上海市“星光计划”第十一届职业院校技能大赛

网络安全赛项技能操作模块样题

一、竞赛时间

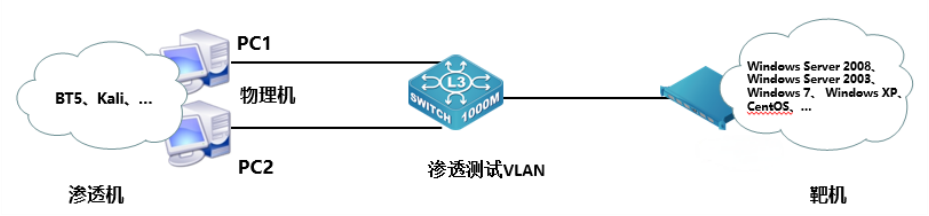
共计 180 分钟。

二、竞赛阶段

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
模块 A	任务一	漏洞扫描与利用	120 分钟	50%
	任务二	Windows 操作系统渗透测试		
	任务三	网页绕过		
	任务四	跨站脚本渗透		
	任务五	内存取证		
	任务六	网络安全事件应急响应		
	任务七	Linux 操作系统渗透测试		
	任务八	恶意 DLL 木马文件分析		
	任务九	Web 信息泄露及渗透		
	任务十	Python 模块利用		
	任务十一	Ubuntu 高级漏洞利用与提权攻防		
	任务十二	Windows 经典漏洞利用与提权		
模块 B	任务一	夺旗挑战	52 分钟	30%
模块 C	任务一	展示讲解	8 分钟	20%

三、竞赛任务书内容

（一）拓扑图



（二）模块 A：安全事件响应、网络安全数据取证、应用安全、系统安全

任务一：漏洞扫描与利用

1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景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 3389 端口对应的服务版本信息字符串作为 Flag 值提交；
2. 在 msfconsole 中用 search 命令搜索 MS12020 RDP 拒绝访问攻击模块，并将回显结果中的漏洞披露时间作为 Flag 值（如：2012-10-16）提交；
3. 在 msfconsole 中利用 MS12020 RDP 拒绝访问漏洞辅助扫描模块，将调用此模块的命令作为 Flag 值提交；
4. 在第 3 题的基础上查看需要设置的选项，并将回显中必须要设置的选项名作为 Flag 值提交；
5. 使用 set 命令设置目标 IP（在第 4 题的基础上），并检测漏洞是否存在，运行此模块将回显结果中最后一个单词作为 Flag 值提交；
6. 在 msfconsole 中利用 MS12020 RDP 拒绝访问攻击模块，将调用此模块的命令作为 Flag 值提交；
7. 使用 set 命令设置目标 IP（在第 6 题的基础上），使用 MS12020 拒绝访问攻击模块，运行此模块将回显结果中倒数第一行的最后一个单词作为 Flag 值提交；
8. 进入靶机关闭远程桌面服务，再次运行 MS12020 拒绝访问攻击模块，运行此模块将回显结果中倒数第二行的最后一个单词作为 Flag 值提交。

任务二：Windows 操作系统渗透测试

1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景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 445 端口对应的服务版本信息字符串作为 Flag 值提交；
2. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景网络连接信息中的 DNS 信息作为 Flag 值（例如：114.114.114.114）提交；
3. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景中的当前最高账户管理员的密码作为 Flag 值提交；
4. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景桌面上 111 文件夹中唯一一个后缀为.docx 文件的文件名称作为 Flag 值提交；
5. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景桌面上 111 文件夹中唯一一个后缀为.docx 文件的文档内容作为 Flag 值提交；
6. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行渗透测试，将该场景桌面上 222 文件夹中唯一一个图片中的英文单词作为 Flag 值提交；

任务三：网页绕过

1. 在渗透机中访问主机地址 http://ip/1.php，将网页中 flag 信息作为 Flag 值提交；
2. 在渗透机中访问主机地址 http://ip/2.php，将网页弹窗结果作为 Flag 值提交；
3. 在渗透机中访问主机地址 http://ip/3.php，将网页中 FLAG 信息作为 Flag 值提交；
4. 在渗透机中访问主机地址 http://ip/4.php，将网页中 flag 信息作为 Flag 值提交；
5. 在渗透机中访问主机地址 http://ip/5.php，将网页中 FLAG 信息作为 Flag 值提交；
6. 在渗透机中访问主机地址 http://ip/6.php，将网页中 flag 信息作为 Flag 值提交。

任务四：跨站脚本渗透

1. 访问服务器网站目录 1，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；
2. 访问服务器网站目录 2，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；
3. 访问服务器网站目录 3，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；
4. 访问服务器网站目录 4，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；
5. 访问服务器网站目录 5，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；
6. 访问服务器网站目录 6，根据页面信息完成条件，将获取到弹框信息作为 Flag 提交；

