渗透测试报告

第1章 概述

1.1测试目的

通过对上海通用的主机系统进行安全性评估，可以了解到其外网主机系统当前的安全现状及其面临的安全威胁，并及时发现存在的技术性安全弱点，作为下一阶段安全加固工作的重要依据。

1.3参考标准

《上海通用安全管理标准》

1.3评估内容

以下是本次主机系统评估的具体范围，共248台。其中内网主机126台，外网映射主机122台。详细见下表：

IP 地址（共4台）
10.8.4.11，10.8.4.12．10.18.70.1. 10.18.70.2

1.4. 风险赋值参照标准

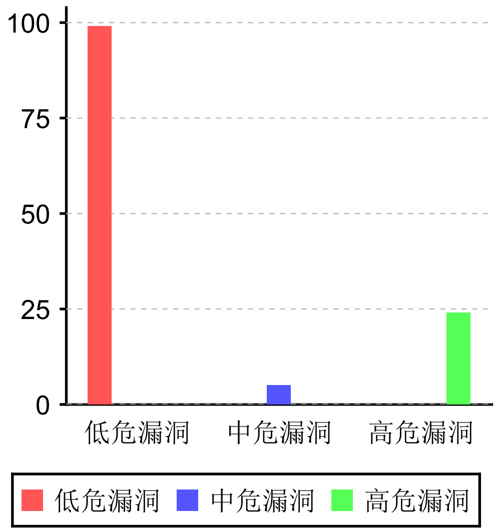
安全风险与信息资产密切相关，在一定条件或环境下可能被威胁利用，从而造成资产损失。风险的出现有各种原因，如软件开发过程中的质量问题，系统管理员的配置问题以及安全管理方面的问题，它们的共同特性就是给攻击者提供了对信息资产进行攻击的机会。

参照国际通行标准和经验，我们在本次评估中将资产存在的风险赋值分为3个等级，分别是高、中、低，如下表所示：

赋值	说明（当该弱点被威胁利用时引起的后果）
高	企业信息资产重大损失或直接导致业务活动大范围中断，影响范围较广
中	企业信息资产一般损失或直接影响业务活动，或局部业务活动的中断
低	企业信息-资产损失很小或间接影响业务活动的连续性
符合	企业信息资产无损失，且可以满足安全要求
说明	信息资产损失包括：信息被窃取、信息被篡改

第2章 扫描结果分析

2.1. 扫描结果综述



2.1.

name	cve	type	description
HTTP Debugging Methods (TRACE/TRACK) Enabled	CVE-2003-1567, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:P/A:
HTTP Debugging Methods (TRACE/TRACK) Enabled	CVE-2003-1567, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:P/A:
HTTP Debugging Methods (TRACE/TRACK) Enabled	CVE-2003-1567, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:P/A:
HTTP Debugging Methods (TRACE/TRACK) Enabled	CVE-2003-1567, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:P/A:
SSL/TLS: Certificate Expired	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:P/A:
SSL/TLS: Report Vulnerable Cipher Suites	CVE-2016-2183, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:P/I:N/A:
SSL/TLS: Certificate Expired	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:P/A:
SSL/TLS: Report Vulnerable Cipher Suites	CVE-2016-2183, CVE-	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:P/I:N/A:
SSL/TLS: Untrusted Certificate Authorities	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:P/A:
SSL/TLS: Certificate Expired	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:P/A:
SSL/TLS: Untrusted Certificate Authorities	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:P/A:
SSH Weak Encryption Algorithms Supported	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:

name	cve	type	description
SSH Weak Encryption Algorithms Supported	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSH Weak Encryption Algorithms Supported	NOCVE	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Report Weak Cipher Suites	CVE-2013-2566,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol	CVE-2016-0800,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Report Weak Cipher Suites	CVE-2013-2566,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol	CVE-2016-0800,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Report Weak Cipher Suites	CVE-2013-2566,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol	CVE-2016-0800,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: SSLv3 Protocol CBC Cipher Suites	CVE-2014-3566	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Report Weak Cipher Suites	CVE-2013-2566,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol	CVE-2016-0800,CVE-	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
SSL/TLS: SSLv3 Protocol CBC Cipher Suites	CVE-2014-3566	高危漏洞	cvss_base_vector=AV:N/AC:M/Au:N/C:P/I:N/A:
TCP timestamps	NOCVE	中危漏洞	cvss_base_vector=AV:N/AC:H/Au:N/C:P/I:N/A:
TCP timestamps	NOCVE	中危漏洞	cvss_base_vector=AV:N/AC:H/Au:N/C:P/I:N/A:
SSH Weak MAC Algorithms Supported	NOCVE	中危漏洞	cvss_base_vector=AV:N/AC:H/Au:N/C:P/I:N/A:
SSH Weak MAC Algorithms Supported	NOCVE	中危漏洞	cvss_base_vector=AV:N/AC:H/Au:N/C:P/I:N/A:
SSH Weak MAC Algorithms Supported	NOCVE	中危漏洞	cvss_base_vector=AV:N/AC:H/Au:N/C:P/I:N/A:
ICMP Timestamp Detection	CVE-1999-0524	低危漏洞	cvss_base_vector=AV:L/AC:L/Au:N/C:N/I:N/A:
OS Detection Consolidation and	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Traceroute	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CPE Inventory	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
ICMP Timestamp Detection	CVE-1999-0524	低危漏洞	cvss_base_vector=AV:L/AC:L/Au:N/C:N/I:N/A:

name	cve	type	description
OS Detection Consolidation and	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Hostname discovery from server	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Traceroute	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CPE Inventory	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
OS Detection Consolidation and	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Hostname discovery from server	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Traceroute	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CPE Inventory	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
FTP Banner Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
vsFTPd FTP Server Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Protocol Versions Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Protocol Algorithms Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Protocol Versions Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Protocol Algorithms Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Protocol Versions Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSH Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:

name	cve	type	description
SSH Protocol Algorithms Supported	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Apache Web Server Version Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Apache Web Server Version Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
RPC portmapper (TCP)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Obtain list of all port mapper registered	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
RPC portmapper (TCP)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Obtain list of all port mapper registered	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
RPC portmapper (TCP)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Obtain list of all port mapper registered	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Certificate - Self-Signed Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Non Weak Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Collect and Report Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Perfect Forward Secrecy (PFS)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:

name	cve	type	description
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Supported Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Apache Web Server Version Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Medium Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Certificate - Self-Signed Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Non Weak Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Collect and Report Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Perfect Forward Secrecy (PFS)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Supported Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Apache Web Server Version Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Medium Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Oracle Version Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Service Detection with nmap	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
MySQL/MariaDB Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Service Detection with 'GET' Request	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
MySQL/MariaDB Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:

name	cve	type	description
Service Detection with 'GET' Request	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Apache JServ Protocol v1.3 Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
DIRB (NASL wrapper)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Security Headers Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Nikto (NASL wrapper)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
HTTP Server type and version	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
DIRB (NASL wrapper)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
CGI Scanning Consolidation	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Nikto (NASL wrapper)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Non Weak Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Collect and Report Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
OpenVAS Manager Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Perfect Forward Secrecy (PFS)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Service Detection with '<xml/>' Request	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Supported Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Medium Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Services	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Non Weak Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:

name	cve	type	description
SSL/TLS: Collect and Report Certificate	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
OpenVAS Manager Detection	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Perfect Forward Secrecy (PFS)	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
Service Detection with '<xml/>' Request	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Supported Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:
SSL/TLS: Report Medium Cipher Suites	NOCVE	低危漏洞	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A: