XCTF

第10章 社会工程学工具包

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

0x01 配置SET工具包

配置SET工具包

- 项目地址： https://github.com/trustedsec/social-engineer-toolkit
- 配置文件： *config/core/set_config*
- 修改metasploit目录为实际目录：
  METASPLOIT_PATH=/usr/share/metasploit-framework
- 开启邮件钓鱼：WEBATTACK_EMAIL=ON
- 关闭自动检测：AUTO_DETECT=OFF
- 开启Apache攻击：APACHE_SERVER=ON

目录 content

XCTF

0x02 针对性钓鱼攻击向量

针对性钓鱼攻击向量

- **Spear-Phishing Attack Vectors**
- Abobe PDF的Collab.collectEmailInfo漏洞
- 设置发件邮箱时需注意，常见邮箱的安全防护措施，如附件检测、第三方邮件客户端认证等

目录 content

0x03 Web攻击向量

Web攻击向量

- Java Applet
- 客户端Web攻击
- 用户名和密码获取
- 标签页劫持攻击（Tabnabbing）
- 中间人攻击
- 网页劫持
- 综合多重攻击方法

目录 content

XCTF

0x04 SET的其他特性

SET的其他特性

- SET的交互式shell：该交互式shell可以替换Meterpreter作为一个攻击载荷
- RATTE：一个基于HTTP隧道攻击载荷，它依赖于HTTP协议进行通信，并利用了目标主机的代理设置
- Web图形界面：一个完整的Web应用攻击程序，能够自动化实施上述讨论的攻击过程
- 无线攻击向量：在目标主机上创建一个假冒的无线热点

XCTF

Thanks for watching 谢谢