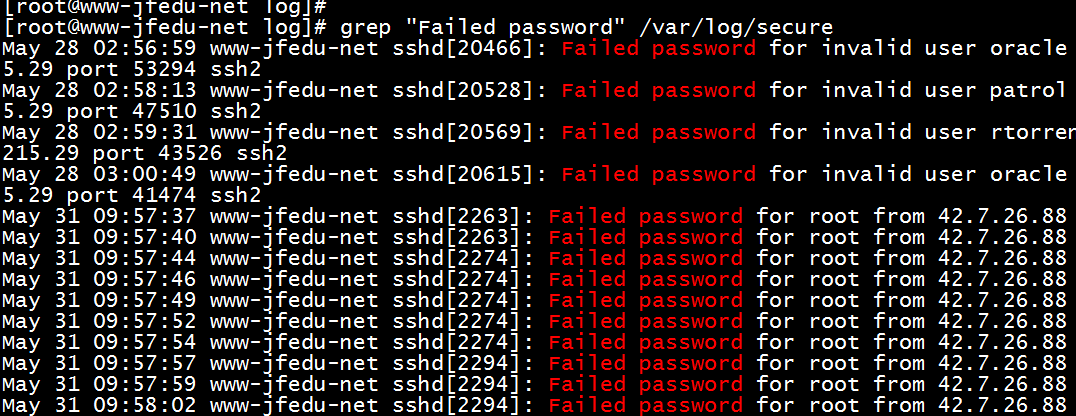
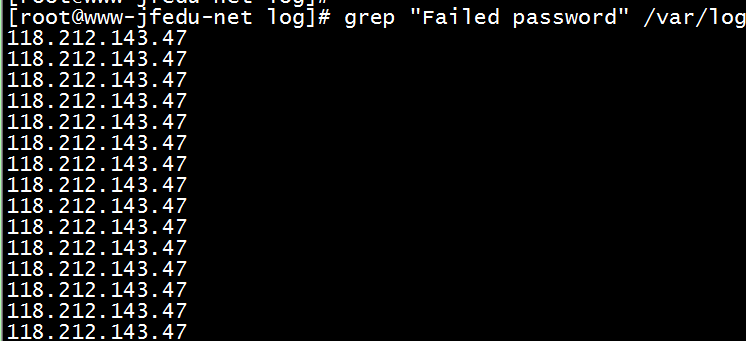
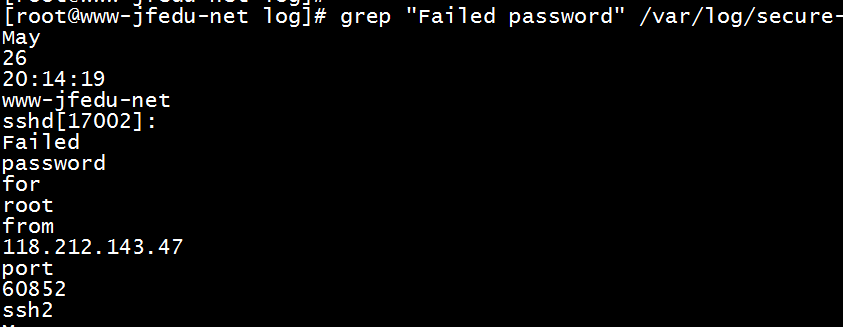
**企业Linux服务器暴力破解安全攻防演练**

1. 剖析黑客攻击的手段和方法；
2. 如何防御黑客暴力破解Linux服务器；
3. 基于SHELL指令自动化防御黑客暴力破解；
4. 基于DenyHosts全自动防御黑客暴力破解；
5. 如何将黑客的IP加入和移除黑名单案例实战；
6. **剖析黑客攻击的手段和方法；**
7. 基于用户名和弱密码字典攻击，方法最简单，一旦攻破，黑客拥有的权限很大；
8. 使用常见端口扫描和攻击，139 445 3389 22等攻击服务器的漏洞；
9. 黑客模拟大量的请求，半连接恶意访问服务器，称为DDOS攻击，利用了TCP三次握手过程用户-服务器请求的机制；
10. 黑客攻击WEB网站，基于WEB网站的漏洞，SQL注入，网站文件的权限，SHELL提权；
11. 黑客攻击WEB网站、数据库系统，CC、跨站、木马、病毒、XSS、HTTP方法攻击、简单密码撞库攻击；
12. **如何防御黑客暴力破解Linux服务器**
13. 随着Linux操作系统被广泛的应用，黑客开始来攻击Linux服务器，黑客攻击Linux服务器最常用的方法使用用户名和密码暴力破解登录；
14. 黑客使用数以万计的字典表，字典将用户名和密码写入字典表，看成用户名和密码的集合文件；
15. 如何判断Linux服务器当前有黑客在暴力破解呢？可以查看服务器的CPU、内存、负载、端口、连接数、异常的进程、应用日志、系统日志、登录日志等；
16. 黑客如果使用用户名和密码攻击Linux服务器，可以通过查看登录日志去判断：/var/log/secure；
17. 通过关键词判断登录失败或者恶意攻击服务器，SHELL指令如下：  
    grep "Failed password" /var/log/secure  
    
