重庆市第十届高职学生技能竞赛“信息安全管理与评估”项目赛项试题

一、赛项时间

8:00-11:00，共计3小时，含赛题发放、收卷。共1000分

二、赛项信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 竞赛阶段 | 任务阶段 | 竞赛任务 | 竞赛时间 | 分值 |
| 第一阶段  平台搭建与配置 | 任务一 | 网络平台搭建 | 8:00-11:00 | 55 |
| 任务二 | 网络安全设备配置与防护 | 345 |
| 第二阶段  系统安全攻防及运维安全管控 | 任务一 | IIS安全加固与证书签发 | 80 |
| 任务二 | Linux操作系统安全防护 | 100 |
| 任务三 | MySQL数据库加固 | 100 |
| 任务四 | 密码嗅探 | 60 |
| 任务五 | SQL注入攻击 | 60 |
| 第三阶段  网络渗透 | 网络渗透 | | 200 |

三、赛项内容

假定各位选手是某公司的信息安全工程师，负责维护公司信息系统安全。你们需要完成三个阶段的任务，其中前两个阶段需要提交任务操作文档留存备案。所有文档需要存放在裁判组专门提供的U盘中。第三阶段是否提交文档，请根据现场具体题目要求。

选手首先需要在U盘的根目录下建立一个名为“xx组”的文件夹，并在“xx组”文件夹下，建立“第一阶段”、“第二阶段”和“第三阶段”三个文件夹，赛题三个阶段的文档分别归类放置在对应的文件夹中。

例如：08组，则需要在U盘根目录下建立“08组”文件夹，并在“08组”文件夹下建立“第一阶段”、“第二阶段”和“第三阶段”三个文件夹。

特别说明：只允许在根目录下的“08组”文件夹中体现一次小组信息，不允许在其他文件夹名称或文件名称中再次体现小组信息，否则按作弊处理。

1. 赛项环境设置

赛项环境设置包含了三个竞赛阶段的基础信息：网络拓扑图、IP地址规划表、设备初始化信息。

1.网络拓扑图



2.IP地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **互联** | **可用IP数量** |
| 防火墙DCFW | EthX | x.x.x.x/x | 与targe相连 | 见赛场IP参数表 |
| EthX | x.x.x.x/x | 与DCRS | 见赛场IP参数表 |
| EthX | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | VPN地址池 | 见赛场IP参数表 |
| Web应用防火墙WAF | EthX | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| EthX | 无 | 与PC2用户 | 见赛场IP参数表 |
| 三层交换机DCRS | Vlan 10 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| Vlan 20 | x.x.x.x/x | 与PC3相连 | 见赛场IP参数表 |
| Vlan 30 | x.x.x.x/x | 与NETLOG相连 | 见赛场IP参数表 |
| Vlan 110 | x.x.x.x/x | 直连PC1用户 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | DHCP地址池 | 见赛场IP参数表 |
| 网络日志系统NETLOG | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| EthX | 无 | 与DCRS相连 | 见赛场IP参数表 |
| PC1 | 无 | x.x.x.x/x | DHCP地址池获取 | 见赛场IP参数表 |
| PC2 | 无 | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| PC3 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| target | 无 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| 备注 | 1.赛题可用IP地址范围见《赛场IP参数表》；  2.具体网络连接接口由自己拟定；  3.设备互联网段内可用地址数量见《赛场IP参数表》；  4.IP地址分配要求，最节省IP地址，子网有效地址规划遵循2n-2的原则；  5.参赛选手按照《赛场IP参数表》要求，自行分配IP地址段、设备互联接口；  6.将分配的IP地址段和接口填入《赛场IP参数表》。） | | | |

3.设备初始化信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **管理地址** | **默认管理接口** | **用户名** | **密码** |
| 防火墙DCFW | http://192.168.1.1 | ETH0 | admin | admin |
| 网络日志系统NETLOG | https://192.168.5.254 | ETH0 | admin | 123456 |
| web应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| **注意：所有设备的默认管理接口、管理IP地址不允许修改;如果修改对应设备的缺省管理IP及管理端口，涉及此设备的题目按 0 分处理。** | | | | |

