1章节目录

2 主机详细

2.1 主机10.34.100.159

资产名称	--
所属部门	--
资产类型	--
资产价值	--
NetBios名	WIN-RUKID8V8CQK
netbios域名/工作组	WORKGROUP
保护等级	--
主机名	WIN-RUKID8V8CQK(00:50:56:8c:2c:a8)
主机风险状态	极度危险
操作系统信息	Microsoft Windows

序号	猜测类型	用户名	密码(隐藏)	描述
N/A				

端口/漏洞列表

0__其他协议__其他服务				
序号	危险级别	漏洞编号	漏洞名称	返回信息
1	信息	001E93A6	ICMP权限许可和访问控制漏洞CVE-1999-0524	
2	信息	0x1ebc5e	目标主机允许Traceroute探测	

80__TCP__http				
序号	危险级别	漏洞编号	漏洞名称	返回信息

3	高危险	00E713C	Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)【原理扫描】	
4	信息	0x0013026A	检测到目标主机IIS服务正在运行	IIS Webserver:[0: 'IIS/7.5', 1: '7.5']
5	信息	0x001303CC	检测到远程主机HTTP Server正在运行	
6	信息	0x1ebe9a	远程主机HTTP协议版本信息泄漏	
7	信息	0xb2d36ca2	通过HTTP获取目标主机的WWW服务信息	

137__TCP__未知服务				
序号	危险级别	漏洞编号	漏洞名称	返回信息
8	信息	0x001303E2	可通过NetBIOS名字服务端口远程获取系统信息	

1433__TCP__ms-sql-s				
序号	危险级别	漏洞编号	漏洞名称	返回信息
9	信息	0x001303C8	检测到远程主机运行着Microsoft SQL Server	Microsoft SQL Server Version:10.50.1600.0
10	信息	0xb2d3b153	远程探测到Microsoft SQL Server正在运行	Microsoft SQL Server Version:10.50.1600.0

3389__TCP__ms-wbt-server				
序号	危险级别	漏洞编号	漏洞名称	返回信息
11	高危险	0xb2d3957fL	Microsoft Windows远程桌面协议代码执行漏洞(CVE-2012-0002)【原理扫描】	
12	高危险	0xb2d3c1ca	Microsoft Windows RDP协议安全漏洞（CVE-2019-0708）【原理扫描】	

137__UDP__netbios-ns
1025__TCP__NFS-or-IIS
1026__TCP__LSA-or-nterm
1027__TCP__IIS
1029__TCP__ms-lsa
1030__TCP__iad1
1032__TCP__iad3
2383__TCP__ms-olap4

2.2 漏洞详细

【1】Microsoft Windows远程桌面协议代码执行漏洞(CVE-2012-0002)【原理扫描】	
漏洞编号	0xb2d3957fL
漏洞类型	NT关键问题类
危险级别	高危险
影响平台	该漏洞已有修复补丁，如果未能及时安装补丁可采取以下临时修复措施：方法一：禁用终端服务、远程桌面、远程协助和 Windows Small Business Server 2003 远程工作网站功能；方法二：在企业周边防火墙中屏蔽TCP端口3389；方法三：在运行 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 的受支持版本
CVSS分值	9.3
bugtraq编号	
CVE编号	CVE-2012-0002
CNCVE编号	CNCVE-20120002
国家漏洞库编号	CNNVD-201203-241
CNVD编号	
简单描述	Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统

详细描述	Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft Windows XP SP2与SP3， Windows Server 2003 SP2， Windows Vista SP2， Windows Server 2008 SP2， R2及R2 SP1，与Windows 7 Gold与SP1版本中的远程桌面协议(RDP)实现中存在漏洞，该漏洞源于没有正确处理内存中的数据包。远程攻击者可通过发送特制RDP数据包触发访问（1）没有正确初始化或者（2）已被删除的对象，执行任意代码。也称‘ Remote Desktop Protocol Vulnerability ’。该漏洞已有修复补丁，如果未能及时安装补丁可采取以下临时修复措施：方法一：禁用终端服务、远程桌面、远程协助和 Windows Small Business Server 2003 远程工作网站功能；方法二：在企业周边防火墙中屏蔽TCP端口3389；方法三：在运行 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 的受支持版本的系统上启用网络级别身份验证。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://technet.microsoft.com/zh-cn/security/bulletin/ms12-020
参考网址	URL:http://www.nsfocus.net/vulndb/19054,Source:NSFOCUS;URL:http://www.nsfocus.net/vulndb/19054http://secunia.com/advisories/48353,Source:SECUNIA;URL:http://www.nsfocus.net/vulndb/19054http://secunia.com/advisories/48353http://technet.microsoft.com/security/bulletin/MS12-020,Source:MS;

【2】Microsoft Windows RDP协议安全漏洞（CVE-2019-0708）【原理扫描】	
漏洞编号	0xb2d3c1ca
漏洞类型	NT补丁类
危险级别	高危险
影响平台	Windows 7, Windows 2008 R2, and Windows 2008， Windows 2003 and Windows XP
CVSS分值	10.0
bugtraq编号	
CVE编号	CVE-2019-0708
CNCVE编号	CNCVE-20190708
国家漏洞库编号	CNNVD-201905-434
CNVD编号	
简单描述	通过Remote Desktop Service（远程桌面服务）向目标设备发送特制的请求，可以在不需要用户干预的情况下远程执行任意代码
详细描述	通过Remote Desktop Service（远程桌面服务）向目标设备发送特制的请求，可以在不需要用户干预的情况下远程执行任意代码，最终可能会像野火一样蔓延至整个系统，从而让整个系统瘫痪
修补建议	厂商已经发布补丁，获取地址https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/?from=groupmessage&isappinstalled=0

