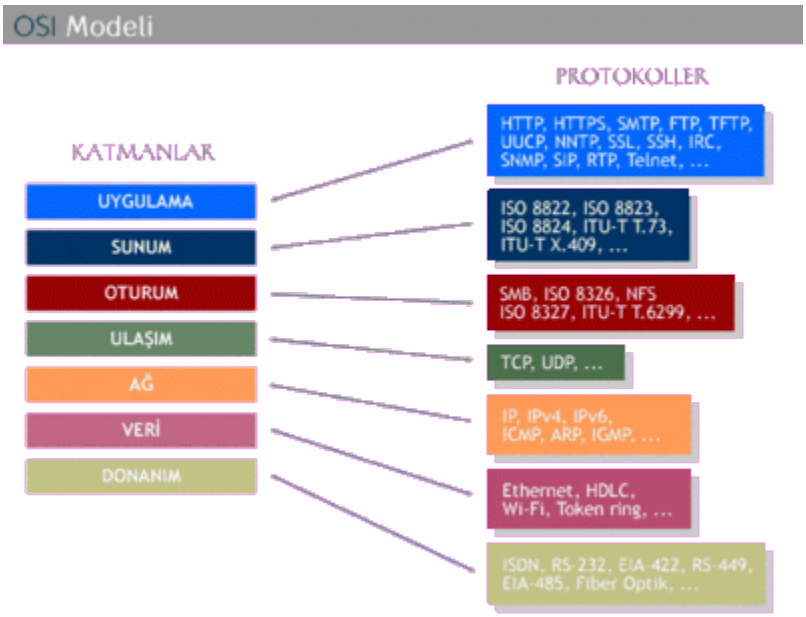
SCANNING NETWORKS:

TCP 3-WAY HANDSHAKE DIAGRAM

Below is a (very) simplified diagram of the TCP 3-way handshake process. Have a look at the diagram on the right as you examine the list of events on the left.

EVENT	DIAGRAM
Host A **sends** a TCP **SYN**chronize packet to Host B Host B receives A's **SYN** Host B **sends** a **SYN**chronize-**ACK**nowledgement Host A receives B's **SYN-ACK** Host A **sends** **ACK**nowledge Host B receives **ACK**. ***TCP socket connection is ESTABLISHED.***	 TCP Three Way Handshake (SYN,SYN-ACK,ACK)

Şekil:Üçlü el sıkışma süreci



NMAP SCANNING TECHNIQUES:

Nmap ön tanımlı olarak well-known(en çok bilinen) 1000 portu tarar.

Bunu yapmaması için nmap'e aşağıdaki parametre verilirse istenilen aralıktaki portlar taranır:

Örnek: nmap -p1-100 www.google.com

	Nmap raporuna göre global olarak en fazla açık olan portlar
TCP	80, 23 ,22 ,443, 3389, 445, 139, 21, 135, 25
UDP	137, 161, 1434, 123, 138, 445, 135, 67, 139, 53

PARAMETRELER	**NMAP ile istenilen portları tarama**
Parametre Kullanımı	**Açıklamalar**
U:UDP	**UDP Portları taranmak istendiği zaman**
T:TCP	**TCP Portları taranmak istediği zaman**
-p1-65535	**65535 portun hepsini taramak için**
-p U:53,111,137	**UDP portlarını taramak için**
T:21-25,80,139,8080	**TCP portlarından 21 ile 25 arasındakiler ile belirtilenleri taramak için**

NMAP Useful Options:

PARAMETRE	KULLANIM AMACI
--reason	Taramanın verdiği sonucun açıklamasını gösterir.
--top-ports 10	Yaygın 10 portu listeler.
--top-ports 100	Yaygın 100 portu listeler.
--top-ports 1000	Yaygın 1000 portu listeler.

Nmap R

Örnek Komut: nmap localhost –reason
Sonuç:nmap sözkonusu komut verildiğinde "1000" tane portu otomatik olarak tarar.Açık olan portlarla ilgili sonuç döker.Buna engel olmak için

Örnek komut ile google.com adresinin 53 portuna istek gönderdik.Cevap olarak verdiği sonuçta "no response" geldiği için portun "filtered" olduğunu gösterdi.

nmap google.com -p53 --reason

Starting Nmap 5.21 (http://nmap.org) at 2014-03-12 16:16 EET

Nmap scan report for google.com (173.194.70.113)

Host is up, received syn-ack (0.058s latency).

Hostname google.com resolves to 6 IPs. Only scanned 173.194.70.113

rDNS record for 173.194.70.113: fa-in-f113.1e100.net

PORT STATE SERVICE REASON

53/tcp filtered domain no-response

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

Örnek komut ile google.com adresini yaygın olarak 100 port içerisinden tarattık.Sonucunda 91 portun filtreli olduğu açık 9 portun türü ve servis versiyon bilgisi listelendi.

nmap google.com --top-ports 100

Starting Nmap 5.21 (http://nmap.org) at 2014-03-12 16:24 EET

Nmap scan report for google.com (173.194.116.200)

Host is up (0.033s latency).

