i春秋-安全产品原理

原创

zac- 于 2021-10-29 10:48:32 发布 18 收藏

分类专栏： i春秋培训测验 文章标签： 安全

本文链接：https://blog.csdn.net/hkk1151043545/article/details/121029614

第1章：防火墙（FW）

课时1：防火墙的工作原理 已看完 24分钟

4、下列哪项不是防火墙常见的工作方式？ ✓

- A 包过滤
- B 状态监测
- C 透明接入
- D 应用代理

CSDN @zac-

1、防火墙访问控制列表"允许任何流量通过"规则 ✓

- A access-list 1 deny 172.16.4.13 0.0.0.0
- B access-list 2 permit 172.16.0.0 0.0.255.255
- C access-list 3 permit 0.0.0.0 255.255.255.255
- D access-list 3 permit 0.0.0.0 255.0.0.255

CSDN @zac-

5、下列选项中关于ACL规则的匹配原则描述不正确的是？ ✓

- A 防火墙安全规则遵循从上到下匹配的原则
- B 如果所有的规则都没有匹配到，数据包将被丢弃
- C 安全过滤规则只包含源、目的地址和端口
- D 防火墙安全规则匹配时一旦有一条匹配，剩余的都不再进行匹配

2、对于“access-list 101 primit tcp any host 198.78.46.8 eq www”的acl规则理解正确的是？ ✓

A 匹配顺序为101，允许ip为198.78.46.8的主机访问任何外部ip

B 规则强度为101，不允许TCP连接，禁止所有主机对198.78.46.8的www服务进行访问

C 匹配顺序为101，允许TCP连接，所有主机对198.78.46.8的www服务进行访问

D 匹配顺序为101，允许TCP连接，禁止禁止所有主机对198.78.46.8的www服务进行访问

2、网络中使用防火墙起到什么作用? ✓

A 防止电脑报错

B 防止流量异常

C 防止黑客

D 保护内部敏感信息资源,防止内部泄露

6、网络传输五元组以下那个正确?

