

目 录

第 1 章 内网渗透测试基础

1.1 内网基础知识	1	1.2.2 Kali Linux 渗透测试平台及常用工具	13
1.1.1 工作组	1	1.2.3 Windows 渗透测试平台及常用工具	15
1.1.2 域	2	1.2.4 Windows PowerShell 基础	16
1.1.3 活动目录	5	1.2.5 PowerShell 的基本概念	17
1.1.4 域控制器和活动目录的区别	6	1.2.6 PowerShell 的常用命令	18
1.1.5 安全域的划分	6	1.3 构建内网环境	23
1.1.6 域中计算机的分类	7	1.3.1 搭建域环境	23
1.1.7 域内权限解读	8	1.3.2 搭建其他服务器环境	31
1.2 主机平台及常用工具	12		
1.2.1 虚拟机的安装	12		

第 2 章 内网信息收集

2.1 内网信息收集概述	33	2.6 扫描域内端口	54
2.2 收集本机信息	33	2.6.1 利用 telnet 命令进行扫描	54
2.2.1 手动收集信息	33	2.6.2 S 扫描器	55
2.2.2 自动收集信息	44	2.6.3 Metasploit 端口扫描	55
2.2.3 Empire 下的主机信息收集	45	2.6.4 PowerSploit 的 Invoke-portscan.ps1 脚本	56
2.3 查询当前权限	46	2.6.5 Nishang 的 Invoke-PortScan 模块	56
2.4 判断是否存在域	47	2.6.6 端口 Banner 信息	57
2.5 探测域内存活主机	50	2.7 收集域内基础信息	59
2.5.1 利用 NetBIOS 快速探测内网	50	2.8 查找域控制器	61
2.5.2 利用 ICMP 协议快速探测内网	51	2.9 获取域内的用户和管理员信息	63
2.5.3 通过 ARP 扫描探测内网	52	2.9.1 查询所有域用户列表	63
2.5.4 通过常规 TCP/UDP 端口扫描探测内网	53	2.9.2 查询域管理员用户组	65



II 内网安全攻防：渗透测试实战指南

2.10 定位域管理员	65	2.14.3 导入数据	81
2.10.1 域管理员定位概述	65	2.14.4 查询信息	82
2.10.2 常用域管理员定位工具	66	2.15 敏感数据的防护	87
2.11 查找域管理进程	70	2.15.1 资料、数据、文件的定位流程	87
2.11.1 本机检查	70	2.15.2 重点核心业务机器及敏感信息 防护	87
2.11.2 查询域控制器的域用户会话	71	2.15.3 应用与文件形式信息的防护	88
2.11.3 查询远程系统中运行的任务	73	2.16 分析域内网段划分情况及拓扑结构	88
2.11.4 扫描远程系统的 NetBIOS 信息	73	2.16.1 基本架构	89
2.12 域管理员模拟方法简介	74	2.16.2 域内网段划分	89
2.13 利用 PowerShell 收集域信息	74	2.16.3 多层域结构	90
2.14 域分析工具 BloodHound	76	2.16.4 绘制内网拓扑图	90
2.14.1 配置环境	76		
2.14.2 采集数据	80		

第 3 章 隐藏通信隧道技术

3.1 隐藏通信隧道基础知识	91	3.5 SOCKS 代理	146
3.1.1 隐藏通信隧道概述	91	3.5.1 常用 SOCKS 代理工具	146
3.1.2 判断内网的连通性	91	3.5.2 SOCKS 代理技术在网络环境中的 应用	148
3.2 网络层隧道技术	94	3.6 压缩数据	159
3.2.1 IPv6 隧道	94	3.6.1 RAR	160
3.2.2 ICMP 隧道	96	3.6.2 7-Zip	162
3.3 传输层隧道技术	103	3.7 上传和下载	164
3.3.1 IEX 端口转发	104	3.7.1 利用 FTP 协议上传	164
3.3.2 netcat	104	3.7.2 利用 VBS 上传	164
3.3.3 PowerCat	115	3.7.3 利用 Debug 上传	165
3.4 应用层隧道技术	123	3.7.4 利用 Nishang 上传	167
3.4.1 SSH 协议	123	3.7.5 利用 bitsadmin 下载	167
3.4.2 HTTP/HTTPS 协议	129	3.7.6 利用 PowerShell 下载	168
3.4.3 DNS 协议	131		

