XCTF

第3章 情报搜集

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

XCTF

0x01 被动信息搜集

XCTF

被动信息搜集

使用被动、间接的信息搜集技巧，你可以在不接触到目标系统的情况下挖掘目标信息。举例来说，你可以使用这些技巧确定网络边界情况和网络运维人员，甚至了解到目标网络中使用的操作系统和网站服务器软件的类型。

公开渠道情报（OSINT）是一类对公开和已知信息来检索和筛选就可以获取到的目标情报集合。一系列工具软件让被动信息搜集工作变得极其便捷，其中包括Yeti和Whois等。

- whois查询
- Netcraft
- nslookup
- Google Hacking

0x01 被动信息搜集

whois查询

- 查找域名的DNS服务器
- 当DNS服务器部署在目标网站的公司内部，则可以作为攻击点
- 很多情况下，DNS服务器由域名服务、CDN等服务商提供，此时我们不能把DNS服务器作为攻击点

0x01 被动信息搜集

Netcraft

- 网页工具
- 能够发现网站服务器的IP地址

0x01 被动信息搜集

nslookup

- 命令行工具
- 大多数操作系统集成了nslookup

0x01 被动信息搜集

XCTF

Google Hacking

- 使用搜索引擎搜集目标站点信息
- 使用搜索关键字
- 使用与渗透攻击目标相关的搜索词

目录 content

0x02 主动信息搜集

主动信息搜集

在主动信息搜集工作中，我们与目标系统直接交互，从而对其进行更深入的了解。举例来说，我们可以执行端口扫描来确定目标系统开放了哪些端口、运行了哪些服务。多发现一个存活的主机或运行中的服务，就多一些渗透成功的机会。但是请注意：如果你在主动信息搜集过程中不够小心，那么你很可能会被入侵检测系统（IDS）或入侵防御系统（IPS）给逮住，这绝对是一个执行隐秘任务的渗透测试者最不愿意看到的结果。

- nmap端口扫描
- msfconsole: db_nmap
- Metasploit端口扫描

0x02 主动信息搜集

使用nmap进行端口扫描

- 发现存活主机
- 判断目标主机上可能提供的服务
- 根据需要选择扫描参数

0x02 主动信息搜集

在Metasploit中使用数据库

- 将nmap扫描结果导出到文件，之后导入至msfconsole
- 在msfconsole连接至数据库的前提下，使用db_nmap
- 在msfconsole中使用db_nmap扫描结束后，可以使用services, hosts，vulns等指令查看扫描获得的服务、主机、漏洞等信息
- 使用workspace实现每次扫描的结果隔离保存

0x02 主动信息搜集

使用Metasploit进行端口扫描

- Metasploit辅助模块包含了几款内建的端口扫描器
- 内建扫描器在很多方面与Metasploit框架融合，相对于第三方扫描器，在辅助进行渗透测试方面更有优势
- msfconsole中的scanner模块
- msf > search portscan

目录 content

XCTF

0x03 针对性扫描

针对性扫描

针对性扫描是指寻找目标网络中存在的已知可利用漏洞或能够轻松获取后门的特定操作系统、服务、软件以及配置缺陷。

- 服务器消息块协议扫描
- 搜寻配置不当的Microsoft SQL Server
- SSH服务器扫描
- FTP扫描
- 简单网管协议扫描

0x03 针对性扫描

服务器消息块协议扫描

- msf > use auxiliary/scanner/smb/smb_version
- 根据扫描范围配置THREADS选项
- 选择常见且大量存在的漏洞作为扫描目标，更快地定位高风险主机

0x03 针对性扫描

搜寻配置不当的Microsoft SQL Server

- msf > use auxiliary/scanner/mssql/mssql_ping
- MS SQL经常作为其他软件的先决条件被安装，导致管理员忽视对它的配置和更新，甚至不知道其存在，使MS SQL成为进入目标系统的常见后门
- 了解MS SQL默认安装下各参数配置有助于提高扫描效率

0x03 针对性扫描

SSH服务器扫描

- msf > use auxiliary/scanner/ssh/ssh_version
- 作为最常见的远程管理组件之一，SSH服务器的数量和利用价值毋庸赘言
- SSH版本信息对后续的漏洞发现与利用很重要

0x03 针对性扫描

XCTF

FTP扫描

- msf > use auxiliary/scanner/ftp/ftp_version，发现ftp服务器
- msf > use auxiliary/scanner/ftp/anonymous，检查是否允许匿名登录
- 与FTP类似的能够获得很高权限，并且常常由于默认配置或管理员/用户偷懒，处于糟糕的安全配置状况下的服务，是进入一个目标网络最便捷的途径

0x03 针对性扫描

XCTF

简单网管协议扫描

- SNMP能够泄漏配置（例：路由配置）、运行状况（例：资源占用率）等大量对渗透测试工作非常有价值的信息
- SNMP v1和v2天生存在安全缺陷，SNMP v3增强了安全性，然而老旧且从不进行安全配置或更新的设备非常常见
- msf > use auxiliary/scanner/snmp/snmp_login

目录 content

XCTF

0x04 编写自己的扫描器

XCTF

自定义扫描器

- 可以使用Metasploit框架中全部的渗透攻击类和方法，框架还内建代理服务器支持、SSL支持、报告生成以及线程设置等
- 注意自定义扫描器保存路径
- 了解和灵活使用Metasploit框架的模块化代码，能够提高编写代码时的工作效率

XCTF

Thanks for watching 谢谢