4.PC环境说明

（1）物理机PC-2 内装有2个虚拟机win-cacqcet和xserver-mysql;

•虚拟机win-cacqcet，操作系统WindowsServer2003；ip:172.18.102.251 用户名：administrator 密码：cqcet2003

•虚拟机xserver-mysql, 操作系统Linux AS5；ip地址 172.18.102.252用户名：root 密码cqcet123

（2）物理机PC-3内装有2个虚拟机centos-sql和kail-attack；

•虚拟机centos-sql操作系统CentOS6.5；ip地址 172.18.162.253

•虚拟机kali-attack操作系统KALI2016.2；ip地址 172.18.162.250

用户名：root 密码cqcetkali

（3）Target服务器所在的网段是200.173.10.0/24

（4）PC-2和PC-3物理机所安装的windows7操作系统中均提供了[PentestBox](http://www.baidu.com/link?url=DaXa3gWOjrafGAGSHXjDT7Xp38xnrTVhtXHNxwxNGgp5AamenkJcgGArWP4ugqPa)、渗透工具集成包和中国菜刀渗透工具。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络日志系统NETLOG | https://192.168.5.254 | ETH0 | admin | 123456 |
| web应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| **注意：所有设备的默认管理接口、管理IP地址不允许修改;如果修改对应设备的缺省管理IP及管理端口，涉及此设备的题目按 0 分处理。** | | | | |

（二）第一阶段任务书

提示：该阶段答案文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第一阶段、任务1、网络安全设备配置与防护”的答案提交文档，文件名称为：第一阶段-任务1-网络安全设备配置与防护.doc或第一阶段-任务1-网络安全设备配置与防护.docx。

任务一：网络平台搭建(55)

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、WAF、NETLOG设备需要提交配置过程截图存入WORD文档，并在截图中加配置说明。提交的答案保存到一个WORD文档中，需标明题号，按顺序答题。

平台搭建要求如下：

|  |  |  |
| --- | --- | --- |
| **题号** | **网络需求** | **分值** |
| 1 | 根据网络拓扑图所示，按照IP地址参数表，对WAF的名称、各接口IP地址进行配置。 | 5分 |
| 2 | 根据网络拓扑图所示，按照IP地址参数表，对DCRS的名称、各接口IP地址进行配置。 | 5分 |
| 3 | 根据网络拓扑图所示，按照IP地址参数表，对NETLOG的名称、各接口IP地址进行配置。 | 5分 |
| 4 | 根据网络拓扑图所示，按照IP地址参数表，在DCRS交换机上创建相应的VLAN，并将相应接口划入VLAN。 | 5分 |
| 5 | 采用RIPV2路由协议，全网络互连。 | 5分 |
| 6 | 修改设备名称 | 5分 |
| 7 | 完整填写“赛场IP参数表”。 | 25分 |

任务二：网络安全设备配置与防护(345)

提示：需要提交所有设备配置文件，其中DCRS设备要求提供show run配置文件保存到WORD文档，DCFW、WAF、NETLOG设备需要提交配置过程截图存入WORD文档，并在截图中加以说明。请顺序答题，并标注题号。每个设备提交的答案各自保存到不同的WORD文档中（本任务可以保存4个WORD文档）。

例：“第一阶段、任务二、网络安全设备配置与防护”关于NETLOG设备的答案提交文档，文件名称为：第一阶段-任务二-网络安全设备配置与防护-NETLOG.doc或第一阶段-任务二-网络安全设备配置与防护-NETLOG.docx。

1. 在公司总部的DCRS上配置，配置设备enable密码，并且在登录设备时必须正确输入enable密码才能进入交换机的配置模式，密码设置方式为明文认证，密码长度为8位。（6分）
2. 在公司总部的DCRS上配置，在交换设备上开启SSH管理功能，用户名和密码都是SZSM，并开启设备的web管理方式， PC1通过浏览器端用https登录交换机。（6分）
3. 在公司总部的DCRS上配置限制IP地址段的RFC5735过滤来限制源IP欺骗攻击。（15分）
4. 在公司总部的DCRS上配置，VLAN110用户可通过DHCP的方式获得IP地址，在交换机上配置DHCP Server，地址池名称为pool110，DNS地址为8.8.8.8，租期为8天，VLAN110网段最后10个可用地址（DHCP地址段参考“赛场IP参数表”）不能被动态分配出去。（6分）
5. 在公司总部的DCRS上配置，在交换机18-21的接入端口开启ARP扫描保护功能，防止某台PC发出网关欺骗报文。并在vlan110所接口接上配置基于数字MAC访问控制，使PC1的主机不能访问PC3的主机，其他主机访问正常，并且绑定PC1的MAC地址。（10分）
6. 在公司总部的DCRS上配置，需要在交换机10接口上开启基于用户模式的认证，认证通过后才能访问网络，认证PC2地址是服务器区内第五个可用地址（服务器区IP地址段参考“赛场IP参数表”），radius key是54321。（15分）
7. 配置公司总部的DCRS，防止来自VLAN110接口的DHCP服务器假冒攻击，以及防止来自VLAN110接口的DHCP地址池耗尽攻击。（10分）
8. 在公司总部的DCRS上配置端口环路检测（Loopback Detection），防止来自接口下的单端口环路，并配置存在环路时的检测时间间隔为30秒，不存在环路时的检测时间间隔为10秒（10分）
9. PC1主机接入直连终端用户VLAN110，通过RIPV2路由协议向DCRS注入度量值更低的外网路由，从而代理内网主机访问外网，进而通过Sniffer来分析内网主机访问外网的流量（如账号、密码等敏感信息）。通过在DCRS上配置HMAC，来阻止以上攻击的实现。（认证Key须使用Key Chain实现）。（15分）
10. 配置公司总部的DCRS，通过控制平面（Control Plane）策略，防止DCRS受到来自于VLAN110接口的DoS（Denial Of Service）攻击；其中CIR(Committed Information Rate)定义为128Kbps，TC（Time Commit）定义为8192ms，速率大于CIR的流量将被DCRS丢弃，其余流量将被正常发送。（15分）
11. 配置公司总部的DCRS，通过DCP（Dynamic CPU Protection）策略，防止DCRS受到来自于全部物理接口的DoS（Denial Of Service）攻击。（6分）
12. 为方便公司总部网络规模扩展，将公司总部的DCRS交换机的24端口配置为Trunk模式，用于将来继续连接其它的交换机，配置公司总部的DCRS，使其能够防御由此带来VLAN Hopping（VLAN跳跃）攻击。（10分）
13. 配置公司总部的DCRS，防止对公司总部服务器的以下3类DOS（Denial Of Service）攻击：ICMP Flood攻击、LAND攻击、SYN Flood攻击。（6分）
14. 在公司总部的DCFW上配置，连接互联网的接口属于WAN安全域、连接内网的接口属于LAN安全域、服务器区域属于DMZ区域。（6分）
15. 在公司总部的DCFW上新增2个用户，用户1（用户）名YH1；密码：yonghu1）：不能进行任何的配置添加与修改，只拥有配置查看权限，删除。 用户2（用户名：YH2；密码：yonghu2）：拥有所有的查看权限，拥有除“用户升级、应用特征库升级、重启设备、配置 日志”模块以外的所有模块的配置添加与修改，删除权限。（10分）
16. 在公司总部的DCFW上配置，DCFWF的DMZ区域和LAN区域针对以下攻击的防护功能：ICMP洪水攻击防护、UDP洪水攻击防护、SYN洪水攻击防护、WinNuke攻击防护、IP地址欺骗攻击防护、IP地址扫描攻击防护、端口扫描防护、Ping of Death攻击防护、Teardrop攻击防护、IP分片防护、IP选项、Smurf或者Fraggle攻击防护、Land攻击防护、ICMP大包攻击防护、TCP选项异常、DNS查询洪水攻击防护、DNS递归查询洪水攻击防护、灰鸽子攻击防护。（6分）
