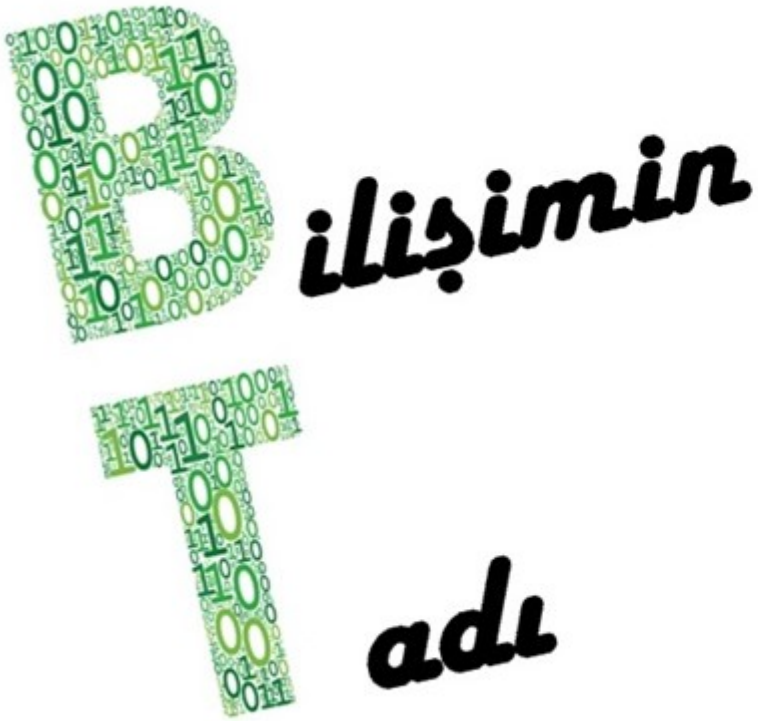

–beş

Bilgi lezzetlidir!

“Bilişimin Tadı” leziz bir BT testi

Umarız hem eğlenir hem öğrenirsiniz!

Bülent Yücesoy

2019

BU KİTAP SINAV TİPİ SORULAR İÇERSE DE SINAV KİTABI DEĞİLDİR, BİR KİŞİSEL GELİŞİM KİTABIDIR.

- Bu kitap sadece bir kişisel gelişim kitabıdır, sınav kitabı değildir.
  Bu kitabın ana amacı, size bazı anahtar kelimeler vererek olası yeni şeyler öğrenmenize yardımcı olmaktır. Sınav biçimi sorular sadece kitap anlatım yöntemi olarak seçilmiştir.
- Eğer siz de sadece yeni şeyler öğrenme amacındaysanız, soruların hiçbirinin puanı yoktur, soruları cevaplamak için süre limitiniz de yoktur. Sorulari anlamaya çalışmak ve cevaplarla yeni şeyler öğrenmek en önemlisidir. Soruları doküman veya internet kullanarak cevaplayabilirsiniz. Soruları hiç anlamaya çalışmadan direkt internette arama yolunu seçmenizi önermeyiz çünkü bu şekilde kişisel gelişim için faydası azalacaktır.
  ⇨ Fakat eğer soruları sınav şeklinde çözmek isterseniz de aşağıdaki sınav kurallarını okuyunuz.
- Keyifli çalışmalar ☺

SINAV ŞEKLİNDE SORU ÇÖZMEK İSTERSENİZ DE KURALLAR AŞAĞIDADIR

- Bu kitapta 50 soru vardır. Her soru 2 puan değerindedir.
- Toplam sınav süresi 75 dakikadır. Sınav geçme notu 100 üzerinden en az 70 tir.
- Sınav doküman veya internet kapalı bir sınavdır.
- Sorularda bir veya daha fazla cevap olabilir.
  Sorular her zaman "**bütün uygun seçenekleri seçiniz"** diyecektir.
  Sorular hiçbir zaman "**n tane cevap seçiniz (n= doğru cevap sayısı) "** demeyecektir.

PUANLAMA

Diyelim ki bir soruda 5 seçenek var. (a,b,c,d,e) Doğru cevap da "a" ve "c" olsun Soru 2 puan olmasi gerektiği için, a ve c seçenekleri BİR PUAN olacaktır, b-d-e de EKSİ BİR PUAN olacaktır.

