32-) Asimetrik algoritmalar, Simetrik algoritmalara göre neden daha yavaştır?
a) Asimetrik algoritmalar, simetrik algoritmalara göre daha fazla hesaplama gerektir
b) Simetrik algoritmalar, asimetrik algoritmalara göre daha fazla hesaplama gerektirir
c) Asimetrik algoritmalarda şifreleme ve deşifreleme için aynı anahtar kullanılır
d) Simetrik algoritmalarda şifreleme ve deşifreleme için farklı anahtar kullanılır
e) Simetrik algoritmalarda kullanılan anahtar boyu 16 bittir

33-) Aşağıda verilenlerden hangisi firewall için yanlış bir ifadedir?
a) Yerel ağlar üzerindeki kaynakları diğer networkler üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi çözümüdür
b) Firewall'un sistem üzerinde etkili kullanılması için ağ ortamı ile Internet arasındaki tüm trafik Firewall üzerinden geçmelidir
c) İç tehditlere karşı, virüslü program ve dosyalara karşı koruma sağlar
d) Genellikle firewall, atakları önlemek için kurulurlar
e) İki ağ arasında konumlandırılarak bir ağı diğerinden korur

34-) Aşağıdakilerden hangisi Saldırı Tespit Sistemlerinin çıktıları arasında yer almaz?
a) Zaman/tarih
b) Saldırının domain ismi
c) Kaynak ve varış IP adresleri
d) Saldırının ne kadar süreceği
e) Kaynak ve varış port numaraları

35-) Aşağıdakilerden hangisi Ağ Tabanlı Saldırı Tespit Sistemlerinin özelliklerinden değildir?
a) Geniş bir ağı görüntüleyebilir
b) Mevcut ağa etkileri azdır
c) Saldırganlar tarafından fark edilmeleri zordur
d) Şifrelenmiş bilgiyi inceleyebilir
e) Genellikle ağı dinleyen pasif cihazlardır

36-) Aşağıdakilerden hangisi WPA2 için yanlıştır?
a) IV 48 bittir
b) Şifreleme algoritması CCMP/AES veya CCMP/TKIP'tır
c) Anahtar yöntemi 802.1x şeklindedir
d) Anahtar değişikliğine gerek yoktur
e) Hiçbiri

37-) WPA (Wi-Fi Protected Access) şifreleme anahtarı uzunluğu kaç bittir?
a) 32
b) 64
c) 128
d) 256
e) 192

38-) Zarar Verici Lojik sınıflandırmasına göre aşağıdakilerden hangisi Konak Programa ihtiyacı olan yazılımlardan biri değildir.
a) Solucan
b) Virüs
c) Key Logger
d) Truva atı
e) Yığın Mesaj

39-) Aşağıdaki atak çeşitleri ve kullanım amaçlarıyla ilgili yapılan açıklamalarından hangisi yanlıştır?
a) Denial-of-Services-DoS Atakları: Saldırılan bilgisayar veya çalışan servisi yavaşlatmak veya durdurmak amacıyla yapılır
b) Phishing: Kullanıcıya sahte bir mail gönderilerek kullanıcının sahte bir siteye çekilmesi amaçlanır
c) Fingerprinting Bu atağın amacı büyük boyutlu paket göndererek sistemi bozmaktır
d) Brute Force Attacks: Olası karakter kombinasyonu deneyerek parolayı tahmin etmeyi amaçlar
e) Hijacking Ataklar: Client ile server arasındaki iletişimin arasına girmeyi, ve kullanıcının oturumunu ele geçirmeyi amaçlayan saldırılardır

-) Aşağıdakilerden hangisi SQL Injection Exploit türlerinden değildir?
Stack edilmiş sorgular
Database tanımlama
nion operatörü
şul İfadeleri
e hashleri oluşturma

ağıdakilerden hangisi SQL Injection saldırılarını engellemek için kullanılabilir?
b) WAF
c) IDPS
d) IPS
e) Hiçbiri