第 4 章 权限提升分析及防御



4.1 系统内核溢出漏洞提权分析及防范.....169	4.4.1 UAC 简介.....195
4.1.1 通过手动执行命令发现缺失补丁...170	4.4.2 bypassuac 模块.....196
4.1.2 利用 Metasploit 发现缺失补丁.....174	4.4.3 RunAs 模块.....197
4.1.3 Windows Exploit Suggester.....174	4.4.4 Nishang 中的 Invoke-PsUACme 模块.....199
4.1.4 PowerShell 中的 Sherlock 脚本.....176	4.4.5 Empire 中的 bypassuac 模块.....200
4.2 Windows 操作系统配置错误利用 分析及防范.....178	4.4.6 针对绕过 UAC 提权的防御措施.....201
4.2.1 系统服务权限配置错误.....178	4.5 令牌窃取分析及防范.....201
4.2.2 注册表键 AlwaysInstallElevated.....181	4.5.1 令牌窃取.....202
4.2.3 可信任服务路径漏洞.....184	4.5.2 Rotten Potato 本地提权分析.....203
4.2.4 自动安装配置文件.....186	4.5.3 添加域管理员.....204
4.2.5 计划任务.....188	4.5.4 Empire 下的令牌窃取分析.....205
4.2.6 Empire 内置模块.....189	4.5.5 针对令牌窃取提权的防御措施.....207
4.3 组策略首选项提权分析及防范.....190	4.6 无凭证条件下的权限获取分析及 防范.....207
4.3.1 组策略首选项提权简介.....190	4.6.1 LLMNR 和 NetBIOS 欺骗攻击的 基本概念.....207
4.3.2 组策略首选项提权分析.....191	4.6.2 LLMNR 和 NetBIOS 欺骗攻击 分析.....208
4.3.3 针对组策略首选项提权的防御 措施.....195	
4.4 绕过 UAC 提权分析及防范.....195	

第 5 章 域内横向移动分析及防御

5.1 常用 Windows 远程连接和相关命令...211	5.3 哈希传递攻击分析与防范.....231
5.1.1 IPC.....211	5.3.1 哈希传递攻击的概念.....231
5.1.2 使用 Windows 自带的工具获取 远程主机信息.....213	5.3.2 哈希传递攻击分析.....232
5.1.3 计划任务.....213	5.3.3 更新 KB2871997 补丁产生的影响...234
5.2 Windows 系统散列值获取分析与防范...216	5.4 票据传递攻击分析与防范.....235
5.2.1 LM Hash 和 NTLM Hash.....216	5.4.1 使用 mimikatz 进行票据传递.....235
5.2.2 单机密码抓取与防范.....217	5.4.2 使用 kekeo 进行票据传递.....236
5.2.3 使用 Hashcat 获取密码.....224	5.4.3 如何防范票据传递攻击.....238
5.2.4 如何防范攻击者抓取明文密码 和散列值.....228	5.5 PsExec 的使用.....238
	5.5.1 PsTools 工具包中的 PsExec.....238
	5.5.2 Metasploit 中的 psexec 模块.....240



5.6 WMI 的使用.....	242	5.9.1 通过本地 DCOM 执行命令.....	259
5.6.1 基本命令.....	243	5.9.2 使用 DCOM 在远程机器上执行命令.....	260
5.6.2 impacket 工具包中的 wmiexec.....	244	5.10 SPN 在域环境中的应用.....	262
5.6.3 wmiexec.vbs.....	244	5.10.1 SPN 扫描.....	262
5.6.4 Invoke-WmiCommand.....	245	5.10.2 Kerberoast 攻击分析与防范.....	266
5.6.5 Invoke-WMIMethod.....	246	5.11 Exchange 邮件服务器安全防范.....	270
5.7 永恒之蓝漏洞分析与防范.....	247	5.11.1 Exchange 邮件服务器介绍.....	270
5.8 smbexec 的使用.....	250	5.11.2 Exchange 服务发现.....	272
5.8.1 C++ 版 smbexec.....	250	5.11.3 Exchange 的基本操作.....	274
5.8.2 impacket 工具包中的 smbexec.py.....	251	5.11.4 导出指定的电子邮件.....	276
5.8.3 Linux 跨 Windows 远程执行命令.....	252		
5.9 DCOM 在远程系统中的使用.....	258		

