XCTF

第5章 渗透攻击之旅

《Metasploit渗透测试指南》

目录 content

目录 content

XCTF

0x01 渗透攻击基础

渗透攻击基础

- msf> show exploits
- msf> show auxiliary
- msf> show options
- msf> show payloads
- msf> show targets
- info
- set和unset
- setg和unsetg
- save

目录 content

XCTF

0x02 你的第一次渗透攻击

XCTF

- 操作机：Kali Linux
- 靶机：Windows XP SP2
- Step 1：Nmap脚本扫描发现漏洞
  - Nmap脚本扫描：nmap --script=SCRIPT-NAME
  - Nmap脚本路径：/usr/share/nmap/scripts/SCRIPT-NAME.nse
- Step 2：使用msf，根据漏洞选择攻击模块
  - msf > search MODULE_KEYWORD
  - 关键字通常为：漏洞编号，漏洞软件名称，msf模块名称
- Step 3：根据信息搜集结果，配置攻击模块，完成攻击
  - msf > show options

目录 content

0x03 攻击Metasploitable主机

- 操作机：Kali Linux
- 靶机：Metasploitable 2（Ubuntu 8.04）
- Step 1：Nmap扫描发现漏洞
  - Nmap脚本扫描：nmap –sT –A –P0
  - Nmap脚本路径：/usr/share/nmap/scripts/SCRIPT-NAME.nse
- Step 2：使用msf，根据漏洞选择攻击模块
  - 根据服务或软件信息，使用搜索引擎查找相关漏洞信息
  - msf > search MODULE_KEYWORD
  - 关键字通常为：漏洞编号，漏洞软件名称，msf模块名称
- Step 3：根据信息搜集结果，配置攻击模块，完成攻击
  - msf > show options
  - Metasploitable 2有很多漏洞，尝试对多个漏洞进行利用

目录 content

XCTF

0x04 全端口攻击载荷：暴力猜解目标开放的端口

- 全端口攻击载荷是为了应对防火墙
- 当然，我们可以使用Nmap达到同样的目的，这样的载荷是为了提高自动化程度
- msf > search allports


```
msf > search allports

Matching Modules
================

   Name                                                  Disclosure Date  Rank    Description
   ----                                                  ---------------  ----    -----------
   payload/windows/dllinject/reverse_tcp_allports                         normal  Reflective DLL Injection, Reverse All-Port TCP Stager
   payload/windows/meterpreter/reverse_tcp_allports                       normal  Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   payload/windows/patchupdllinject/reverse_tcp_allports                  normal  Windows Inject DLL, Reverse All-Port TCP Stager
   payload/windows/patchupmeterpreter/reverse_tcp_allports                normal  Windows Meterpreter (skape/jt Injection), Reverse All-Port TCP Stager
   payload/windows/shell/reverse_tcp_allports                             normal  Windows Command Shell, Reverse All-Port TCP Stager
   payload/windows/upexec/reverse_tcp_allports                            normal  Windows Upload/Execute, Reverse All-Port TCP Stager
   payload/windows/vncinject/reverse_tcp_allports                         normal  VNC Server (Reflective Injection), Reverse All-Port TCP Stager
```

目录 content

XCTF

0x05 资源文件

- 资源文件（resource files）是MSF终端内包含一系列自动化命令的脚本文件。这些文件实际上是一个可以在MSF终端中执行的命令列表，列表中的命令将按顺序执行。
- FILENAME.rc
- 对于以下情况，资源文件很实用：
  - MSF中常用的指令序列
  - 某一次渗透任务中需要重复使用的载荷的配置指令
  - 其他需要重复执行的MSF指令序列

XCTF

Thanks for watching 谢谢