* Soruyu cevapsız bırakırsanız – puan = 0
* Sadece "a" olarak işaretlerseniz – puan=1
* a-b-c olarak işaretlerseniz – puan = 1+ (-1) + 1= 1
* b-d-e olarak işaretlerseniz – puan= (-1) + (-1) +(-1) = -3
* a-b-c-d-e olarak işaretlerseniz –puan = 1+ (-1) +1 + (-1) + (-1) = -1

Başka örnek şöyle verilebilir:

Bir soruda 4 seçenek var diyelim. (a-b-c-d) Doğru cevaplar da diyelim ki (a,b,d) olsun.

Bu durumda doğru her seçenek 0,66 puan olacak,yanlış her seçenek de "-0,66 puan" olacak.

- Keyifli sınavlar ☺

OLASI TÜRKÇE HATALARI

- Bazı kelimeler, terim olarak düşünülüp bilerek çevrilmemiştir.

- Türkçe dil bilgisi hataları varsa affınızı dilerim, hataları iletirseniz düzeltmeye çalışacağım, sağolun.

ÇÖZÜMLER

- **Çözümler,kısa özet cümleler olarak verilmiştir,bütün detayına kadar anlatım yapılmamıştır.**
- Bütün detayları merak ediyorsanız bunu araştırıp bulmak sizin ödeviniz.
- Eğer merak edip araştırırsanız bu kitap hedefine ulaşmış olacak,kişisel gelişime katkı sağlayacak.

YORUMLAR

- Bu ücretsiz hobi aktivitesine dair bütün yorumlarınız için teşekkürler (bulent.yucesoy@gmail.com)
- **"Bilişimin Tadı" serisi devam edecek. Eğer yorumlarınız olursa hepsini dikkate almaya çalışacağım.**
- Yorumların özetini internet sayfamda yayınlayacağım. (**http://web.itu.edu.tr/~yucesoyb/books**)

Bülent Yücesoy, İstanbul , 2019

Soru-1: Hangisi blok temelli çalışır?

a. CIFS
b. SMB
c. NFS
d. iSCSI

Soru-2: VoIP çözümlerinin klasik telefon hatlarına göre bariz üstün olmadığı nokta ne(ler)dir?

a. Daha güvenli olması
b. Daha fazla esnek özellik barındırması
c. Daha ucuza maliyet
d. Daha az gürültü taşıması

Soru-3: Hangi dosya sistemi diğerlerinden farklı bir kategoride değerlendirilir?

a. LustreFS
b. GFS2
c. GPFS
d. GlusterFS

Soru-4: Bütün doğru "saldırı/koruma" eşleştirmelerini seçiniz.

a. DNS DDoS / Anycast DNS
b. Arp değiştirme / DHCP takip etme
c. IP değiştirme / Dönüş yoluna göre filtreleme
d. Ağdaki paket baskınları / IDS

Soru-5: DNS ile ilgili bütün doğru ifadeleri seçiniz

a. IDN sayesinde DNS isimlerinde dilinize ait özel karakterleri kullanabilirsiniz
b. DNS sunucuları round-rubin kayıtlar arasında ağ sıralaması seçimi yapabilir
c. DNS Scavenging sadece Microsoft DNS sunucularda bulunan bir özelliktir.
d. Dinamik DNS kayıt güncellemesi kontrollü sekilde incelenmelidir.

Soru-6: Bütün doğru ifadeleri seçiniz

a. Spanning bir porttaki trafiği başka portlara da kopyalar.
b. Span portunun ucuna IDS cihazı bağlamak güvenlik açısından iyi olacaktır.
c. RSPAN diye bir opsiyon da mevcuttur.
d. Spanning ağdaki sadece belli bir VLAN için de yapılabilir.

