网安联
Wang An Lian

抗击“疫”情，我们在行动！
我国网络安全等级保护2.0制度解读及测评实战（案例）分享

广州华南信息安全测评中心
袁毅鸣

总体一览

- 1、等级保护发展历程

1、等级保护发展历程-等保1.0时代

1994-2003
政策环境营造

- 1994年，国务院颁布《中华人民共和国计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。
- 2003年，中央办公厅、国务院办公厅颁发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）明确指出“实行信息安全等级保护”。

2004-2006
工作开展准备

- 2004-2006年，公安部联合四部委开展涉及65117家单位，共115319个信息系统的等级保护基础调查和等级保护试点工作，为全面开展等级保护工作奠定基础。

2007-2010
工作正式启动

- 2007年6月，四部门联合出台《信息安全等级保护管理办法》。
- 2007年7月，四部门联合颁布《关于开展全国重要信息系统安全等级保护定级工作的通知》。
- 2007年7月20日，召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施。

2010-2016
工作规模推进

- 2010年4月，公安部出台《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》，提出等级保护工作的阶段性目标。
- 2010年12月，公安部和国务院国有资产监督管理委员会联合出台《关于进一步推进中央企业信息安全等级保护工作的通知》，要求中央企业贯彻执行等级保护工作。

1、等级保护发展历程-等保2.0工作

- 2016年10月10日，第五届全国信息安全等级保护技术大召开，公安部网络安全保卫局郭启全总工指出“**国家对网络安全等级保护制度提出了新的要求，等级保护制度已进入2.0时代**”。
- 2016年11月7日，《中华人民共和国网络安全法》正式颁布，第二十一条明确“**国家实行网络安全等级保护制度……**”

- 以《GB17859 计算机信息系统安全保护等级划分准则 》、《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求 》为代表的等级保护系列配套标准，习惯称为**等保1.0标准**。
- 2013年，全国信息安全标准化技术委员会授权**WG5-信息安全评估工作组**开始启动等级保护新标准的研究。
- 2017年1月至2月，**全国信息安全标准化技术委员会**发布《 网络安全等级保护基本要求》系列标准、《 网络安全等级保护测评要求 》系列标准等“征求意见稿”。
- 2017年5月，**国家公安部发布**《GA/T 1389—2017 网络安全等级保护定级指南》、《GA/T 1390.2—2017 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求 》等4个公共安全行业等级保护标准。

1、等级保护发展历程-等保2.0工作

等级保护2.0时代，将根据信息技术发展应用和网络安全态势，不断丰富制度内涵、拓展保护范围、完善监管措施，逐步健全网络安全等级保护制度政策、标准和支撑体系。

口等级保护上升为法律

《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

口等级保护对象将不断拓展

随着云计算、移动互联、大数据、物联网、人工智能等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，等保保护对象的外延将不断拓展。

口等级保护工作内容将持续扩展

在定级、备案、建设整改、等级测评和监督检查等规定动作基础上，2.0时代风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

口等级保护体系将进行重大升级

2.0时代，主管部门将继续制定出台一系列政策法规和技术标准，形成运转顺畅的工作机制，在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。

1、等级保护发展历程

第二十一条

国家实行网络安全等级保护制度、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）**制定内部安全管理制度和操作规程**，确定网络安全负责人，落实网络安全保护责任；

（二）**采取防范计算机病毒和网络攻击、网络侵入**等危害，网络安全行为**的技术措施**；

（三）**采取监测、记录网络运行状态**、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于**六个月**；（日志留存）；

（四）采取数据分类、重要数据备份和加密等措施；（数据安全）；

（五）法律、行政法规规定的其他义务。

。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰

等级保护发展历程

第五十九条

网络运营者不履行本法**第二十一条、第二十五条**规定的网络安全保护义务的，由有关主管部门**责令改正，给予警告**；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对**直接负责的主管人员**处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

总体一览

- 2、网络安全等级保护2.0
  标准的特点和变化

2、网络安全等级保护2.0-标准的特点和变化

	等保1.0				等保2.0			
要求	层面	等保二级	等保三级	等保四级	层面	等保二级	等保三级	等保四级
技术要求	物理安全	19	32	33	安全物理环境	15	22	24
	网络安全	18	33	32	安全通信网络	4	8	11
	主机安全	19	32	36	安全区域边界	11	20	21
	应用安全	19	31	36	安全计算环境	23	34	36
	数据安全	4	8	11	安全管理中心	4	12	13