42-) KAA'da düşman bir bölümdeki paketleri toplayan ve bunları başka bir bölgeye yönlendirerek tünel oluşturarak gerçekleştirilen saldırı tipi hangisidir?
a) WormHole Saldırısı
b) Jamming Saldırısı
c) BlackHole/SinkHole Saldırısı
d) Sybil Saldırısı
e) Mote Sınıfı – Laptop Sınıfı Saldırıları

43-) Aşağıdakilerden hangisi "Steganografi" ile "Kriptoloji" arasındaki farktır?
a) Steganografi veri şifrelemek için kullanılır
b) Kriptografi mesajın içeriğini anlaşılmaz hale getirirken, steganografi mesajı görülemeyecek şekilde saklar
c) Steganografi,kriptoloji gibi veriyi saklamaz,şifreler
d) Kriptoloji ve steganografi veriyi farklı şekilde şifreler
e) Fark yoktur, iki terimde aynı şeyi ifade eder

44-) Aşağıdakilerden hangisi Ses Steganografi uygulamalarında kullanılmamaktadır?
a) Low bit encoding
b) Phase coding
c) Spread spectrum
d) Echo data hiding
e) S-I

45-) Aşağıdakilerden hangisi Uygulama (Application) Güvenlik Protokollerine örnek olarak verilemez?
a) SET
b) HTTPS
c) KERBEROS
d) SSH
e) Sniffing

46-)

ACTION	Source	Port	Destination	Port
Allow	*	*	192.168.1.20	25

Yandaki firewall kuralı için aş
hangisi doğrudur?

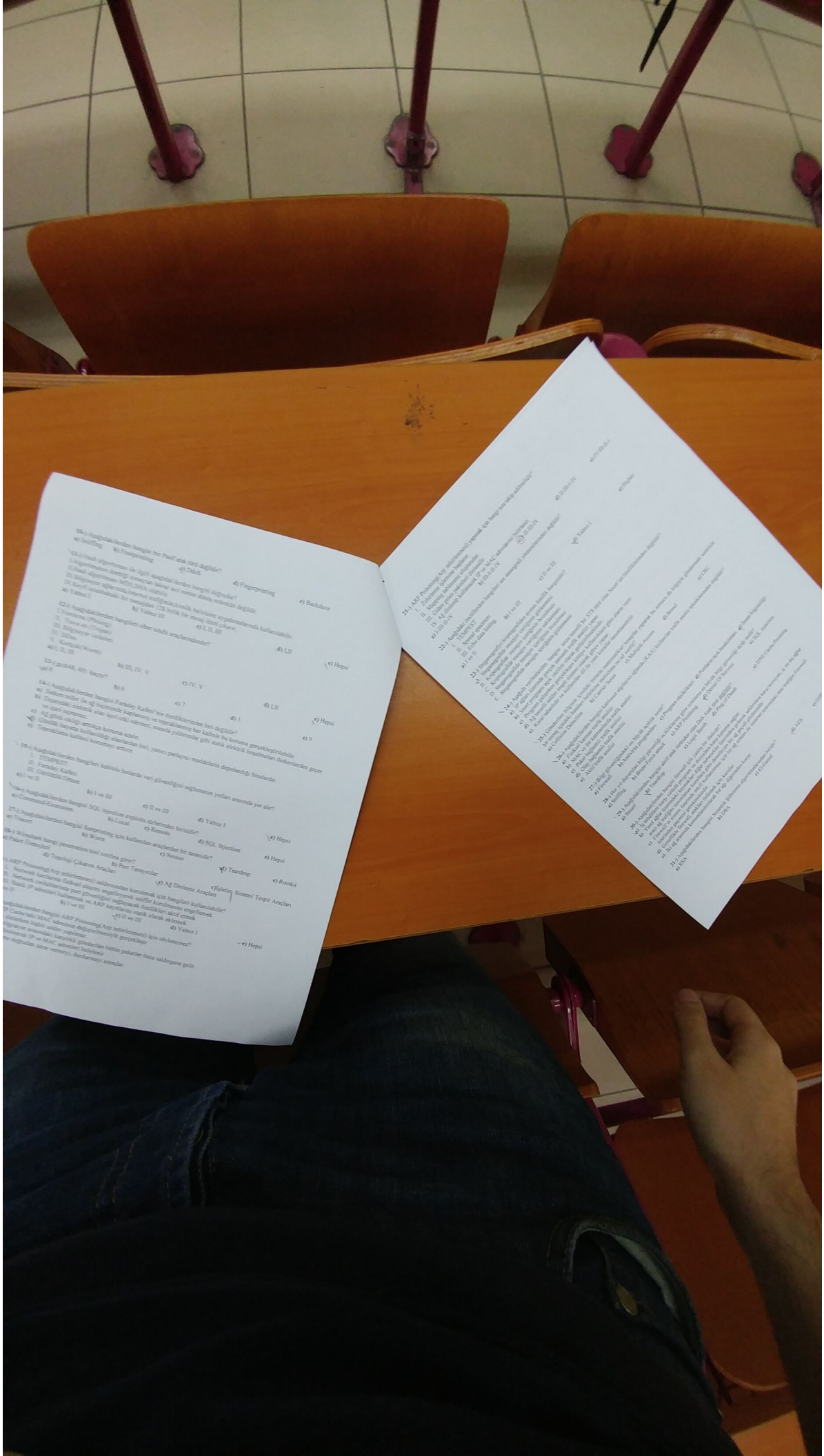
a) 25 numaralı portan bütün çıkışlara izin verir
b) 25 numaralı portan sadece 192.168.1.20 IP adresine sahip kullanıcılar çıkış yapabilir
c) 25 numaralı portan bütün kullanıcılar sadece 192.168.1.20 IP adresli kullanıcıya paket
d) 25 numaralı portan bütün gelen trafiğe izin verir
e) 25 numaralı portan bütün gelen trafiği yasaklar