第 6 章 域控制器安全

6.1 使用卷影拷贝服务提取 ntds.dit.....	282	6.3.1 使用 mimikatz 转储域散列值.....	296
6.1.1 通过 ntdsutil.exe 提取 ntds.dit.....	282	6.3.2 使用 dcsync 获取域账号和域散列值.....	298
6.1.2 利用 vssadmin 提取 ntds.dit.....	284	6.4 使用 Metasploit 获取域散列值.....	298
6.1.3 利用 vssown.vbs 脚本提取 ntds.dit.....	285	6.5 使用 vshadow.exe 和 quarkspwdump.exe 导出域账号和域散列值.....	301
6.1.4 使用 ntdsutil 的 IFM 创建卷影拷贝.....	287	6.6 Kerberos 域用户提权漏洞分析与防范.....	302
6.1.5 使用 diskshadow 导出 ntds.dit.....	288	6.6.1 测试环境.....	303
6.1.6 监控卷影拷贝服务的使用情况.....	291	6.6.2 PyKEK 工具包.....	303
6.2 导出 NTDS.DIT 中的散列值.....	292	6.6.3 goldenPac.py.....	307
6.2.1 使用 esedbexport 恢复 ntds.dit.....	292	6.6.4 在 Metasploit 中进行测试.....	308
6.2.2 使用 impacket 工具包导出散列值.....	295	6.6.5 防范建议.....	310
6.2.3 在 Windows 下解析 ntds.dit 并导出域账号和域散列值.....	296		
6.3 利用 dcsync 获取域散列值.....	296		

第 7 章 跨域攻击分析及防御

7.1 跨域攻击方法分析.....	311	7.2.1 域信任关系简介.....	311
7.2 利用域信任关系的跨域攻击分析.....	311	7.2.2 获取域信息.....	312



7.2.3 利用域信任密钥获取目标域的 权限.....	315	7.2.5 外部信任和林信任.....	321
7.2.4 利用 krbtgt 散列值获取目标域的 权限.....	318	7.2.6 利用无约束委派和 MS-RPRN 获取 信任林权限.....	323
第 8 章 权限维持分析及防御		7.3 防范跨域攻击.....	327
8.1 操作系统后门分析与防范.....	328	8.2.4 ASPX meterpreter 后门.....	347
8.1.1 粘滞键后门.....	328	8.2.5 PHP meterpreter 后门.....	347
8.1.2 注册表注入后门.....	330	8.3 域控制器权限持久化分析与防范.....	347
8.1.3 计划任务后门.....	331	8.3.1 DSRM 域后门.....	347
8.1.4 meterpreter 后门.....	335	8.3.2 SSP 维持域控权限.....	352
8.1.5 Cymothoa 后门.....	335	8.3.3 SID History 域后门.....	354
8.1.6 WMI 型后门.....	336	8.3.4 Golden Ticket.....	356
8.2 Web 后门分析与防范.....	339	8.3.5 Silver Ticket.....	362
8.2.1 Nishang 下的 WebShell.....	339	8.3.6 Skeleton Key.....	367
8.2.2 weeveily 后门.....	340	8.3.7 Hook PasswordChangeNotify.....	370
8.2.3 webacoo 后门.....	344	8.4 Nishang 下的脚本后门分析与防范.....	371
第 9 章 Cobalt Strike			
9.1 安装 Cobalt Strike.....	374	9.4.1 监听模块.....	387
9.1.1 安装 Java 运行环境.....	374	9.4.2 监听器的创建与使用.....	389
9.1.2 部署 TeamServer.....	376	9.4.3 Delivery 模块.....	391
9.2 启动 Cobalt Strike.....	378	9.4.4 Manage 模块.....	392
9.2.1 启动 cobaltstrike.jar.....	378	9.4.5 Payload 模块.....	393
9.2.2 利用 Cobalt Strike 获取第一个 Beacon.....	379	9.4.6 后渗透测试模块.....	395
9.3 Cobalt Strike 模块详解.....	384	9.5 Cobalt Strike 的常用命令.....	403
9.3.1 Cobalt Strike 模块.....	384	9.5.1 Cobalt Strike 的基本命令.....	403
9.3.2 View 模块.....	384	9.5.2 Beacon 的常用操作命令.....	404
9.3.3 Attacks 模块.....	385	9.6 Aggressor 脚本的编写.....	415
9.3.4 Reporting 模块.....	386	9.6.1 Aggressor 脚本简介.....	415
9.4 Cobalt Strike 功能详解.....	387	9.6.2 Aggressor-Script 语言基础.....	415
		9.6.3 加载 Aggressor 脚本.....	418



跋.....419