17. 在公司总部的DCFW上配置网页内容过滤：内网用户不能访问互联网网站：www.tmall.com；（6分）
18. 在公司总部的DCFW上配置，使内网所有用户网段都可以通过DCFW外网接口IP地址访问互联网。但要求公司PC1只能通过固定的公网地址的第四个可用地址。（6分）
19. 在公司总部的DCFW上配置,使得PC2通过SNAT地址转换，能够正常通过DCFW外网接口访问target。（6分）
20. 在公司总部的DCFW上配置，使内网访问Internet网站时，不允许访问MSI(.msi)、EXE(.exe)、COM(.com)、(.bat)类型的文件。（6分）
21. 在公司总部的DCFW上配置，在内网接口上开启防护功能，每秒钟最大接收1000个ARP包，超过的将被丢弃。（6分）
22. 在公司总部的DCFW上配置，开启网络管理功能（SNMP），服务器连接在PC2端，IP地址是PC2第二个可用地址（服务端IP地址段参考“赛场IP参数表”），community名字为public，软件对DCFW没有写权限。（10分）
23. 为了保证正常工作，在公司总部的DCFW上配置：对于上班时间（8：30-18：30）公司总部内网浏览Internet网页，连接总数不超过2000。（6分）
24. 在公司总部的DCFW上配置，在上班时间如有事情需要访问网络，限制只有通过DCFW的WEB认证后才能访问互联网，且在连接网络一个小时后如果不重新认证则断开网络访问。（6分）
25. 在公司总部的DCFW上启用L2TP VPN，使PC2通过L2TP VPN拨入公司总部，访问内网的所有信息资源。L2TP VPN地址池x.x.x.x/x 测试成功并截图（具体IP地址参考“赛场IP参数表”） （15分）
26. 在公司总部的DCFW上启用SSL VPN，使PC2通过VPN拨入公司总部，访问内部的所有服务器资源。SSL VPN地址池x.x.x.x/x 测试成功并截图（具体IP地址参考“赛场IP参数表”）（15分）
27. 在公司总部的WAF上配置，编辑防护策略，定义HTTP请求体的最大长度为128，防止缓冲区溢出攻击。（6分）
28. 在公司总部的WAF上配置，禁止黑客IP地址（218.240.143.219）访问PC2。 （10分）
29. 在公司总部的WAF上配置，对公司PC2(地址使用为网段内的第五个可用地址，“赛场IP参数表”）进行安全评估，检查是否存在安全漏洞，便于在攻击没有发生的情况下提前做出防护措施。（10分）
30. 在公司总部的WAF上配置，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务。大量请求的确认值是：10秒钟超过3000次请求。（5分）
31. 在公司总部的WAF上配置，编辑防护策略，要求客户机访问网站时，禁止访问\*.exe的文件。（5分）
32. 在公司总部的WAF上配置，设备状态告警、攻击告警、漏洞状态告警信息通过邮件（发送到jiang123@digitalchina.com）及短信方式(发送到15312345678)发送给管理员。（10分）
33. 在公司总部的DCBI上配置，设备部署方式为旁路模式，并配置监控接口。（5分）
34. 在公司总部的DCBI上配置，增加非admin账户CQdcn1234，密码CQdcn1234，该账户仅用于用户查询设备的浏览权限。（10分）
35. 在公司总部的DCBI上配置，监控PC1所在网段用户的即时聊天记录。（5分）
36. 在公司总部的DCRS交换机上配置SPAN，使内网经过DCRS交换机的全部流量均交由NETLOG分析。（10分）
37. 在公司总部的DCBI上配置，使DCBI能够通过邮件方式发送告警信息，邮件服务器在PC2，（PC2地址段参考“赛场IP参数表”），端口号25，账号CQtest，密码CQtest。（5分）
38. 在公司总部的DCBI上配置，将DCBI的日志信息发送到PC2，IP地址是PC2第十个可用地址（IP地址段参考“赛场IP参数表”），community名字public。（10分）
39. 在公司总部的DCBI上配置，监控工作日（每周一到周五）期间PC1访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警。（10分）
40. 在公司总部的DCBI上配置，使DCBI可以通过交换机（DCRS）获得内网PC的MAC地址，并在记录日志时显示内网PC的MAC地址。（10分）