任务五：内存取证

1. 在服务器中下载内存片段，在内存片段中获取主机信息，将管理员密码作为 Flag 值提交；
2. 在内存片段中获取主机信息，将此片段的地址作为 Flag 值提交；
3. 在内存片段中获取主机信息，将此片段的主机名作为 Flag 值提交；
4. 在内存片段中获取主机信息，将挖矿程序的地址及端口号作为 Flag 值提交；（若为多个用;分开）
5. 在内存片段中获取主机信息，将后台恶意程序所用的程序名称作为 Flag 值提交；
6. 在内存片段中获取主机信息，将此时的浏览器搜寻的关键词作为 Flag 值提交。

任务六：网络安全事件应急响应

1. 找出黑客植入到系统中的二进制木马程序，并将木马程序的名称作为 Flag 值（若存在多个提交时使用英文逗号隔开，例如 bin,sbin,...）提交；
2. 找出被黑客修改的系统默认指令,并将被修改的指令里最后一个单词作为Flag值提交；
3. 找出被黑客替换的系统指令，并将其绝对路径作为 Flag 值提交；
4. 找出被黑客修改的服务配置文件，将文件的 md5 值前四位作为 Flag 值提交；
5. 找出系统中的弱口令账号，将该账号的用户名及密码作为 Flag 值(用户名和密码之间用英文冒号隔开，例如：root:toor)提交

任务七：Linux 操作系统渗透测试

1. 通过本地PC中渗透测试平台Kali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MySQL数据库对应 的服务版本信息字符串作为Flag提交；
2. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行渗透 测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文 件名称作为Flag提交；
3. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行渗透 测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文 件内容作为Flag提交；
4. 通过本地PC中渗透测试平台Kali对服务器场景Linux进行渗透 测试，将该场景/root目录中唯一一个后缀为.bmp文件的文件名称作 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进行渗透 测试，将该场景/root目录中唯一一个后缀为.bmp的图片文件中的英 文单词作为Flag提交。

任务八：恶意 DLL 木马文件分析

1. 分析桌面上的恶意木马压缩文件，找出木马调用的dll文件名称，并将调用的dll文件名作为Flag值提交(Flag排序按照首英文首字母的顺序，多个dll之间以英文逗号隔开)；
2. 分析第一个dll文件，找出恶意文件为防止程序多开创建的函数，并将该函数名称作为Flag值提交；
3. 分析第一个dll文件，找出该代码构造出的可执行文件，并将可执行文件的名称作为Flag值提交;
4. 分析第二个dll文件,找出它最终跳转的有效dll,并将该dll作为Flag值提交；
5. 分析恶意木马文件,找出木马运行后调用的四个可执行文件，并将调用的exe文件名作为Flag值提交(Flag排序按照首英文首字母的顺序,多个exe之间以英文逗号隔开)；
6. 分析恶意木马文件，找出木马运行后对键盘活动进行记录后存储的文件，并存储键盘记录文件的绝对路径作为Flag值提交；
7. 分析第三个dll文件，找出恶意DLL装载病毒的函数位置，并将函数位置作为Flag值提交（例如：sub_10010010,sub_10010020）；

任务九：Web 信息泄露及渗透

1. 通过本地PC中渗透测试平台kali2.0对服务器场景进行渗透测试，将该场景中WordPress的版本号（例如：2.2.3）作为Flag值提交；
2. 服务器场景的网站存在隐藏登录入口,通过流量分析找出管理员登录的URL路径，将完整URL路径作为Flag值提交（IP固定为192.168.111.201）；
3. 使用流量分析工具获取管理员登录请求中的用户名和密码，将用户名和密码作为Flag值（如：admin:123456）提交；
4. 服务器场景的MySQL服务存在配置泄露，提交数据库配置文件中的密码作为Flag值；
5. 利用sudo权限漏洞通过tcpdump提权，提交提权成功后将输出结果的第一行作为Flag值；
6. 服务器场景用户的密码信息可以通过漏洞得到,计算root用户密码位于/etc/shadow中的加密字段信息最后6位（字母小写，不含特殊符号）的SHA-1哈希值作为Flag值；（假设最后6位为123456，示例计算：echo -n "123456" | sha1sum）
7. 服务器场景的/root目录中存在一个加密文件secret_flag.bin，其中包含一段经过编码的字符串。请通过提权获取root权限后，解码该文件内容并提交最后8位明文作为Flag。