2、网络安全等级保护2.0-安全物理环境

表1 安全物理环境控制点/要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	物理位置的选择	0	2	2	2
2	物理访问控制	1	1	1	2
3	防盗窃和防破坏	1	2	3	3
4	防雷击	1	1	2	2
5	防火	1	2	3	3
6	防水和防潮	1	2	3	3
7	防静电	0	1	2	2
8	温湿度控制	1	1	1	1
9	电力供应	1	2	3	4
10	电磁防护	0	1	2	2

- 对部分要求内容的进行了修订，从整体显得更加的合理化，人性化。
- 增加了防静电的消除措施要求项。

2、网络安全等级保护2.0-安全通信网络

表2 安全通信网络控制点/要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	网络架构	0	2	5	6
2	通信传输	1	1	2	4
3	可信验证	1	1	1	1

- 对部分要求内容的进行了修订，删除了带宽控制的要求，强调了通信链路和关键网络设备的冗余，更加合理化。
- 新增了通信传输、可信验证控制点。

2、网络安全等级保护2.0-安全区域边界

表3 安全区域边界控制点/要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	边界防护	1	1	4	6
2	访问控制	3	4	5	5
3	入侵防范	0	1	4	4
4	恶意代码防范	0	1	2	2
5	安全审计	0	3	4	3
6	可信验证	1	1	1	1

- 对部分要求内容的进行了修订，访问控制细粒度更细，强调了无线网络的安全防护，使边界防护更严格。
- 新增了垃圾邮件防范、远程访问&互联网访问独立审计、可信验证控制点。

2、网络安全等级保护2.0-安全计算环境

表4 安全计算环境控制点/要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	身份鉴别	2	3	4	4
2	访问控制	3	4	7	7
3	安全审计	0	3	4	4
4	入侵防范	2	5	6	6
5	恶意代码防范	1	1	1	1
6	可信验证	1	1	1	1
7	数据完整性	1	1	2	3
8	数据保密性	0	0	2	2
9	数据备份与恢复	1	2	3	4
10	剩余信息保护	0	1	2	2
11	个人信息保护	0	2	2	2

- 检测对象：包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等，强调了网络设备、计算设备的安全配置统一化。
- 新增了增加了可信验证和个人信息保护两个控制点，减少了通信完整性、通信保密性、抗抵赖、软件容错、资源控制五个控制点。

2、网络安全等级保护2.0-安全管理中心

表5 安全管理中心控制点/要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	系统管理	2	2	2	2
2	审计管理	2	2	2	2
3	安全管理	0	2	2	2
4	集中管控	0	0	6	7

- 对原系统运维管理中监控管理和安全管理中心进行了调整，增加了相关管理要求，使管理更集中化。
- 新增了系统管理员、审计管理员、安全管理员的要求。

2、标准的特点和变化归纳

特点1— 对象范围扩大

新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容

2、标准的特点和变化归纳

特点2— 分类结构统一

新标准“基本要求、设计要求和测评要求”分类框架统一，形成了“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”支持下的三重防护体系架构。

2、标准的特点和变化归纳

特点3—强化可信计算

新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求。

2、标准的特点和变化归纳

变化1—名称的变化

- 原来：
  - 《信息系统安全等级保护基本要求》
- 改为：
  - 《信息安全等级保护基本要求》
- 再改为（与《网络安全法》保持一致）
  - 《网络安全等级保护基本要求》

2、标准的特点和变化归纳

变化2—对象的变化

- 原来：信息系统
- 改为：等级保护对象（网络和信息系统）
- 安全等级保护的对象包括网络基础设施（广电网、电信网、专用通信网络等）、云计算平台/系统、大数据平台/系统、物联网、工业控制系统、采用移动互联技术的系统等。

2、标准的特点和变化归纳

变化3—安全要求的变化

- 原来：安全要求
- 改为：安全通用要求和安全扩展要求
- 安全通用要求是不管等级保护对象等级保护对象形态如何必须满足的要求，针对云计算、移动互联、物联网和工业控制系统提出了特殊要求，称为安全扩展要求。

