–five

Information is delicious !

“Information Taste” is a tasty IT test.

Hope you learn new things & enjoy !

Bülent Yücesoy

2019

THIS BOOK HAS EXAM-LIKE FORMAT, BUT IT IS NOT AN EXAM , IT IS JUST A BOOK !

- Don't get surprised, it is really just a book, it is not an exam !
The main aim of this book is mentioning some key topics and helping you learn more & wonder more.
This book is not intended to make you a suffering exam.
Notes are preferred to be given in exam format, so exam is just a format, that's all.
If you agree this concept, then there are no question points, no exam duration limit etc.
You will decide how to answer the questions. (with internet or without internet)
Just try to understand and try to answer, don't google immediately from the very first beginning.
➔ But if you want answering this test-book as an exam, you can read criterias below.
- Happy testing :)

IF YOU WANT ANSWERING THIS TEST-BOOK AS AN EXAM, YOU CAN READ CRITERIAS BELOW

- This book has 50 questions. So all true options in a question have a total point of 2.
- Total exam duration is 75 minutes. Passing score is at least 70 of 100.
- Exam is documentation/internet closed exam.
- Questions have one or many answers. Questions will ALWAYS say "SELECT ALL THAT APPLY".
Questions will NEVER say "SELECT n THAT APPLY (n = total true option number)"

SCORING ALGORITHM

Think that a question has 5 options (a,b,c,d,e) but answer set is "a" and "c".
Question must have totally "2 points", so "a" is "1 point" + "c" is "1 point".
This makes score of all false options (b,d,e) each having "-1 point" separately.

* If you dont give any answer (empty question) - your score is already "0 point"
* If you just answer "a"-> your score is "1 point"
* If your answers are "a,b,c" -> your score is = 1+ (-1) + 1 = "1 point"
* If your answers are "b,d,e" -> your score is = (-1) + (-1) + (-1) = "-3 points"
* If your answers are "a,b,c,d,e" -> score = 1 + (-1) + 1 + (-1) + (-1) = "-1 point"

Similar example can be given like below
4 options (a,b,c,d) exist for a question. 3 is correct. (a,b,d)
This makes each true option "0,66 point" , which makes any false option (c) having each "-0,66 point"
You can calculate your score accordingly.
- Happy examining :)

SOLUTIONS

- Solutions are given but they are short descriptions, not whole all story.
It is your homework to examine in detail if you wondered the rest of story.
If you really wondered something and examined it, this book will succeed its mission.

COMMENTS

- All comments, advises are welcomed in this non-profit hobby activity (**bulent.yucesoy@gmail.com** **)**
- "Information taste" series will continue annually. I will care all comments. (thanks if you comment)
- I will publish your summarized comments in my web site. **(http://web.itu.edu.tr/~yucesoyb/books**)

Bulent Yucesoy, Istanbul , 2019

Question-1: Which one works block-based?

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

Question-2: VoIP solutions are not exactly better than traditional subscriber lines on which areas?

a. Being more secure
b. Being more flexible
c. Having less cost
d. Being more converged

Question-3: Which file system is in a different class?

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

Question-4: Select all correct "attack/protection" matchings

a. DNS DDoS / Anycast DNS
b. Arp Spoofing / DHCP Snooping
c. IP Spoofing / Reverse Path Filtering
d. Network Packet Floods / IDS

Question-5: Select all true about DNS

a. IDN provides your language's special characters in DNS names
b. DNS servers may implement netmask ordering among multiple round-rubin record response.
c. DNS Scavenging is a special feature only available in Microsoft DNS servers
d. Dynamic DNS record update feature must be handled carefully.

Question-6: Select all true statement(s)

a. Spanning makes network traffic mirroring to a specific port
b. An IDS device can be connected to span port for security
c. There is also another option called RSPAN
d. Spanning network traffic can also be done for a specific source VLAN

Question-7: Select all remote support services tools

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

Question-8: Select all true about IBM AIX

a. AIX rpm command comes with rpm.rte installation
b. you can run "/usr/sbin/updtvpkg" periodically, it does not harm anything
c. if "/usr/sbin/updtvpkg" gives error, you can run "rpm --rebuilddb"
d. "/usr/sbin/updtvpkg" informs RPM DB about AIX LPP installations.

Question-9: Which is not VLAN related network protocol

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

Question-10: Select all true about TCP states

a. SYN_SENT stays short-time and generally shows a firewall block
b. TIME_WAIT can affect application scalability
c. Application connection pooling can solve TIME_WAIT issues
d. TIME_WAIT stays there for a period that is 2 x Maximum Segment Lifetime in duration.
e. CLOSE_WAIT tells remote node closed first. TIME_WAIT tells local node closed first.

