视频监控系统
信息安全检查报告

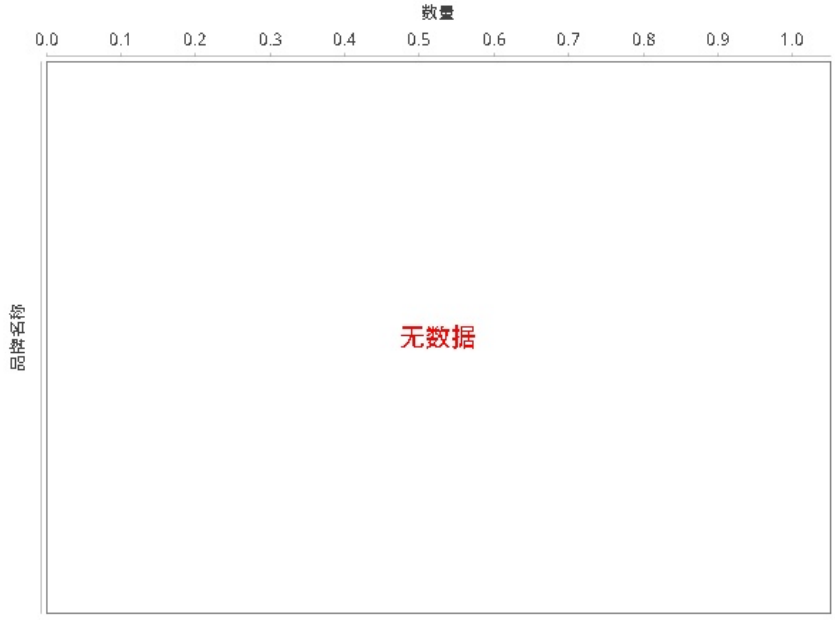
项目名：实验室网络
任务编号：2
检查日期：2018.09.17
检查人员：admin

技术支持中国科学院信息工程研究所

1.综合分析

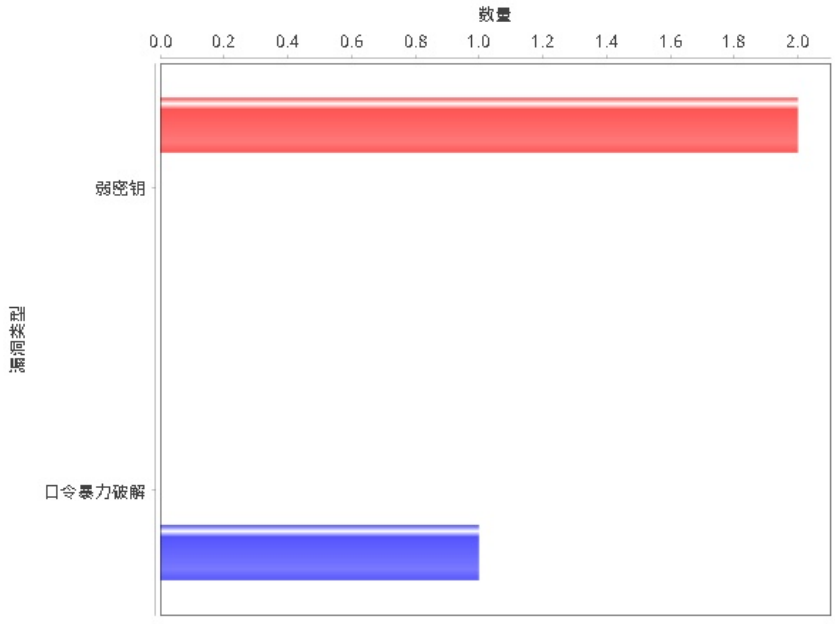
本次检查共发现31台存活主机。经深度检测分析，31个存活主机中工控设备0台，其他设备31台。工控设备中，具体分布如图1。

图1 工控设备品牌分布



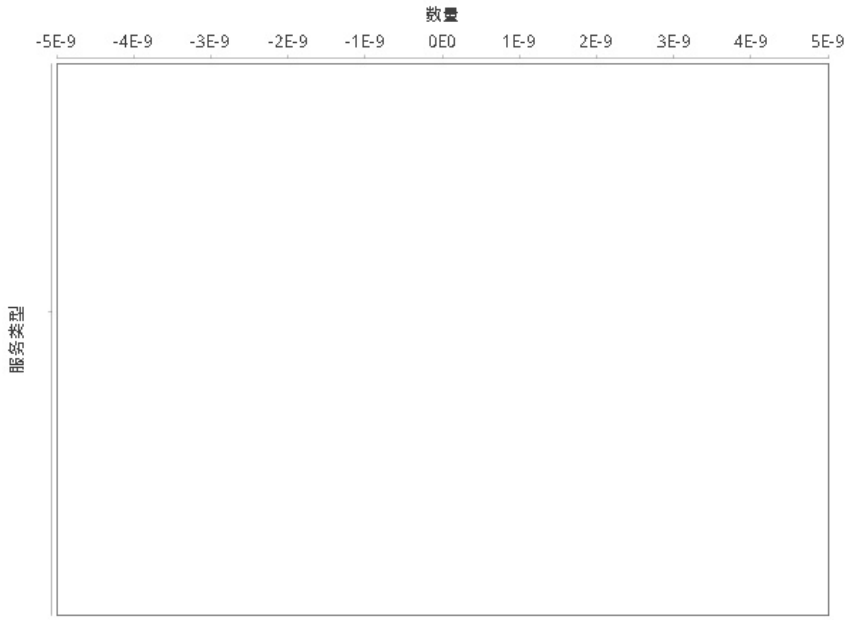
本次检查共发现漏洞3个，其中3个已验证，0个未验证，本地漏洞库扫描出3个，exploit扫描出0个，openVAS扫描出0个。存在漏洞的主机2台，占比6.45%。存在漏洞的工控设备0台，占比0。所有漏洞中，弱密钥2个，口令暴力破解1个，具体分布如图2。

