1章节目录

2 主机详细

2.1 主机10.34.100.151

资产名称	--
所属部门	--
资产类型	--
资产价值	--
NetBios名	VCONTRAYCOMMSRV
netbios域名/工作组	WORKGROUP
保护等级	--
主机名	VCONTRAYCOMMSRV(00:50:56:b3:00:16)
主机风险状态	极度危险
操作系统信息	Microsoft Windows 7

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	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
2	信息	0x0013026A	检测到目标主机IIS服务正在运行	IIS Webserver:[0: 'IIS/7.0', 1: '7.0']

3	信息	0x001303CC	检测到远程主机HTTP Server正在运行	
4	信息	0x1ebe9a	远程主机HTTP协议版本信息泄漏	
5	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
6	信息	0x001303E2	可通过NetBIOS名字服务端口远程获取系统信息	

3389__TCP__ms-wbt-server				
序号	危险级别	漏洞编号	漏洞名称	返回信息
7	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】	
8	高危险	0xb2d3c1ca	Microsoft Windows RDP协议安全漏洞（CVE-2019-0708）【原理扫描】	
9	中危险	001E88F7	RC4 加密问题漏洞CVE-2015-2808【原理扫描】	
10	中危险	001EA184	TLS/SSL协议 RC4算法安全漏洞CVE-2013-2566【原理扫描】	

137__UDP__netbios-ns
8000__TCP__http-alt

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】RC4 加密问题漏洞CVE-2015-2808【原理扫描】	
漏洞编号	001E88F7
漏洞类型	其他漏洞
危险级别	中危险
影响平台	Microsoft IIS nullMozilla Firefox nullOpera Opera Browser nullApple Safari Google Chrome IBM WebSphere Application Server RedHat JBoss Oracle Glassfish Microsoft IE
CVSS分值	4.3
bugtraq编号	
CVE编号	CVE-2015-2808
CNCVE编号	CNCVE-20152808
国家漏洞库编号	0!#!
CNVD编号	CNVD-2015-02171
简单描述	RC4 加密问题漏洞

详细描述	TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。
修补建议	禁用RC4算法。请参考https://blog.csdn.net/Nedved_L/article/details/81110603以及https://support.microsoft.com/zh-cn/help/2868725/microsoft-security-advisory-update-for-disabling-rc4
参考网址	CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21883640

【4】TLS/SSL协议 RC4算法安全漏洞CVE-2013-2566【原理扫描】	
漏洞编号	001EA184
漏洞类型	CGI类
危险级别	中危险
影响平台	
CVSS分值	5.9
bugtraq编号	
CVE编号	CVE-2013-2566
CNCVE编号	CNCVE-20132566
国家漏洞库编号	0!#!
CNVD编号	CNVD-2013-02724
简单描述	TLS/SSL协议 RC4算法安全漏洞
详细描述	TLS协议和SSL协议中使用的的RC4算法中存在漏洞，该漏洞源于使用大量的单字节偏差。通过在使用相同明文的大量会话中密文的统计分析，远程攻击者利用该漏洞进行明文恢复攻击。
修补建议	禁用RC4算法。请参考https://blog.csdn.net/Nedved_L/article/details/81110603以及https://support.microsoft.com/zh-cn/help/2868725/microsoft-security-advisory-update-for-disabling-rc4
参考网址	MISC:http://cr.yp.to/talks/2013.03.12/slides.pdf

【5】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	

【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】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	

【9】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	

【10】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	