Question-11: Select all true about logging

a. you cant specify remote log forwarding port at /etc/syslog.conf
b. rsyslog supports TCP,UDP and RELP protocols
c. rsyslog supports TLS encryption for logs
d. you can enable modules at rsyslog (eg: data masking) before sending logs to remote

Question-12: Which DNS record is used for mail signing?

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

Question-13: Which are prerequisites for DMARC DNS record?

a. DKIM DNS record
b. SPF DNS record
c. DNSSEC must be used
d. There is no prerequisite for DMARC DNS record

Question-14: Which is a hybrid (both host and network) IDS system

a. SNORT
b. OSSEC
c. PRELUDE

Question-15: Select all true

a. Run levels have different meaning at Linux/Solaris/AIX
b. You can see your current run level with "who -r" command
c. you can switch between run levels with "init" command
d. Linux single user mode is same Windows Safe Mode.

Question-16: Select all true

a. auditing enables auid, which is critical for user tracking
b. auditing does not use any kind of syslog mechanism
c. SELinux access allow/disallow data is cached inside Access Vector Cache.
d. SELinux logs its events into auditing log files.

Question-17: Select all true statement(s)

a. kdump must be configured to analyze kernel crash issues
b. best practice is to save vmcore files in a central NFS location
c. crash command must be installed to analyze vmcore outputs
d. kernel-debuginfo package must also be installed at same kernel level

Question-18: Which is Oracle Solaris correspondant of Linux “swappiness”

a. user_reserve_hint_pct
b. swapfs_reserve
c. virtual_swap
d. correspondant parameter does not exist

Question-19: Select all beter sides of “DevOps Assembly Lines” compared to “DevOps Pipelines”

a. Assembly lines also include workflow-as-code with a YML based language
b. Assembly lines are more agile due to having less human interaction dependency
c. You can integrate Business Intelligence (BI) applications with Assembly Lines to create "Continous Improvement" for your total processes
d. Your all legacy and modern applications can be mixed inside Assembly Lines to create a better visibility.

Question-20: What are keypoints to determine ASPECTS in AOP programming?

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

Question-21: Which is not an implementation that can work with CRI (Container Runtime Interface) ?

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

Question-22: Which is not an attack-modelling tool used in DevSecOps

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

Question-23: Which statement(s) are what DevOps aim?

a. Accelerate the flow
b. Amplify Feedback Loops
c. Culture of Continual Experimentation and Learning

Question-24: Which is a different category bencharking command

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/urandom
d. mkdir -p /1; mount tmpfs -t tmpfs /1; dd if=/dev/zero of=/1/data_tmp bs=1M count=512

Question-25: Which is not a partition inside Active Directory Domain Service

a. Schema partition
b. Domain partition
c. Configuration partition
d. Replication partition

Question-26: Which is not a CPU family

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

Question-27: Select all true statement(s)

a. Developers generally use pthreads in paralel programming
b. SMT/HT hw threading models fit better with pthreads codes
c. CMT hw threading model fits better with openmp codes
d. Any hw can run any software code perfect

Question-28: Select all UNIX/Linux compiler(s)

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

Question-29: Which may ocur when heavy TCP-traffic and UDP-traffic exist in same subnet

a. congestion
b. packet drops
c. tcp starvation
d. udp dominance

Question-30: Which is not a term related to hardware failures?

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

Question 31: Which file formats can be used with “oc create” command?

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

Question-32: Select all Linux Qdisc layer option(s) that prevent transport layer flood problem

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

Question-33: which is the script in Redhat Linux that can be immediately run after network interface goes up?

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

Question-34: which below linux commands may help when there is network performance problem

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

Question-35: Which values must be known for a network to tell if it LFN or not?

a. RTT (second)
b. RTD (second)
c. Bandwith (bit/ second)
d. max hop count

Question-36: Select all true statement(s)

a. icmp works tcp
b. icmp works udp
c. icmp guarantess package delivery
d. icmp works with encapsulation inside ip datagrams
e. you can get "buffer full" response to your icmp

Question-37: You can buy ------ as-a-service.