Soru-7: Bütün uzaktan bağlantı ve destek hizmeti programlarını seçiniz.

a. Bomgar
b. Shared Shell
c. Webex
d. Teamviewer

Soru-8: IBM AIX ile ilgili bütün doğru ifadeleri seçiniz

a. AIX rpm komutu rpm.rte kurulunca gelir.
b. Periyodik olarak /usr/sbin/updtvpkg komutu çalıştırmak sisteme zarar vermez
c. "/usr/sbin/updtvpkg" hata verirse "rpm --rebuilddb" çalıştırabilirsin
d. "/usr/sbin/updtvpkg" komutu LPP kurulumları sonrası RPM DB yi günceller.

Soru-9: Hangisi VLAN ile ilişkili bir protokol değildir?

a. GVRP
b. MVRP
c. VRRP
d. VTP

Soru-10: TCP statü leri ile ilgili bütün doğru ifadeleri seçiniz

a. SYN_SENT bilgisi genelde çok kısa süreli görülür, güvenlik duvarı problemine işaret eder.
b. TIME_WAIT statusu uygulama ölçeklenebilirliğini olumsuz etkileyebilir.
c. Uygulamada bağlantı havuzu devreye almak TCP_WAIT sorunlarını çözebilir.
d. TIME_WAIT statü bilgisi en fazla 2 x MSL süresi kadar sürer.
e. CLOSE_WAIT uzak sistemin bağlantıyı kapattığını gösterir. TIME_WAIT ise yerel sistemin bağlantıyı kapattığını gösterir.

Soru-11: Loglama ile ilgili bütün doğru ifadeleri seçiniz.

a. /etc/syslog.conf da log yönlendirmenin yapılacağı hedef port yazılabilir.
b. rsyslog TCP,UDP ve RELP protokollerini destekler
c. rsyslog loglar için TLS sifreleme destekler
d. rsyslog da logları uzak sisteme yollamadan önce modüller devreye alıp data işleme yapabilirsin (ornegin, kritik data maskelenebilir)

Soru-12: Hangi DNS kaydı e-posta imzalamada kullanılır?

a. DKIM
b. DMARC
c. SPF
d. TSIG

Soru-13: DNS DMARC kaydının ön gereksinimleri nelerdir?

a. DKIM DNS kaydı yapılmış olmalı
b. SPF DNS kaydı yapılmış olmalı
c. DNSSEC kullanılıyor olmalı
d. DMARC da sıradan bir DNS kaydıdır, herhangi bir ön gereksinimi yoktur

Soru-14: Hangisi hibrit (hem işletim sistemi hem ağ) IDS sistemidir?

a. SNORT
b. OSSEC
c. PRELUDE

Soru-15: Bütün doğru ifadeleri seçiniz

a. Çalışma seviyelerinin Linux/Solaris/AIX te farklı anlamları olabilir.
b. Şu vea hangi seviyede çalışıldığı "who -r" ile görülebilir.
c. Çalışma seviyeleri arasında "init" komutu ile geçiş yapılabilir.
d. Linux teki tek kullanıcı modu, Windows un Güvenlik Modu ile aynıdır.

Soru-16: Bütün doğru ifadeleri seçiniz

a. Takip sistemi, auid yapısını devreye alır, kullanıcı takibi için önemlidir.
b. Takip sistemi, log yazmak için syslog ürünlerini kullanmaz.
c. SELinux ün erişim izin/ret datası Access Vector Cache isimli önbellektedir.
d. SELinux bütün loglarını, takip sistemine yazar.

Soru-17: Bütün doğru ifadeleri seçiniz

a. Çekirdek panik sorunlarının sebebini bulmak için kdump aktif edilmelidir.
b. En önerilen tavsiye, vmcore dosyalarını merkezi NFS alanlarına kaydetmektir
c. Vmcore dosyalarını analiz edebilmek için crash komutu yüklü olmalıdır
d. Mevcut çekirdek ile aynı sürümde kernel-debuginfo paketi de kurulu olmalıdır.

