XCTF

第2章 Metasploit基础

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

XCTF

0x01 专业术语

- 渗透攻击（Exploit）
- 攻击载荷（Payload）
- Shellcode
- 模块（Module）
- 监听器（Listener）

0x01 专业术语

XCTF

渗透攻击（Exploit）

渗透攻击是指由攻击者或渗透测试者利用一个系统、应用或服务中的安全漏洞，所进行的攻击行为。攻击者使用渗透攻击去入侵系统时，往往会造成开发者所没有预期到的一种特殊结果。流行的渗透攻击技术包括缓冲区溢出、Web应用程序漏洞攻击（比如SQL注入），及利用配置错误等。

0x01 专业术语

XCTF

攻击载荷（Payload）

攻击载荷是我们期望目标系统在被渗透攻击之后去执行的代码，在Metasploit框架中可以自由地选择、传送和植入。例如，反弹式shell是一种从目标主机到攻击主机创建网络连接，并提供Windows命令行shell的攻击载荷，而bindshell攻击载荷则在目标主机上将命令行shell绑定到一个打开的监听端口，攻击者可以连接这些端口来取得shell交互。攻击载荷也可能是简单的在目标操作系统上执行一些命令，如添加用户账号等。

0x01 专业术语

XCTF

Shellcode

Shellcode是在渗透攻击时作为攻击载荷运行的一组机器指令。Shellcode通常以汇编语言编写。在大多数情况下，目标系统执行了Shellcode这一组指令之后，才会提供一个命令行shell或者Meterpreter Shell，这也是shellcode名称的由来。

0x01 专业术语

XCTF

模块（Module）

在本书的上下文环境中，一个模块是指Metasploit框架中所使用的一段软件代码组件。在某些时候，你可能会在使用一个渗透攻击模块（exploit module），也就是用于实际发起渗透攻击的软件组件。而在其他时候，你则可能在使用一个辅助模块（auxiliary module），用来执行一些诸如扫描或系统查点的攻击动作。这些在不断变化和发展中的模块才是使Metasploit框架如此强大的核心。

0x01 专业术语

XCTF

监听器（Listener）

监听器是Metasploit中用来等待连入网络连接的组件，举例来说，在目标主机被渗透攻击之后，它可能会通过互联网回连到攻击主机上，而监听器组件在攻击主机上等待被渗透攻击的系统来连接，并负责处理这些网络连接。

目录 content

0x02 Metasploit用户接口

XCTF

MSF终端

- msfconsole
- 能够访问Metasploit框架中几乎每一个选项和配置
- 在Metasploit框架不断更新的过程中，一些接口和工具被替代或修改，msfconsole的命令集合还保持着相对稳定
- msfconsole是使用Metasploit框架进行渗透测试时最常用的工具
- 熟练掌握msfconsole使用方法很重要

Armitage

- Kali GUI启动；armitage命令启动

目录 content

XCTF

0x03 Metasploit功能程序

XCTF

MSFvenom

- msfvenom
- 集成了载荷生成器、载荷编码器、空指令生成器的功能
- 查看详细指令选项：msfvenom -h

0x03 Metasploit功能程序

XCTF

Nasm Shell

- msfvenom
- 集成了载荷生成器、载荷编码器、空指令生成器的功能
- 查看详细指令选项：msfvenom -h

目录 content

XCTF

0x04 Metasploit Express和Metasploit Pro

XCTF

所有特性		Pro	Express	Community	Framework
情报搜集	导入网络扫描数据	✔	✔	✔	✔
	网络发现	✔	✔	✔	
	基本的渗透攻击	✔	✔	✔	✔
	支持分离任务的MetaModules	✔			
	通过Remote API进行集成	✔			
自动化	易于使用的Web接口	✔	✔	✔	
	智能化渗透	✔	✔		
	自动化的凭据破解	✔	✔		
	渗透测试基准报告	✔	✔		
	向导化的标准基线评估	✔			
	自动化定制工作流的任务链	✔			
	闭环漏洞验证，支持优先修补措施	✔			
隐蔽式渗透能力	动态载荷以规避反病毒软件检测	✔			
	鱼叉式钓鱼及攻击管理	✔			
	OWASP Top 10 Web安全漏洞检测	✔			
	支持高级命令行和 Web接口	✔			

XCTF

Thanks for watching 谢谢