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

Question-38: Which is not Threat Modelling Technique

a. STRIDE
b. DREAD
c. Attack trees
d. RPEDA

Question-39: Select all true statement(s)

a. IPFIX is a flow standard based on Netflow version 7
b. IPFIX uses SCTP for packet transport
c. SCTP has more advanced features than TCP and UDP

Question-40: Select all DDoS detection tools

a. Netflow
b. FastNetMon
c. Learn2Ban

Question-41: select criterias inside exploitability metrics, of which considered as base metric groups of CVSS

a. attack vector
b. attack complexity
c. privileges required
d. exploit code maturity

Question-42: Next-gen firewalls widen classical 5-tuple firewall rules by which fields?

a. application
b. user identity
c. reputation

Question-43: select all true statements

a. PKI just links NAMES to CERTS
b. SPKI additionally links AUTHORIZATIONS to CERTS
c. SPKI REVOCATION is more deterministic than PKI revocation
d. SPKI uses S-EXPRESSIONS syntax instead of X509

Question-44: Security Services Markup Language (S2ML) works with which frameworks

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

Question-45: How many steps Cyber Kill Chain include?

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

Question-46: which is not a phase of Cyber Kill Chain

a. Reconnaissance
b. Weaponization
c. C2
d. Termination

Question-47: which is not cyber security weaponization tool?

a. metasploit
b. luckystrike
c. veil framework
d. none

Question-48: what are the required components of Intrusion Analysis Diamond Model.

a. Infrastructure
b. Capabilities
c. Adversary
d. Victim

Question-49: Adversaries use which one(s) to access victims due to Diamond Intrusion Model

a. Infrastructure
b. Capabilities
c. Meta-features

Question 50: Which can identify application running on a server?

a. nmap scanning
b. nbar tools
c. web proxy servers
d. Layer-7 firewalls

SOLUTIONS

Solution-1: d
Solution-2: a
Solution-3: Gluster is scalable network file system, others are cluster file systems
Solution-4: all true
Solution-5: all true
Solution-6: all true
Solution-7: all true
Solution-8: all true
Solution-9: c
Solution-10: all true
Solution-11: all true
Solution-12: a
Solution-13: a and b
Solution-14: snort is NIDS, ossec is HIDS, prelude is hybrid
Solution-15: all true
Solution-16: all true
Solution-17: all true
Solution-18: d
Solution-19: all true
Solution-20: a,b and c
Solution-21: runc is alternative to cri. others work with cri
Solution-22: StackStorm is automation tool
Solution-23: all true
Solution-24: a-b-c are cpu benchmarks. d is memory benchmark.
a is multi-threaded, b and c are single threaded
Solution-25: d
Solution-26: spark is big data component, sparc is cpu family
Solution-27: a,b and c
Solution-28: a,b and c are compilers.
Solution-29: all reference same issue
Solution-30: there is nothing called FRC, all others exist
Solution-31: YML and JSON are supported
Solution-32: b and c solve transport layer flood
Solution-33: ifup-local file solves this requirement
Solution-34: all help with error counters, drop counts etc..
Solution-35: a,b and c help. a and b are same thing
Solution-36: d and e are correct
Solution-37: c
Solution-38: there is nothing called RPEDA
Solution-39: b and c are correct. IPFIX is Netflow version 9
Solution-40: all true
Solution-41: a,b and c are correct. d is temporal metric.
Solution-42: all true
Solution-43: all true
Solution-44: S2ML works with all options
Solution-45: Cyber Kill Chain includes 7 options.
Solution-46: There is no phase called Termination
Solution-47: all are weaponization tool, so answer is D
Solution-48: all are Diamon Model components
Solution-49: adversaries use infrastructure and capabilities
Solution-50: all can identify applications running on a server

Bulent Yucesoy was born in Ankara at 16.04.1982.

He went to elementary school and middle school at Izmir. (1988-1996)

He later on was accepted to Izmir Science High School. (1997-2000)

He won university and entered ITU Computer Engineering Department. (ITU = Istanbul Technical University)

He loved computer engineering and continued at same university for his master degree (2004-2007) after he finished bachelor. (2000-2004)

While making master education, he also worked at university IT Office (www.bidb.itu.edu.tr).

After his military service, he worked for 2 years at Kocnet Telecom (Vodafone acquired it) company (2008-2010).

Afterwards he joined Garanti Technology and he is working there since 2010. (www.garantiteknoloji.com.tr)

He likes details, thinks that devil hides inside details.

He loves his wife Ipek, his son Cagan and lastly he loves learning. (that's why he thinks information is delicious.)

This book is for people who also loves learning.

Hope you also like the book.

You can send comments to bulent.yucesoy@gmail.com

Let’s summarize Bulent’s philosophy with a wonderful Ataturk’s saying. It is valid for all the world, all the people;

“If you love your country, do your best in your job”