33- Kurulum ve çeşitli konfigürasyon özelliklerini ders kapsamında paylaştığımız SNORT konseptinde açık kaynak bir yazılımdır.

- ağ tabanlı saldırı tespit sistemi
 tuzak sistem
- anti malware
- security information event management
- · honeypot temelli saldırı tespit sistemi

16-Hangisi dönem projesi olarak önerdiğim konseptlerden birisi değildir?

- · Antivirüs sistemleri
- Security information event management
- · Sosyal medya analizi
- Arama motoru optimizasyonu
 - · Biyometrik güvenlik sistemleri

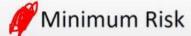
150 27-001

18- Bilgi güvenliği alanında dünya genelinde yaygın olarak kullanılan

uluslararası standart.................. dır.

6- Bilgi güvenliğinin temel amacı hangisidir?

- · Gizliliğin sağlanması
- · Bütünlüğün sağlanması
- Erişilebilirliğin sağlanması
- · Yetkilendirmenin sağlanması



- 8- Verilenlerden hangisi yanlıştır?

 Bir konu ile ilgili belirsizliği azaltan kaynak veridir.
- Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.
 - Bir sistem yazılımı ihtiyaçlarınız ve beklentileriniz doğrultusunda çalışıyorsa güvenlidir.
 - · Güvenlik risk yönetimidir.
 - Bilgi güvenliğinin sağlanmasından herkes sorumludur.

20- Bir dosyanın değişip değişmediği bilgi güvenliği ilkelerindenile ilgilidir.

butuduk

36-Hangisi bilgi güvenliği alanındaki güncel mesleklerden biri değildir?

- Incident Responder
- Security Architect
- Malware Analyst
 - Computer Security Developer
- Network Security Engineer

22- Dijital delillerin

dijital delillerin özellik ya da sorunlu bazı durumlarının ifade edilmek istendiğini düşünün. Buna göre yukarıdaki ifade aşağıdakilerden hangisi ile tamamlanamaz?

- bütünlüğü
- inkar edilememesi
- #doğrulanamaması
 - doğruluğu
 - · farklı zamanlarda değerlendirilebilmesi

28-DNS'in açılımı:

- 7- Hangisi diğerlerinden farklıdır?
- Test edilmemiş güvenlik sistemi
- · Çalışandan gelen tehditler
- · Yetkisiz kişilerin erişimi
- ∦ Bant genişliğine kasteden saldırılar
 - · Yanlış eksik altyapı yatırımları

• Doğru

Yanlış

ters oranti vardir.

26-Günümüzde saldırı karmaşıklığı ile saldırganın teknik bilgisi arasında

10- Aşağıdakilerden hangisi internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" amacı ile düzenlenmiştir?

- ISO 27001-5651
- TS ISO IEC 27001
- ISO 27001 LA
- **# TCK 5651**
- UEKAE BGYS-0001

32- Bir şifre için olası tüm ihtimallerin denenmesi şeklindeki saldırıya denir. (cevabınızı ya ingilizce ya da türkçe olarak yazın. her iki dilde birlikte yazmayın!)

Laba-Kurret

14- Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin asılmasına neden olan eksikliklere

denir.

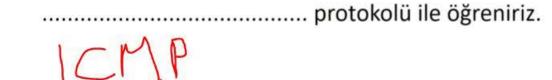
15-Nicel risk değerlendirmesi kapsamındaki hesaplardan biri olan yıllık kayıp beklentisi hesaplanırken yıllık gerçekleşme ihtimalini nasıl değerlendirirsiniz?

Sonraki yılda gerçekleşme oranını tahmin ederek

in Önceki gerçekleşme değerlerine bakarak

- Tekil kayıp beklentisine bakarak
- Varlık değerine bakarak
- . Vancana malicatina baland
- Korunma maliyetine bakarak

27-Uzak bir hedefdeki sunucunun aktif olup olmadığını



37-Uzaktaki bir makinenin işletim sistemini tespit etmek için yapılan

çalışmalara genel olarak ne ad verilir. finger printing

40-Ders kapsamında tanıtılan üstveri analiz aracının adı nedir?

..... başvuru yapılır.

Geliştirilecek bir yazılımda özel bir

port kullanılacaksa

29- IP, ifadesinin kısaltmasıdır.

Interes Postocol

17-Güvenlik yönetim süreci, yazılım yaşam döngüsü gibi bir güvenlik yaşam döngüsü olarak ele alındığında 3. aşamada hangisi yer alır?

- Oluşturma
- İzleme
- Analiz
- Uygulama
- Gelistirme

38-snort saldırı tespit sisteminde paket yakalamak için kullanılan

Lib pcap

kütüphane nedir?

35-Açık istihbarat toplama anlamındaki metodolojiye ne isim verilir?



Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:
 Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- · Gizlenmiş dosya bulma.





adli bilişim



yapınacak araşınınınını kapsar.

