UNIS XScan-G 系列漏洞扫描系统

Web 配置指导

Copyright © 2021 紫光恒越技术有限公司及其许可者版权所有,保留一切权利。 非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部, 并不得以任何形式传播。本文档中的信息可能变动,恕不另行通知。

目录

1 产品简介	1
1.1 产品概述	1
1.2 登录介绍	1
2 网络部署	1
2.1 拓扑示例	1
3 系统管理	
3.1 系统信息	
3.2 账号管理	
3.2.1 账号管理	5
3.2.2 用户管理	
3.2.3 用户锁定	
3.3 网络配置	7
3.4 外发配置	
3.4.1 邮件服务器配置	
3.4.2 短信网关配置	
3.4.3 SNMPTrap 配置	
3.4.4 SYSLOG 配置	
3.4.5 FTP 配置	
3.5 告警配置	
3.5.1 CPU 告警选项	
3.5.2 内存告警选项	
3.5.3 磁盘告警选项	
3.5.4 网络状态告警选项	
3.5.5 设备授权到期告警选项	
3.5.6 特征库授权到期告警选项	
3.6 系统告警日志	
3.7 分布式部署	
3.7.1 分布式设置	
3.7.2 引擎列表	
3.8 日期时间	
3.9 配置备份恢复	
3.10 漏洞检测备份	

3.1	1版本/特征库升级
	3.11.1 自动升级
	3.11.2 手动升级
	3.11.3 本地升级
3.1	2 信任 IP17
3.1	3 诊断工具
3.1	4 验证工具19
	3.14.1 通用验证
	3.14.2 SQL 注入验证
3.1	5 SNMP 管理22
4 许可;	正管理1
5 策略相	莫板1
5.1	系统插件1
5.2	WEB 插件
5.3	口令字典3
6 任务	中心4
6.1	新建任务4
	6.1.1 系统漏洞扫描任务4
	6.1.2 Web 漏洞扫描任务11
	6.1.3 数据库扫描任务14
	6.1.4 口令猜解任务
6.2	任务列表20
6.3	工作列表21
6.4	探测未知站点22
	6.4.1 新建探测任务
	6.4.2 探测详情22
6.5	会话录制23
	6.5.1 开始录制会话23
	6.5.2 停止会话23
	6.5.3 保存会话
	6.5.4 录制的会话列表24
	6.5.5 下发任务24
	6.5.6 查看录制的会话内容

资产管理
报表管理24
8.1 在线查询2
8.2 对比分析2
8.3 导出报表2
8.4 审计日志2
快速向导
0 出厂参数3

1 产品简介

1.1 产品概述

漏洞扫描系统是通过对系统漏洞、服务后门、网页挂马、SQL注入漏洞以及跨站脚本等攻击手段多年的研究积累,总结出了智能主机服务发现、智能化爬虫和 SQL 注入状态检测等技术,可以通过智能遍历规则库和多种扫描选项组合的手段,深入准确的检测出系统和网站中存在的漏洞和弱点。最后根据扫描结果,提供测试用例来辅助验证漏洞的准确性,同时提供整改方法和建议,帮助管理员修补漏洞,全面提升整体安全性。

漏洞扫描系统以综合的漏洞规则库(本地漏洞库、ActiveX 库、网页木马库、网站代码审计规则库 等)为基础,采用深度主机服务探测、Web 智能化爬虫、SQL 注入状态检测、主机配置检查以及 弱口令检查等方式相结合的技术,实现了将 Web 漏洞扫描、系统漏洞扫描、数据库漏洞扫描与弱 口令扫描于一体的综合漏洞评估系统。

1.2 登录介绍

设备已经设置了默认的 Web 登录信息,用户可以通过管理地址(初始默认地址 https://192.168.0.1), 直接使用默认信息登录 Web 界面,首次登录会强制更改初始密码(建议使用 firefox 浏览器)。默认 Web 登录信息请参见<u>表 1-1</u>。

登录信息项		默认配置					
用户名	admin account		audit	report			
密码	admin	account	audit	report			
描述	系统管理员	账户管理员	审计管理员	报表管理员			

表1-1 漏洞扫描系统-分布式管理平台默认 Web 登录信息表

2 网络部署

2.1 拓扑示例

对于组网集中,网络规模较大但无绝对隔离限制的场景,可旁路部署在核心交换机上,对各个区域 的设备进行扫描,单机部署操作简单,不改变客户现有网络结构。拓扑结构如下图。

图2-1 单机部署拓扑结构图



大型企业在全国各地都设有办公地,通常是大规模跨区域的网络,漏洞扫描产品部署在各个地区, 在总部进行集中管理。漏洞扫描系统支持分布式部署,集中管控中心既可作为管理端,也可以作为 扫描引擎,统一下发扫描任务至下级引擎,并在管控中心统一分析、统一展示。拓扑结构如下图。





3 系统管理

本章介绍漏洞扫描系统提供的如下管理功能:

- 账号管理
- 网络配置
- 外发配置
- 告警配置
- 系统告警日志
- 分布式部署
- 日期时间
- 配置备份恢复
- 版本/特征库升级
- 信任 IP
- 诊断工具
- 验证工具
- SNMP 管理

3.1 系统信息

系统信息用于展示当前软件系统版本、规则特征库版本、系统时间、系统资源使用率,以及 syslog 配置、系统时间配置等信息。

(1) 登录 account 账户,选择系统管理>版本/特征库升级,可以查看系统/规则特征库版本;

图3-1 系统/规则特征库版本信息

▲ 版本/特征库升级							
特征库自动升级	版本/特征库手	动升级 版本/特征库本	也升级				
升级服务器地址		https://47.92.55.33/				* 例如: http://update.exam	ple.com:8090/
执行周期		每天执行一次	Ŧ	02:11	0	*	
Proxy代理服务器						通过设置的代理地址上网获取	服务器地址的升级包
代理服务器用户名							
代理服务器密码							
保存	立即升级						
特征库升级时间							
特征库升级结果						规则库已经是最新版本	
当前特征库版本						20190327115745	
系统升级时间							
系统升级结果						升级成功	
当前系统版本						V3.1,ESS 6201	

(2) 选择系统管理>外发配置>syslog 配置,可以查看或修改 syslog 配置信息;

图3-2 syslog 配置信息

▶ 邮件配置	□ 短信配置	✓ SNMP Trap	■ SYSLOG配置	▲ FTP配置		
基本选项						
是否启用		×				
服务器地址		127.0.0.1				*提示:填写指定的服务器地址 (默认:本机)
端口		514				*提示:填写指定的端口 (默认: 514)
协议		UDP			٣	*提示:选择指定的协议
提交						

(3) 选择系统管理>日期/时间,可以查看或修改系统时间配置信息。

图3-3 日期/时间

◎ 日期/时间			
■ 设置当前系统时间			
日期/时间类型	时间基准服务器	•	* 手工配置适用于内网环境。若设备在公网环境下将会自动同步标准时间
当前时间	2019-03-29 09:33:10		*
通用的服务器地址	0.cn.pool.ntp.org		*请填写正确的时间服务器地址
提交			

3.2 账号管理

本章介绍账户管理的相关内容。

3.2.1 账号管理

在主页面选择:系统管理>账号管理>账号管理

- (1) 修改口令必须输入正确的旧密码,如果旧密码输入错误,则不允许修改,口令长度最少为8 位;
- (2) 修改口令成功后,将在下次登录时要求输入新的口令。

图3-4 修改密码

 ● 账号管理 督用户管理 三用户权限模板 	
■ 修改密码	
旧密码	*
新密码	* 密码要求:【字母 、 数字 、 特殊符号 、 长度大于等于8的组合密码】, 示例:access@12
确认新密码	* 密码要求:【必须与 新密码 一致】
验证码	X) Z W
4 4	

3.2.2 用户管理

- (1) 系统设置了两个缺省用户: account 账户管理员和 admin 系统管理员。account 账户可以新建 普通用户。在 account 账户配置网络。
- (2) 用户可根据实际情况在 account 和 admin 上做用户管理;
- (3) 所以账户的总和,无限制,包括系统管理员、账户管理员、审计管理员、报表管理员;
- (4) 新创建的账户默认密码与账户名相同。

1. 新增用户

在主页面选择:系统管理>账号管理>用户管理

(1) 选择系统管理>用户管理>用户管理;

(2) 点击新增,添加新用户并配置新增用户信息如图 3-6。

图3-5 用户管理

图3-6 新增用户

0)	账号管理 臂 用户管理 ≡ 用户权限	根模板			新増+ 刷新 €	捜索[回车]
	用户名	用户权限模板	最近登录日期	状态	是否锁定	登录超时 (分钟)
	admin [默认用户]	高级管理员功能组	2019-03-28 18:22:08	启用	否	30
	audit [默认用户]	审计管理员功能组		启用	否	30
	report [默认用户]	报表管理员功能组		启用	否	30
						< 1 >

新增用户			×
用户名称		* 初始密码与用户名相同	
用户权限模板	普通管理员功能组	不同的权限模板对应的功能模块各不相同 具体权限详情请查看"用户权限模板"	
登录错误锁定	5	* 内容: 连续登录多少次锁定。锁定后需管理员解锁	
登录超时 (分钟)	30	* 内容: 请输入1-1440内的整数	
限制系统扫描IP范围	×		
是否开启密码期限策略	×	*如不开启,默认使用期限为无限制	
是否开启密码强度策略	×	*如不开启,默认密码强度为中,密码长度为8	
提交			

表3-1 用户管理参数说明

参数	说明
用户名称	自定义用户名称
用户权限模板	不同的权限模板对应的功能模块各不相同
登录错误锁定	登录错误超过次数后,账户被锁
登录超时(分钟)	登录后无操作等待超时时间
限制系统扫描IP范围	该账户将无法扫描该IP
是否开启密码期限策略	密码的使用期限设置
是否开启密码强度策略	密码强度设置

3.2.3 用户锁定

登录 account 账户,在主页面选择:系统管理>账号管理>用户管理

当账号被锁定时,登录 account 账户将锁定账号解除锁定。

- (1) 选择系统管理>账号管理>用户管理;
- (2) 点击被锁定用户>点击解除锁定。

图3-7 用户锁定列表

0 ;	账号管理 嶜 用	沪管理	模板	编辑✔ 删除★	解除锁定 ┏ 重置 🖬	₩新増+ 刷新2	捜索回车」
	用户名		用户权限模板	最近登录日期	状态	是否锁定	登录超时 (分钟)
\checkmark	admin	[默认用户]	高级管理员功能组	2019-03-28 20:11:26	启用	是	30
	audit	[默认用户]	审计管理员功能组		启用	否	30
	report	[默认用户]	报表管理员功能组		启用	否	30
	lxh001		普通管理员功能组		启用	否	30
	tss001		普通管理员功能组		启用	是	30
							< 1 →

3.3 网络配置

在主页面选择:系统管理>网络接口

该功能用于配置漏洞扫描系统的网桥配置、路由配置、接口配置、DNS 配置。

(1) 选择系统管理>网络接口>IP 管理配置,进入网桥配置,默认有 MngtVlan, IP 地址为 192.168.0.1(管理地址),可在 MngtVlan 中新增 IP 地址,点击编辑,添加业务 IP。点击新 增可添加网桥,点击 IP 管理可为新增网桥添加 IP 地址,每个网桥最多支持配置 8 个 IP 地址。 点击删除可删除当前网桥。选择系统管理>配置备份恢复,点击备份可备份当前网络配置;勾 选此备份可将当前网络配置备份下载或恢复;点击上传,可将之前下载备份的网络配置恢复。