（三）第二阶段：系统安全攻防及安全管控（400分）

提示1：本阶段的任务在PC-2和PC-3的环境中完成。

提示2：每个任务提交一个word文档，请在文档中标明题号，按顺序答题。将关键步骤和操作结果进行截屏，并辅以文字说明，保存到提交文档中。

提示3：文档命名格式为：“第X阶段”-“任务X”-“任务名称”。

例：“第二阶段、任务二”的答案提交文档，文件名称为：第二阶段-任务二- Linux操作系统安全防护.doc或第二阶段-任务二- Linux操作系统安全防护.docx

任务一：IIS安全加固与证书签发（80分）

任务描述：贵公司的IIS服务器并不是那么安全，很有可能会被境外黑客攻击，并且可以作为跳板攻入贵公司的内网，所以需要对IIS服务器进行加固，尤其是安全证书的签发是安全管理员必不可少的工作，请对公司的win-cacqcet服务器进行加固。

任务要求：

1. 配置Windows 防火墙，使IIS Web服务能够被访问，对配置进行截屏。（5分）
2. 使用windows 自带的防火墙加固IIS Web服务器的安全配置，使得Web服务只能被172.18.102.0/24用户所在的网段访问，对加固配置进行截屏。（10分）
3. 为IIS Web服务器申请服务器证书，对申请摘要进行截屏。（10分）
4. 为IIS Web服务器颁发一年期服务器证书，对颁发过程进行截屏。（10分）
5. 将IIS服务器启动SSL安全通信，并安装服务器证书。远程客户端的浏览器访问该Web服务进行测试。由于cn和IIS 的域名不一致，所以一定有警报弹出窗，请将该窗口截屏。（10分）
6. 将IIS 服务器启用客户端证书设置。再使用远程客户端自带的浏览器访问该Web服务进行测试。将要求客户端提供证书的弹出页面截屏。（15分）
7. 为win-cacqcet服务器申请CA证书。颁发该证书。对申请和颁发过程截屏。（15分）
8. 在win-cacqcet服务器上安装CA证书。使用PC浏览器访问该Web服务进行测试，对操作过程截屏。（5分）

任务二：Linux操作系统安全防护 （100分）

任务描述：贵公司的服务器以Linux居多，你不要说自己是Windows专家，Linux操作系统的安全防护是基本功，如果不会，那么请学好再来上班吧。

请对xserver-mysql服务器完成以下加固操作：

1. 修改ssh的配置文件，禁止root直接登录，退出所有账号，使用root直接ssh登录操作系统，将提示信息截图。（10分）
2. 修改密码策略配置文件，确保密码最小长度为8位，然后创建新账号，并赋予密码低于8位，将错误提示信息截图。（10分）
3. 修改/etc/pam.d/ system-auth文件，确保错误登录10次，锁定此账户10分钟，将配置截图。（20分）
4. 配置至少三个配置文件的umask值为027，将配置截图并说明是哪个配置文件。（10分）
5. 自编脚本，查找本机存在SUID与SGID的文件，并截图。（10分）
6. 自编脚本，查找本机存在的所有人均有写权限的目录，并截图。（10分）
7. 修改配置文件，将登录超时设置为10分钟，并截图。（10分）
8. 修改syslog.conf配置文件，将认证日志、邮件日志，备份存储到指定服务器，并截图。（10分）
9. 使用root帐号登录系统，创建一个UID为0的帐号，然后使用一行命令查找本系统UID为0的帐号有哪些，并截图。（10分）

