1章节目录

2 主机详细

2.1 主机10.34.100.35

资产名称	--
所属部门	--
资产类型	--
资产价值	--
NetBios名	WIN-5D4D1FH7N6H
netbios域名/工作组	WORKGROUP
保护等级	--
主机名	WIN-5D4D1FH7N6H(08:94:ef:6e:42:bf)
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	0x00130403	检测到远程主机FileMaker service服务正在运行	
2	信息	001E93A6	ICMP权限许可和访问控制漏洞CVE-1999-0524	
3	信息	0x1ebc5e	目标主机允许Traceroute探测	

80__TCP__http

主机详细

序号	危险级别	漏洞编号	漏洞名称	返回信息
4	高危险	00E713C	Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)【原理扫描】	
5	信息	0x0013026A	检测到目标主机IIS服务正在运行	IIS Webserver:[0: 'IIS/8.5', 1: '8.5']
6	信息	0x001303CC	检测到远程主机HTTP Server正在运行	
7	信息	0x1ebe9a	远程主机HTTP协议版本信息泄漏	
8	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
9	信息	0x001303E2	可通过NetBIOS名字服务端口远程获取系统信息	

443__TCP__https				
序号	危险级别	漏洞编号	漏洞名称	返回信息
10	中危险	001E88F7	RC4 加密问题漏洞CVE-2015-2808【原理扫描】	
11	中危险	001EA184	TLS/SSL协议 RC4算法安全漏洞CVE-2013-2566【原理扫描】	
12	中危险	0x1eb685	DES和Triple DES 信息泄露漏洞(CVE-2016-2183)【原理扫描】	
13	低危险	004119A	SSL3.0 加密协议信息泄露漏洞(CVE-2014-3566)【原理扫描】	
14	信息	0x1ebc5d	远程服务使用的是自签名的证书	
15	信息	0x1ebda1	目标服务加密通信使用的SSL加密算法可列取	
16	信息	0x1ebda2	SSL弱加密算法检查【原理扫描】	
17	信息	0x1ebe19	SSL证书使用了弱签名算法sha1【原理扫描】	

18	信息	0xb2d37168	可获取目标服务支持的SSL加密协议	

2179__TCP__vmrdp				
序号	危险级别	漏洞编号	漏洞名称	返回信息
19	信息	0xb2d3c186	探测到Hyper-V管理服务正在运行	

137__UDP__netbios-ns
593__TCP__http-rpc-epmap
1801__TCP__msmq
2103__TCP__zephyr-clt
2105__TCP__eklogin
2107__TCP__msmq-mgmt
3388__TCP__cbserver
3389__TCP__ms-wbt-server
5003__TCP__filemaker
5005__TCP__avt-profile-2
5985__TCP__wsman
8000__TCP__http-alt
49152__TCP__unknown
49153__TCP__unknown
49154__TCP__unknown
49155__TCP__unknown
49157__TCP__unknown
49173__TCP__unknown

49175__TCP__unknown
49201__TCP__unknown

2.2 漏洞详细

【1】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

【2】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

【3】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

【4】DES和Triple DES 信息泄露漏洞(CVE-2016-2183)【原理扫描】	
漏洞编号	0x1eb685
漏洞类型	信息收集类
危险级别	中危险
影响平台	in the TLS SSH and IPSec protocols and other protocols and products have a birthday bound of approximately four billion blocks makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session
CVSS分值	5.3
bugtraq编号	
CVE编号	CVE-2016-2183
CNCVE编号	CNCVE-20162183
国家漏洞库编号	CNNVD-201608-448
CNVD编号	
简单描述	DES和Triple DES 信息泄露漏洞
详细描述	TLS（Transport Layer Security，安全传输层协议）是一套用于在两个通信应用程序之间提供保密性和数据完整性的协议。SSH（全称Secure Shell）是国际互联网工程任务组（IETF）的网络小组（Network Working Group）所制定的一套创建在应用层和传输层基础上的安全协议。IPSec（全称InternetProtocolSecurity）是国际互联网工程任务组（IETF）的IPSec小组建立的一组IP安全协议集。DES和Triple DES都是加密算法。;TLS、SSH和IPSec协议和其它协议及产品中使用的DES和Triple DES密码算法存在安全漏洞。远程攻击者可通过实施生日攻击利用该漏洞获取明文数据。
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://www.openssl.org/blog/blog/2016/08/24/sweet32/

