2018年山东省职业技能大赛

中职组“网络空间安全”赛项竞赛赛题

一、竞赛时间

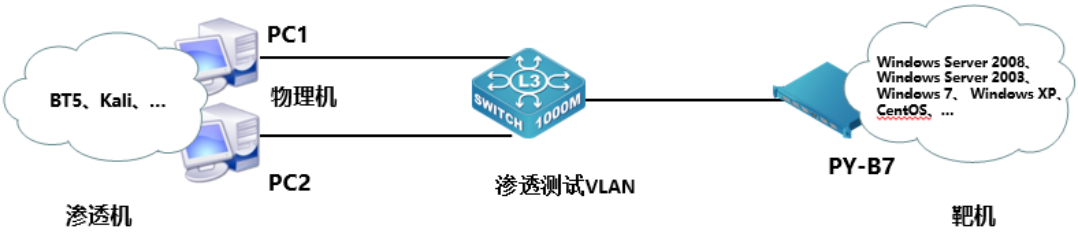
8:30-11:30，共计3小时。

二、竞赛阶段

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段 单兵模式系统渗透测试	任务一	Nmap扫描渗透测试	100分钟	50
	任务二	Web应用程序SQL Inject安全攻防		50
	任务三	Linux系统安全加固		100
	任务四	服务端口扫描渗透测试		100
	任务五	数据库安全攻防		100
	任务六	SSH弱口令渗透测试		100
	任务七	Web信息收集		100
	任务八	数据分析与取证		100
备战阶段	攻防对抗准备工作		20分钟	0
第二阶段 分组对抗	系统加固：15分钟		60分钟	300
	渗透测试：45分钟			

三、竞赛任务书内容

（一）拓扑图



（二）第一阶段任务书

任务一、 Nmap 扫描渗透测试

任务环境说明：

- ✓ 服务器场景：Linux
- ✓ 服务器场景操作系统：Linux（版本不详）
- ✓ 渗透机场景：Kali
- ✓ 渗透机用户名：root,密码：toor

提示：使用 nmap 进行脆弱性漏洞扫描应使用命令
nmap -p 3306 --script=mysql-brute.nse【ip】,则脚本名称为 mysql-brute.nse

1.在本地 PC 渗透测试平台 Kali 中使用 nmap 工具查看本地路由与接口，并将该操作使用的全部命令作为 FLAG 提交；

2.通过本地 PC 中渗透测试平台 Kali 对服务器场景 Linux 进行 VNC 服务扫描渗透测试，并将使用的脚本名称作为 FLAG 提交（例 mysql-brute.nse）；

3.通过本地 PC 中渗透测试平台 Kali 对服务器场景 Linux 进行 VNC 服务扫描渗透测试，并将该操作显示结果中 VNC 版本号作为 FLAG 提交；

4.在本地PC渗透测试平台Kali中使用nmap发送空的UDP数据对类DNS服务avahi进行拒绝服务攻击，并将使用的脚本名称作为FLAG提交（例mysql-brute.nse）；

5.通过本地PC中渗透测试平台Kali对服务器场景Linux进行模糊测试，来发送异常的包到靶机服务器，探测出隐藏在服务器中的漏洞，并将使用的脚本名称作为FLAG提交（例mysql-brute.nse）；

6.在本地PC渗透测试平台Kali中使用zenmap工具扫描服务器场景可能存在远程任意代码执行漏洞,并将使用的脚本名称的字符串作为FLAG提交;（例mysql-brute.nse）；

7.在本地PC渗透测试平台Kali中使用zenmap工具扫描服务器场景可能存在远程任意代码执行漏洞（提示：检测路径为/cgi-bin/bin，需添加--script-args uri=/cgi-bin/bin参数），并将该操作显示结果中漏洞编号和发布时间作为FLAG提交（漏洞编号和发布时间的字符串之间以分号隔开）。

任务二、 Web应用程序SQL Inject安全攻防

任务环境说明：

- ✓ 服务器场景：WebServ2003
- ✓ 服务器场景操作系统：Microsoft Windows2003 Server
- ✓ 服务器场景用户名：administrator,密码：空
- ✓ 渗透机场景：Kali（用户名：root；密码：toor）
- ✓ 渗透机场景：BT5（用户名：root；密码：toor）
- ✓ 渗透机场景：WindowsXP（用户名：administrator 密码:123456）