任务三：MySQL数据库加固（100分）

任务描述：贵公司的很多服务都是用了MySQL数据库，但是MySQL数据库是个开源的程序，有很多已知的漏洞，如果没有很好的进行安全配置，将会带来很大的灾难。

请对xserver-mysql服务器完成以下加固操作：

1. 进入xserver-mysql, 加固MySQL服务器，使所有的访问能被审计；将MySQL最大连接数设为100，对加固操作进行截屏。（10分）
2. 配置Linux 防火墙，允许MySQL服务能够被访问，要求规则中只包含端口项，对防火墙规则列表进行截屏。（10分）
3. 进入xserver-mysql，查看所有用户及权限，找到可以从任何IP地址访问的用户，对操作过程进行截屏。（20分）
4. 对题号3中的漏洞进行加固，设定只允许与服务器在同一个网段的用户访问，用update 命令进行管理，并将加固过程截屏。（10分）
5. 检查xserver-mysql中的是否存在数据库匿名用户，如果存在数据库匿名用户，则删除该用户，将发现的数据库匿名用户信息以及删除过程进行截屏。（20分）
6. 改变默认MySQL管理员的名称，将系统的默认管理员root 改为admin，防止被列举，将执行过程进行截屏。（10分）
7. 禁止MySQL对本地文件进行存取，对mysqld 的启动项进行加固，将加固部分截屏。（10分）
8. 限制一般用户浏览其他用户数据库，对mysqld 的启动项进行加固，将加固部分截屏。（10分）

任务四：密码嗅探（60分）

任务描述：你以为自己的密码很安全么？有一种局域网密码嗅探器，在你的电脑上运行便可获取局域网中任意一台电脑的账号密码，你的POP3、FTP、SMTP、NNTP、IMAP、TELNET、HTTP、IRC协议中的密码，都将公开于天下，你的秘密都会被别人发现。尽快解决它吧。

1. win-cacqcet服务器启动wireshark，并且设定过滤条件为telnet，并启动telnetp程序，每1分钟访问1次centos-sql的telnet 服务器，将过程进行截屏。（5分）
2. 在win-cacqcet 用抓包工具捕获自动连接软件使用的telnet 用户和密码，然后退出telnetp程序，对整个执行过程进行截图。（10分）
3. 在win-cacqcet设定wireshark 的过滤条件是ftp。（5分）
4. 运行win-cacqcet桌面上的ftp自动连接软件ftpp，在win-cacqcet中用抓包工具捕获ftp 的用户名和密码并截图。（10分）
5. 在win-cacqcet用浏览器访问172.18.162.253的web服务，在打开的网站页面中，点击“漏洞发现”链接,分析登录页面的源码,指出用户名数据和密码数据提交的方法以及相应的变量名。（10分）
6. 在wireshark中设定web服务的过滤条件，包括WEB服务的协议和目标地址，截屏。（10分）
7. 运行在win-cacqcet桌面上的Web自动连接软件httpp，用抓包工具捕获输入的管理用户名和密码并截图。（10分）

任务五：SQL注入攻击（60分）

任务描述：SQL注入是从正常的WWW端口访问，而且表面看起来跟一般的Web页面访问没什么区别，所以市面的[防火墙](http://baike.baidu.com/view/3067.htm)都不会对SQL注入发出警报，如果你没查看ⅡS日志的习惯，可能被入侵很长时间都不会发觉。SQL注入的手法相当灵活，在注入的时候会碰到很多意外的情况，需要构造巧妙的SQL语句，从而成功获取想要的数据。你是猎人，他是狐狸，你们谁更厉害？

1. 登录win-cacqcet，打开桌面上 Acunetix Web Vulnerability Scanner 扫描器，对http://172.18.162.253/sql地址进行扫描，识别存在SQL注入风险以及注入点的URL，并截图。（10分）
2. 通过对注入点手工判断，根据报错信息或者输入’and 1=1 以及’and 1=2 比对返回不同结果确定是注入点 并截图。（10分）
3. Get型注入，使用sqlmap对注入点的URL进行注入测试，获得当前的数据库名称，并截图。（10分）
4. POST型注入，使用sqlmap对注入点的URL以及POST数据进行注入测试，获得所有数据库的名称及个数，并截图。（10分）
5. 登录认证型，在网站注册任意帐号，对后台指定的URL进行SQL注入测试，通过SQLMAP工具dump到管理员帐号admin的加密密码并截图 。（10分）
6. 对第五步获取的加密密码进行md5破解，破解成功后的使用admin 帐号进行登录，并截图。（10分）
7. 第三阶段：网络渗透（200分）

