

TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!



Exam : **GB0-540**

Title : Advanced Intrusion
Prevention System
Configuration

Version : DEMO

1. TippingPoint IPS 对应用保护的过滤器分为哪几类？

- A. Attack Protection, Reconnaissance, Security Policy, Informational
- B. Attack Protection, Scan, Security Policy, Informational
- C. Attack Protection, Reconnaissance, Misuser&Abuse, Informational
- D. Attack Protection, Scan, Security Policy, Misuser&Abuse

Answer: A

2. 客户想下载最新的数字疫苗，可以从下列哪个网站获取？

- A. www.huawei-3com.com
- B. www.3com.com
- C. www.huawei.com
- D. www.tippingpoint.com

Answer: D

3. 使用 Web 方式登陆 TippingPoint，每次最多只能同时登录一个用户。

- T. True
- F. False

Answer: F

4. Notification Contacts 包括的组合有（ ）。

- A. SMS + Remote system log + LSM
- B. Remote System Log + Management Console
- C. Management Console + SMS
- D. LSM + Management Console + SMS

Answer: AB

5. TippingPoint 支持单设备管理 LSM 和企业级集中管理 SMS 两种管理架构。

- T. True
- F. False

Answer: T

6. TippingPoint 对 BT 下载进行限流，依靠的是 TippingPoint 的哪种保护功能？

- A. 应用层保护
- B. 基础设施保护
- C. 性能保护

Answer: C

7. TippingPoint 设备支持的网管设备只有 SMS，其它网管设备不支持。

- T. True
- F. False

Answer: F

8. 在 SMS 操作中，当 TippingPoint 检测到接入客户端的非法活动时，SMS 进行基于策略的门限控制，SMS 发送 Trap 到 NMS 或者根据配置执行相应的动作。

- T. True
- F. False

Answer: T

9. 在 CLI 操作中，显示 TippingPoint 配置的命令是（ ）。。

- A. show config
- B. dis config
- C. dis configuration
- D. show configurarion

Answer: D

10. TippingPoint 的优势在于（ ）。

- A. 对第二层到第七层实行全部的检查
- B. 对存在的漏洞提供保护
- C. 实现零时差攻击保护
- D. 防止应用程序和操作系统损坏或宕机

E. 不必紧急实施为危险漏洞打补丁

Answer: ABCDE

11. 网络钓鱼的危害表现在 ()。

- A. 盗取用户的银行卡或者信用卡的帐户的密码，使用户遭受经济上的损失。
- B. 产生大量的 TCP 连接，使网络资源被大量消耗。
- C. 大量占用网络带宽，使其他用户无法正常浏览网页。
- D. 传播大量的病毒到网络上，造成其它设备无法正常使用。

Answer: A

12. 下列选项中，属于 DoS 攻击的有 ()。

- A. TFN
- B. Syn Flood
- C. Land
- D. ICMP Flood

Answer: ABCD

13. 攻击者向目标主机发送源地址和目的地址均为该主机地址的 TCP SYN 报文，并以此来达到攻击目的，这种攻击的名称是 ()。

- A. Smurf
- B. Land
- C. Fraggle
- D. IP Spoofing

Answer: B

14. Smurf 攻击为了达到攻击的目的，采用的攻击手段是 ()。

- A. 伪造一个 SYN 报文，其源地址是伪造的不存在的地址，向受害主机发起连接。
- B. 向同一个子网的主机发送 ICMP 重定向报文，请求主机改变路由。
- C. 发送 ICMP 应答请求报文，该请求的目的地址设置为受害网络的广播地址。
- D. 利用那些在 TCP/IP 堆栈实现中信任 IP 碎片中的报文头所包含的信息来实现自己的攻击。

Answer: C

15. 下面属于泛洪攻击的是（ ）。

- A. ICMP-flood
- B. UDP-flood
- C. TCP-flood
- D. SYN-flood

Answer: ABD

16. 对报文的源地址反查路由表，入接口与以该地址为目的地址的最佳出接口不同的 IP 报文被视为（ ）攻击。

- A. IP Spoofing
- B. Land
- C. Fraggle
- D. ICMP Redirect

Answer: A

17. CodeRed 蠕虫是利用了一个缓冲区溢出漏洞通过 TCP/IP 协议和端口 135 进行传播。

- T. True
- F. False

Answer: F

18. 蠕虫病毒的传播过程一般包括（ ）。

- A. 探测
- B. 渗透
- C. 扎根
- D. 传播
- E. 破坏

Answer: ABCDE

19. DuDu 加速、迅雷等断点传输软件也支持 BT 下载。

T. True

F. False

Answer: T

20. BT 连接建立的过程是：BT 对等协议的二次握手，握手成功后，接着是 TCP 的三次握手，握手成功后，进行数据的传输。

T. True

F. False

Answer: F