i春秋 Web安全从入门到“放弃”-完结

原创

zac- 于 2021-10-28 17:04:54 发布 66 收藏

分类专栏： i春秋培训测验 文章标签： web安全 安全

本文链接：https://blog.csdn.net/hkk1151043545/article/details/121005039

版权

i春秋培训测验 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

第1章：课程介绍

课时1：课程大纲介绍及实验环境部署 已看完 9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

第2章：暴力破解
课时1：暴力破解原理和测试流程 已看完 11分钟
课时2：暴力破解演示及burpsute使用介绍 已看完 24分钟
课时3：验证码绕过-on client相关问题 已看完 13分钟
课时4：验证码绕过之服务端相关问题 已看完 14分钟
课时5：暴力破解防范措施和防范误区 已看完 6分钟
第3章：跨站脚本(xss)
课时1：xss基本概念和原理介绍 已看完 11分钟
课时2：一个基础的反射型xss 已看完 10分钟
课时3：存储型xss漏洞实验演示和讲解 已看完 6分钟
课时4：dom型xss详解及多种场景演示 已看完 16分钟
课时5：cookie获取及xss后台使用 已看完 13分钟
课时6：post方式下的xss漏洞利用 已看完 7分钟
课时7：xss钓鱼演示 已看完 6分钟
课时8：xss获取键盘记录实验演示 已看完 11分钟
课时9：xss的盲打以及盲打实验演示 已看完 4分钟
课时10：xss绕过思路讲解和案例演示 已看完 10分钟
课时11：xss之htmlspecialchars绕过演示 已看完 4分钟
课时12：xss防范措施及href和js输出点的案例演示 已看完 8分钟
第4章：CSRF跨站请求伪造
课时1：csrf漏洞概述及原理 已看完 10分钟
课时2：通过csrf进行地址修改实验演示 已看完 6分钟
课时3：token详解及常见防范措施 已看完 9分钟
第5章：SQL注入(sql inject)
课时1：SQL注入基本概念和原理 已看完 10分钟
课时2：从一个数字型注入认识sql注入漏洞 已看完 8分钟
课时3：字符型注入 已看完 6分钟
课时4：搜索型及xx型SQL注入 已看完 11分钟
课时5：union注入 已看完 11分钟
课时6：information_schema注入 已看完 13分钟
课时7：基于函数报错的注入 已看完 13分钟
课时8：基于insert update delete的注入利用案 已看完 13分钟
课时9：http header注入讲解和案例演示 已看完 7分钟
课时10：sqli盲注原理及基于boolean盲注的案例演示 已看完 15分钟

课时11：sqli盲注-base on time的盲注案例演示 已看完 5分钟
课时12：通过sqli进行服务器的远程控制案例测试 已看完 9分钟
课时13：暴力破解在sqli漏洞中的应用 已看完 7分钟
课时14：sqli漏洞常见防范措施 已看完 6分钟
课时15：sqlmap工具使用入门及案例介绍 已看完 7分钟
第6章：RCE(远程命令、代码执行漏洞)
课时1：远程命令、代码执行漏洞原理及案例演示 已看完 7分钟
第7章：Files Inclusion(文件包含漏洞)
课时1：文件包含原理及本地文件包含漏洞案例演示 已看完 8分钟
课时2：远程文件包含漏洞案例讲解和演示 已看完 7分钟
课时3：文件包含漏洞防范措施 已看完 3分钟
第8章：不安全的文件下载和上传
课时1：不安全的文件下载原理和案例演示 已看完 6分钟
课时2：不安全的文件上传原理及客户端绕过案例 已看完 6分钟
课时3：上传漏洞之MIME type验证原理和绕过 已看完 7分钟
课时4：文件上传之getimagesize绕过案例和防范措施 已看完 13分钟
第9章：越权漏洞
课时1：越权漏洞原理及水平越权案例演示 已看完 6分钟
课时2：垂直越权漏洞原理和测试流程案例 已看完 8分钟
第10章：php反序列化、XXE、SSRF
课时1：php反序列化原理和案例演示 已看完 10分钟
课时2：xxe漏洞原理和案例实验演示 已看完 9分钟
课时3：ssrf漏洞原理和实验案例演示 已看完 7分钟
第11章：其他常见问题
课时1：目录遍历和敏感信息泄露原理及案例演示 已看完 8分钟
课时2：不安全的url重定向原理和案例演示 已看完