Target服务器中存在着各种问题和漏洞（见漏洞列表）。请对该服务器进行渗透尽可能的发现漏洞获取key值，并利用漏洞对服务器进行攻击，获取到root权限。攻击环境是PC-3中的kail-attack虚拟机。

提示1：Target服务器所在的网段是200.173.10.0/24

提示2：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示3：渗透该服务器尽可能多的获得隐藏在服务器漏洞点的key，每得到一个key值获得20分。

提示4：如能获取到服务器根目录下keygent文件中的flag值该题直接得满分。

提示5：请为该题创建一个文档“第三阶段答案.doc”，将获得的key和flag值放入该文档中；

漏洞列表

1. Target服务器的ip地址需要通过相关技术手段获得，如果能访问到该Target服务器的web服务即可得到KEY的内容。
2. Web服务器包含SQL注入的漏洞，用户通过SQL注入的漏洞获取数据库表单KEY的内容。
3. Web服务器中的网站后台的密码是加密的，需要获取到该用户的密码并登陆网站后台获取KEY的内容。
4. Web服务器存在命令执行漏洞，需要利用该漏洞进行获取KEY并进行提权。
5. Target服务器的内核存在“条件竞争”漏洞，需要利用该漏洞获取系统root权限。
6. Target服务器中的数据库组件存在远程代码执行漏洞，需要利用该漏洞获取系统root权限。

除了能获取上述key值得分，还可以对该Target服务器进行安全渗透最终获取到系统的root权限，并读取目录下keygent文件中的flag值。

1. （三）评分细则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **竞赛任务** | **考核内容** | **分值** | **评分方式** |
| 第一阶段  权重40% | 网络平台搭建 | 网络规划文档 | 5% | 结果评分-客观 |
| 三层交换机配置文件 | 13% | 结果评分-客观 |
| 网络安全设备配置与防护 | 防火墙配置截图文件 | 10% | 结果评分-客观 |
| 网络流控系统配置截图文件 | 5% | 结果评分-客观 |
| 网络日志系统配置截图文件 | 7% | 结果评分-客观 |
| 第二阶段  权重40% | 系统安全攻防及运维安全管控 | IIS安全加固与证书签发 | 8% | 结果评分-客观 |
| Linux操作系统安全防护 | 10% | 结果评分-客观 |
| MySQL数据库加固 | 10% | 结果评分-客观 |
| 密码嗅探 | 6% | 结果评分-客观 |
| SQL注入攻击 | 6% | 结果评分-客观 |
| 第三阶段  权重20% | 网络渗透 | 有5个key值，每个20分。  得到Flag本题得满分200分 | | |

# 十三、建议使用的比赛器材、技术平台和场地要求

（一）网络设备竞赛器材（硬件平台）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **参考型号1** |
| 1 | 三层交换机 | 1 | 神州数码DCRS-5650系列交换机 |
| 2 | 防火墙 | 1 | 神州数码DCFW-1800E系列防火墙 |
| 3 | WEB应用防火墙 | 1 | 神州数码DCFW-1800-WAF-LAB |
| 4 | 网络日志系统 | 1 | 神州数码DCBI-NetLog-LAB |
| 5 | PC机 | 4 | 多核CPU，CPU 主频>=3.5GHZ,>=四核心八线程，内存>=8G，具有串口或者配置USB转串口的配置线，支持硬件虚拟化 |

（二）软件技术平台：

比赛的应用系统环境主要基于桌面版和服务器版组成，桌面版主要采用Windows 7 (中文版)，服务器版本根据需要以windows和linux系统为主，版本涉及各类版本；办公软件主要为Microsoft Office 2013(中文版).比赛提供sercureCRT7.0作为终端。

具体软件参数如下表所示：

1．微软 Windows 7 (中文版)

2．微软 Microsoft Office 2013(中文版)

3．SercureCRT 7.0绿色版