1.进入WebServ2003服务器场景，分析源文件login.php，找到提交的变量名，并将全部的变量名作为Flag（形式：[变量名1&变量名2&变量名3…&变量名n]）提交；

2.通过万能用户名、任意密码登录进入WebServ2003服务器场景，"/"->"Employee Information Query"，查看该页面源文件，找到提交的变量名，并将全部的变量名作为Flag(形式:[变量名1&变量名2&变量名3…&变量名n]）提交；

3.通过对任务第2题页面注入点“_”进行SQL注入渗透测试，在WebServ2003服务器场景中添加账号“Hacker”，密码“P@ssword”，并将注入语句作为Flag提交；

4.进入WebServ2003服务器场景的C:\AppServ\www目录，找到QueryCtrl.php程序，使用EditPlus工具分析并修改PHP源文件，使之可以抵御SQL注入渗透测试，并将修改后的PHP源文件中的F1和F2作为Flag(形式:[F1]+[F2]）提交；

5.再次对该任务第2题页面注入点进行渗透测试，验证此次利用注入点对该WebServ2003服务器场景进行SQL注入渗透测试无效，并将测试后页面回显倒数第2行作为Flag提交。

任务三、Linux系统安全加固

任务环境说明：

- ✓ 服务器场景：CentOS5.5
- ✓ 服务器场景操作系统：CentOS5.5
- ✓ 服务器场景用户名：root；密码：123456
- ✓ 渗透机场景：BT5
- ✓ 渗透机用户名：root,密码：toor

1.在本地PC渗透测试平台BT5对服务器场景CentOS5.5进行服务扫描渗透测试，并将扫描结果上数第5行的4个单词作为Flag（形式：单词1|单词2|单词3|单词4）提交；

2.通过本地PC渗透测试平台BT5对服务器场景CentOS5.5进行远程超级管理员口令暴力破解(使用PC中的渗透测试平台中的字典文件superdic.txt)，并将破解结果Success：后面2个空格之间的字符串作为Flag提交；

3.通过本地PC渗透测试平台BT5打开已经建立的会话，在与CentOS5.5的会话中新建用户admin，并将该用户提权至root权限，并将新建用户admin并提权至root权限全部命令作为Flag(形式:命令1|命令2|…|命令n)提交；

4.修改并在原目录下编译、运行./root/autorunp.c木马程序，使该木马程序能够实现远程连接 8080端口，并在该端口上运行/bin/sh命令行程序，并将运行./root/autorunp.c木马程序以及运行后的系统网络连接状态（netstat -an）增加行内容作为Flag提交；

5.将autorunp.c木马程序设置为系统启动后自动加载，并转入系统后台运行，并将在配置文件中增加的内容作为Flag提交；

6.重新启动CentOS5.5服务器场景,通过PC中渗透测试平台NETCAT远程打开CentOS5.5服务器场景./bin/sh程序，并运行查看IP地址命令，并将运行该命令需要输入的字符串作为Flag提交；

7.对CentOS5.5服务器场景进行安全加固，阻止PC中渗透测试平台对服务器场景CentOS5.5进行远程超级管理员口令暴力破解,并将配置文件增加的内容字符串作为Flag提交；

任务四、 服务端口扫描渗透测试

任务环境说明：

- ✓ 服务器场景：CentOS5.5
- ✓ 服务器场景操作系统：CentOS5.5
- ✓ 服务器场景用户名：root，密码：123456
- ✓ 渗透机场景：BT5
- ✓ 渗透机用户名：root,密码：toor

1.进入本地虚拟机平台BT5中的/root目录,完善该目录下的PortScan.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（PortScan.py脚本功能见该任务第6题）

2. 进入本地虚拟机平台BT5中的/root目录，完善该目录下的PortScan.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（PortScan.py脚本功能见该任务第6题）

3. 进入本地虚拟机平台BT5中的/root目录，完善该目录下的PortScan.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（PortScan.py脚本功能见该任务第6题）

4. 进入本地虚拟机平台BT5中的/root目录，完善该目录下的PortScan.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（PortScan.py脚本功能见该任务第6题）

5. 进入本地虚拟机平台BT5中的/root目录，完善该目录下的PortScan.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（PortScan.py脚本功能见该任务第6题）