18. 如何只获取黑客的部分IP地址，SHELL指令如下：  
    grep "Failed password" /var/log/secure-20180528|awk '{print $11}'  
    
19. 将/var/log/secure，匹配结果的空格换成换行符；

grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|more

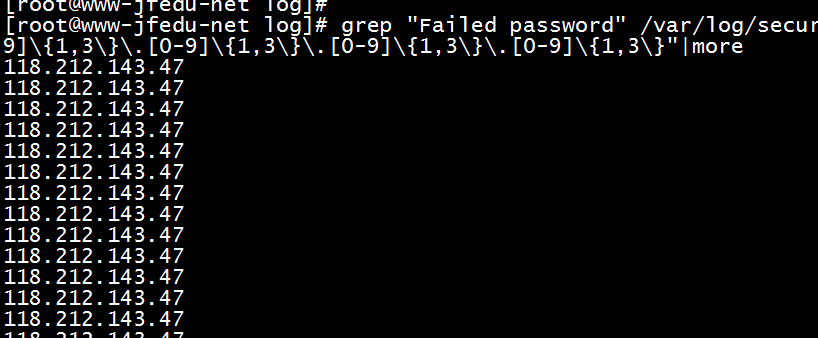
  
8）匹配连续的三位0-9的数字，指令如下：  
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep "[0-9][0-9][0-9]\."|more  
9）匹配任意的1、2、3位[0-9]的数字，指令如下：

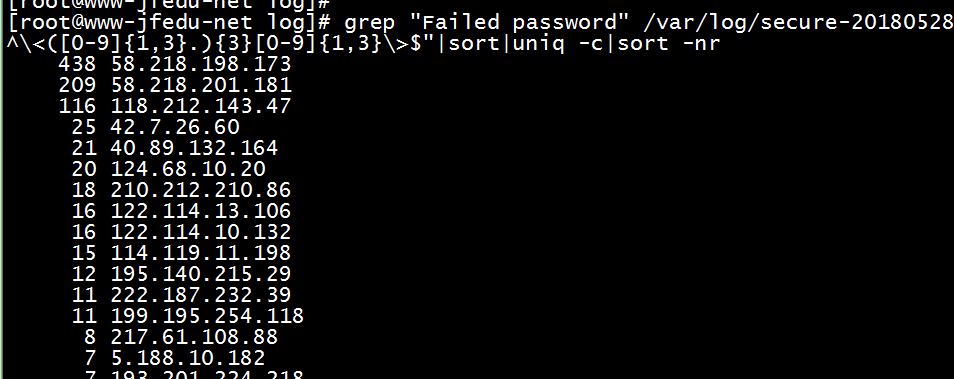
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep "[0-9]\{1,3\}\."|more

10）匹配连续三次的1、2、3位[0-9]的数字，指令如下：

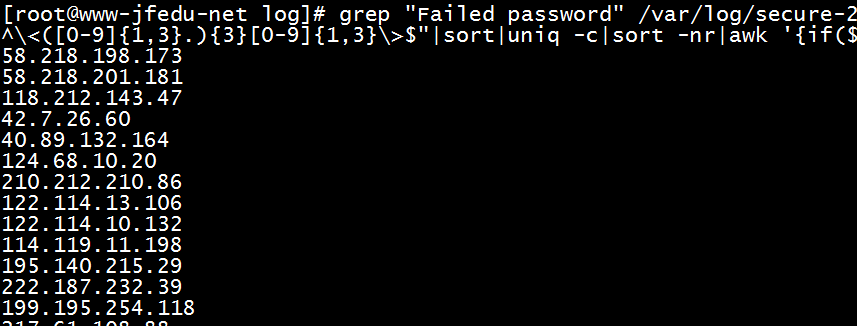
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep "[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}"|more  
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "([0-9]{1,3}.){3}[0-9]{1,3}"|more  
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "\<([0-9]{1,3}.){3}[0-9]{1,3}\>"|more

grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "^\<([0-9]{1,3}.){3}[0-9]{1,3}\>$"|more



1. 从大到小排列的黑客的IP，指令如下：  
   grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "^\<([0-9]{1,3}.){3}[0-9]{1,3}\>$"|sort|uniq -c|sort -nr  
   

12)从大到小排列的黑客的IP，只查看攻击次数超过5次（包含），指令如下：  
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "^\<([0-9]{1,3}.){3}[0-9]{1,3}\>$"|sort|uniq -c|sort -nr|awk '{if($1>=5) print $2}'



13)从大到小排列的黑客的IP，只查看攻击次数超过5次（包含），并且将其IP加入到黑名单，指令如下：  
grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "^\<([0-9]{1,3}.){3}[0-9]{1,3}\>$"|sort|uniq -c|sort -nr|awk '{if($1>=5) print $2}'|sed 's/^/&sshd:/g' >>/etc/hosts.deny

grep "Failed password" /var/log/secure-20180528|sed 's/ /\n/g'|grep -E "^\<([0-9]{1,3}.){3}[0-9]{1,3}\>$"|sort|uniq -c|sort -nr|awk '{if($1>=5) print "sshd:"$2}'>>/etc/hosts.deny