图3-8 配置备份

夏添俗斎屋 C	下载▲ 恢复≕ 割除★ 上传▲ 备份 0 限新 2 搜索回车]			
备份文件名称	备份日期			
Jokup_v45889-20190614211249_d20190624144033.bak	2019-06-24			
bakup_v45074-20190519002756_d20190520171949.bak	2019-05-20			
bakup_v45074-20190519002756_d20190520151859.bak	2019-05-20			

图3-9 网桥配置

	A 接口配置		I DNS配置				新増+ 刷新3 捜索[回车]
VLAN名称		IP地址		子网掩码	Mtu	状态	操作
MngtVlan		192.168.0.1 192.168.7.253		255.255.255.0 255.255.255.0	1500	启用	编辑✔ 删除★

图3-10 IP 管理配置

VLAN接口配置	×
1 → 基本配置	2 接口IP地址配置
新增+	

支持IPv4以及IPv6网络地址

IPv6示例: 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 IPv6子网前缀长度:2位数字,如64

IP地址	子网掩码	操作
192.168.0.1	255.255.255.0	刪除★
192.168.7.253	255.255.255.0	删除★

	\sim
201-20	9

表3-2 网桥配置参数

参数	说明
网桥名称	网桥口的名称
IP/掩码	网桥的IP地址、掩码
状态	设置网桥接口的启用或禁用
操作	对网桥口做删除或编辑的操作

(2) 选择系统管理>网络接口>路由配置,进入路由配置界面,点击新增路由,添加相关路由配置。 添加缺省静态路由,保证系统到被扫目标网络可达。

图3-11 路由配置

≓ IP	管理配置	A 接口配置	心 路由配置	I DNS配置		関新2 捜索[回车]			
	目的地址				子网掩码/子网前缀长度		下一跳	Metric	
	0.0.0.0				0.0.0.0 192.168.7.1		192.168.7.1	0	

(3) 选择系统管理>网络接口>接口配置,进入接口配置界面,点击对应接口的编辑按钮,可配置 当前接口所属网桥,以及物理状态是否开启。

图3-12 接口配置

≓ IP管理配置	▲ 接口配置	n DNS配置						刷新2 搜索[回车	1
接口名称	Vlan名称		接口启用/禁用	端口状态	发送速率(bps)	发包速率(pps)	接收速率(bps)	收包速率(pps)	操作
GE0/0	MngtVlan		启用	down	98	0	1	0	编辑
GE0/1	2		启用	up	0	0	0	0	编辑。
GE0/2	MngtVlan		启用	down	0	0	0	0	编辑。
GE0/3	MngtVlan		启用	down	0	0	0	0	编辑。
GE0/4	MngtVlan		启用	down	0	0	0	0	编辑。
GE0/5	MngtVlan		启用	down	0	0	0	0	编辑
GE1/0	MngtVlan		启用	down	0	0	0	0	编辑
GE1/1	MngtVlan		启用	down	0	0	0	0	编辑
GE1/2	MngtVlan		启用	down	0	0	0	0	编辑
GE1/3	MngtVlan		禁用	down	0	0	0	0	编辑
GE1/4	MngtVlan		启用	down	0	0	0	0	编辑
GE1/5	MngtVlan		启用	down	0	0	0	0	编辑
GE1/6	MngtVlan		启用	down	0	0	0	0	编辑
GE1/7	MngtVlan		启用	down	0	0	0	0	编辑

表3-3 接口配置参数

参数	说明
接口名称	管理界面显示的接口名称,如GE0/0
网桥名称	当前接口所处网桥
状态	设置接口的启用或禁用
端口状态	实际的物理接口的链路状态
发送速率	当前接口发送流量速率
发包速率	当前接口发包速率
接收速率	当前接口接收流量速率
收包速率	当前接口收包速率
操作	编辑当前接口所属网桥、启用或者禁用

(4) 选择系统管理>网络接口>DNS 配置,进入 DNS 配置界面,编辑主备 DNS 服务器地址。

图3-13 DNS 配置

≓ IP管理配置	A 接口配置	心 路由配置	I DNS配置					
■ 主备DNS								
主DNS服务器		8.8.8.8	8.8.8.8		* 提示:支持IPv4以及IPv6网络地址 IPv6示例: 2001:fecd:ba23:cd1f:dcb1:1010:9234:40		1:1010:9234:4088	
备DNS服务器		114.114.1	14.114					
保存								

表3-4 DNS 服务器说明

参数	说明
主DNS服务器	主用DNS服务器的IP地址,默认为8.8.8.8
备DNS服务器	备用DNS服务器的IP地址,默认为114.114.114.114

3.4 外发配置

3.4.1 邮件服务器配置

告警设置包括邮件告警与短信告警,本系统可以通过设置电子邮件进行邮件通知,在配置完成并保 存以后可以通过发送测试邮件,确定配置的是否正确。

在主页面选择:系统管理>外发配置>邮件配置,进入邮件服务器配置界面,填入邮件服务器地址、端口、邮件地址、密码、邮件主题,提交即可。(告警不支持配置需要授权码进行第三方邮件登录的邮箱,如QQ、163邮箱等)

图3-14 邮件服务器配置

☑ 邮件配置	0 短信配置	✓ SNMP Trap	■ SYSLOG配置	▲ FTP配置		请输入收件箱地址	发送测试邮件
基本选项							
自定义邮件		×			* 提示: 若接收不到邮件? 推荐使用自定义邮件配置		
邮件服务器					* 提示: 请设置可用的邮件服务器 限制字符输入: '` \$;\\n < > /?:"()		
服务器端口		25			* 提示:不加密端口号默认为25;加密ssl,端口号默认为4	465、994端口	
邮箱账号					*提示:发送邮件账号		
邮箱密码					*提示:密码为必填项		
SSL证书		×			*		
邮件主题		邮件告警中	Ù		*提示:接收者收到告警邮件的邮件主题。限制:字符长	度在2-60之间。	
提交							

表3-5 邮件服务器

参数	说明
邮件服务器地址	此处需填用来发送报警邮件的SMTP服务器地址
邮件地址	用来发送报警邮件的邮件地址
密码	发送报警邮件的邮件地址的密码
发送标题	告警邮件的邮件标题

3.4.2 短信网关配置

告警设置包括邮件告警与短信告警,本系统可以通过设置短信网关通知,在配置完成并保存以后可 以通过发送测试短信。确定配置是否正确。

在主页面选择:系统管理>外发配置>短信配置

- (1) 选择系统管理>外发配置>短信配置,短信网关配置是短信报警的前提,需要合作的短信平台 提供短信告警服务;
- (2) 添加短信网关接收短信的网址;
- (3) 根据短信网关接收参数的方式,选择提交参数的方法;
- (4) 根据短信网关接受的编码方式,选择提交内容的编码方式;
- (5) 根据短信平台提供的 API 参数,填写相应的请求参数。

图3-15 短信网关配置

▶ 邮件配置	□ 短信配置	🖌 SNMP Trap	■ SYSLOG配置	▲ FTP配置		请输入手机号码 发送测试短信
基本选项						
是否启用		×				
网关地址						*提示:填写短信网关url地址
提交方式		POST			٣	*提示:选择数据处理提交方式
编码格式		UTF-8			٣	*提示:选择编码格式
请求参数/宏		username= mobile=\${	=xxx&password=xx MOBILE}&apikey=x	x&content=\${MESSAGE}& xx	h.	◆\$(MESSAGE)为短信内容,\$(MOBILE)为接收者,无需修改! 更多的请求参数,请用&符号连接
提交						

表3-6 默认短信内容参数说明

参数	说明					
\$MESSAGE	为平台内置的告警内容模板,填写请求参数时,无需更改					
\$MOBILE	为平台内用户的创建告警联系人的手机号码,填写请求参数时,无需更改					

3.4.3 SNMPTrap 配置

SNMP 功能是为了方便管理员集中管理设备,对漏洞扫描系统的系统信息,资源及状态等进行统一监控管理。目前支持的协议包括 SNMPv1、SNMPv2,可以同使用标准 SNMP 协议的集中管理软件或设备配合使用。

在配置 SNMP 功能时,用户需要确定使用哪个版本的 SNMP 协议,以便漏洞扫描系统同 SNMP 服务器使用的 SNMP 版本保持一致。

图3-16 SNMPTrap 配置

▶ 邮件配置	□ 短信配置	✓ SNMP Trap	■ SYSLOG配置	✿ FTP配置					
基本选项									
是否启用		×							
服务器地址		127.0.0.1				* 提示:	填写指定的服务	器地址 (默认:	本机)
端口		162				* 提示:	填写指定端口(默认: UDP端[]: 162)
SNMP口令		•••••				* 提示:	填写SNMP口令	(默认: publie	c)
OID信息		.1.3.6.1.4.1	2021.251.1			* 提示:	填写OID信息		
提交									

3.4.4 SYSLOG 配置

图3-17 SYSLOG 配置

SYSLOG 配置用于指定日志外发的服务器地址,默认使用 UDP 协议的 514 端口。协议、端口配置 以自定义,但是必须与日志服务器的配置一致,否则日志服务器将无法接受漏洞扫描系统的日志。

▶ 邮件配置	□ 短信配置	✓ SNMP Trap	■ SYSLOG配置	▲ FTP配置		
基本选项						
是否启用		×				
服务器地址		127.0.0.1				* 提示:填写指定的服务器地址 (默认:本机)
端口		514				*提示:填写指定的端口 (默认: 514)
协议		UDP			٣	*提示:选择指定的协议
提交						

3.4.5 FTP 配置

通过 FTP 配置可将扫描结果保存到 FTP 服务器上,用户需要添加 FTP 服务器地址、端口、FTP 用 户名和密码,以及工作目录,并确保漏洞扫描系统到 FTP 服务器可达。

图3-18 FTP 配置

▶ 邮件配置	□ 短信配置	 SNMP Trap 	■ SYSLOG配置	▲ FTP配置	
基本选项					
eran					
是否启用					
服务器地址		127.0.0.1		*提示:填写指定的服务器地址(黑	状认:本机
唯口		21		* 提示: 填写指定端口 (默认: 21))
14 CT		21			
ftp用户名		mailsender		*	
ftn宓码				*	
rep man 3					
工作目录		/		*提示:指定工作目录	
10-2-					
提父					

3.5 告警配置

3.5.1 CPU 告警选项

CPU使用率【百分比】,请输入[1-100]的整数值! 写入周期: 1天/次或者模块状态发生变化时写入。

3.5.2 内存告警选项

内存使用率【百分比】,请输入[1-100]的整数值!写入周期:1天/次或者模块状态发生变化时写入。

3.5.3 磁盘告警选项

磁盘使用率【百分比】,请输入[1-100]的整数值!写入周期:1天/次或者模块状态发生变化时写入。

3.5.4 网络状态告警选项

开启网络状态告警选项,可以根据网络接口的存在异常则会在下次登录时告警。

3.5.5 设备授权到期告警选项

开启设备授权到期告警选项,若当前时间离授权结束时间不到 30 天 (默认 30 天),则会告警。写入周期: 1 天/次或者模块状态发生变化时写入。

3.5.6 特征库授权到期告警选项

开启特征库授权到期告警选项,若当前时间离授权结束时间不到 60 天 (默认 60 天),则会告警。 写入周期: 1 天/次或者模块状态发生变化时写入。

3.6 系统告警日志

当超出告警配置的值时,会产生告警日志。

图3-19 系统告警日志界面

	系统告警日志]	备份导出 🛛 清空日志 🖉	刷新	00:00 * 至	23:59 🔻 全部		
每页	每页显示 25 🔻							
	日期/时间 🔹	主机	模块名称	严重等级!	概要	告警信息		
	2019-03-29 01:15:51	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port2状态为up		
	2019-03-29 01:15:45	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port1状态为up		
	2019-03-29 00:35:50	h3c-os	内存	已清除	内存恢复正常	内存的使用率为: 66.724, 阈值:80		
	2019-03-29 00:35:16	h3c-os	内存	紧急	内存异常	内存的使用率为: 80.721, 阈值:80		
	2019-03-29 00:01:07	h3c-os	CPU	已清除	CPU恢复正常	CPU的使用率为: 34.740, 阈值:80		
	2019-03-29 00:00:56	h3c-os	CPU	紧急	CPU异常	CPU的使用率为: 81.900, 阈值:80		
	2019-03-29 00:00:46	h3c-os	CPU	已清除	CPU恢复正常	CPU的使用率为: 78.390, 阈值:80		
	2019-03-29 00:00:31	h3c-os	CPU	紧急	CPU异常	CPU的使用率为: 85.500, 阈值:80		
	2019-03-28 21:12:33	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port2状态为up		
	2019-03-28 21:11:36	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port3状态为down		
	2019-03-28 21:10:47	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port3状态为up		
	2019-03-28 21:09:59	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port3状态为down		
	2019-03-28 21:06:17	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port3状态为up		
	2019-03-28 21:00:50	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port1状态为up		
	2019-03-28 21:00:45	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port1状态为down		