参考网址	

【3】Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)【原理扫描】	
漏洞编号	00E713C
漏洞类型	NT关键问题类
危险级别	高危险
影响平台	Microsoft Windows 7 SP1 Windows Server 2008 R2 SP1Windows 8 Windows 8.1 and Windows Server 2012 Gold and R2
CVSS分值	10.0
bugtraq编号	
CVE编号	CVE-2015-1635
CNCVE编号	CNCVE-20151635
国家漏洞库编号	CNNVD-201504-257
CNVD编号	CNVD-2015-02422
简单描述	Microsoft Windows HTTP.sys 远程执行代码漏洞
详细描述	使用Microsoft IIS 6.0以上版本的Microsoft Windows的HTTP协议堆栈(HTTP.sys)中存在远程执行代码漏洞，该漏洞源于HTTP.sys文件没有正确分析经特殊设计的HTTP请求。成功利用此漏洞的攻击者可以在系统帐户的上下文中执行任意代码。Microsoft Windows 7 SP1，Windows Server 2008 R2 SP1，Windows 8，Windows 8.1，Windows Server 2012 和 Windows Server 2012 R2。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://technet.microsoft.com/library/security/ms15-034
参考网址	URL:http://www.securitytracker.com/id/1032109

【4】检测到目标主机IIS服务正在运行	
漏洞编号	0x0013026A
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0

bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	IIS 是一个WWW服务
详细描述	IIS是一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面
修补建议	信息收集，无需修复
参考网址	

【5】检测到远程主机运行着Microsoft SQL Server	
漏洞编号	0x001303C8
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	SQL Server 是Microsoft 公司推出的关系型数据库管理系统。
详细描述	Microsoft SQL Server 是一个全面的数据库平台，使用集成的商业智能 BI工具提供了企业级的数据管理。Microsoft SQL Server 数据库引擎为关系型数据和结构化数据提供了更安全可靠的存储功能，使您可以构建和管理用于业务的高可用和高性能的数据应用程序。
修补建议	信息收集，无需修复
参考网址	

【6】检测到远程主机HTTP Server正在运行	
漏洞编号	0x001303CC
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	一个开放源代码的网页服务器
详细描述	可以在大多数电脑操作系统中运行，由于其具有的跨平台性和安全性，被广泛使用，是最流行的Web服务器端软件之一。
修补建议	信息收集，无需修复
参考网址	

【7】可通过NetBIOS名字服务端口远程获取系统信息	
漏洞编号	0x001303E2
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	

CNVD编号	
简单描述	NETBIOS协议是由IBM公司开发，主要用于数十台计算机的小型局域网。
详细描述	该协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的统一的命令集，作用是为了给局域网提供网络以及其他特殊功能。
修补建议	信息收集，无需修复
参考网址	

【8】ICMP权限许可和访问控制漏洞CVE-1999-0524	
漏洞编号	001E93A6
漏洞类型	CGI类
危险级别	信息
影响平台	所有系统
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-1999-0524
CNCVE编号	CNCVE-19990524
国家漏洞库编号	0!#!
CNVD编号	
简单描述	ICMP权限许可和访问控制漏洞
详细描述	ICMP信息如netmask和timestamp允许任意主机访问。
修补建议	配置防火墙或过滤路由器以阻止传出的ICMP数据包。阻止类型13或14和/或代码0的ICMP数据包
参考网址	

【9】目标主机允许Traceroute探测	
漏洞编号	0x1ebc5e
漏洞类型	信息收集类
危险级别	信息
影响平台	Traceroute

CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	0
简单描述	目标主机允许Traceroute探测
详细描述	使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者可以利用这些信息来了解目标网络的网络拓扑。
修补建议	信息收集，无需修复
参考网址	

【10】远程主机HTTP协议版本信息泄漏	
漏洞编号	0x1ebe9a
漏洞类型	WEB类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	远程获取主机的HTTP协议版本信息
详细描述	远程获取主机的HTTP协议版本信息，这些信息可能会帮助攻击者决定如何对目标靶机进行攻击。
修补建议	可以修改WEB服务器配置，隐藏协议版本信息。
参考网址	

【11】通过HTTP获取目标主机的WWW服务信息	
漏洞编号	0xb2d36ca2
漏洞类型	WEB类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	探测到目标主机的HTTP Server信息。这可能使得攻击者了解远程www服务的类型，以便进行下一步的攻击。
详细描述	探测到目标主机的HTTP Server信息。这可能使得攻击者了解远程www服务的类型，以便进行下一步的攻击。
修补建议	建议隐藏您HTTP服务器的banner信息
参考网址	

【12】远程探测到Microsoft SQL Server正在运行	
漏洞编号	0xb2d3b153
漏洞类型	MSSQL系统配置
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	

CNVD编号	
简单描述	Microsoft SQL Server是一款流行的SQL数据库系统
详细描述	Microsoft SQL Server是一款流行的SQL数据库系统
修补建议	信息收集，无需修复
参考网址	