参考网址	链接:https://sweet32.info/ 链接:https://www.sigsac.org/ccs/CCS2016/accepted-papers/ 链接:https://github.com/ssllabs/ssllabs-scan/issues/387#issuecomment-242514633 链接:https://www.openssl.org/blog/blog/2016/08/24/sweet32/ 链接:https://access.redhat.com/security/cve/cve-2016-2183 链接:https://nakedsecurity.sophos.com/2016/08/25/anatomy-of-a-cryptographic-collision-the-sweet32-attack/ 链接:https://www.teskalabs.com/blog/teskalabs-bulletin-160826-seacat-sweet32-issue 链接:https://www.ietf.org/mail-archive/web/tls/current/msg04560.html 链接:https://blog.cryptographyengineering.com/2016/08/24/attack-of-week-64-bit-ciphers-in-tls/ 链接:https://access.redhat.com/articles/2548661 链接:https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2016/august/new-practical-attacks-on-64-bit-block-ciphers-3des-blowfish/ 链接:https://bugzilla.redhat.com/show_bug.cgi?id=1369383 链接:http://www.securityfocus.com/bid/92630

【5】SSL3.0 加密协议信息泄露漏洞(CVE-2014-3566)【原理扫描】	
漏洞编号	004119A
漏洞类型	WEB类
危险级别	低危险
影响平台	OpenSSL through 1.0.1i
CVSS分值	3.1
bugtraq编号	
CVE编号	CVE-2014-3566
CNCVE编号	CNCVE-20143566
国家漏洞库编号	CNNVD-201410-267
CNVD编号	CNVD-2014-06718
简单描述	SSL protocol是Secure Socket Layer（安全套接层协议）的缩写，其目的是为互联网通信提供安全及数据完整性保障。
详细描述	SSL protocol是Secure Socket Layer（安全套接层协议）的缩写，其目的是为互联网通信提供安全及数据完整性保障。OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.1i及之前版本中使用的SSL protocol 3.0版本中存在安全漏洞，该漏洞源于程序使用非确定性的CBC填充。攻击者可借助padding-oracle攻击利用该漏洞实施中间人攻击，获取明文数据。
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://www.openssl.org/news/

参考网址	MLIST:[openssl-dev] 20141014 Patch to mitigate CVE-2014-3566 ("POODLE") URL:http://marc.info/?l=openssl-dev&m=141333049205629&w=2 MISC:http://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html MISC:https://www.openssl.org/~bodo/ssl-poodle.pdf MISC:http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566 MISC:http://blog.cryptographyengineering.com/2014/10/attack-of-week-poodle.html MISC:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html MISC:https://www.imperialviolet.org/2014/10/14/poodle.html CONFIRM:http://blogs.technet.com/b/msrc/archive/2014/10/14/security-advisory-3009008-released.aspx CONFIRM:https://technet.microsoft.com/library/security/3009008.aspx CONFIRM:http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-3566.html CONFIRM:https://access.redhat.com/articles/1232123 CONFIRM:https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/ CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=1076983 CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=1152789 CONFIRM:https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip CONFIRM:https://www.suse.com/support/kb/doc.php?id=7015773

【6】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	

【7】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	

【8】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	

【9】检测到远程主机FileMaker service服务正在运行	
漏洞编号	0x00130403
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	FileMaker是一款功能强大且简单易用的数据库软件
详细描述	用于创建可在 iPad、iPhone、Windows、Mac 和 Web 上运行的自定义商业解决方案。可使用 FileMaker Pro 管理信息，并与团队共享信息。
修补建议	信息收集，无需修复
参考网址	

【10】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	

【11】远程服务使用的是自签名的证书	
漏洞编号	0x1ebc5d
漏洞类型	OpenSSL
危险级别	信息
影响平台	SSL
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	远程服务使用的是自签名的证书
详细描述	目标机器提供的服务使用的是自签名的证书，请确保您的通信安全。
修补建议	请检查证书，及时更换认证证书。

参考网址	

【12】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	

【13】目标服务加密通信使用的SSL加密算法可列取	
漏洞编号	0x1ebda1
漏洞类型	OpenSSL
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	目标服务加密通信使用的SSL加密算法可获取。
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	信息收集，无需修复
参考网址	

【14】SSL弱加密算法检查【原理扫描】	
漏洞编号	0x1ebda2
漏洞类型	OpenSSL
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	目标机器存在SSL弱加密算法
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	信息收集，无需修复
参考网址	

【15】SSL证书使用了弱签名算法sha1【原理扫描】	
漏洞编号	0x1ebe19

漏洞类型	其他漏洞
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	SSL证书使用了弱签名算法sha1
详细描述	SSL证书使用了弱签名算法sha1
修补建议	可通过配置禁用弱签名算法.
参考网址	

【16】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	

【17】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	

【18】可获取目标服务支持的SSL加密协议	
漏洞编号	0xb2d37168
漏洞类型	DNS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	可获取目标服务支持的SSL加密协议
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	扫描过程中获取的信息，可以不做修复。
参考网址	

【19】探测到Hyper-V管理服务正在运行	
漏洞编号	0xb2d3c186
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	探测到Hyper-V管理服务正在运行
详细描述	Hyper-V是微软提出的一种系统管理程序虚拟化技术，能够实现桌面虚拟化
修补建议	信息收集，无需修复
参考网址	