Soru-18: Linux “swappiness” ın Oracle Solaris teki karşılığı nedir?

a. user_reserve_hint_pct
b. swapfs_reserve
c. virtual_swap
d. karşılığı parametre yoktur

Soru-19: “DevOps Assembly Lines” hangi noktalarda “DevOps Pipelines” dan iyidir?

a. “Assembly lines” ile YML tabanlı bir dil ile akışın kendisi de programlanabilir
b. “Assembly lines” ile daha az interaktiflik gerekir, süreçler daha çevik işler
c. “Assembly Lines” ile Is Zekası (BI) uygulamalarını birleştirip süreçlerinde sürekli gelişim (continous improvement) yapabilirsin.
d. “Assembly Lines” ile eski-yeni bütün yazılımlar akış içinde daha net görülebilir

Soru-20: AOP programlamada “ASPECT” leri bulmak için neler dikkate alınmalıdır?

a. Concerns
b. Pointcuts
c. Join Points
d. Dependencies

Soru-21: Hangileri CRI (Container Runtime Interface) ile birlikte çalışmaz?

a. dockershim
b. frakti
c. rkt
d. runc

Soru-22: Hangileri DevSecOps taki saldırı-modelleme gereçlerinden değildir?

a. StackStorm
b. CAPEC
c. STIX
d. SeaSponge

Soru-23: DevOps un amaçları arasında olmayanları seçiniz

a. Süreçleri iyileştirmek, hızlveırmak
b. Geri besleme döngüleri kurmak
c. Sürekli deneyim ve öğrenim kültürü kazveırmak

Soru-24: Hangi komut(lar) farklı bir kategoride kıyaslama yapmaktadır?

a. time cat /proc/cpuinfo |grep proc|wc -l|xargs seq|parallel -N 0 --gnu echo "2^2^20" '|' bc
b. openssl speed des des-ede3 dsa2048 hmac idea-cbc md5
c. md5sum /dev/urveom
d. mkdir -p /1; mount tmpfs -t tmpfs /1; dd if=/dev/zero of=/1/data_tmp bs=1M count=512

Soru-25: Active Directory Domain servisi içinde olmayan bölümü bulunuz.

a. Şema bölümü
b. Domain bölümü
c. Yapılveırma bölümü
d. Replikasyon bölümü

Soru-26: Hangileri bir CPU ailesinin ismi değildir?

a. spark
b. power
c. nehalem
d. epyc

Soru-27: Bütün doğru ifadeleri seçiniz

a. Yazılımcılar genelde paralel programlamada PTHREADS kullanırlar.
b. SMT/HT donanım iplik modellerinde PTHREADS yazılımlar daha iyi çalışır.
c. CMT donanım iplik modellerinde OPENMP yazılımlar daha iyi çalişır.
d. Her donanımda her yazılım iyi çalışır, donanım-yazılım eşleşmesine gerek yoktur.

Soru-28: Bütün UNIX/Linux derleyicileri seçiniz.

a. cc
b. xlc
c. g++
d. cmp

Soru-29: Aynı ağda hem TCP hem UDP yoğun trafik olursa ne(ler) gerçekleşir?

a. Ağda tıkanma
b. Paket kayıpları
c. TCP açlığı
d. UDP üstünlüğü

Soru-30: Donanım arızaları ile ilgili olmayan terim(ler)i seçiniz

a. MTBF
b. MTTR
c. MTTF
d. FIT
e. FRC

Soru-31: "oc create" komutu hangi dosya biçimlerini destekler?

a. CSV
b. XML
c. YML
d. JSON

Soru-32: Iletim katmanı paket baskınlarını engelleyen Linux Qdisc katmanı yöntemlerini seçiniz

a. pfifo_fast
b. sqf
c. fq_codel
d. bql

Soru-33: Redhat Linux te ağ adaptörü aktif olduktan hemen sonra komut çalıştırılmasına imkan tanıyan betik ismi nedir?

a. /sbin/ifup-after
b. /sbin/ifup-post
c. /sbin/ifup-local
d. /sbin/ifup-then

Soru-34: Ağ problemi varken hangi Linux komutları yardımcı olabilir?

a. sar -n EDEV
b. netstat –s
c. ethtool -S ethX
d. dropwatch -l kas

Soru-35: Bir ağ için LFN yorumunu yapabilmek hangi parametrelerin bilinmesine bağlıdır?

a. RTT (saniye)
b. RTD (saniye)
c. Ağ hattı genişliği (bit/ saniye)
d. Maksimum düğüm sayısı

Soru-36: Bütün doğru ifadeleri seçiniz

a. icmp TCP çalışabilir
b. icmp UDP çalışabilir
c. icmp paketin eriştiğini kesinlikle garanti eder.
d. icmp IP datagramlar içinde enkapsülasyon ile çalışır
e. icmp isteklerine "tampon bellek dolu" hatası alabilirsiniz.