- 2.Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) : iletişimine yönelik incelemeyi kapsar.
- 3.Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Do Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi ka
- 4.İnternet Adli Bilişimi (İnternet Forensics): Genel olarak internet sistemleri üzerinde yapılan araştırmayı kapsar.
- 5.Bilgi Adli Bilişimi (Information Forensics): Bütün olarak bilgiyi materyali barındıran sistemler üzerinde yapılan incelemeyi kapsa

Dr. Muhammet BAYKARA - Firat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği Bolümü

Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şı
- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Dr. Muhammet BAYKARA - Firat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği Bolümü

Bilişim Suçları

(Adli Bilişimin Faydaları)

 Adli bilişim, yalnızca bilişim suçlarına has bir delil tol değildir. Bilişim suçlarından başka, klasik suçlara iliş ihtiyaç duyulan deliller, yine elektronik aygıtlar içer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsı soygun planı ve buna ilişkin haritalar bilgisayar ile halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmad bilişim devreye girecektir. Bu duruma en bariz örne

devam etmekte olan Ergenekon soruşturması ile alaka

bilgisayar kayıtlarından ulaşılması gösterilebilir.

Önceki

Ileri

- - · Proje

Ödev

Quiz

Ara Sınav

unsurlardan biri değildir?

1-Hangisi dersin bu dönemlik değerlendirmesinde başvurulacak

Final

yazılıma denir.

21- Güncel bir kötücül yazılım türü olan ve fidye yazılımı olarak bilinen

ransomware

24-Dijital delillerin kanıt olarak değer kazanabilmesi için incelenmesi gereken son aşama......'dır.

raporlama

3-Hangisi dersin temel kaynakları arasında önerilen kaynaklardan birisidir?

- Kamil Burlu, Bilişimin Karanlık Yüzü, Nirvana yayınları.
- Hamza Elbahadır, Saldırı ve Savunma Teknikleri, Kodlab Yayınları.
- Bünyamin Demir, Bilgisayar ve Casus Yazılımlar, Dikeyeksen Yayınları.
- Muhammet Baykara, Bilişim Sistemleri İçin Saldırı Tespit ve Engelleme Yaklaşımlarının Tasarımı ve Gerçekleştirilmesi, Fırat Üniversitesi Yayınları.
- · Ömer Çıtak, Beyaz Şapkalı Hacker Eğitimi, Papatya Yayınları.

13-Kurum ya da kuruluşları olumsuz etkileyebilecek unsurlara denir.

tahdit

Bilginin sadece yetkili kişiler tarafından erişilebilir olması
ilkesi ile sağlanır.

Gieli/ik

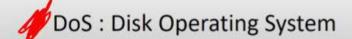
- 2-Hangisi dersin amaçlarından biri değildir?
- Bilgi güvenliği konularında farkındalık ve temel düzeyde teorik ve pratik bilgiler öğrenmenizi sağlamak.
- Bilgi güvenliği temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak.
- · Araştırma yeteneğinizi geliştirmek.
- Kişisel ve kurumsal bilgi güvenliğinin sağlanması konusunda fikir sahibi olmanızı sağlamak.
- Bilgi sistemlerinin açıklıklarını tespit ederek sistemlere sızma yapabilmeniz için teknikler öğrenmenizi sağlamak.

19- Beyaz şapkalı hacker anlamına gelen kısaltmadır. Aynı zamanda bilgi

güvenliği alanındaki temel standart ve yine bu alandaki önemli

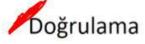
eğitimlerden biri..... dır.

- 4-Dersle ilgili olarak verilen temel kavramlardan hangisi yanlış ifade edilmiştir?
- · Confidentiality: Gizlilik
- Integrity : Bütünlük
- Non-repudiation : İnkar Edilemezlik



Exploit : Korunmasızlık Sömürücü

12- Hangisi bilgi güvenliğinin temel unsurlarından birisi değildir?



- Kullanılabilirlik
- Gizlilik
- Bütünlük
- Erişilebilirlik

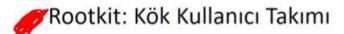


11-Hangisi güvenlik yönetim pratiklerinden birisi değildir?

- Politika, Prosedür ve Rehberler
- Denetim
- Eğitim
- Siber Saldırı Analiz Sistemi
- · Risk Değerlendirmesi ve Yönetimi

5-Hangi temel kavramın anlamı doğru olarak verilmiştir?

• Exploit: Arka Kapı



- Worm: Truva Atı
- Spyware: Ağ İzleyici
- · Wisdom: Öz Bilgi

31-Ağ cihazlarının aksaklıklarını bulması ile ünlenen yazılım hangisidir?

- Shadow Security Scanner
- Acunetix Vulnerability Scanner
- GFI Lan Guard Network Security Scanner
- Nmap
- Net Gadgets

34-Yakın tarihin en büyük siber saldırılarından biridir. İran nükleer santrallerini hedef alsa da birçok ülke etkilenmiştir. Bu saldırı hangi

isimle bilinir?

STUNNET

39- snort saldırı tespit sisteminde paket analizi için kullanılan

kütüphane nedir?

• Şifre Çözme

Steganografi

Veri Üretme

Veri Kurtarma

• Veri İmha Etme

23-Hangisi adli bilişim görev alanlarından biri değildir?