6. 进入本地虚拟机平台BT5下执行PortScan.py文件,对靶机服务器(IP:192.168.1.113）进行TCP服务端口号（1-1024）扫描渗透测试，使该渗透测试结果能够在屏幕上打印出靶机服务器的TCP服务端口号(1-1024)当中开放的端口，将PortScan.py文件执行以后，屏幕上的打印结果中的最后一行，最后一个单词字符串作为Flag值提交;

任务五、 数据库安全攻防

任务环境说明：

- ✓ 服务器场景名称：WinServ2003
- ✓ 服务器场景安全操作系统：Microsoft Windows2003 Server
- ✓ 服务器场景用户名：administrator，密码：空

- ✓ 渗透机场景：BT5
- ✓ 渗透机用户名：root,密码：toor

1. 进入PC（虚拟机：Backtrack5），使用Metasploit程序的arp_sweep模块，对数据库服务器所在网段（192.168.1.0/24）进行扫描测试，将该程序执行后的显示结果中的倒数第二行所有字符作为Flag值提交；

2. 通过PC（虚拟机：Backtrack5）中的渗透测试工具对服务器场景WinServ2003进行TCP服务扫描渗透测试（使用工具nmap，使用必须要使用的参数），并将该操作使用命令中必须要使用的参数作为Flag提交；

3.通过PC（虚拟机：Backtrack5）中渗透测试工具对服务器场景WinServ2003进行ping扫描渗透测试(使用工具nmap,使用必须要使用的参数)，并将该操作显示结果中的SqlServer服务名称字符串作为Flag提交；

4.在PC（虚拟机：Backtrack5）下使用Metasploit程序mssql_login,进行数据库超级管理员密码暴力破解渗透测试(使用字典文件./root/dic.txt)，将该程序执行后的显示结果中的倒数第三行successful后面的所有字符作为Flag值提交；

5.通过对服务器场景WinServ2003的数据库服务进行安全加固,阻止攻击机对其进行数据库超级管理员密码暴力破解渗透测试,并将进行安全配置的数据库身份验证选项中的英文单词字符串作为Flag值（形式：进行安全配置的数据库身份验证选项中的唯一一个英文单词字符串）提交；

6.验证在WinServ2003的数据库服务进行安全加固后，再次在PC（虚拟机：Backtrack5）下使用Metasploit程序mssql_login，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/dic.txt），将该程序执行后的显示结果中的倒数第三行failed后面的所有字符作为Flag值提交；

任务六、 SSH弱口令渗透测试

任务环境说明：

- ✓ 服务器场景：Linux
- ✓ 服务器场景操作系统：Linux（版本不详）
- ✓ 渗透机场景：BT5
- ✓ 渗透机用户名：root,密码：toor

1.在本地PC渗透测试平台BT5中使用zenmap工具扫描服务器场景Linux所在网段(例如:172.16.101.0/24)范围内存活的主机IP地址和指定开放的21、22、23端口。并将该操作使用的命令中必须要添加的字符串作为FLAG提交（忽略ip地址）；

2.通过本地PC中渗透测试平台BT5对服务器场景Linux进行系统服务及版本扫描渗透测试，并将该操作显示结果中SSH服务对应的服务端口信息作为FLAG提交；

3.在本地PC渗透测试平台BT5中使用MSF模块对其爆破,使用search命令，并将扫描弱口令模块的名称信息作为FLAG提交；

4.在上一题的基础上使用命令调用该模块，并查看需要配置的信息（使用show options命令），将回显中需要配置的目标地址,密码使用的猜解字典,线程,账户配置参数的字段作为FLAG提交（之间以英文逗号分隔，例hello,test，..,..）；

5.在msf模块中配置目标靶机IP地址，将配置命令中的前两个单词作为FLAG提交；

6.在msf模块中指定密码字典，字典路径为/root/2.txt，用户名为test爆破获取密码并将得到的密码作为FLAG提交；

7.在上一题的基础上，使用第6题获取到的密码SSH到靶机，将test用户家目录中唯一一个后缀为.bmp图片的文件名的字符串作为FLAG提交。

任务七、 Web信息收集

任务环境说明：

- ✓ 服务器场景：Linux
- ✓ 服务器场景操作系统：Linux（版本不详）
- ✓ 渗透机场景：Kali
- ✓ 渗透机用户名：root,密码：toor

1.通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，查看该命令的完整帮助文件），并将该操作使用命令中固定不变的字符串作为Flag提交；