47-) Aşağıdakilerden hangisi bulut bilişimde veri güvenliği için Tam Homomorfik Encryption -FHE)'nin tercih edilmesinin başlıca sebebidir?
a) Yeni bir şifreleme tekniği olması
b) Bulut sağlayıcısının veri şifrelenmiş olsa bile veri üzerinde anlamlı hesapla
c) Şifreleme için (Public key, Secret key) anahtar çiftinin kullanılması
d) Simetrik şifreleme modeline sahip olası
e) Öklid Kafesleri temelli şifreleme şeması oluşturulabilmesi

48-) IPv4 ve IPv6'nın güvenliği ile ilgili aşağıdakilerden hangisi(leri)
I- IPv6 nın hiçbir ağ güvenlik sorunu yoktur.
II- IPv4de şifreleme yapılmaması eavesdropping ataklarını mümk
III- Kimlik doğrulama ve şifreleme IPv6 ya IPv4 den miras kal
IV- Eavesdropping, bilgi gönderilirken uygun araçlar kullan
saldırıya uğraması ile meydana gelen atak çeşididir.
a) Yalnız I
b) I-III
c) II-IV

49-) Sensör Ağ DoS tipi saldırılar göz önüne alındığı
yanlıştır?
a) Ağ Katmanı - Kara Delik (Black Hole) Saldırısı
b) Ulaşım Katmanı - Sel (Flooding) Saldırısı
c) Ağ Katmanı - Yanlış Yönlendirme Saldırısı
d) Veri Bağı Katmanı – Çarpışma Saldırısı
e) Ulaşım Katmanı – Kurcalama (Tampering

50-) Aşağıdakilerden hangisi Kara Delik
a) Sadece asılanmış düğümlerin yol bi
b) Düğümlerin gözlemlenmesi ve yan
c) Ara düğümlerde başlık bilgisinin
d) Ağın bağlılığının (connectivity)
e) Mesajların çoğullanıp yolland