任务十：Python 模块利用

1. 通过本地 PC 中渗透测试平台 Kali 对服务器场景进行脚本扫描渗透测试，并将该操作显示结果中 80 端口对应服务版本字符串作为 Flag 值提交(如:Weblogic 8.3.6)；
2. 根据扫描得到的信息，请将 tomcat 版本信息作为 Flag 值提交；
3. 找到网站根路径下的唯一的压缩包文件，并将压缩包的解压密码作为 Flag 提交;
4. 找出 tomcat 后台的用户名和密码,并将 tomcat 后台的密码作为 Flag 值提交；
5. 使用 john 工具破解服务器中除 root 以外的用户密码，并将破解出的用户名及密码的作为 Flag 值提交（用户名和密码之间使用英文冒号分割，多个用户之间用分号隔开，如：qwe:123;john:456）；
6. 找到服务器场景中能够实现提权的模块，将该模块的绝对路径作为 Flag 值提交（绝对路径包括模块自身的名称）；
7. 找出/root 路径下的唯一的 txt 文本，将该文件的内容作为 Flag 值提交；

任务十一：Ubuntu 高级漏洞利用与提权攻防

1. 通过本地PC中渗透测试平台kali2.0对服务器场景进行端口扫描，将发现开放的非标准HTTP服务端口及服务版本（格式：端口号/服务/版本）作为Flag值提交；
2. 通过本地PC中渗透测试平台kali2.0对服务器场景进行Nmap脚本扫描，发现靶机HTTP服务支持危险方法，提交允许上传文件的HTTP方法及测试路径（格式：方法+/path）；
3. 通过上传WebShell反弹Shell后，发现防火墙限制端口，将用于绕过限制的监听端口号作为Flag值提交；
4. 服务器场景存在计划任务提权漏洞,将漏洞关联的软件名称及CVE编号（格式：软件-CVE-XXXX-XXXX）作为Flag值；
5. 服务器场景存在计划任务提权漏洞，利用漏洞进行提权,通过写入/etc/sudoers赋予当前用户root权限,将触发漏洞的恶意脚本路径及写入的内容（格式：路径:命令）作为Flag值提交；
6. 服务器场景的/root目录中存在文件hidden_flag.txt，最终获取root权限后，提交靶机/root目录中的唯一后缀txt文件内容作为Flag值。

任务十二：Windows 经典漏洞利用与提权

1. 通过本地PC中渗透测试平台kali2.0对服务器场景对目标服务器进行端口扫描时，发现非标准HTTP服务端口，将发现的端口号及服务名称（格式：端口/服务）作为Flag值提交；
2. 通过目录扫描工具发现服务器场景的网站存在关键备份文件，将泄露数据库账号密码的文件名及路径（格式：路径/文件名）作为Flag值提交；
3. 使用泄露的数据库账号密码登录SQL Server，提交管理员表中的密码明文作为Flag值；
4. 利用文件上传漏洞获取WebShell，提交上传的木马文件完整路径以及操作系统的主机名（格式：路径/主机名）作为Flag值；
5. 服务器场景存在本地提权漏洞,通过MSF生成后门并反弹Shell后，将用于提权的Windows本地漏洞CVE编号作为Flag值提交；
6. 服务器场景存在本地提权漏洞,提权成功后解密系统用户Hash，将Administrator用户的明文密码作为Flag值提交；
7. 提权成功后，对服务器场景进行文件遍历，找到sqlserver数据库超级管理员账户和密码，将账户和密码（格式：账户/密码）作为Flag值提交；
8. 服务器场景中存在三个key文件，其中包含一段经过编码的字符串。请通过提权获取root权限后，将三个文件的内容（假设三个文件的内容分别为key1,key2,key3,格式：key1/key2/key3）作为Flag值提交。

（三）模块 B：夺旗挑战

一、项目和任务描述：

假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，以便了解最新的攻击手段和技术，了解网络黑客的心态，从而改善您的防御策略。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录答题平台。

二、操作系统环境说明：

客户机操作系统：Windows 10/Windows7

靶机服务器操作系统：Linux/Windows

三、漏洞情况说明：

1.服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.靶机服务器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；

3.靶机服务器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；

4.靶机服务器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；

5.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；

6.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；

7.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。

四、注意事项：

1.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

2. Flag值为每台靶机服务器的唯一性标识，每台靶机服务器同一时间内仅有1个；

3.在登录自动评分系统后，提交靶机服务器的Flag值，同时需要提交该靶机服务器的网关地址；

4.本环节不予补时。

模块 C：展示讲解模块

展示讲解模块总分占比为 20%，面向全部赛队的全部选手，时间限制在 8 分钟以内。参赛队伍应根据赛项设置，围绕生产、管理、服务一线岗位实际需求和实践要求，立足技能创新，并结合专业要求，自行确定展示内容及形式。