A 目的端口,源端口,应用层,传输层,物理层

B 原Mac,目的MAC,数据链路层,网络层,会话层

C 目的IP,原IP,协议号,目的端口，原端口,会话层

D 目的IP,原IP,协议号,目的端口，原端口

7、防火墙访问控制列表"允许任何流量通过"规则

一、单选题

1、网络中使用防火墙起到什么作用? ✓

A 防止电脑报错

B 防止流量异常

C 防止黑客

D 保护内部敏感信息资源,防止内部泄露

2、网络传输五元组以下那个正确? ✓

A 目的端口,源端口,应用层,传输层,物理层

B 原Mac,目的MAC,数据链路层,网络层,会话层

C 目的IP,原IP,协议号,目的端口，原端口,会话层

D 目的IP,原IP,协议号,目的端口，原端口

3、对于“access-list 101 primit tcp any host 198.78.46.8 eq www”的acl规则理解正确的是? ✓

A 匹配顺序为101，允许ip为198.78.46.8的主机访问任何外部ip

B 规则强度为101，不允许TCP连接，禁止所有主机对198.78.46.8的www服务进行访问

C 匹配顺序为101，允许TCP连接，所有主机对198.78.46.8的www服务进行访问

D 匹配顺序为101，允许TCP连接，禁止禁止所有主机对198.78.46.8的www服务进行访问

4、防火墙访问控制列表"允许任何流量通过"规则 ✓

A access-list 1 deny 172.16.4.13 0.0.0.0

B access-list 2 permit 172.16.0.0 0.0.255.255

C access-list 3 permit 0.0.0.0 255.255.255.255

D access-list 3 permit 0.0.0.0 255.0.0.255

5、下列关于标准防火墙的描述错误的是? ✓

A 防火墙安全规则遵循从上到下匹配原则，一旦有一条匹配，剩余的规则就不匹配了

B 所有的规则都没有匹配到，数据包将丢弃

C 安全过滤规则主要包含源、目的地址和端口

D 防火墙的主要功能是防止病毒等恶意程序的传输

6、下列选项中关于ACL规则的匹配原则描述不正确的是？ ✓

A 防火墙安全规则遵循从上到下匹配的原则

B 如果所有的规则都没有匹配到，数据包将被丢弃

C 安全过滤规则只包含源、目的地址和端口

D 防火墙安全规则匹配时一旦有一条匹配，剩余的都不再进行匹配

7、下列哪项不是防火墙常见的工作方式？ ✓

A 包过滤

B 状态监测

C 透明接入

D 应用代理

课时2：防火墙应用与发展趋势 已看完 28分钟

1、透明模式和桥模式说法正确的有？ ✓

A 内外网在一个网段内

B 有点是直接串联到链路上,不改变原有的网络IP地址

C 缺点是像玻璃一样,屋内屋外一览无余

D 以上全对

4、下列选项中关于防火墙的透明部署方式描述错误的是？ ✓

A 内外网在一个网段内

B 优点是直接串联到链路上，不改变原有的网络IP地址配置

C 缺点是像玻璃一样，屋内屋外一览无余

D 透明模式即用户可以访问到网络安全设备

1、下列对于下一代防火墙的描述错误的是？ ✓

A 将访问控制对象从网络层、传输层延伸到应用层

B 下一代防火墙能够识别应用和内容

C 下一代防火墙可以限制用户是否能在上班时间访问娱乐社交软件

D 下一代防火墙已经丢弃了传统防火墙的工作模式

4、虚拟化主机安全? ✓

- A 云存储安全,云存储杀毒,访问控制,源数据备份
- B vVirus,vFw,vSwitch,vIDS,运维审计,安全加固
- C 云安全管理平台,SDN+VxLan,安全域划分,网络边界防护,运维审计
- D 温、温度,接地,防静电,消防

CSDN @zac-

私网地址的范围:

A类地址：10.0.0.0～10.255.255.255

B类地址：172.16.0.0 ～172.31.255.255

C类地址：192.168.0.0～192.168.255.255

CSDN @zac-

第2章：入侵检测系统（IDS）

课时1：入侵检测技术就是抓黑客的 已看完 35分钟

1、论文《计算机安全威胁监控与监视》提出的监视入侵活动的思路是 ✓

- A 利用日志作为审计数据监视入侵活动
- B 利用流量作为审计数据监视入侵活动
- C 利用恶意代码作为审计数据监视入侵活动

2、IDS设备部署的关键是 ✓

- A 关键是查杀恶意代码
- B 关键是设备的正确配置
- C 关键是阻断攻击流量
- D 关键是日常安全事件的跟踪与处理

CSDN @zac-

一、单选题

1、IDS设备部署的关键是 ✓

- A 关键是查杀恶意代码
- B 关键是设备的正确配置
- C 关键是阻断攻击流量
- D 关键是日常安全事件的跟踪与处理

2、论文《计算机安全威胁监控与监视》提出的监视入侵活动的思路是 ✓

- A 利用日志作为审计数据监视入侵活动
- B 利用流量作为审计数据监视入侵活动
- C 利用恶意代码作为审计数据监视入侵活动

二、多选题

1、入侵检测部署方式是 ✓

- [x] HUB旁路方式
- [ ] HUB串联方式
- [x] 交换机端口镜像方式
- [x] 光纤分光器

2、防火墙的安全缺陷是 ✓

- [ ] 只判定数据包内容的合法性，未判定访问规则
- [x] 只判定访问规则，未判定数据包内容的合法性
- [x] 作为边界设备，提高访问门槛
- [ ] 作为动态设备，动态检测入侵行为

三、判断题

1、入侵检测系统可以检测存在的恶意代码 ✓

- ( ) 对
- (•) 错

课时2：入侵与检测是永远的“矛与盾” 已看完 35分钟

1、沙箱是通过哪种方式检测入侵

- A 逆向分析
- B 虚假目标
- C 行为表现
- D 流量检测

2、IDS难以确定的评价指标是 ✓

- [ ] 误杀率
- [x] 误报率
- [ ] 漏杀率
- [x] 漏报率

1、把IDS串联在保护目标前就成了IPS ✓

- 对
- 错

2、入侵检测技术面临的挑战有哪些 ✓

- [x] 数据加密
- [ ] 旁路传输
- [x] 网络逃逸
- [x] 沙箱逃逸

1、入侵检测技术的未来发展 ✓

- [ ] 行为模式匹配增多，特征库减小
- [x] 依托云安全服务
- [x] NIDS与HIDS相融合
- [x] 多维关联分析

第3章：网闸的原理与技术发展
课时1：网闸一词的由来 已看完 16分钟
课时2：网闸实现的原理及功能 已看完 17分钟
课时3：未来网闸的发展趋势 已看完