

Chapter 1 Q and A

Q1 cyber security?

Answer: A

Solution ① A. tech, stand, polic. manage.
keep secure ✓

② B: tech X only 绝对

③ C: just best X 绝对

Q2: important?

Answer: A

Solution ① high tech. organ depend ✓

② hype 炒作 media媒体 X

③ traditional brick → physical attacks X

④ offline X

Q3: three basic cyber security concept

Ans C

Solution: ① Confidentiality 机密性 ✓

Consideration 考虑

Integrity 完整性 ✓

Access 可访问

Availability 可用性 ✓

② CIA 1.1.1. Pr-8

Q4. organ. web sensitive not your fault
consider breach 漏洞

Answer: TRUE

Solution ① not authorized

Q5: verify users trust -

Ans: Authenticity

Solu: 鉴别 from 1.1.5.1 认证

Q6: three stage cycle

plan - protect
- respond

Ans A

45% wrong

Solution planning, protection and response

Q7 consume most time?

Ans: A

Solu: protection → 24h - 全天候

Planning → 开始, 就做好了, 基于不意

Response → under attack 才能时间
Same time

Q 8 How to protection defined

Ans: D

Solu: ① 保护 定义为 基于计划的行动 和 对策制定
不随意、详细分析、评估风险、明确目标、系统化日常运行、定期安全、安全监控、日志管理、应急预案、事后恢复

② tech $\xrightarrow{\text{protect}}$ attack

③ policy prot. → attack

④ All ✓

Q 9 response defined.

Ans: A

Solu: ① recovery

② punish

③ destroy ability

} we don't know who they are
so we can't do that

④ None

Q10 ^{why} understand threat?

Ans: A

Solu: ① 不知无防 ✓

② 业务需求 无关 ✗

③ policy ✗ 无关

④ None

Q11 Auto. speed. action of attack

Ans: TRUE

Q12: attacks is?

Ans: E

Solu: ① A ✓ B ✓ C ✓ D ✓ E ✓

Q13: 伪造信息, 声称自己是 XX

Ans: A

Solu: ① Masquerading 伪装

Eavesdropping 窃听

Spoofing

欺骗 → eg. computer using
diff IP address

None

Q14 Malware

Ans: True

Q15: Distinguish between viruses & worms

Ans: A

Solu: ① Virus host need
worms don't need

From 1.2.2.1.1
P1-35

② B X C X D X

Q16 interruption or degradation called
中断 降低

Ans: A

Q17: virus spread most

Ans: A

Solution: ① email ✓

thumb drives: U~~盘~~ ✓

file share programs ✓

downloading ✓

- ② install app not most
- ③ Hacker not virus
- ④ None

Q 18 logic Bomb

Ans B

Solution ① program useful harmful X Trojan.
 ② codes execute ^{time} _{event} ✓ LB
 ③ virus bypasses X virus
 ④ None

Q 19 motivation hackers

Ans E

Solu. ① \$ ✓
 ② Smart → know ✓
 ③ challenge ✓
 ④ bored ✓
 ⑤ All ✓

Q 20 virus / worm payload

Ans B

Solu ① definition

part of code cause damage

Q 21 hacking

Ans B

Q 22 spyware

Ans A

Solu ① spectrum Trojan horse.
范围

gather infor. → attack

② infected x

③ adware x

Q 23 cookies danger?

Ans : A

Solu : ① sensitive → spyware ✓

② legally x

③ past x

④ None x

Q24 social engineering?

Ans: B

Solu: ① definition ✓

trap trick share info.
sensitive

Q25 spam 垃圾邮件

Ans: A

Solu: ① A unsolicited 未经请求 email ✓

② BX CX full

Q26 phishing

Ans: B

Solu: ① AX

B email appears
看似

Q27 social be used access

Ans: A

Solu: ① ask ✓ from P1-45
1.2.2.2.3

② brute force attack password

③ crack