22/10/2003

Bilgisayar Ağları Uygulamaları Genel Sınavı

Sınav soruları 3 kategori halinde verilmiştir. İlk kategoride yer alan 1 ve 2 numaralı soru mutlaka cevaplanmalıdır. İkinci kategori yer alan 15'er puanlık 6 sorudan 4 tanesi cevaplanmalıdır. Son kategoride yer alan 10'ar puanlık 3 sorudan yanlızca biri cevaplanmalıdır.

Başarılar...

Kerem Erzurumlu

Yapılması Zorunlu Sorular (15 Puan);

1. 193.140.236.0/24 C sınıfı IP bloğunu aşağıdaki yerel ağları içerecek şekilde yeniden yapılandırınız ve her blok için ağ maskesi, IP bloğu ve öntanımlı ağ geçidi bilgilerini veriniz. Tüm tasarım bittikten sonra boşta kalan IP bloğu varsa bunu da belirtiniz.
    a. 12 adet hoca bilgisayarı
    b. 29 adet asistan bilgisayarı
    c. 10 adet sunucu bilgisayar
    d. 32 adet genel kullanım bilgisayarı – 1
    e. 24 adet genel kullanım bilgisayarı – 2
    f. 29 adet genel kullanım bilgisayarı – 3
    g. 8 adet genel kullanım bilgisayarı – 4
    h. 16 adet genel kullanım bilgisayarı – 5
2. TCP'de üç yönlü el sıkışmayı açıklayınız.

15 Puanlık Sorular;

3. Aşağıdaki tcpdump filtrelerini açıklayınız. E seçeneği örnek olarak açıklanmıştır.
    a. src net 193.140.236.0/24 dst host 193.140.216.2
    b. dst host 193.140.236.44 port 80
    c. src host 193.140.236.44 and not port 80
    d. dst net 0.0.0.0/0 and port 80
    e. src port 80 (kaynak portu 80 olan paketler)
4. TCP SYN ve TCP FIN taramalarını açıklayınız.
5. nmap ile nessus programlarının farklarını açıklayınız.
6. DNS komutlarından "dig" ve "host" komutlarını açıklayınız. MX ve NS kayıtlarının ne olduğunu açıklayınız.
7. Sniffer tespit yöntemlerinden iki tanesini açıklayınız.
8. Güvenlik duvarları ile saldırı tespit sistemleri arasındaki farkları açıklayınız.

10 Puanlık Sorular;

9. HUB ile switch aktif ağ cihazları arasındaki farkı açıklayınız.
10. "netstat –an" komutu ne işe yarar açıklayınız.
11. Nessus/Balista/ISS türü programların neden uzak makinalar üzerinde kullanılmaması gerektiğini açıklayınız.

Cevaplar;

1. IP bölmeleme esnasında kullanabileceğimiz IP bloklarının büyüklüğü sırası ile 128, 64, 32, 16, 8, 4 dür. IP bloklarının ilk ve son IP'leri network ve broadcast'i tanımladığından kullanılmayan IP'lerdir. Bir de ağ geçidi tanımlanacağından dolayı seçeneklerde verilen IP adetlerine 3 adet eklendikten sonra bulunan sayı kaç adetlik IP bloğu gerekeceğini belirtir.

Bu durumda;

a, c, g seçenekleri 16'lık IP bloğu,

b, e, f, h seçenekleri 32'lik IP bloğu,

d seçeneği ise 64'lük IP bloğu gerektirmektedir.

Tüm ağ 16'lık segmentlere ayrılırsa oluşacak ağlar, ağ maskeleri ve öntanımlı ağ geçitleri;

IP ARALIĞI	AĞ MASKESİ	AĞ GEÇİDİ
193.140.236.0-15	255.255.255.240 (28)	193.140.236.14
193.140.236.16-31	255.255.255.240 (28)	193.140.236.30
193.140.236.32-47	255.255.255.240 (28)	193.140.236.46
193.140.236.48-63	255.255.255.240 (28)	193.140.236.62
193.140.236.64-79	255.255.255.240 (28)	193.140.236.78
193.140.236.80-95	255.255.255.240 (28)	193.140.236.94
193.140.236.96-111	255.255.255.240 (28)	193.140.236.110
193.140.236.112-127	255.255.255.240 (28)	193.140.236.126
193.140.236.128-143	255.255.255.240 (28)	193.140.236.142
193.140.236.144-159	255.255.255.240 (28)	193.140.236.158
193.140.236.160-175	255.255.255.240 (28)	193.140.236.174
193.140.236.176-191	255.255.255.240 (28)	193.140.236.190
193.140.236.192-207	255.255.255.240 (28)	193.140.236.206
193.140.236.208-223	255.255.255.240 (28)	193.140.236.222
193.140.236.224-239	255.255.255.240 (28)	193.140.236.238
193.140.236.240-255	255.255.255.240 (28)	193.140.236.254

Tüm ağ 32'lık segmentlere ayrılırsa oluşacak ağlar, ağ maskeleri ve öntanımlı ağ geçitleri;

IP ARALIĞI	AĞ MASKESİ	AĞ GEÇİDİ
193.140.236.0-31	255.255.255.224 (27)	193.140.236.30
193.140.236.32-63	255.255.255.224 (27)	193.140.236.62
193.140.236.64-95	255.255.255.224 (27)	193.140.236.94
193.140.236.96-127	255.255.255.224 (27)	193.140.236.126
193.140.236.128-159	255.255.255.224 (27)	193.140.236.158
193.140.236.160-191	255.255.255.224 (27)	193.140.236.190
193.140.236.192-223	255.255.255.224 (27)	193.140.236.222
193.140.236.224-255	255.255.255.224 (27)	193.140.236.254