2、标准的特点和变化归纳

变化4— 章节结构的变化

- 8 第三级安全要求
- 8.1 安全通用要求
- 8.2 云计算安全扩展要求
- 8.3 移动互联安全扩展要求
- 8.4 物联网安全扩展要求
- 8.5 工业控制系统安全扩展要求

2、标准的特点和变化归纳

变化5— 分类结构的变化

- **技术部分：**
  - 安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心
  - **管理部分：**
  - 安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

2、标准的特点和变化归纳

变化6—增加了云计算安全扩展要求

- 云计算安全扩展要求章节针对云计算的特点提出特殊的保护要求。对云计算环境主要增加的内容包括“基础实施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”、和“云计算环境管理”等方面。

2、标准的特点和变化归纳

变化7— 增加了移动互联安全扩展要求

- 移动互联安全扩展要求章节针对移动互联的特点提出特殊的保护要求。对移动互联环境主要增加的内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”、和“移动应用软件开发”等方面。

2、标准的特点和变化归纳

变化8— 增加了物联网安全扩展要求

- 物联网安全扩展要求章节针对物联网的特点提出特殊的保护要求。对物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”、和“数据融合处理”等方面。

2、标准的特点和变化归纳

变化9— 增加了工业控制系统安全扩展要求

- 工业控制系统安全扩展要求章节针对工业控制系统的特点提出特殊的保护要求。对工业控制系统主要增加的内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”、和“控制设备安全”等方面。

2、标准的特点和变化归纳

变化10— 增加了应用场景的说明

- 增加附录C描述等级保护安全框架和关键技术，增加附录D描述云计算应用场景，附录E描述移动互联应用场景，附录F描述物联网应用场景，附录G描述工业控制系统应用场景。
- 附录H描述大数据应用场景（安全扩展要求）。

2、标准的特点和变化归纳

变化10— 增加了应用场景的说明

- 增加附录C描述等级保护安全框架和关键技术，增加附录D描述云计算应用场景，附录E描述移动互联应用场景，附录F描述物联网应用场景，附录G描述工业控制系统应用场景。
- 附录H描述大数据应用场景（安全扩展要求）。

2、标准的特点和变化归纳

总体一览

-
- 3、测评实战（案例）分享

3、网络安全等级保护测评具体流程

一，定级

信息系统安全等级，由系统运用、使用单位根据《信息系统安全等级保护定级指南》自主确定信息系统的安全保护等级，有主管部门的，应当经主管部门审批。对于拟确定等级的信息系统，还应经专家评审会评审。新建信息系统在设计、规划阶段确定安全保护等级。

二，备案

运营、使用单位在确定等级后到所在地的市级及以上公安机关备案。新建二级及以上信息系统在投入运营后30日内、已运行的二级及以上信息系统在等级确定30日内备案。

3、网络安全等级保护测评具体流程

三，开展等级测评

运营、使用单位或者主管部门应当选择合规测评机构，定期对信息系统安全等级状况开展等级测评。三级及以上信息系统至少每年进行一次等级测评

。

四，系统安全建设

运营使用单位按照管理规范和技术标准，选择管理办法要求的信息安全产品，建设符合等级要求的信息安全设施，建立安全组织，制定并落实安全管理制度。

五，监督检查

公安机关依据信息安全等级保护管理规范，监督检查运营使用单位开展等级保护工作，定期对信息系统进行安全检查。运营使用单位应当接受公安机关的安全监督、检查、指导，如实向公安机关提供有关材料。

3、网络安全等级保护测评-定级备案

定级备案常见需要提交材料：

1、备案单位表（按系统所属单位情况填写）

2、备案系统表（按系统情况进行填写，如：资产数量）

3、定级报告

4、工作小组名单（根据某地市的要求为单位一把手或党委书记，副组长为分管部门领导）

5、（1）上级主管部门意见；（2）行业定级指标；（3）专家评审意见（一般为这三种中的其中一种，常见为专家评审）

6、按标准刻录光盘（RAR格式，广州局除外）

3、网络安全等级保护测评-定级备案（2）

3级系统额外需要提交材料：

1、拓扑结构及说明；

2、组织机构及管理制度；

3、系统安全保护设施设计实施方案或改建实施方案；

4、系统使用的安全产品清单及认证、销售许可证明。

3、网络安全等级保护测评-定级材料填写（单位表

表一

01 单位名称	XXX 局	
02 单位地址	广东 省(自治区、直	
	越秀 县(区、市、旗	
03 邮政编码	5 1 0 0 0 0	
05 单位负责人	姓 名	张三
	办公电话	020-81000000
06 责任部门	信息中心	
07 责任部门联系人	姓 名	李四
	办公电话	020-81000000
	移动电话	13800000000
08 隶属关系	□1 中央 □2	
	盟)	
	□4 县（区、市、旗） □9	
09 单位类型	□1 党委机关 √2 政府机	