3.7 分布式部署

3.7.1 分布式设置

登录 account 账户,在主页面选择:系统管理>分布式部署

- (1) 选择系统管理>分布式部署;
- (2) 根据实际情况填写相关信息;
- (3) 点击提交;
- (4) 配置成功后, 会在管理中心的引擎列表中查看到子引擎。

图3-20 分布式部署

♪ 分布式设置 ↓ 目擎列表		
基本选项		
作为分布式引擎	×	
引擎名称(别名)	local	*提示:分布式引擎建议以IP地址组合的方式命名。例如:dist_192.168.1.100
管理中心地址	127.0.0.1	*提示:本机地址为127.0.0.1;其他管理地址需填可达且有效的IP地址
提交		

表3-7 分布式部署参数说明

参数	说明
管理中心地址	填写需要接入的漏洞扫描系统-管理中心地址
任务分发	管理中心在创建任务时,分配执行该任务的子引擎
引擎名称	在配置分布式引擎时命名的引擎名称,尽量不要跟其它引擎名称冲突

3.7.2 引擎列表

图3-21 引擎列表

♪ 分布式设置 ↓ 引擎列表				增加引擎地址+ 刷新2 携	嗦[@车]
引擎名称	引擎类型	引擎IP	状态	自动同步策略	自动同步规则
local	WEB扫描引擎	127.0.0.1	启用	Yes	Yes
local	口令猜解引擎	127.0.0.1	启用	Yes	Yes
local	系统扫描引擎	127.0.0.1	启用	Yes	Yes

3.8 日期时间

NTP 提供漏洞扫描系统与时间服务器进行的同步的功能。通过 NTP 配置,漏洞扫描系统可以从 NTP 服务器上同步漏洞扫描系统的系统时间。

日期/时间类型:手工配置适用于内网环境。若设备在公网环境下将会自动同步标准时间。 通用的服务器地址:填写正确的时间服务器地址。

图3-22 日期/时间

◎ 日期/时间			
■ 设置当前系统时间			
日期/时间类型	时间基准服务器	•	* 手工配置适用于内网环境。若设备在公网环境下将会自动同步标准时间
当前时间	2019-03-29 09:33:10		*
通用的服务器地址	0.cn.pool.ntp.org		* 请填写正确的时间服务器地址
提交			

3.9 配置备份恢复

备份主要是针对漏洞扫描系统配置文件的备份。建议用户定期对漏洞扫描系统的配置信息进行备份, 以供将来恢复系统配置时使用。另外备份数据还可以导入导出系统,这样增加了系统的可靠性。

图3-23 配置备份恢复

໊	配置备份恢复	上传上は「留份町」」を注意して、「日本の日本」を注意に見ていた。
	备份文件名称	备份日期
	bakup_v43665-20190327120031_d20190329110800.bak	2019-03-29
	bakup_v43665-20190327120031_d20190329110748.bak	2019-03-29

3.10 漏洞检测备份

备份当前系统漏洞检测信息。

图3-24 漏洞检测备份

1	漏洞检测备份	备份♥	刷新€捜
	漏洞结果名称	生成日期	
	jrbak-20190329111045.xls	2019-03-29	
	jrbak-20190329111041.xls	2019-03-29	

可对备份的文件进行删除和下载操作。

图3-25 漏洞检测备份操作

1	扇洞检测备份	下载之 删除× 备份 刷新 ご 捜索[四]
	漏洞结果名称	生成日期
\checkmark	jrbak-20190329111045.xls	2019-03-29
	jrbak-20190329111041.xls	2019-03-29

3.11 版本/特征库升级

升级是对漏洞扫描系统版本的管理,分为整个系统的升级、特征库升级。

3.11.1 自动升级

主要针对系统的特征库进行升级,需要填写升级服务器地址,访问服务器地址的用户名和密码,并 选择执行周期可以设置每天执行,每周执行,每月执行进行自动升级。

图3-26 自动升级

₲ 版本/特征库升	级						
特征库自动升级	版本/特征库手动升线	升级 版本/特征库本地升级					
升级服务器地址 执行周期 Proxy代理服务器 代理服务器用户名	htty	https://47.92.55.33/ 每天执行一次		02:11	0		* 例如: http://update.example.com:8090/ * 通过设置的代理地址上网获取服务器地址的升级包
保存	立即升级						
特征库升级时间							
特征库升级结果							规则库已经是最新版本
当前特征库版本							20190327115745
系统升级时间							2019-03-28 17:45:42
系统升级结果							[失败] 解压升级包失败,请检查升级包是否正确!
当前系统版本					V3.1,ESS 6201		

3.11.2 手动升级

如果要对特征库和系统升级,需要下载特征库包或者系统升级包,搭建 FTP 服务器根据命令 ftp://user:pass@ip:port/xxx.img 进行升级。

图3-27 手	动升级							
▲ 版本/特征库升	级							
特征库自动升级	版本/特征库手动升级	版本/特征库本地升级						
特征库升级	ftp://u	ftp://user:pass@ip:port/xxx.img		停止	提示:升级前系统会自动保存配置,升级过程中系统扫描引擎会重启			
系统升级	ftp://u	ftp://user:pass@ip:port/xxx.img		停止	提示:升级前系统会自动保存配置,系统升级过程中系统会重启			
特征库升级时间								
特征库升级结果				规则库	已经是最新版本			
当前特征库版本			20190327115745					
系统升级时间					2019-03-28 17:45:42			
系统升级结果			[失败] 解压升级包失败,请检查升级包是否正确!					
当前系统版本				V3.1,E	SS 6201			

3.11.3 本地升级

在本地下载好特征库升级包或系统升级包后,直接点击导入选择包等待上传,在上传过程中可以看 到上传进度。

图3-28 本地升级

▲ 版本/特征库升级								
特征库自动升级	版本/特征库手动升级	版本/特征库本地升级						
特征库升级	导。	入升级包并升级特征库	操作提示:上传特征库升级包后,稍后请手动确认进行升级。提示:升级过程中系统扫描引擎会重启					
系统升级	Ę	入升级包并升级系统	操作提示:上传系统升级包后,稍后请手动确认进行升级。提示:系统升级过程中系统会重启					
特征库升级时间								
特征库升级结果			规则库已经是最新版本					
当前特征库版本			20190327115745					
系统升级时间			2019-03-28 17:45:42					
系统升级结果			[失败] 解压升级包失败,请检查升级包是否正确!					
当前系统版本			V3.1,ESS 6201					

3.12 信任IP

使用该功能可以设置 IP 网段对漏洞扫描系统进行管理。同时也可以设定允许访问的类型,如 Https、 Shell。

HTTPS: 是否允许上面设置的网段的机器访问漏洞扫描系统的 HTTPSWeb 服务。

Shell: 是否允许上面设置的网段的机器访问漏洞扫描系统的 WebShell 服务。

图3-29 信任 IP 配置

a,信任IP	解锁SSF	新増+ 清空× 刷新ご 搜索[回车]					
IP地址/掩码	Https	Shell					
没有检索到数据							

3.13 诊断工具

诊断工具包含 PING 命令、WEBGET 命令、端口探测工具、Tcpdump 抓包工具以及故障信息收集。 一键诊断功能能快速对 PING、DNS、WEBGET 进行检测。

在主页面选择:系统管理>诊断工具,进入诊断工具,进行相应的配置。

- PING 命令 测试系统与远程主机之间的连通性。
- WEBGET 命令 测试网站能否被平台正常访问。
- 端口探测工具 测试远程主机端口是否开放。
- Tcpdump 抓包工具 抓包检测流量传输情况。
- 故障信息收集
 对发生故障的信息进行收集。

图3-30 PING 命令

▶ 诊断工具						
PING命令	WEE	3GET命令	端口探测工具	Tcpdump抓包工具	故障信息收集	
PING		请输入U	RL或IP地址			测试
注:限制字符	输入:	'` \$;\\n	< > / ? : " ()			

图3-31 WEBGET 命令

▶ 诊断工具					
PING命令	WEBGET命令	端口探测工具	Tcpdump抓包工具	故障信息收集	
请输入URL				测试	注: 限制字符输入: '` \$;\\n < > /?:"()

图3-32 端口探测工具

▶ 诊断工具					
PING命令 WE	BGET命令	耑口探测工具	Tcpdump抓包工具	故障信息收集	
探测IP/域名					* 请输入主机IP/域名 限制字符输入: '` \$;\\n < > /?:*()
探测端口/范围					请输入探测端口:例:22,80,443,8080,20-200 不填入端口内容,默认查找最有可能开放的1000端口。(下载探测数据(XML格式),可以查看详细探测端口)
探测					

图3-33 Tcpdump 抓包工具

	全部	•	*
据亲曰 []	GE0/1(up)	v	*提示:禁用接口默认不可选择。
Ξ机IP/域名			* 请输入主机IP/域名 限制字符输入: '`\\$:\\n < > /?:"()
注意:完成配置后,点击"启动"开好	始截取报文。点击*停止"可以截取报文,点击	节"下载"可	下载己截取的报文。

✔ 沙町工具					
PING命令	WEBGET命令	端口探测工具	Tcpdump抓包工具	故障信息收集	
收集日志并了	下载 一键清理日	志 升级日志下载			
log_190328	3152649.zip				

3.14 验证工具

3.14.1 通用验证

验证工具主要提供两个验证工具,一个是通用验证,一个是 SQL 注入验证, SQL 注入验证是专门 针对注入类漏洞的验证工具,通用验证是针对除注入类漏洞外的其它 web 漏洞的验证工具。通过这 两类验证工具可以直接手动添加 URL 和问题参数进行验证,主要是用来针对平台 web 扫描扫描出 的漏洞进行验证可以直接将漏洞 URL 和参数同步到验证工具中的 URL 和参数中进行验证。

图3-35 通用验证

● 通用验证 ▲ SQL注入验证				
请求方式 GET T 协议 HTTP/1.1	* URL		验证	
■ 请求头信息(Request Headers)		新增+ ~	■ 请求数据(Request Data)	
名称(Header Name) 值(Header Value)		操作		
没有检索到数据				
响应返回头(Response Headers) 返回数据(Response	Data)			
名称(Header Name)	值(Header Text)			

3.14.2 SQL 注入验证

在主页面选择:系统管理>验证工具>SQL注入验证 能够进行一些 SQL注入验证操作,正确填写参数后点击<验证>,即可验证

图3-36	SQL	注入	、验证
図2-20	SQL	エハ	、河虹川工

● 通用验证 ▲ SQL注入验证		
问题参数	URL	验证
响应数据(Response Data)		

一般来说,扫描出网站漏洞后在网站详情查询中,可以查看漏洞详情 漏洞详情页面中点击 SQL 注入验证

图3-37 漏洞详情

盲注漏洞 (字符或)					
概要 目标存在SQL注入攻 2. SQL注入攻 时, SQL注入 意查词。SQL 被SQL注入后 1.网页被篡改 3. 核心数据减 4. 数据库所在	注入漏洞。 由就是攻击者通过欺骗数据库服务器执行非授权的任意查询过程。 击就其本质而言,它利用的工具是SQL的语法,针对的是应用程序开发者在编程过程中的漏洞,"当攻击者能够操作数据,向应用程序中插入一些SQL语句 攻击就发生了"。实际上,SQL注入攻击是攻击者通过在应用程序中预先定义好的查询语句结尾加上额外的SQL语句元素,欺骗数据库服务器执行非授权的任 注入漏洞是目前互联网最常见也是影响非常广泛的漏洞。 可能导致以下后果: 					
解决方法						
如下一些方法 1.在网页代码 2.部署Web应 3.对数据库操 建议过滤用户	能够防止注入攻击: 中需要对用户输入的数据进行严格过滤。 用防火墙 作进行监控 输入的数据,切记用户的所有输入都要认为是不安全的。					
风险级别						
扫描详情						
漏洞URL	http://183.1.0.12:8080/WebGoat/attack?Screen=128&menu=900					
问题参数	数 Screen					
测试用例	战用例 http://183.1.0.12:8080/WebGoat/attack?Screen=-1'%20OR%203*2*0%3d6%20AND%20000125%3d000125%20&menu=900 [POST] message=1&title=&SUBMIT=Submit [COOKIE] JSESSIONID=03614DC585F6778BACF0788958D36A11					
备注信息	注信息 对比参数值替换-1%20OR%203*2*1%3d6%20AND%20000125%3d000125%20和 -1%20OR%203*2*0%3d6%20AND%20000125%3d000125%20和 ら判断。					

此时会跳转到通用验证页面,显示如下

图3-38 SQL 注入验证页面

操作 SQL注入验证 通用验证

 SQL注入验证 						
问题参数	Screen	URL	http://183.1.0.12:8080/WebGoat/attack?Screen=128&rmenu=900	验证		
順应数据(Response Data)						
[09:32:26] [INFO] testing connection to the target URL [09:32:26] [CRITICAL] not authorized, try to provide right HTTP authentication type and valid credentials (401) [09:32:26] [CRITICAL] not authorized, try to provide right HTTP authentication type and valid credentials (401) [09:32:26] [WARNING] HTTP error codes detected during run:						

3.15 SNMP管理

图3-39 snmp 管理 snmpv3 协议界面

♀ SNMP管理			
基本选项			
是否启用	×		
SNMP版本	SNMP V3	Ψ.	
SNMP V3 用户名	rosnmp	*	* 提示:填写SNMP V3 用户名
SNMP V3 密码	<u> </u>	*	* 提示: 密码要求: 【字母 、数字、特殊符号 、长度大于等于6的组合密码】。示例: access12@1
密码哈希算法	SHA	* *	* 提示:选择密码哈希算法
加密算法	AES128	* *	* 提示: 选择加密码算法
加密口令		*	*提示:输入加密口令
允许访问IP/网段	127.0.0.1 x	*	* 提示:允许访问的ip或网段,以,隔开,网段示例:192.168.1.0/24
_			
提交			

表3-8 用户管理参数说明

参数	说明
SNMP版本	可选择snmpv3或snmpv1c/snmpv2c。使用snmpv1c/snmpv2c不安全
SNMPV3用户名	填写SNMPV3用户名
SNMPV3密码	密码要求:【字母、数字、特殊符号、长度在[8-32]之间的组合密码】。示例: access12@1
密码哈希算法	选择加密码算法
加密口令	输入加密口令
允许访问IP/网段	允许访问的ip或网段,以,隔开,网段示例: 192.168.1.0/24
协议公共体	SNMPv1SNMPv2c协议公共体,当不配置该项或为空时,禁用SNMPv1SNMPv2c

4 许可证管理

登录 account 账户,在主页面选择:license 管理,进入 license 管理页面 点击导入许可证可将获得的许可证文件导入;

图4-1 导入许可证

导入许可证

请选择需要上传的文件
 浏览…
 未选择文件。
 支持.dat格式
 ▲上传
 ② 重置

授权导入成功后,重新登录可查看授权信息。

图4-2 查看授权信息

■ License管理	导入许可证上
授权信息	
机器码	THE REPORT OF A DESCRIPTION OF A DESCRIP
硬件序列号	CONTRACT CONTRACTOR
许可证类型	正式版
注册时间	2021-07-01
许可证到期时间	无限制
最大IP数	128 (剩余:126)
系统&数据库并发扫描任务数	6
并发IP总数	60
最大站点数	128 (剩余:125)
WEB扫描并发站点数	1
口令猜解并发任务数	4
规则库升级到期时间	2023-07-01
产品型号	AND NO AND ADDRESS OF ADDRESS ADDRE
产品名称	漏洞扫描系统
版本号	UNE Disare Schwarz, Sector 1.0, 853-8855

5 策略模板

策略模板是基于脚本的规则库,包括系统插件和 web 插件,其中系统漏洞检测插件 20 多类,60000 多条;web 漏洞检测插件共覆盖 OWASP 定义的 10 大类漏洞规则,且覆盖了 CVE、CNVD、CNNVD、 CNCVE、Bugtraq 等多个漏洞库中的所有漏洞。我们将定期发布最新的规则库,用户可以通过公司 官方网站获得最新的规则库。

5.1 系统插件

系统漏洞插件库

系统内置全面的漏扫扫描插件,可以灵活的定义扫描策略。

图5-1 系统漏洞插件库

瀨洞插件					
漏洞模板	増加模板 🗸 💭	🛔 漏洞类别	✓ Q	✓ 高 ✓ 中 ✓ 低 搜索名称/编号/	CVE[回车]
莫板名称	▼ 操作	类别名称	▲ 总计	漏洞	
NS安全		✓已启用 Linux本地安全	29829	○ ◆已启用 OpenSSL死亡警报拒绝服务漏洞 (POC)	
nix安全漏洞		✓已启用 Unix本地安全	12159	● ◆已启用 OpenSSL死亡警报拒绝服务漏洞	
nux安全漏洞		✓已启用 Windows安全	5477	● 2 2 2 2 2 2 2 2 2 2 2 2 2	
规性检查漏洞		✓已启用 Web安全	5596	✓已启用 Jenkins远程代码执行 (CVE-2016-9299)	
全设备漏洞		✓已启用 网络设备安全	2292	✓已启用 Elasticsearch远程代码执行 (CVE-2014-3120)	
绝服务漏洞			1679	✓ 已启田 Webl ogic任意文件上载 (CVF-2018-2894)	
P安全漏洞			90	▲ 日白田 Webl ogic注册执行代码 (CVE-2018-2893)	
程溢出安全漏洞			30		:20)
动设备安全漏洞			30		20)
C安全漏洞			297	✓已启用 HTTP响应实使用X-XSS-Protection	
与安全漏洞		✓已启用云安全	748	✓已启用 HTTP响应头部使用X-Frame-Options	
eb安全漏洞		◆已启用 数据库安全	569	▲ ●已启用 HTTP相应头X-Content-Options: nosniff	
NMP安全漏洞 中心浸湿		→ 已启用 远程溢出	281		
安全漏洞		✓已启用 FTP安全	255	□ V已启用 Debian DSA-4170-1: pjproject - 安全更新	
ド女王庸洞		◆已启用 安全设备	218	□ □ □ ■ Debian DSA-4168-1: squirrelmail - 安全更新	
们的安主潮河		✓已启用 DNS安全	171	□ ◆ 已启用 Debian DLA-1343-1: 安全更新	
终设各央全漏洞		◆已启用 拒绝服务	111	□ □ <p< td=""><td>r安全更新</td></p<>	r安全更新
坦医安全漏洞		✓ 已启用 SNMP安全	33	✓已启用 Debian DLA-1341-1: sdl-image1.2安全更新	
indows安全漏洞		✓已启用 SMTP安全	139	✓已启用 Debian DLA-1340-1: sam2p安全更新	
		◆已启用 移动安全	75	✓已合用 CentOS 6: libvorbis (CESA-2018: 0649)	
-21条记录	< 1 2 >		112	CentOS 7: thunderbird (CESA-2018: 0648)	

5.2 WEB插件

预置的 web 漏洞插件库,包含当前最新的检测规则,提供全面的安全扫描策略,并能灵活定义扫描策略。

图5-2 web 漏洞插件库

♣ WEB插件								
漏洞插件								
■ 漏洞模板	増加模板 🗸 💭	▲ 漏洞类别		✓ Ø	✓ 宿	5 🗸 中	✔ 低 ✔ 信息	搜索[回车]
模板名称	▼ 操作	类别名称		▲ 总计	"	洞		,
高风险WEB漏洞[362]		✔已启用	A1 注入	165		✔已启用	DeltaSql 1.8.2 源码变更日志信机	急泄露
高/中风险WEB漏洞[419]		✔已启用	A2 失效的身份认证和会话管理	13		✔已启用	DeltaSql 1.8.2 dbsync.php页面	跨站脚本攻击漏洞
高/中/低风险WEB漏洞[474]		✔已启用	A3 跨站脚本 (XSS)	52		✔已启用	SiteServer CMS 远程模板下载G	ietshell漏洞
全部WEB漏洞[496]		✔已启用	A4 不安全的直接对象引用	98		✔已启用	Listing Hub CMS 1.0 sql注入漏	洞
总计4条记录	< 1 →	✔已启用	A5 安全配置错误	55		✔已启用	KindEditor<=4.1.11版本文件上	传漏洞
		✔已启用	A6 敏感信息泄漏	69		✔已启用	thinkphp5.0.x<5.0.24版本远程	代码执行漏洞
			A7 功能级访问控制缺失	14		✔已启用	中兴MF65 BD_HDV6MF65V1.0).0B05 跨站脚本攻击漏洞
		✔已启用	A8 跨站请求伪造 (CSRF)	1		✔已启用	phpmyadmin 4.8.1版本文件包括	含漏洞 (CVE-2018-12613)
		─ ◆已启用	A9 使用含有已知漏洞的组件	24		✔已启用	thinkphp5 SQL注入和信息泄露	漏洞
		✔已启用	A10 未验证的重定向和转发	5		✔已启用	thinkphp5.x<5.0.23,5.1.31版本	远程代码执行漏洞
						✔已启用	Wordpress插件Corner Ad 1.0.	7版本跨站脚本攻击漏洞
		总计10条记录				✔已启用	Wordpress插件Tribulant News	sletters 4.6.4.2版本跨站脚本攻击…
						✔已启用	Wordpress插件Site Editor 1.1.	1版本本地文件包含漏洞
						✔已启用	WordPress插件Gift Voucher 1.	.0.5版本SQL注入漏洞
						✔已启用	Cybrotech CyBroHttpServer 1	.0.3跨站脚本攻击漏洞
						✔已启用	Chamilo LMS 1.11.8跨站脚本功	て击漏洞
						✔已启用	发现网站备份文件(web.rar)	
						✔已启用	发现网站备份文件(upload.rar)	
						✔已启用	Super Cms Blog Pro 1.0版本SC	QL注入漏洞
						✔已启用	Delta Sql 1.8.2 sql注入漏洞	
					总计4963	条记录		< 1 2 3 4 5 3

5.3 口令字典

有系统默认的口令字典组合模式模板和单独的用户名字典模板和密码字典,也可以自定义字典按照 文件内容特征和所属服务类型进行上传字典。

图5-3 口令字典

组合字典		搜索	回车] く 2	🚢 用户名字典		搜索	回车] 🗸 🖓	* 密码字典		搜索	回车] 🗸 🗸
字典名称	所属服务	总数	操作	字典名称	所属服务	总数	操作	字典名称	所属服务	总数	操作
SMTP组合字典	SMTP	26		SMTP用户名字典	SMTP	3		REDIS密码字典	REDIS	253	
MongoDB组合字典	MongoDB	3		MongoDB用户名字典	MongoDB	3		SMTP密码字典	SMTP	253	
DB2组合字典	DB2	181		DB2用户名字典	DB2	6		MongoDB密码字典	MongoDB	4	
MsSQL组合字典	MsSQL	735		MsSQL用户名字典	MsSQL	10		DB2密码字典	DB2	337	
Postgres组合字典	Postgres	1		Postgres用户名字典	Postgres	1		MsSQL密码字典	MsSQL	292	
MySQL组合字典	MySQL	72		MySQL用户名字典	MySQL	5		Postgres密码字典	Postgres	248	
Oracle组合字典	Oracle	253		Oracle用户名字典	Oracle	28		MySQL密码字典	MySQL	339	
RDP组合字典	RDP	105		RDP用户名字典	RDP	3		Oracle密码字典	Oracle	269	
SMB组合字典	SMB	105		SMB用户名字典	SMB	3		RDP密码字典	RDP	412	
POP3组合字典	POP3	28		POP3用户名字典	POP3	3		SNMP密码字典	SNMP	51	
SH组合字典	SSH	299		SSH用户名字典	SSH	6		SMB密码字典	SMB	426	
TP组合字典	FTP	1045		FTP用户名字典	FTP	6		POP3密码字典	POP3	426	
ELNET组合字典	TELNET	204		TELNET用户名字典	TELNET	5		SSH密码字典	SSH	345	
								FTP密码字典	FTP	426	
计13条记录			< 1 →	总计13条记录			< 1 >	TELNET密码字典	TELNET	461	



6.1 新建任务

6.1.1 系统漏洞扫描任务

1. 扫描基本配置

针对漏洞扫描,添加需要扫描的目标,填写形式为单个主机或者主机组,配置任务名称,选择漏洞 扫描插件模板并提交扫描。

图6-1 添加漏洞扫描任务

□ 系统扫描 ● WEB扫描 □ 数据库检测 ◆ 口令猜解								
扫描基本配置 自主选择插件	探测选项检测选项]擊选项 登录信息选项						
扫描目标方式	 手动输入 使用 	资产 🔿 批量导入						
扫描目标			* 输入的内容有[单个主机]和[主机组]两种,多个之间以英文逗号()减换行分隔 种个主机示例: 192.168.1100 也可使用感答:www.example.com IPv6示例: 2001/fecdba23cd1f.tdcb1:10109234:4088 主机组示例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 排除某个IP: 192.168.1.0/241192.168.1.100					
任务名称	系统扫描-		*提示:请填写任务名称,长度在[1-40]字符之间					
执行方式	立即执行	▼ *提示:请选择执行方式						
检测模式	完全扫描	 完全扫描:采用主机存活判断、端口扫描、服务判 强制扫描:使用强制手段对扫描目标进行主机存活 登录审计:利用配置好的用户名密码列表对主机进 	I断、漏洞测试的步骤对扫描目标进行完整的安全扫描 5、端口服务探测 行登录后的本地审计					
漏洞插件模板	全部漏洞扫描	▼ *提示:请选择漏洞插件模板						
分布式引擎	默认	▼ 默认:系统将根据引擎的负载情况,智能选择工作 local:系统将会选择本地引擎。	司際。					
执行优先级别	中	▼ 当任务达到并发上限时, '排队等待中'级别高的任务	务将优先执行。					
检测结束发送邮件	×							
检测结束发送短信	×							
坦本								

扫描目标:

输入的内容有[单个主机]和[主机组]两种,多个之间以英文逗号(,)或换行分隔。 单个主机示例: 192.168.1.100,也可使用域名: www.example.com, IPv6示例: 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088, 主机组示例: 192.168.1.0/24.192.168.2.1-254.192.168.3.1-192.168.3.254:

排除某个 IP: 192.168.1.0/24!192.168.1.100。

任务名称:

填写新建的系统扫描任务名称。

执行方式:

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

检测模式:

完全扫描:采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全 扫描。强制扫描:使用强制手段对扫描目标进行主机存活、端口服务探测。登录审计:利用配置好 的用户名密码列表对主机进行登录后的本地审计

漏洞插件模板:

选择漏洞插件模板

分布式引擎:

可选择默认/local,两台及以上数量的设备协同工作的一种部署方式,其中一台作为管理中心,其它的设备作为引擎,管理中心统一进行任务调度及结果展示等操作,管理中心可同时做任务调度和作为分布式引擎使用。默认:系统将根据引擎的负载情况,智能选择工作引擎。同时也可以指定引擎。

执行优先级:

当任务达到并发上限时,'排队等待'级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件:

需要在告警配置中配置邮件网关,多个邮箱可用英文逗号(,)分割。

检测结束发送短信:

需要在告警配置中配置了短信网关,多个手机号码可用英文逗号(,)分割。

2. 自主选择插件

可对扫描任务使用的插件进行修改,使用"启用"或者"禁用"在漏洞插件的基础上来增删漏洞插件,实现插件库自定义。

图6-2 漏洞扫描-自主选择插件

🛛 系统扫描	♀ WEB扫描	□ 数据库检测	◆ □令猜解						
扫描基本配置	自主选择插作	牛 探测选项	检测选项	引擎选项	登录信息	选项			
上 风险级别					$\sim c$	✓ 高	✓ 中	✔ 低 搜索[[]]	年]
类别名称						漏洞			Å
✓已启用 Li	inux本地安全[29	829]				✔已启用	ColdFusion	多个漏洞(文件上传/操作)	
✔已启用 U	nix本地安全[121	59]				✔已启用	Microsoft II	S advsearch.asp直接请求远程DoS	
✔已启用 W	/indows安全[54	77]				✔已启用	Microsoft II	S query.asp直接请求远程DoS	
✔已启用 W	/eb安全[5596]					✔已启用	Microsoft II	S search.asp直接请求DoS	
◆已启用 网	网络设备安全[229	2]				✔已启用	NetSphere	后门检 测	
✔已启用 其	[1679]					✔已启用	Microsoft II	S / Site Server showcode.asp source参数遍历任意文件访问	
◆已启用 P2	2P安全[90]					✔已启用	O'Reilly We	bSite win-c-sample远程溢出	
✓已启用 R	PC安全[38]					✔已启用	AIX FTPd lif	oc库远程缓冲区溢出	
✔已启用 Ⅰ	业控制系统[297	1				✔已启用	阿里巴巴get	32.exe任意命令执行	
◆已启用 云	安全[748]					✔已启用	阿里巴巴We	b Server 2.0 HTTP请求溢出DoS	
◆已启用 数	(据库安全[569]					✔已启用	阿里巴巴tst.	bat任意指挥执行	
◆已启用 远	程溢出[281]					✔已启用	AltaVista In	tranet搜索CGI查询遍历任意文件访问	
✓已启用	TP安全[255]					✔已启用	AN-HTTPd	多测试CGI任意命令执行	
◆已启用 安	全设备[218]					✔已启用	Xylogics附作	毕终端服务ping CGI程序DoS	
✔已启用 D	NS安全[171]					✔已启用	Knox Arkeia	备份服务缓冲区溢出	
◆已启用 指	連服务[111]					✔已启用	Ascend MA	X / Pipeline Router Discard Port Malformed Packet DoS	
✓已启用 SI	NMP安全[33]					✔已启用	+ + + ATH)调制解调器挂起字符串远程DoS	
✓已启用 SI	MTP安全[139]					✔已启用	Axent猛禽防	i火墙零长度IP远程DoS	
◆已启用 移	动安全[75]					✔已启用	Axis Storpo	int CD管理员验证旁路	
◆已启用 后	门检测[112]					✔已启用	BackOrifice	软件检测	
****				Ĩ.	(1)	✔已启用	大哥bb-hist	sh历史模块目录遍历	
尽计20余记录							ø	CPU使用率: 69.84% 内存使用率: 5985.9MB/15946MB 硬盘使用率: 2.6G/9020	

3. 探测选项

图6-3 漏洞扫描-探测选项

🛛 系统扫描	♥ WEB扫描	□ 数据库检测	
扫描基本配置	自主选择插	井 探测选项	检测选项 引擎选项 登录信息选项
提示被扫目标		×	在扫描之前提示被扫描主机,需要扫描目标支持messager服务
开启存活探测		×	如果开启,引擎使用如下探测方法进行探测,如果不能确定存活,则不进行检测,提高检测速度 如果不开启,则对所有主机进行漏洞监测,会延长检测时间
主机存活测试		✓ ARP	ICMP PING TCP PING UDP PING
端口扫描范围		● 标准	 ○ 快速 ○ 全部 指定 标准: 默认端口4000多个。快速: 100个常用端口。全部: 端口0-65535 指定: 单个或范围如22,1-1024,指定TCP端口: TCP:1024-65535,指定 UDP端口: UDP:1025-65535

提示扫描目标

在扫描之前提示被扫主机,需要扫描目标支持 messager 服务。

开启存活探测

如果开启,引擎使用如下探测方法进行探测,如果不能确定存活,则不进行探测,提高检测速度; 如果不开启,则对所有主机进行漏洞检测,会延长检测时间。

主机存活测试

可以复选 ARP、ICMP PING、TCP PING、UDP PING。默认选择前三种。

端口扫描范围

可以选择:标准、快速、全部、指定。

标准:默认端口 4000 多个。快速: 100 个常用端口。全部:端口 0-65535。

指定: 单个或范围如 22, 1-1024, 指定 TCP 端口: TCP:1024-65535, 制定 UDP 端口: UDP:1025-65535。

端口扫描方式

CONNECT方式为全连接扫描,完成TCP/IP的三次握手,速度较慢。SYN方式,只需要发送TCPSYN 包即可完成检测,速度快,建议使用 SYN。

4. 检测选项

图6-4 漏洞扫描-检测选项

□ 系统扫描 ♀ WEB扫描 □ 数据库检	● 口令猜解				
扫描基本配置 自主选择插件 探测选	私测选项 引擎选项 登录信息选项				
最大限度报告漏洞 🗸	若选择开启,扫描结果中不是所有漏洞都经过原理扫描得出,会有一些根据版本信息推测出来的漏洞。				
执行所有规则检测	若选择开启:检测耗时越久、对检测目标的覆盖面更广。				
执行相关联漏洞	若选择开启:某些已例外的漏洞将加入到扫描结果当中。				
保存漏洞检测详情	若选择开启:漏洞的详细打印信息将加入到扫描结果当中。				
自适应网络	根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度				
危险测试	包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用				
停止探测无响应主机	如果扫描过程中发现扫描目标没有反应,停止对该目标的探测				
随机顺序扫描					
启用口令破解 イ	使用默认字典对系统或服务的口令进行猜解				
测试Oracle账号	1				
启用Web检测					
SMB信息探测 🗸					

最大限度报告漏洞

若选择关闭,则将大大提高扫描速率,部分耗时长的规则将跳过执行。

执行所有规则检测

若选择开启:检测耗时越久、对检测目标的覆盖面更广。

执行相关联漏洞

若选择开启:某些已例外的漏洞将加入到扫描结果当中。

保存漏洞检测详情

若选择开启:漏洞的详细打印信息将加入到扫描结果当中。

自适应网络

根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度 **危险测试**

包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用。 停止探测无响应的主机 如果扫描过程中发现扫描目标没有反应,停止对该目标的探测。

启用口令破解

使用默认字典对系统或服务的口令进行猜解。

测试 Oracle 账号

对 Oracle 数据库进行深度检测。

启用 Web 检测

开启则可进行 web 检测。

SMB 信息探测

启用则可进行 SMB 信息检测。

5. 引擎选项

图6-5 漏洞扫描-引擎选项



插件超时

单个插件执行时间最长设置[10-300]。

网络时延

网络连接超时设置[10-300]。

单个主机检测并发数

针对单个的检测目标,并发的检测插件数量[1-50]。

单个扫描任务并发主机数

单个扫描任务,可同时扫描的主机数量[1-120]。注:根据型号不同,最大并发主机数有差异。

单个主机 TCP 连接数:

针对单个检测目标,并发的 TCP 连接数量[1-1024]。

单个扫描任务 TCP 连接数:

单个扫描任务,最多可同时并发的TCP连接数[1-1024]。

6. 登录信息选项

图6-6 漏洞扫描-登录信息选项

□ 系统扫描 ♀ WEB扫描 ♀	数据库检测 💠 口令猜解		
扫描基本配置 自主选择插件	探测选项 检测选项 引擎选项	登录信息选项	
预设登录账号	SSH ▼ 用户名	密码	< 登录验证
		^	
数据库类型	None	v	€数据库验证
SNMPv1/v2-通信串			
SNMPv1/v2-端口			
微软WSUS地址			
微软WSUS端口			
微软WSUS账号			
微软WSUS密码			
使用https	× .		

预设登录账号

下拉选择 SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS、SNMP、 RDP 共 12 种,主要选择主机相应的服务并填写用户名密码,再进行登录验证,提交扫描即可;

数据库类型

下拉选择 None、Postgres、Oracle、Mysql、Mssql、DB2、Informix、Sybase。选择需要检测的 主机上的数据库类型,填写相对应的端口,用户名,密码提交即可,目前数据库验证支持 PostgreSQL、 MsSQL、MySQL 认证;

登录验证

下拉选择 TELNET、SSH、SMB、RDP 共 4 种,登录扫描验证。

图6-7 强	登录验证
--------	------

登录验证				×
目标地址			* 可填入IP: 192.168.1.100 或者域名: www.example.com	
服务	SSH	Ŧ	*	
端口	22		*限制:整数, [1-65535]之间	
用户名				
密码				
验证				

数据库验证

下拉选择 Postgres、MySqpl、MsSql 共 3 种,数据库登录扫描验证。

图6-8 数据库验证

数据库验证				×
目标地址			* 可填入IP: 192.168.1.100 或者域名: www.example.com	
数据库类型	Postgres	•	*	
数据库端口	5432		*排除某个IP: 192.168.1.0/24!192.168.1.100端口限制:整数, [1-65535]之间	
数据库用户名			*	
数据库密码				
验证				

微软 WSUS 账号

WSUS 是个微软推出的网络化的补丁分发方案。通过对 WSUS 账号配置与 WSUS 服务器建立连接,从 WSUS 获取补丁信息,或者反馈给 WSUS 哪些 Windows 主机缺少哪些补丁,在报表中显示获取的补丁信息。

图6-9 WSUS 账号

微软WSUS地址	
微软WSUS端口	
微软WSUS账号	
微软WSUS密码	

表6-1 WSUS 账号参数说明

参数	说明
微软WSUS地址	填写微软WSUS地址
微软WSUS端口	填写微软WSUS端口
微软WSUS账号	填写微软WSUS账号
微软WSUS密码	填写微软WSUS密码

https 参数

与 WSUS 通信使用 http 协议或 https 协议,勾选代表使用 https 协议,否则代表使用 http 协议。

图6-10 https 参数

使用https

6.1.2 Web 漏洞扫描任务

1. 扫描基本配置

针对 web 扫描,添加需要扫描的目标,填写形式为单个站点或者站点组,配置任务名称,选择 web 扫描插件模板并提交扫描。

图6-11 添加任务

□ 系统扫描 ♥ WEB扫描 □ 對	数据库检测 ◆ 口令猜解					
扫描基本配置 自主选择插件 引擎配置 检测选项						
扫描目标方式						
扫描目标			a	* URL地址: http://www.example.com/或https://www.example.com/ URL地址: http://192.168.1.100/或https://192.168.1.100/ IPv6 URL示例: http://[2001:fecd:ba23:cd1f.dcb1:1010:9234:4088]/ 多个URL以及文逗号()或回年分隔		
任务名称	WEB扫描-			*提示:请填写任务名称,长度在[1-40]字符之间		
执行方式立即执行		٣	*提示:请选择执行方式			
漏洞插件模板	全部WEB漏洞	٣	*提示:请选择漏洞插件模板			
分布式引擎	默认	۳	默认:系统将根据引擎的负载情况,智能选择工作引导	擎。同时也可以指定引擎		
执行优先级别中		۳	当任务达到并发上限时,'排队等待中'级别高的任务将优先执行。			
检测结束发送邮件						
检测结束发送短信						
坦六						

扫描目标

URL 地址: http://www.example.com/或 https://www.example.com/*URL 地址: http://192.168.1.100/ 或 https://192.168.1.100/*IPv6URL 示例: http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/*多个 URL 以英文逗号(,)或回车分隔。

任务名称

填写新建的 WEB 扫描任务名称。

执行方式

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

漏洞插件模板

选择漏洞插件模版。

分布式引擎

可选择默认/local。两台及以上数量的设备协同工作的一种部署方式,其中一台作为管理中心,其它的作为引擎,管理中心统一进行任务调度及结果展示等操作,管理中心可同时做任务调度和作为分布式引擎使用。默认:系统将根据引擎的负载情况,智能选择工作引擎。同时也可以指定引擎。

执行优先级

当任务达到并发上限时,排队等待中'级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件

需要在告警配置中配置了邮件网关,多个邮箱可用英文逗号(,)分隔。

检测结束发送短信

需要在告警配置中配置了短信网关,多个手机号码可用英文逗号(,)分隔。

2. 自主选择插件

可对扫描任务使用的插件进行修改,使用"启用"或者"禁用"在漏洞插件的基础上来增删漏洞插件,实现插件库自定义。

图6-12 WEB 扫描-自主选择插件



3. 引擎配置

图6-13 WEB 扫描-引擎配置

🖵 任务中心 💦 🗸	□ 系統扫描 • WEB扫描 □ 数据	库检测 ◆ □令猜解	
新建任务	扫描基本配置 自主选择插件 引き	擎配置 检测选项	
任务列表	并发线程数	5	单个扫描目标,并发执行的线程数量[1-20]
探测未知站点	区分大小写	~	网站对于Url中字母大小写是否敏感
204000	最大美似页面数	20	引擎用于归并类似链接时需要保留类似链接的数量[1-1000]
◎ 资产管理	同目录下最大页面数	100	引擎在归并抛接时,同一目录下需要保留的抛接数量[1-1024]
★・策略模板 <	まは とう 教	2 ^	当時接天法访问时,重新访问的次数[1-10]
→ 报表管理 <	2.60/A9X		memory and a substant and a substant and a sub-
	超时时间(秒)	30	当访问链接时超过多长时间,判定链接无法访问[1-300]
◎ 系统管理 <	代理类型	无	▼ 网站访问目标网站时,可能需要通过代理才能访问

并发线程数

单个扫描目标,并发执行的线程数量[1-20]。

区分大小写

网站对于 Url 中字母大小写是否敏感。

最大类似页面数

引擎用于归并类似链接时需要保留类似链接的数量[1-1000]。

同目录下最大页面数

引擎在归并链接时,同一目录下需要保留的链接数量[1-1024]。

重试次数

当链接无法访问时,重新访问的次数[1-10]。

超时时间

当访问链接时超过多长时间,判定链接无法访问[1-300]。

代理类型

网站访问目标网站时,可能需要通过代理才能访问,代理类型有2种:HTTP、SOCKS。

图6-14 HTTP 代理

代理类型	НТТР	٣	网站访问目标网站时,可能需要通过代理才能访问
代理IP地址	127.0.0.1		
代理IP端口	8080		
代理用户名			
代理密码			

图6-15 SOCKS 代理

代理类型	SOCKS	٣	网站访问目标网站时,可能需要通过代理才能访问
代理IP地址	127.0.0.1		
代理IP端口	8080		
代理用户名			
代理密码			

4. 检测选项

图6-16 WEB 扫描-检测选项

□ 系统扫描 • WEB扫描 •	数据库检测 ◆ 口令猜解
扫描基本配置 自主选择插件	引擎配置 检测选项
暗链检测	★ 发现网站中的存在的其他隐藏链接
网站木马检测	☆ 检測网站中是否存在恶意脚本
检测深度	5 合义 检测网站时爬虫爬取网站的页面深度
爬虫策略	广度优先 ▼ 引擎的爬虫在爬取网站页面多叉树时,采用的先后顺序策略
HTTP请求头	Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 引擎爬虫模拟浏览器的UserAgent
表单填充内容	1 引擎爬虫模拟提交时需要填充的表单的内容
最大页面数	5000 🗘 引擎爬虫爬取页面时超过最大页面数后,不做爬取
页面最大KB数	5120 🛟 引擎爬虫爬取页面时,如果页面大小超过一定大小,则放弃爬取
例外URL	logout.x sigout.x exit.x 引擎爬虫不爬取的url关键字,一般为登出页面、危险操作、或不想做检测的链接
例外文件类型	Image: frame of the first state of the
例外特定参数	ASPNET_SessionID x ASPSESSIONID x PHPSESSID x SITESERVER x 引擎对默认的参数不做安全检测 sessid x

暗链检测

发现网站中的存在的其它隐藏链接.

网站木马检测

检测网站中是否存在恶意脚本。

检测深度

检测网站时爬虫爬取网站的页面深度。

爬虫策略

引擎的爬虫在爬去网站页面多叉树时,采用的先后顺序策略:广度优先和深度优先。广度优先指横向爬取,又叫层次遍历,从上往下对每一层依次访问,在每一层中,从左往右(也可以从右往左)访问结点,访问完一层就进入下一层,直到没有结点可以访问为止。深度优先指纵向爬取,是对每一个可能的分支路径深入到不能再深入为止,而且每个结点只能访问一次。

Http 请求头

引擎爬虫模拟浏览器的 UserAgent。

表单填充内容

引擎爬虫模拟提交时需要填充的表单的内容。

最大页面数

引擎爬虫爬去页面时超过最大页面数后,不做爬取。

页面最大 KB 数

引擎爬虫爬去页面时,如果页面大小超过一定大小,则放弃爬去。

例外 URL

引擎爬虫不爬取的 url 关键字,一般为登出页面、危险操作、或不想坐检测的链接。

例外文件类型

引擎爬虫不对如下类型的链接爬取,一般为非文本的链接。

例外特定参数

引擎对默认的参数不做安全检测。

6.1.3 数据库扫描任务

1. 扫描基本配置

针对数据库扫描,添加需要扫描的目标,填写形式为单个主机或者主机组,配置任务名称,选择数 据库扫描插件模板并提交扫描。

图6-17 添加数据库扫描任务

□ 系统扫描 ② WEB扫描 □	数据库检测 � 口令猜解		
检测基本配置 自主选择插件	探测选项检测选项	引擎选项	
扫描目标方式	 手动输入 使用 	资产 🔿 批量导入	
扫描目标			* 输入的内容有单个主机和主机组两种,多个之间以英文逗号,或换行分隔 单个主地示例:192.168.1.100 也可使用域名:www.example.com IPv6示例:2001;fecd:ba23;cd1f.dcb1:1010;9234:4088 主机组示例:192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 排除某个IP:192.168.1.0/24;192.168.1.100
数据库类型	None		▼ * ●数据库验证
任务名称	数据库检测-		* 提示: 请填写任务名称,长度在[1-40]字符之间
执行方式	立即执行	▼ *提示:请选择执行方式	
分布式引擎	默认	▼ 默认:系统将根据引擎的负载情况,智能选	择工作引擎。同时也可以指定引擎
执行优先级别	中	▼ 当任务达到并发上限时, '排队等待中'级别?	前的任务将优先执行。
检测结束发送邮件	×		
检测结束发送短信	×		
提交			