Soru-37: "------ as-a-service" hizmetini satın alabilirsiniz.

a. SD-LAN
b. SD-PAN
c. SD-WAN
d. SD-MAN

Soru-38: Hangileri tehdit modelleme tekniklerinden değildir?

a. STRIDE
b. DREAD
c. Saldırı ağaçları
d. RPEDA

Soru-39: Bütün doğru ifadeleri seçiniz

a. IPFIX , Netflow versiyon 7 tabanlı bir stvearttır
b. IPFIX paket iletimi için SCTP protokolünü kullanır.
c. SCTP protokolünde TCP ve UDP den gelişkin özellikler vardır.

Soru-40: Bütün DDoS saldırı algılama gereçlerini seçiniz.

a. Netflow
b. FastNetMon
c. Learn2Ban

Soru-41: Hangisi CVSS stveardındaki zaafiyet noktalarından değildir?

a. Saldırı vektörü
b. Saldırı karmaşıklığı
c. Gerekli ayrıcalıklar
d. Zaafiyet programının olgunluğu

Soru-42: Yeni nesil güvenlik duvarları, klasik 5'li ifade haricinde neleri kullanır?

a. Uygulama ismi
b. Kullanıcı kimliği
c. Itibar

Soru-43: bütün doğru ifadeleri seçiniz

a. PKI sadece isimleri sertifikalara eşleştirir.
b. SPKI ilave olarak yetkileri de sertifikalara eşleştirir
c. SPKI daki iptal süreçleri PKI dan daha deterministtir.
d. SPKI da X509 yerine S-IFADELERI kullanılır

Soru-44: Security Services Markup Language (S2ML) hangi altyapılarla çalışabilir?

a. SOAP
b. OAG
c. MIME
d. ebXML

Soru-45: Sanal Ölüm zinciri kaç adımdan oluşur?

a. 5
b. 6
c. 7
d. 8

Soru-46: Hangisi sanal ölüm zinciri adımlarından değildir?

a. Keşif
b. Silahlanma
c. C2
d. Terminasyon

Soru-47: Hangileri sanal ölüm zincirindeki silahlanma gereçlerinden değildir?

a. metasploit
b. luckystrike
c. veil altyapısı
d. Hiçbiri

Soru-48: Ihlal algılama'nın Elmas modeline ait bütün bileşenleri seçiniz

a. Altyapı
b. Fonksiyonlar
c. Düşmanlar
d. Mağdurlar

Soru-49: Ihlal algılamanın Elmas modeline göre düşmanlar mağdurlara saldırıda neleri kullanır?

a. Altyapı
b. fonksiyonlar
c. Meta-fonksiyonlar

Soru-50: Bir sunucuda çalışan uygulamaları hangi yöntemlerle algılayabilirsin?

a. nmap taraması
b. nbar gereçleri
c. internet sitesi vekil sunucuları
d. katman-7 güvenlik duvarları