2.通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，扫描目标服务器8080端口，检测其开放状态），并将该操作使用命令中固定不变的字符串作为Flag提交（目标地址以http://10.10.10.1来表示）；

3. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，扫描目标服务器80端口），将回显信息中apache服务的版本参数作为flag提交；

4. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，扫描目标服务器80端口），将回显信息中php的版本参数作为flag提交；

5. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试（使用工具nikto，扫描CGI-BIN目录的文件），将该操作使用的命令中固定不变的字符串作为Flag(目标地址以:http://10.10.10.1来表示)提交；

6. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试，使用工具nikto并结合nmap的扫描结果进行扫描，首先使用nmap

工具对靶机所在网段的80端口进行扫描，并将扫描结果以输出至所有格式的方式输出到指定文件target中,将输出至所有格式需要用到的参数作为flag提交;

7. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行Web扫描渗透测试，使用工具nikto扫描第六题生成的target文件中的网站，并将该操作使用的所有命令作为FLAG提交。

任务八、数据分析与取证

任务环境说明：

- ✓ 服务器场景：WinSrv2003
- ✓ 服务器场景操作系统：Window Server 2003
- ✓ 服务器场景用户名：administrator,密码：空
- ✓ 渗透机场景：WindowsXP
- ✓ 渗透机场景用户名：administrator,密码：123456

1.使用Wireshark查看并分析WindowsXP桌面下的attack.pcapng数据包文件，通过分析数据包attack.pcapng找出黑客的IP地址，并将黑客的IP地址作为FLAG（形式：[IP地址]）提交;

2.继续查看数据包文件attack.pacapng，分析出黑客扫描了哪些端口，并将全部的端口作为FLAG（形式：[端口名1，端口名2，端口名3…，端口名n]）从低到高提交;

3.继续查看数据包文件attack.pacapng分析出黑客最终获得的用户名是什么，并将用户名作为FLAG（形式：[用户名]）提交;

4.继续查看数据包文件attack.pacapng分析出黑客最终获得的密码是什么，并将密码作为FLAG（形式：[密码]）提交;

5.继续查看数据包文件 attack.pacapng 分析出黑客连接一句话木马的密码是什么，并将一句话密码作为 FLAG（形式：[一句话密码]）提交；

6.继续查看数据包文件 attack.pacapng 分析出黑客下载了什么文件，并将文件名及后缀作为 FLAG（形式：[文件名.后缀名]）提交；

7.继续查看数据包文件 attack.pacapng 提取出黑客下载的文件，并将文件里面的内容为 FLAG（形式：[文件内容]）提交；

（三）第二阶段任务书

各位选手是某公司的系统安全管理员，负责服务器（受保护服务器 IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行攻击。

提示：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；需要加固常规漏洞；并对其它参赛队系统进行渗透测试，取得 FLAG 值并提交到裁判服务器。

十五分钟之后，各位选手将真正进入分组对抗环节。

注意事项：

注意 1：任何时候不能人为关闭服务器常用服务端口（21、22、23、53、80），否则将判令停止比赛，第三阶段分数为 0 分；

注意 2：不能对裁判服务器进行攻击，否则将判令停止比赛，第三阶段分数为 0 分。

注意 3：在加固阶段（前十五分钟，具体听现场裁判指令）不得对任何服务器进行攻击，否则将判令攻击者停止比赛，第三阶段分数为 0 分。

注意 4：FLAG 值为每台受保护服务器的唯一性标识，每台受保护服务器仅有一个。

在渗透测试环节里，各位选手需要继续保护你的服务器免受各类黑客的攻击，你可以继续加固你的服务器，你也可以选择攻击其他组的保护服务器。

漏洞列表如下：

1. 靶机上的网站可能存在命令注入的漏洞，要求选手找到命令注入的

相关漏洞，利用此漏洞获取一定权限。

2. 靶机上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限

3. 靶机上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权

4. 操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限。

5. 操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限。

6. 操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

选手通过以上的所有漏洞点，最后得到其他选手靶机的最高权限，并获取到其他选手靶机上的FLAG值进行提交。