扫描目标

*输入的内容有单个主机和主机组两种,多个之间以英文逗号,或换行分隔。

*单个主机示例: 192.168.1.100 也可使用域名: www.example.com。

*IPv6示例: 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088。

*主机组示例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254。

*排除某个 IP: 192.168.1.0/24!192.168.1.100。

数据库类型

可下拉选择: None、Postgres、Oracle、MySQL、msSQL、DB2、Informix、Sybase。

任务名称

填写新建的数据库扫描任务名称。

执行方式

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

漏洞插件模板

选择数据库漏洞插件模板。

分布式引擎

可选择默认/local。两台及以上数量的设备协同工作的一种部署方式,其中一台作为管理中心,其它的作为引擎,管理中心统一进行任务调度及结果展示等操作,管理中心可同时做任务调度和作为分 布式引擎使用。默认:系统将根据引擎的负载情况,智能选择工作引擎。同时也可以指定引擎。

执行优先级

当任务达到并发上限时, '排队等待中'级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件

需要在告警配置中配置了邮件网关,多个邮箱可用英文逗号(,)分隔。

检测结束发送短信

需要在告警配置中配置了短信网关,多个手机号码可用英文逗号(,)分隔。

2. 自主选择插件

可对扫描任务使用的插件进行修改,使用"启用"或者"禁用"在漏洞插件的基础上来增删漏洞插件,实现插件库自定义。

图6-18 数据库扫描-自主选择插件

□ 系统扫描	♀ WEB扫描	□ 数据库检测	✿ □令猪解										1
检测基本配置	自主选择插作	牛 探测洗项	检测选项	引擎洗项									
よ 风险级别				✓ Ø	✓ 高	✓ 中	✓ ft	Æ				搜索[回车]	
类别名称				*	漏洞								
✔已启用 数	如据库安全[569]				✔已启用	MS99-059	: Micro	osoft SQL Serv	er制作的TCP数据	居包远程DoS (未约	圣认证的检查)		
					✔已启用	Oracle Wel	ebserver	PL / SQL存储	过程GET请求Dos	5			
总计1条记录				$\langle 1 \rangle$	✔已启用	MySQL短档	金查字符目	串验证旁路					
					✔已启用	MySQL未密	密码帐户相	检查					
					✔已启用	PostgreSQ	L默认无	密码帐号					
					✔已启用	Oracle应用	I服务器X	(SQL样式表任意	意Java代码执行				
					✔已启用	Oracle XSC	QL query	y.xsql sql参数S	SQL注入				
					✔已启用	MySQL <3.	3.23.36多	8个漏洞					
					✔已启用	Oracle应用	I服务器n	ndwfn4.so HTT	「P请求远程溢出				
					✔已启用	Oracle数据	引库tnslsn	nr服务远程版本	披露				
					✔已启用	Oracle数据	居库监听和	望序 (tnslsnr)	服务空白密码				
					✔已启用	Microsoft S	SQL Ser	rver sa帐户默认	人空白密码				
					✔已启用	Microsoft 9	SQL Ser	rver UDP查询近	远程版本披露				
					✔已启用	MySQL服务	身器检测						
					✔已启用	Oracle应用	I服务器V	Web缓存多个远	程DoS				
					✔已启用	Oracle 9iAs	S mod_p	plsql帮助页面词	请求远程溢出				
					✔已启用	Oracle 9iAs	S DMS /	/ JPM页面匿名	访问				
					✔已启用	Oracle 9iAs	S mod_p	plsql DAD管理	界面访问				
					✔已启用	Oracle 9iAs	S global	lls.jsa数据库凭持	据远程披露				
					✔已启用	Oracle 9iAs	S Java P	Process Manag	ger / oprocmgr-	status匿名进程操	鮮作		
					✔已启用	Oracle 9iAs	S_page	es目录编译JSP》	原公开				

3. 探测选项

图6-19 数据库扫描-探测选项

□ 系统扫描	数据库检测 💠 口令猜解					
检测基本配置 自主选择插件	探测选项 检测选项 引擎选项					
提示被扫目标	✓ 在扫描之前提示被扫描主机,需要扫描目标支持messager服务					
开启存活探测	✓ 如果开启,引擎使用如下探测方法进行探测,如果不能确定存活,则不进行 如果不开启,则对所有主机进行漏洞监测,会延长检测时间	如果开启,引擎使用如下探测方法进行探测,如果不能确定存活,则不进行检测,提高检测速度 如果不开启,则对所有主机进行漏洞监测,会延长检测时间				
主机存活测试	ARP ICMP PING TCP PING UDP PING					
端口扫描范围	 ● 标准 ● 快速 ○ 全部 ○ 指定 标准:默认端□400 指定:单个或范围 	00多个。快速:100个常用端口。全部:端口0-65535 g22,1-1024,指定TCP端口:TCP:1024-65535,指定UDP端口:UDP:1025-65535				
TCP端口扫描方式	□ CONNECT	CP/IP的三次握手,速度较慢 J完成检测,速度快,建议使用SYN				

提示扫描目标

在扫描之前提示被扫描主机,需要扫描目标支持 messager 服务。

开启存活探测

如果开启,引擎使用如下探测方法进行探测,如果不能确定存活,则不进行检测,提高检测速度; 如果不开启,则对所有主机进行漏洞监测,会延长检测时间。

主机存活测试

可以复选 ARP、ICMPPING、TCPPING、UDPPING。默认选择前三种。

端口扫描范围

标准:默认端口 4000 多个。快速: 100 个常用端口。全部:端口 0-65535,指定:单个或范围如 22,1-1024,指定 TCP 端口: TCP:1024-65535,指定 UDP 端口: UDP:1025-65535。

端口扫描方式

CONNECT方式为全连接扫描,完成TCP/IP的三次握手,速度较慢。SYN方式,只需要发送TCPSYN 包即可完成检测,速度快,建议使用 SYN。

4. 检测选项

□ 系统扫描 ② WEB扫描 □ 数据库检测	◆ □令猜解
检测基本配置 自主选择插件 探测选项	检测选项 引擎选项
最大限度报告漏洞	若选择开启,扫描结果中不是所有漏洞都经过原理扫描得出,会有一些根据版本信息推测出来的漏洞。
执行所有规则检测	若选择开启: 检测耗时越久、对检测目标的覆盖面更广。
执行相关联漏洞	若选择开启:某些已例外的漏洞将加入到扫描结果当中。
保存漏洞检测详情	若选择开启:漏洞的详细打印信息将加入到扫描结果当中。
自适应网络	根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度
危险测试	包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用
停止探测无响应主机	如果扫描过程中发现扫描目标没有反应,停止对该目标的探测
随机顺序扫描	
启用口令破解	使用默认字典对系统或服务的口令进行猜解
测试Oracle账号 ×	
启用Web检测 ×	
SMB信息探测	

图6-20 数据库扫描-检测选项

最大限度报告漏洞

若选择关闭,则将大大提高扫描速率,部分耗时长的规则将跳过执行。

执行所有规则检测

若选择开启:检测耗时越久、对检测目标的覆盖面更广。

执行相关联漏洞

若选择开启:某些已例外的漏洞将加入到扫描结果当中。

保存漏洞检测详情

若选择开启:漏洞的详细打印信息将加入到扫描结果当中。

自适应网络

根据网络的反应速度,适当调整发包的速率,从而不至于将网络扫瘫痪,但会影响扫描速度。

危险测试

包含一些危险的测试方法,如:拒绝服务检测,导致扫描目标的拒绝服务,因此慎用。

停止探测无响应的主机

如果扫描过程中发现扫描目标没有反应,停止对该目标的探测。

启用口令破解

使用默认字典对系统或服务的口令进行猜解。

测试 Oracle 账号

对 Oracle 数据库进行深度检测。

启用 Web 检测

开启则可进行 Web 检测。

SMB 信息探测

启用则可进行 SMB 信息检测。

5. 引擎选项

图6-21 数据库扫描-引擎选项

检测基本配置 自主选择插件	探测选项	检测选项	引擎选项
插件超时 (秒)	30	$\hat{\mathbf{v}}$	单个插件执行时间最长设置[10-300]
网络时延 (秒)	30	$\hat{\boldsymbol{\cdot}}$	网络连接超时设置[10-300]
单个主机检测并发数	5	$\hat{\boldsymbol{\cdot}}$	针对单个的检测目标,并发的检测插件数量[1-50]
单个扫描任务并发主机数	120	$\hat{\boldsymbol{\cdot}}$	单个扫描任务,可同时扫描的主机数量[1-120]
单个主机TCP连接数	15	$\hat{\boldsymbol{\cdot}}$	针对单个检测目标,并发的TCP连接数量[1-1024]
单个扫描TCP连接数	19	$\hat{\boldsymbol{\cdot}}$	单个扫描任务,最多可同时并发的TCP连接数[1-1024]

插件超时

单个插件执行时间最长设置[10-300]。

网络时延

网络连接超时设置[10-300]。

单个主机检测并发数

针对单个的检测目标,并发的检测插件数量[1-50]。

单个扫描任务并发主机数

单个扫描任务并发主机数。注: 根据漏扫不同型号最大并发主机数会有差异。

单个主机 TCP 连接数

针对单个检测目标,并发的 TCP 连接数量[1-1024]。

单个扫描任务 TCP 连接数

单个扫描任务,最多可同时并发的TCP连接数[1-1024]。

6.1.4 口令猜解任务

1. 扫描的基本配置

针对口令猜解任务是基于资产的,首先需要选择资产,自定义任务名称,选择执行方式,选择扫描 的服务类型和数据库类型,其中检测模式有两种,标准模式和组合模式,标准模式是指只针对用户 名或密码一项扫描,组合模式是针对用户名和密码一起进行扫描。针对字典可以选择系统自带的默 认字典也可以自定义按照相应格式上传自定义字典进行扫描,再填写相对应的端口号提交即可。

图6-22 口令猜解任务基本配置

□ 系统扫描 ♀ WEB扫描	□ 数据库检测 �	口令猜解						
基本配置 引擎选项								
资产名称	WEB扫描-192.	168.0.123资产			* 若资产为空,请先在资产管理处添加资产或者先执行系统或WEB扫描。			
任务名称	口令猜解-					* 提示: ;	青填写任务名称,长	度在[1-40]字符之间
执行方式	立即执行	▼ * 请〕	先择执行方式	¢				
服务类型	TELNET	组合模式	Ŧ	TELNET组合字典	٣	端口	23	* 勾选项端口必填
	FTP	组合模式	*	FTP组合字典	٣	端口	21	
	SSH	组合模式	v	SSH组合字典	٣	端口	22	
	POP3	组合模式	*	POP3组合字典	٣	端口	110	
	SMB	组合模式	v	SMB组合字典	٣	端口	445	
	SNMP	标准模式	v	SNMP密码字典	v	端口	161	
	RDP	组合模式	Ψ.	RDP组合字典	٣	端口	3389	
	SMTP	组合模式	Ψ.	SMTP组合字典	Ŧ	端口	25	
	REDIS	标准模式	٣	REDIS密码字典	٣	端口	6379	
数据库类型	Oracle	组合模式	Ŧ	Oracle组合字典	v	端口	1521	* 勾选项端口必填
	MySQL	组合模式	Ŧ	MySQL组合字典	٣	端口	3306	
	Postgres	组合模式	Ψ.	Postgres组合字典	v	端口	5432	
	MsSQL	组合模式	٣	MsSQL组合字典	٣	端口	1433	
	DB2	组合模式	*	DB2组合字典	٣	端口	50000	
	MongoDB	组合模式		MongoDB组合字典	٣	端口	27017	
公布式引擎	明十十1	▼ 野认	: 系统将根	民引擎的负载情况 智能洗掉	¥⊤作司!	警局时也可	可以指定引擎	