Tüm ağ 64'lık segmentlere ayrılırsa oluşacak ağlar, ağ maskeleri ve öntanımlı ağ geçitleri;

IP ARALIĞI	AĞ MASKESİ	AĞ GEÇİDİ
193.140.236.0-63	255.255.255.192 (26)	193.140.236.62
193.140.236.64-127	255.255.255.192 (26)	193.140.236.126
193.140.236.128-191	255.255.255.192 (26)	193.140.236.190
193.140.236.192-255	255.255.255.192 (26)	193.140.236.254

Bu IP bloklarından çalışma olmamasına dikkat edilerek bir adet 64'lük, 4 adet 32'lik, 3 adet 16'lık kullanılır. Bir adet 16'lık blokda boş olarak kalır.

2. TCP'de üç yönlü elsıkışma iletişimlerin başlaması için kullanılır. Açık olan bir servise istemcinin bağlanmaya çalışması ile başlar. Bu ilk pakettir.

- **a. İstemciden sunucuya (1)**
  - **i. Sıra numarası S**
  - **ii. SYN bayrağı işaretli**
- **b. Sunucudan istemciye (2)**
  - **i. Sıra numarası C**
  - **ii. SYN ve ACK bayrakları işaretli**
  - **iii. S+1 için ACK**
- **c. İstemciden sunucuya (3)**
  - **i. Sıra numarası S+1**
  - **ii. ACK bayrağı işaretli**
  - **iii. C+1 için ACK**

3. a. 193.140.236.0/24 ağından olup, 193.140.236.2 bilgisayarına giden paketler,

b. 193.140.236.44 IP'li bilgisayarın 80 (web) kapısını hedef alan paketler,

c. 193.140.236.44IP'li bilgisayarın 80 harici kapılarından gönderilen paketler,

d. İnternet'e 80 (web) kapısına giden paketler.

4. TCP SYN: üç yönlü iletişim başlatılır. Fakat istemciden gitmesi gereken 3 numaralı paket iletilmez. Hali ile iletişim başlamadığı için bilgisayarlarda bir kayıt oluşmaz.

TCP FIN: Başlatılmamış bir iletişim sonlandırılmaya çalışılır.

İki tarama yöntemi içinde sunucudan gelen cevap paketi ilgili servisin verilip verilmediğini göstermektedir.

5. **nmap yanlızca açık kapıların testlerini ve uzak işletim sistemi belirlemede kullanılır. Gizli çalışma yeteneği vardır. Nessus ise gizli çalışma yeteneğine sahip olmayıp, açık kapılar için mevcut olan zayıflık testleri (vulnerability tests) ve servis engelleme saldırıları (Denial Of Service) yapabilmektedir.**

6. host: Unix tabanlı işletim sistemlerinde IP bilgisinden bilgisayar adına yada bilgisayar adından IP bilgisine ulaşmayı sağlar. Aynı zamanda alanların MX, NS ve SOA gibi gelişmiş bilgilerini de sorgulayabilir.

dig: DNS'in hiyerarşik yapısından dolayı karşılaşılan bir hatayı takip etmek için kullanılır. DNS'in traceroute komutudur denilebilir.

MX: alan adının posta sunucusunu belirtir (Mail eXchanger).

NS: alan adının DNS sunucusunu belirtir (Name Server).

7. Snifferların en yaygın tespit yöntemi yanlış MAC adresi ile hazırlanmış fakat doğru IP bilgisi içeren bir paketin gönderilmesidir. Normal koşullar altında bu paket işleme alınmaz. Fakat sniffer çalışan bir makina bu paketi işleme alır ve bu paket için cevap üretir.

Diğer bir tespit yöntemi ise ping yöntemidir. İlgili makinaya bir ping paketi gönderilerek zamanı tespit edilir. Birden çok ping paketi gönderilerek gecikme ölçülmeye çalışılır. Eğer sniffer MAC kontrolü yapmıyorsa gecikme yaşanmaz.

8. Güvenlik duvarları yanlızca IP paketlerinin başlık kısımları ile ilgilenir. Bir diğer değişle güvenlik duvarları yanlızca paketin kimden gelip kime gittiği ile ilgilenir. Kendi üzerindeki kural yapısına uyması durumunda paketin geçmesine izin verir.

Saldırı tespit sistemleri ise paketlerin başlığı ile ilgilenmez. Paketin içeriği daha önemlidir. Saldırı tespit sistemleri paket içeriklerindeki karakteristik özellikleri inceleyerek bu paketin bir saldırı paketi olup olmadığına karar verir.

9. **HUB akıllı olsun yada olmasın bir bağlantı ucuna gelmiş paketi tüm bağlantı uçlarına "broadcast" olarak dağıtır.**

Anahtarlayıcı ise gelen paketin ikinci katmanda analizini yaparak hedef MAC adresini çözer, kendi üzerinde tutmakta olduğu adres tablosundan karşılaştırır ve yanlızca gerekli bağlantı ucuna ilgili paketi gönderir. Bu nedenle anahtarlayıcı cihazlarda sniffer çalışamaz.

10. **"netstat –an" o anda bilgisayar üzerinde çalışmakta olan ve aktif olan tüm bağlantı kapıları ile ilgili bilgileri gösterir.**