Hostname google.com resolves to 11 IPs. Only scanned 173.194.116.200

Not shown: 91 filtered ports

PORT STATE SERVICE

25/tcp open smtp

80/tcp open http

110/tcp open pop3

113/tcp closed auth

143/tcp open imap

443/tcp open https

2000/tcp open cisco-sccp

5060/tcp open sip

5190/tcp open aol

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds

ICMP ECHO Scanning:

Ping taraması hedef host'a ICMP ECHO isteği gönderir.Eğer hedef ICMP ECHO reply isteği dönerse hedef sistemin ayakta olduğu bilgisi elde edilir.

ICMP ECHO scan yöntemiyle firewall tespiti yapılabilir!

NMAP komutu:
nmap -sP -v 192.168.2.1

Ping Sweep:

Belirli IP aralıklarına ICMP ECHO istekleri göndererek o aralıktaki "live hostlar" tespit edilebilir.

Komutları sırasıyla,	**Komut Açıklaması**
nmap -PE	ICMP echo
nmap -PP	timestamp
nmap -PM	netmask tespiti

OTOMATİZE NMAP TARAMASI:

İşletim Sistemi tespiti, çalışan servisler, traceroute ve nmap script taramaları toplu halde gerçekleştirilir.
Örnek komut: nmap -A www.example.com

NMAP TCP Taramaları:

TCP Connect Taraması:

Tcp Connect taraması ile three way handshake gerçekleştirilerek hedef portların açık olduğu anlaşılır.Tam bağlantı gerçekleştirilir.Hedefe RST paketi gönderilerek bağlantı sonladırılır.

Örnek: nmap -sT 192.168.2.2 --reason

Stealth Syn Taraması:

TCP Syn taraması ile üçlü el sıkışma gerçekleştirilmez. İstek gönderene sunucu RST isteği döndüğü takdir de portun kapalı olduğu anlaşılır. Port açık ise sunucu syn ack isteği döner.

İstemci bağlantı tam olarak gerçekleşmemesi için RST paketi gönderek bağlantıyı kapatır.

Örnek komut: nmap -sS 192.168.2.2 --reason

XMAS Taraması:

Örnek komut: nmap -sX 192.168.2.2 --reason

Hedefe URG,ACK,RST,SYN ve FIN bayraklı paketleri gönderilir.

Sunucu "No Response" cevabı dönerse port açıktır.

Port kapalıysa "RST" isteği döner.

Bu tarama çeşidi microsoft windows sunuculara karşı çalışmaz.

FIN Taraması:

Hedefe "FIN" bayraklı paket gönderilir.

Sunucu "No Response" cevabı dönerse port açıktır.

Sunucu "RST ACK" cevabı dönerse port kapalıdır.

Örnek komut: nmap -sF 192.168.2.2 --reason

Bu tarama çeşidi microsoft windows sunuculara karşı çalışmaz.

NULL TARAMASI:

Hedefe “NO FLAG SET” şeklinde bayraksız bir paket gönderilir.

“No response” cevabı dönerse port açıktır.

Sunucu “RST ACK” cevabı dönerse port kapalıdır.

ACK Taraması:

Örnek komut: nmap -sA 192.168.2.2

Window Taraması:

Örnek komut: nmap -sW 192.168.2.2

NMAP VERSİYON BİLGİSİ LİSTELEME:

Kullanımı:
-sV parametresi ile çalışan servis versiyon bilgisi listelenebilir.
Örnek komut:nmap -sT -sV -p80 www.example.com

Sunucu işletim sistemi bilgisi listeleme
Örnek komut:nmap -O **www.example.com**

UDP PROTOKOLÜ:

UDP Connectionless bir prokoldür.

UDP TCP'nin aksine üçlü el sıkışma gerçekleştirmez.

Unreliable:

TCP protokolünün yaptığı şekilde verinin alınma kontrolünü gerçekleştirmez.

Veriyi hızlı şekilde iletmek üzere çalışır.

NMAP UDP Taraması:

İnternette genel olarak çoğu servis TCP protokolü üzerinde çalışır.DHCP,DNS,SNMP servisleri yaygın olarak UDP üzerinde hizmet verir.Hedefe udp paketi gönderilirse "ICMP Port unreachable" mesajı alınıyorsa port kapalıdır.Paket gönderildiğinde alınan cevap "no response" ise port açıktır.

Parametre:-sU

Örnekte dönen cevap "no response" olduğu için port açıktır.
Örnek komut:sudo nmap -sU google.com -p53 --reason

Starting Nmap 5.21 (http://nmap.org) at 2014-03-12 17:55 EET

Nmap scan report for google.com (173.194.116.133)

Host is up, received echo-reply (0.056s latency).

Hostname google.com resolves to 11 IPs. Only scanned 173.194.116.133

PORT   STATE   SERVICE REASON

53/udp open|filtered domain no-response

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

Banner Grabbing:

Banner grabbing örnek komut:
telnet www.example.com 80
HEAD / HTTP/1.0

Örnek Komut:

telnet www.microsoft.com 80

Trying 64.4.11.42...

Connected to lb1.www.ms.akadns.net.

Escape character is '^]'.

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Cache-Control: no-cache

Content-Length: 1020

Content-Type: text/html

Last-Modified: Mon, 16 Mar 2009 20:35:26 GMT

Accept-Ranges: bytes

ETag: "67991fbd76a6c91:0"

Server: Microsoft-IIS/8.0

X-Powered-By: ASP.NET

Date: Wed, 12 Mar 2014 15:58:51 GMT

Connection: close