09 单位类型	□1 党委机关 √2 政府机关 □3 事业单位 □4 企业 □9 其他_____			
10 行业类别	□11 电信	□12 广电	□13 经营性公众互联网	
	□21 铁路	□22 银行	□23 海关	□24 税务
	□25 民航	□26 电力	□27 证券	□28 保险
	□31 国防科技工业	□32 公安	□33 人事劳动和社会保障	□34 财政
	□35 审计	□36 商业贸易	□37 国土资源	□38 能源
	□39 交通	□40 统计	□41 工商行政管理	□42 邮政
	□43 教育	√44 文化	□45 卫生	□46 农业
	□47 水利	□48 外交	□49 发展改革	□50 科技
	□51 宣传	□52 质量监督检验检疫		
	□99 其他_____			

11 信息系统总数	2 个	12 第二级信息系统数	1 个	13 第三级信息系统数	1 个
		14 第四级信息系统数	0 个	15 第五级信息系统数	0 个

3、网络安全等级保护测评-定级材料填写（系统表

表二（行政审批系统）信息系统情况

01 系统名称		行政审批系统			02 系统编号	0	0	0	1
03 系统承载业务情况	业务类型	□1 生产作业 □2 指挥调度 □3 管理控制 □4 内部办公 √5 公众服务 □9 其他_____							
	业务描述								
04 系统服务情况	服务范围								
	服务对象								
05 系统网络平台	覆盖范围								
	网络性质								
06 系统互联情况									
07 关键产品使用情况									
08 系统采用服务情况		序号	服务类型		服务责任方类型				
					本行业（单位）		国内其他服务商		国外服务商
		1	等级测评	√有□无	√		□		□
		2	风险评估	√有□无	√		□		□
		3	灾难恢复	√有□无	√		□		□
		4	应急响应	√有□无	√		□		□
		5	系统集成	√有□无	√		□		□
		6	安全咨询	√有□无	√		□		□
		7	安全培训	√有□无	√		□		□
		8	其它_____		□		□		□
09 等级测评单位名称		XX 公司							
10 何时投入运行使用		XX 年 X 月 X 日							
11 系统是否是分系统		√是 □否（如选择是请填下两项）							
12 上级系统名称									
13 上级系统所属单位名称									

3、网络安全等级保护测评-录入测评联盟系统


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，广州医科大学单位的：

第三级 校园一卡通 系统

予以备案。

证书编号：4401184338800001

中华人民共和国公安部监制

3、网络安全等级保护测评-测评准备阶段

资产材料收集：

序号	机房名称	物理位置	重要程度	是否抽选
1	机房1	机房1	关键	是

序号	设备名称	是否虚拟设备	系统及版本	品牌型号	用途	IP地址	数量（台/套）	重要程度	是否抽选
1	接入交换机	是	hos12.3	华为NSP5000	云平台接入交换机	10.10.1.12		重要	是

