XCTF

第17章 一次模拟的渗透测试过程

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

XCTF

0x01 前期交互

目标信息

- Windows XP
  - 网络环境：互联网+内网
  - 开放端口：80
- Metasploitable Linux
  - 网络环境：内网
  - 在内网开发大量端口
- 目标：
  - 控制内网中的Metasploitable主机

目录 content

XCTF

0x02 情报搜集

情报搜集

- Nmap扫描：nmap –sT –P0
- 发现80端口的http服务
- 确认为Web服务器

目录 content

XCTF

0x03 威胁建模

威胁建模

- 手动测试/工具测试
- 手动测试是否存在SQL注入漏洞
- 确定攻击路径

目录 content

XCTF

0x04 渗透攻击

渗透攻击

- 根据攻击建模结果选择方式或工具
- Sqlmap利用MS SQL注入漏洞
- 获取注入点，用于MSF终端中的渗透攻击

目录 content

XCTF

0x05 MSF终端中的渗透攻击过程

MSF终端中的渗透攻击过程

- msf > use exploit/windows/mssql/mssql_payload_sqli
- 完成Meterpreter Shell植入

目录 content

XCTF

0x06 后渗透攻击

后渗透攻击

- 扫描Metasploitable靶机
  - 在跳板机上使用nmap扫描内网
- 识别存有漏洞的服务
  - 根据端口扫描结果，使用msf辅助模块中针对特定服务的扫描器

目录 content

XCTF

0x07 攻击Postgresql数据库服务

攻击Postgresql数据库服务

- 根据扫描结果，确认存在Postresql服务及端口号
- 搜索msf中与Postgresql相关的模块
- 选择合适的模块进行渗透攻击，这一过程需要尝试，并不是每一个查找到的模块都能成功利用
- 弱口令字典：
  - Wordlists
  - 。。。

目录 content

XCTF

0x08 攻击一个偏门的服务

攻击一个偏门的服务

- 根据扫描结果，目标提供IRC服务
- 遇到不熟悉的应用或服务，在攻击前需要更多的时间进行深入研究
- 通过MSF的攻击模块查找、exploit-db、搜索引擎等对目标服务的进行研究，查找可能存在的漏洞信息

目录 content

XCTF

0x09 隐藏你的踪迹

隐藏你的踪迹

- 修改时间戳： meterpreter > timestomp
- 修改事件日志： meterpreter > run event_manager
- 流行的取证分析工具：Encase
- 记录下攻击过程对目标系统进行了哪些修改，可以更容易地隐藏踪迹

XCTF

Thanks for watching 谢谢