图2 漏洞类型分布



本次检查共识别出工控服务0个。

图3 工控服务分布



2.设备详情

表1 设备详情表

编号	IP	品牌	操作系统	协议服务	漏洞名称	漏洞等级	是否验证	来源
1	10.10.12.90		Linux	ssh，tcp，22	无	N/A	N/A	N/A
				http，tcp，80	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
2	10.10.12.92		Windows	https，tcp，443	无	N/A	N/A	N/A
3	10.10.12.183		embedded	https，tcp，443	无	N/A	N/A	N/A
4	10.10.12.32		Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A

5	10.10.12.35		Windows	https，tcp，443	无	N/A	N/A	N/A
6	10.10.12.73		Windows	ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
				http-alt，tcp，8000	无	N/A	N/A	N/A
7	10.10.12.52		Windows	http，tcp，80	无	N/A	N/A	N/A
8	10.10.12.96		embedded	https，tcp，443	无	N/A	N/A	N/A
9	10.10.12.31		Windows	http，tcp，80	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
10	10.10.12.37		FreeBSD	ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
11	10.10.12.16		embedded	telnet，tcp，23	无	N/A	N/A	N/A
12	10.10.12.131		embedded	https，tcp，443	无	N/A	N/A	N/A
13	10.10.12.210		embedded	http，tcp，80	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
				printer，tcp，515	无	N/A	N/A	N/A
14	10.10.12.211		embedded	ftp，tcp，21	FTP服务弱密钥漏洞	高危	已验证	本地漏洞库
				telnet，tcp，23	FTP服务弱密钥漏洞	高危	已验证	本地漏洞库
				http，tcp，80	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
				printer，tcp，515	无	N/A	N/A	N/A
15	10.10.12.171		Windows	http-proxy，tcp，8080	无	N/A	N/A	N/A
16	10.10.12.172		Windows	unknown，tcp，49152	无	N/A	N/A	N/A
				unknown，tcp，49154	无	N/A	N/A	N/A
17	10.10.12.65		Windows	http，tcp，80	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
18	10.10.12.87		Windows	ssh，tcp，22	无	N/A	N/A	N/A
				shell，tcp，514	无	N/A	N/A	N/A
				http-alt，tcp，8000	无	N/A	N/A	N/A
19	10.10.12.83		Linux	ssh，tcp，22	无	N/A	N/A	N/A

				shell，tcp，514	无	N/A	N/A	N/A
				http-alt，tcp，8000	无	N/A	N/A	N/A
20	10.10.12.42		Windows	http，tcp，80	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
				LSA-or-nterm，tcp，1026	无	N/A	N/A	N/A
				IIS，tcp，1027	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
21	10.10.12.207		Linux	ssh，tcp，22	无	N/A	N/A	N/A
				smtp，tcp，25	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				http-proxy，tcp，8080	无	N/A	N/A	N/A
22	10.10.12.25			http，tcp，80	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
23	10.10.12.1		embedded	telnet，tcp，23	无	N/A	N/A	N/A
24	10.10.12.209		embedded	http，tcp，80	无	N/A	N/A	N/A
				rpcbind，tcp，111	无	N/A	N/A	N/A
				printer，tcp，515	无	N/A	N/A	N/A
25	10.10.12.163		Windows	http，tcp，80	无	N/A	N/A	N/A
				printer，tcp，515	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
26	10.10.12.164		Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
27	10.10.12.241		Linux	onvif，tcp，80	ONVIF 暴力破解用户名密码漏洞	低危	已验证	本地漏洞库
				http，tcp，80	无	N/A	N/A	N/A
				rtsp，tcp，554	无	N/A	N/A	N/A

30	10.10.12.166		Windows	ms-wbt-server，tcp，3389	无	N/A	N/A	N/A

3.漏洞详情

表2 漏洞详情表

漏洞来源	漏洞名称	等级	设备IP	是否验证
本地漏洞库	FTP服务弱密钥漏洞	高危	10.10.12.211	已验证
			10.10.12.211	已验证
			10.10.12.241	已验证
	ONVIF 暴力破解用户名密码漏洞	低危	10.10.12.211	已验证
			10.10.12.211	已验证
			10.10.12.241	已验证