序号	文档名称	主要内容
1	内部信息安全组织管理制度	内部信息安全组织管理
2	内部人员安全管理制度	内部人员安全管理
3	外部组织管理制度	外部组织管理

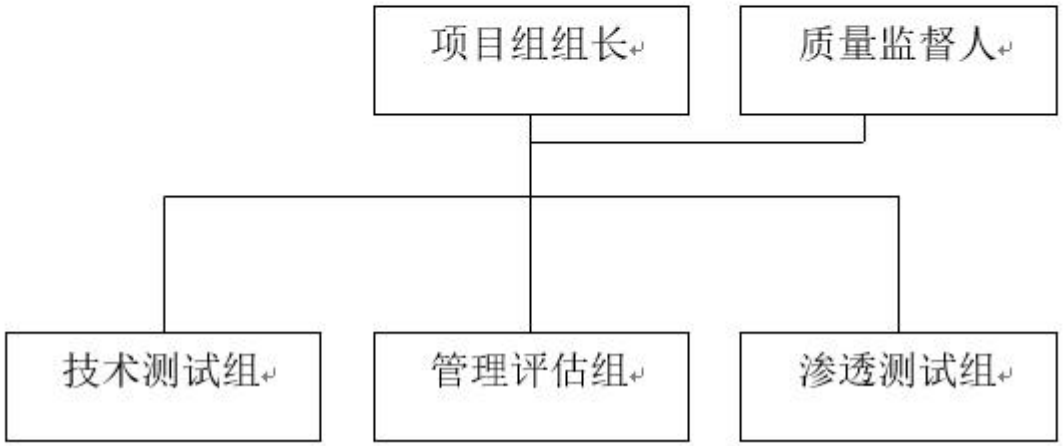
序号	姓名	岗位/角色	联系方式
1	玛丽	信息负责人	010-82023002
2	刘刚	网络人员	010-82023002
3	张三	管理制度人员	
4	赵四	主机管理员	
5	王五	应用管理	

3、网络安全等级保护测评-方案编制阶段

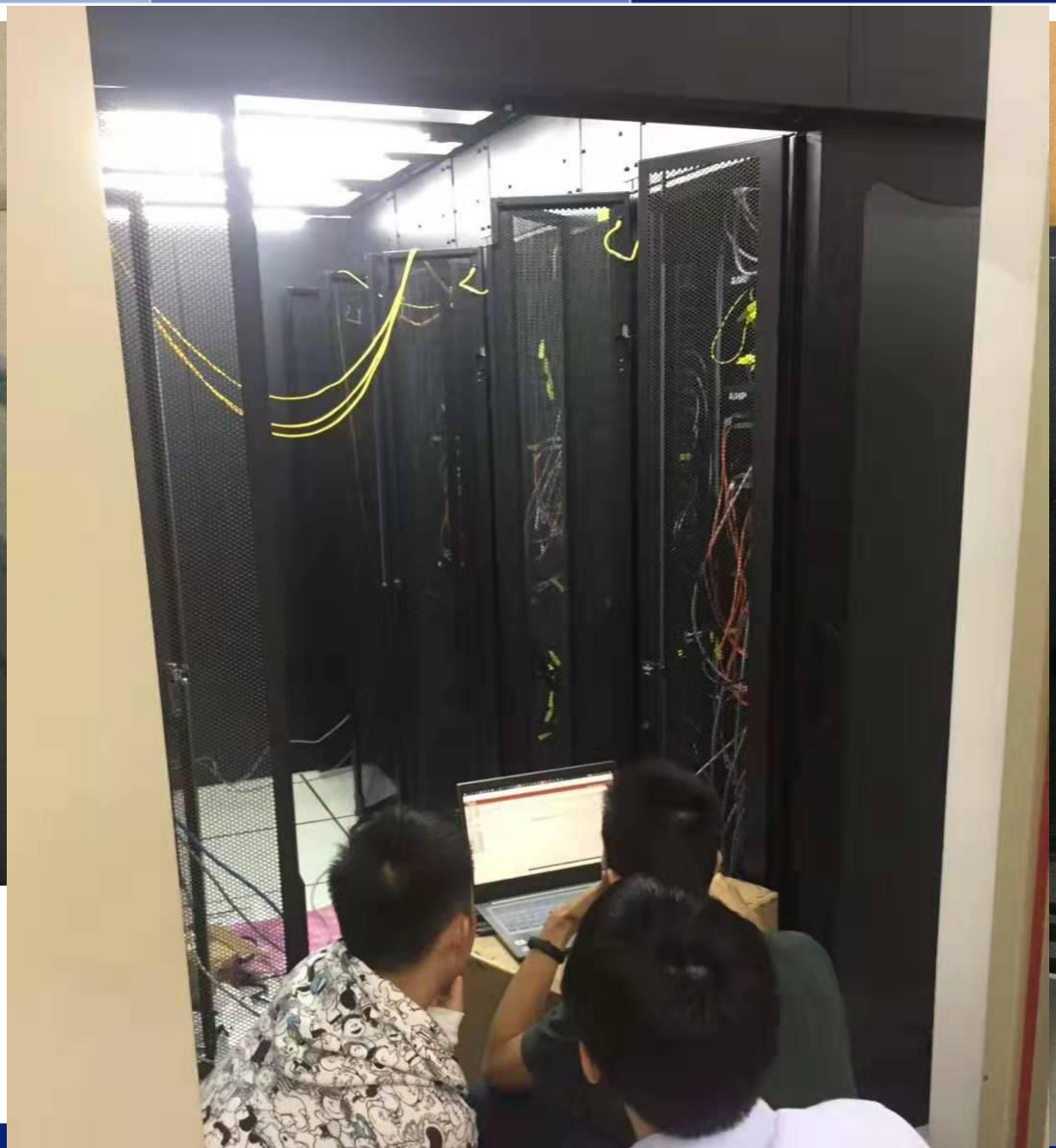
- **4.3.3 测评工具接入点说明**

8.1 项目组织

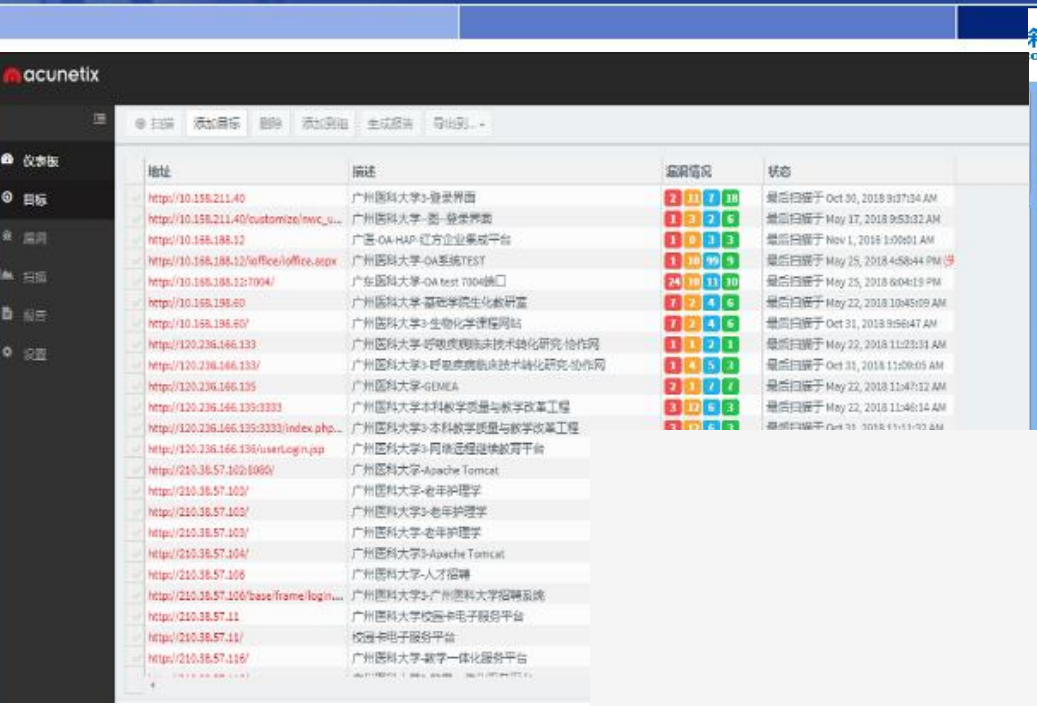
为了保证项目的顺利实施，确保项目质量达到预期目标，广州华南信息安全测评中心将成立项目实施组，以利于加强项目管理和各方面协调合作，使工作和责任更加清晰明确。



3、网络安全等级保护测评-现场实施阶段（差距）

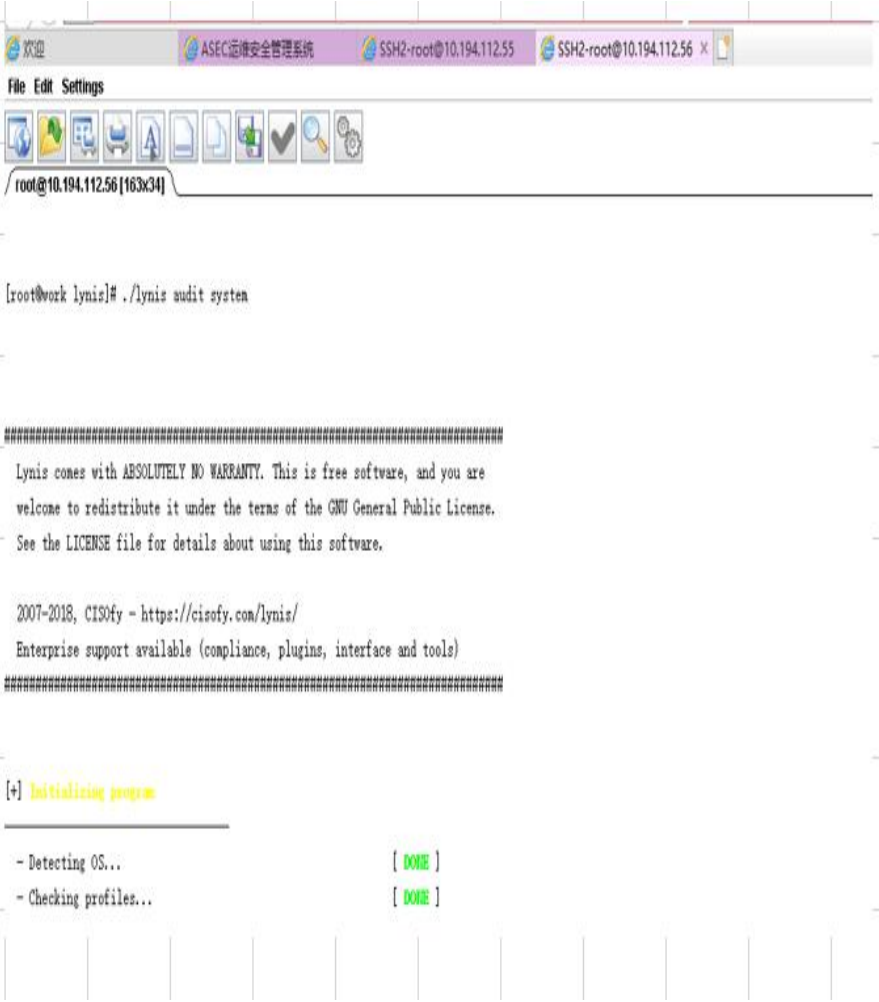


3、网络安全等级保护测评-整改阶段



3、网络安全等级保护测评-验收阶段

	漏。				
恶意代码防范	a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	操作系统未安装防恶意代码软件，未更新防恶意代码软件版本和恶意代码库。	不符合	建议操作系统安装防恶意代码软件和更新防恶意代码库。	已整改，安装lynis
	b)应支持防恶意代码软件的统一管理。	操作系统未安装防恶意代码软件，不支持恶意代码的统一管理。	不符合	建议操作系统安装网络版或企业版的防恶意代码软件，并支持统一管理。	
资源控制	a)应通过设定终端接入方式、网络地址范围等条件限制终端登录；	操作系统未限制终端接入方式，以及限制接入的IP地址。	不符合	建议操作系统限制终端的接入方式和接入IP地址。	通过VPN拨号，堡垒机统一管理，远程协议ssh
	b)应根据安全策略设置登录终端的操作超时锁定；	操作系统未设置登录终端的操作超时锁定。	不符合	建议操作系统设置登录超时锁定功能，建议设置在10分钟以内。	已整改
	c)应限制单个用户对系统资源的最大或最小使用限度。	操作系统未限制单个用户对系统资源的最大或最小使用限度。	不符合	建议操作系统限制单个用户对系统资源的最大或最小使用限度。	
身份鉴别	b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	操作系统用户身份标识容易被冒用，密码策略配置过低：PASS_MAX_DAYS 99999；PASS_MIN_DAYS 0；PASS_MIN_LEN 5；PASS_WARN_AGE 7。	不符合	建议操作系统修改密码策略，设置密码8位以上，至少为大小写字母+数字的组合，每季度更换一次密码。	已整改
	c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	操作系统未启用登录失败处理功能。	不符合	建议操作系统使用登录失败功能，限制非法登录次数和自动退出等措施。	已整改
访问控制	c)应严格限制默认帐户的访问权限，重命名系统默认帐户，修	操作系统已修改默认帐户口令，但未限制了默认帐	部分符合(3	建议操作系统限制默认账户的访问	



3、网络安全等级保护测评-报告阶段

3、网络安全等级保护测评-项目完结

双方盖章后，把报告与备案证一致的公安机关处，进行审核，一般情况下公安机关会出具相应的回执。

Thank you !

广州华南信息安全测评中心