ÇÖZÜMLER

Çözüm-1: d
Çözüm-2: a
Çözüm-3: GlusterFS ölçeklenebilir ağ dosya sistemi, diğerleri kümeleme dosya sistemi
Çözüm-4: hepsi doğru
Çözüm-5: hepsi doğru
Çözüm-6: hepsi doğru
Çözüm-7: hepsi doğru
Çözüm-8: hepsi doğru
Çözüm-9: c
Çözüm-10: hepsi doğru
Çözüm-11: hepsi doğru
Çözüm-12: a
Çözüm-13: a ve b
Çözüm-14: snort NIDS, ossec HIDS, prelude hibrit
Çözüm-15: hepsi doğru
Çözüm-16: hepsi doğru
Çözüm-17: hepsi doğru
Çözüm-18: d
Çözüm-19: hepsi doğru
Çözüm-20: a,b ve c
Çözüm-21: runc, cri üzerinde çalışamaz, cri ye alternatif bir ortam runc.
Çözüm-22: StackStorm otomasyon aracıdır
Çözüm-23: hepsi doğru
Çözüm-24: a-b-c işlemci kıyaslaması, d bellek kıyaslaması, cevap D.
A çoklu iplik paralel çalışarak işlemci test eder, B-C tek iplik çalışır
Çözüm-25: d
Çözüm-26: spark big data bileşeni, sparc cpu ailesi.
Çözüm-27: a,b ve c
Çözüm-28: a,b ve c derleyicidir.
Çözüm-29: hepsi aynı durumu ifade eden terimlerdir, hepsi gerçekleşir
Çözüm-30: FRC diye bir şey yok, diğerleri var.
Çözüm-31: YML ve JSON destekleniyor oc create komutunda
Çözüm-32: b ve c iletim katmanındaki paket baskınlarını çözer.
Çözüm-33: ifup-local betiği isteneni yapar.
Çözüm-34: hepsi ağ sorunlarına dair paket kayıpları,hatalar vb şeklinde bilgi verir
Çözüm-35: a,b ve c yardım eder. A ve B zaten aynı kavramın farklı isimleridir.
Çözüm-36: d ve e doğrudur
Çözüm-37: c
Çözüm-38: RPEDA diye bir şey yoktur.
Çözüm-39: b ve c doğrudur. IPFIX Netflow versiyon 9 ile çıkmıştır.
Çözüm-40: hepsi doğru
Çözüm-41: a,b ve c doğrudur. D geçici (temporal) metrik olarak tanımlanmaktadır.
Çözüm-42: hepsi doğru
Çözüm-43: hepsi doğru
Çözüm-44: S2ML bütün opsiyonlarla çalışır
Çözüm-45: sanal ölüm zincirinin 7 aşaması vardır
Çözüm-46: sanal ölüm zincirinde terminasyon diye bir aşama yoktur.
Çözüm-47: Hepsi geçerli silahlanma yöntemleridir, dolayısıyla doğru cevap D oluyor
Çözüm-48: Hepsi elmas modelinin bileşenidir.
Çözüm-49: Düşmanlar, mağdurlara ulaşmak için altyapıyı ve fonksiyonları kullanır.
Çözüm-50: Bütün gereçler, bir sunucuda çalışan uygulamaları algılayabilir.

Bulent Yucesoy 16 Nisan 1982 de Ankara'da doğdu.

İlkokul ve ortaokulu İzmir'de okudu. (1988-1996)

Fen Lisesi sınavını kazanıp İzmir Fen Lisesini bitirdi.(1997-2000)

ÖSS 2000 ile İTÜ Bilgisayar Müh. Kazveı. (2000-2004)

Bilgisayar mühendisliğini sevdi ve aynı bölümde yüksek lisans da yaptı. (2004-2007)

Yüksek lisansını yaparken bir yvean da İTÜ Bilgi İşlem Daire Başkanlığında sistem yöneticisi olarak çalıştı.
(www.bidb.itu.edu.tr).

Askerlik görevini yaptıktan sonra 2 yıl KoçNet Telekom AŞ de (sonra Vodafone satın aldı) çalıştı. (2008-2010).

2010 yılından beridir de Garanti Teknoloji'de çalışıyor.
(www.garantiteknoloji.com.tr)

Bülent detayları sever, hayatın gizli ve güzel tatlarının ayrıntılarda saklı olduğunu düşünür.

Bülent'in sevdiği 3 şey: Eşi İpek, Oğlu Çağan ve yeni şeyler öğrenmek (Bülent'e göre yeni şeyler öğrenmek hayata lezzet katar.)

Bu kitap yeni şeyler öğrenmeyi seven insanlar içindir.

Umarız kitabı beğenirsiniz ve size yeni bilgiler katar.

Bütün yorumlarınızı bulent.yucesoy@gmail.com adresine gönderebilirsiniz.

Bülent'in inveığı felsefeyi Ulu Önder Atatürk'ün muhteşem bir sözü ile özetleyebiliriz. Bu söz, bütün Ülkeler ve bütün insanlar için geçerlidir.

" Vatanını en çok seven, görevini en iyi yapandır."