BİLGİSAYAR AĞLARINDA GÜVENLİK FİNAL SINAVI

23.05.2017

1-) Yukarıda verilen 802.1x ile kimlik doğrulama adımlarının doğru sıralanışı hangisidir?
1-İstemci doğrulama sunucusundan, onun kimliğini ister. Doğrulama sunucusu, kimlik bilgisini istemciye gönderir.
2-.Doğrulayıcı bağlantı isteğini alınca, tüm portları kapalı tutar, sadece istemci ile arasında bir port açar.
3-.İstemci doğrulayıcıya bağlantı talebinde bulunur.
4-Doğrulayıcı, kullanıcıdan kimliğini ister. İstemci kimliğini gönderir, doğrulayıcı kimlik bilgisini doğrulama sunucusuna gönderir. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. Sunucu kimliği doğrular ve doğrulayıcıya gönderir. Doğrulayıcı, istemcinin portunu yetkilendirilmiş duruma getirir.
5-İstemci, doğrulama sunucusunun kimliğini doğruladığında, veri trafiğine başlanır.
a) 3-2-4-1-5 b) 5-3-1-4-2 c) 3-2-5-1-4 d) 4-2-5-3-1 e) 1-5-2-4-3

2-) Aşağıdakilerden hangisi ulaşım katmanı güvenlik protokollerinden biri değildir?
a) Pertty Good Privacy (PGP)
b) Secure Shell (SSH)
c) Private Communication Technology (PCT)
d) Secure Socket Layer (SSL)
e) Trasport Layer Security (TLS)

3-) Aşağıdakilerden hangisi SET (Secure Electronic Transactions-Güvenli Elektronik İşlemler) protokolünün sağladığı temel servislerden biri değildir?
a) Kimlik Tanılama b) Mesaj Bütünlüğü c) Anahtar Değişimi d) Gizlilik e) Linkleme

4-) Aşağıdakilerden hangisi ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür?
a) TLS (Transport Layer Security / İletim Katmanı Güvenliği)
b) SET (Secure Electronic Transactions / Güvenli Elektronik İşlemler)
c) PCT (Private Communication Technology / Kişisel İletişi Teknolojisi)
d) SSH (Secure Shell / Güvenlik Kabuk)
e) SSL (Secure Socket Layer / Güvenli Yuva Katmanı)

5-) Aşağıdakilerden hangisi steganografi yöntemleri arasında yer almaz?
a) Mobil Steganografi (Mobile Steganography)
b) Görüntü Steganografi (Image Steganography)
c) Ses Steganografi (Audio Steganography)
d) Video Steganografi (Video Steganography)
e) Metin Steganografi (Text Steganography)

6-) PPP(Point to Point Protocol)'nin asıl çalışan kısmı, bağlantı kurulması, yapılandırılması, test edilmesi, parametrelerin ayarlanması ve bağlantının kapanmasından sorumlu olan; paket boyutunu düzenleyen, yapılandırma hatalarını tespit eden protokol hangisidir?
a) LCP (Bağlantı Kontrol Protokolü) b) NCP c) IPCP d) HDLC e) TACACS+

7-) Aşağıdakilerden hangisi Cloud Defenderın filtreme aşamalarından değildir?
a) Sensor Filter b) Double Signature Filter c) Embedded Filter d) Puzzle Resolver Filter e) Hop Count Filter

8-) Aşağıdakilerden hangisi yanlıştır?
a) Gizlice Dinleme: MAC çerçeveleri ve veri paketleri parçalanarak başlık elde edilir. Komşu düğümler, yönlendirme bilgisi elde edilir.
b) Aktif Ataklar: Amaç sadece gizlilik değil, bütünlüğü de bozmaktır. Ağa yetkisiz giriş, kaynakların izinsiz kullanımı, haberleşmenin ele geçirilmesidir.
c) Pasif Ataklar: Amaç KAA üzerindeki verinin gizliliğini bozmak, herhangi bir emisyon gerçekleşmez.
d) Trafik Analizi: Önemli bilgiler içeren ağ topolojisi düşman tarafından ele geçirilebilir. Merkeze yakın düğümlerden daha çok ağ trafiği olacağı için bu tip düğümlerin analiz ile tespit edilmesi ve DoS ataklara maruz bırakılması ağın erişilebilirliğini engelleyecektir.
e) Hepsi

9-) Aşağıdakilerden hangisi kod atak türü değildir?
a) Solucan b) Trojen Atı c) Sosyal Mühendislik d) Lojik Bombalar e) Rootkit