2. 引擎选项

图6-23 口令猜解任务—引擎选项

日 系统扫描	♀ WEB扫描	□ 数据库检测	◆ 口令猜解	
基本配置	引擎选项			
口令猜解速率		3	\$	对单个服务进行口令猜解的探测速度,值越小,探测速度越慢。 值越小,目标主机对引擎的阻断概率越小。
最大线程并发	数	5	$\hat{\boldsymbol{\cdot}}$	对单个服务进行口令猜解的并发线程数,值越大,探测速度越快。

口令猜解速率

对单个服务进行口令猜解的探测速度,值越小,探测速度越慢。值越小,目标主机对引擎的阻断概 率越小。

最大线程并发数

对单个服务进行口令猜解的并发线程数,值越大,探测速度越快。

6.2 任务列表

任务列表模块列出了目前存在的全部扫描任务,并可对任务扫描进行各种操作管理。方便用户开启 任务和查看每个资产组的主机数,进度栏可显示扫描出的漏洞数,进度栏模块可以查看每个主机的 检测进度、历史执行记录和漏洞风险分布情况。

图6-24 任务列表-任务列表

♀ 任务列表 ■ 工作列表						新增+ 刷新2 全	部任务 ▼ 担	[四车]	Q
每页显示 25 🔻									
任务名称	•	执行方式	开始时间	结束时间	检测耗时	进度		操作	
WEB扫描-192.168.0.123		手动执行	2019-03-29 15:04:50		11分27秒	漏洞数: 46 网页数: 3020 剩余时	1间:大于1小时	暂停 📕 停止 🗌	

< 1 >

任务列表中,各项参数含义如下:

任务名称

显示当前任务的名称,格式为用户在添加任务时的命名。

执行方式

执行方式分为手动执行、定时执行、每日执行、每周执行、每月执行、离线执行。

开始时间/结束时间

显示当前评估任务的开始和结束时间,对于尚未结束的任务,只显示其开始时间。

操作

可以选择立即开始或者禁用当前任务,对于正在执行的任务,可以选择暂停或者停止该任务。

检测耗时

可以实时的展示出任务执行检测大致需要的执行时间,执行完成会显示整个任务扫描花费的时长。

进度

显示当前任务执行的进度情况,点击进度栏可以查看当前任务的漏洞数,资产组的主机漏洞排名,风险等级分布及历史执行记录。

图6-25 任务列表-任务列表进度

 任务列表 	麦 🗷 工作列表			►
主机列表	漏洞列表 漏洞目录树 历史执行记录			WEB扫描详情
风险级别	漏洞名称	漏洞所属分类	总计	网站域名 192168.0.123
中风险	启用了目录列表	A6 敏感信息泄漏	6	四時時 192.168.0.123
低风险	Cookie未配置HttpOnly标志	A2 失效的身份认证和会话管理	1	服务器信息 Apache/2.2.19 (Win32) PHP/5.2.17
低风险	SetCookie未配置Secure	A2 失效的身份认证和会话管理	1	网站标题 论坛-PoweredbyDiscuz!
低风险	发现内网IP地址	A6 敏感信息泄漏	10	网页编码 gbk
低风险	用户认证信息明文传输	A2 失效的身份认证和会话管理	1	服务器语言 PHP/5.2.17
低风险	未禁用密码表单自动完成属性	A2 失效的身份认证和会话管理	5	物理地址 局域网-对方和您在同一内部网[192,168,0.0-192,16
低风险	发现可暴力猜解的登录表单	A2 失效的身份认证和会话管理	5	网页总数 3020
信息	敏感文件或备份	A5 安全配置错误	17	
				漏洞风险分布



6.3 工作列表

工作列表主要展示了当前开启的任务中正在执行的任务。可以看到该任务的任务名称,开始时间, 检测耗时以及执行的进度。也可以对正在执行的任务进行暂停或停止操作。

图6-26 任务列表-工作列表

♀ 任务列表 ■ 工作列表				刷新2	搜索[回车]	¢
检测对象	▼ 任务名称	开始时间	检测耗时	进度	操作	
192.168.0.123	WEB扫描-192.168.0.123	2019-03-29 15:04:50	12分38秒	漏洞数: 46 网页 数: 3020 剩余时间:大于	1小时 停止	
						< 1 >

工作列表中,各项参数含义如下:

检测对象

显示当前任务中里包含的检测对象。

任务名称

显示当前任务的名称,格式为用户在添加任务时的命名。

开始时间

显示当前评估任务的开始时间。

检测耗时

可以实时的展示出任务执行检测大致需要的执行时间,执行完成会显示整个任务扫描花费的时长。

进度

显示当前任务执行的进度情况,如果是 web 扫描可以展示漏洞数,网页数,剩余时间,如果是系统 扫描会展示漏洞数,主机数,剩余时间。

操作

对于正在执行的任务,可选择停止/强制停止当前任务。

6.4 探测未知站点

探测未知站点是扫描 IP 范围内可能存在的 web 站点。

6.4.1 新建探测任务

图6-27 探测未知站点-新建探测任务

新建探测任务			×
任务名称	探测目标-	*提示:请自定义任务名称,长度在[6-40]字符之间	
探测IP/IP范围	đ	* 多个之间以英文逗号(.)或换行分隔 IP范围示例: 192.168.1.0/24,192.168.2.1-254 192.168.1-2.1-254	
探测端口/范围	80,443,8080,3128,8081,9080	* 可填入端口或端口范围示例: 1-65535 多个之间以英文逗号())分隔	
开始探测			

探测端口范围

填写 web 站点常用的端口及自定义端口。

6.4.2 探测详情

图6-28 探测未知站点-探测详情

探测详情

URL地址	服务器特征					
https://192.168.0.1:443/	nginx					
http://192.168.0.123:80/	Apache/2.2.19 (Win32) PHP/5.2.17					
https://192.168.0.123:443/						
转成任务 转成资产组						

 \times

转成任务

自动跳转到 web 漏洞扫描,将探测出的 web 站点添加到扫描目标中。

转成资产

自动添加资产,提交到资产组中。

6.5 会话录制

6.5.1 开始录制会话

首先填写需要录制的域名,点击开始按钮开始录制,其次在另外一个浏览器配置 http 代理,代理服务 IP 为此设备 IP 端口为 8080,然后在配置了 http 代理的浏览器上,依次访问需要录制的 url。 注: 域名对字符限制: '\''、''、'|'、'\$'、';'、'\'、'\n'、'<'、'>'、'/'、'?'、':'、'''、'('、')、" 注: 此次录制只允许在本机所在的浏览器进行录制

×

图6-29 录制会话界面

会话录制

*域名 多个域名之间以英文逗号()分隔	• •
 步骤1:首先填写需要录制的域名,点击开始按钮开始录制 步骤2:其次在另外一个浏览器配置http代理,代理服务IP为此设备IP端口为8080 步骤3:然后在配置了http代理的浏览器上,依次访问需要录制的url 注:域名对字符限制: '\''、'`'、' '、'\$'、';'、'\'、'\n'、'<'、'>'、'/'、'?'、':'、'''、'('、')'、 注:此次录制只允许在本机所在的浏览器进行录制 	
● 已录制的URL	~
	~
开始录制▶	

6.5.2 停止会话

将正在录制的会话停止。

6.5.3 保存会话

将已录制的会话保存。

6.5.4 录制的会话列表

图6-30 会话录制列表

□ 会活录制 录制+ 刷									ĺ
	历史会话名称	检测目标	开始时间	结束时间	URL数量	操作			
	172.16.102.88_20180826011555.dat	172.16.102.88	2018-08-26 01:15:36	2018-08-26 01:15:55	59	下发任务▶	查看《	٥	
总计1	条记录						<	1	>

6.5.5 下发任务

将已录制的会话下发 web 扫描任务。

6.5.6 查看录制的会话内容

图6-31 查看录制

		×		录制+	刷新2	
UNLIH I用			URL数量	操作		
请求方式	URL		59	下发任冬	奇景の	
GET	https://172.16.102.88:443/			1-2211235		
POST	https://172.16.102.88:443/customer/createcode/				< 1	
GET	https://172.16.102.88:443/img/code/1535217337784.png					
GET	https://172.16.102.88:443/					
GET	https://172.16.102.88:443/assets/plugins/font-awesome/css/font-awesome.min.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap/css/bootstrap.min.css					
GET	https://172.16.102.88:443/assets/plugins/uniform/css/uniform.default.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-switch/static/stylesheets/bootstrap-switch-metro.css					
GET	https://172.16.102.88:443/assets/plugins/jquery-multi-select/css/multi-select.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-toastr/toastr.min.css					
GET	https://172.16.102.88:443/assets/plugins/nouislider/jquery.nouislider.css					
GET	https://172.16.102.88:443/assets/plugins/gritter/css/jquery.gritter.css					
GET	https://172.16.102.88:443/assets/plugins/select2/select2_metro.css					
GET	https://172.16.102.88:443/assets/plugins/clockface/css/clockface.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-wysihtml5/bootstrap-wysihtml5.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-datepicker/css/datepicker.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-timepicker/compiled/timepicker.css					
GET	https://172.16.102.88:443/assets/plugins/bootstrap-colorpicker/css/colorpicker.css		/			

7 资产管理

管理员可以对所有资产设备进行风险资产管理,在进行资产风险管理时,首先需要创建资产。通过 资产,管理员可以浏览网内全部资产的数量以及资产的安全情况。

图7-1 资产管理

Ģ	任务中心	<	❷ 资产管理							新增资	i#+ 🔿	
۲	资产管理		▲ 资产组	搜索[回车] 丶	♥ 资产详情						\sim	
ġ.	策略模板	<	一王系统扫描-192p资产		资产风险	漏洞详情						
	捉主管理		─────────────────────────────────────		开始时间	开始时间 结束时间 高				低	信息	
	1KWEH		──王系统扫描-1922资产		没有检索到数据							
ф	系统管理		─────────────────────────────									
			────────────────────────────────────									
			────────────────────────────────────									
			────────────────────────────────────									
			王系统扫描-192资产									

对于其中一个资产,点击可以显示资产树,管理员可以通过查看资产树来了解自己的网络资产情况。 系统扫描资产:点击系统扫描资产中的资产会显示该资产的资产风险,漏洞详情及资产指纹信息以 及系统资产组属性。资产风险描述了每个资产不同执行时间段的漏洞数,具体到高、中、低危的风 险;漏洞详情描述了每个漏洞的具体信息;资产信息描述了每个资产的主机信息;系统资产属性主 要描述了该资产所属的资产名称,及其扫描 IP/域名。

图7-2 系统资产管理-资产详情

❷ 资产管理					
盐 资产组 搜索	[回车] >	❥ 资产详情			
─────────────────────────────────────		资产风险	结果详情	资产指纹信息	系统资产组属性
—————————————————————————————————————		÷+n 14644			
─────────────────────────────────────		±0,00,11; 10	05.1.1.20		
		王机名称: ₩]	IN-PG9DIE	A2BVU	
✓ 105.1.1.20		操作系统: Mi	icrosoft	Windows Serv	ver 2008 R2 Standard Service Pack 1
		物理地址: 00	C:DA:41:1	D:87:2C	
——网站地址:http://183.1.1.224:80/					
——网站地址:http://183.1.1.223:8080/					
——网站地址:http://183.1.1.222:8081/					

Web 扫描资产:点击 web 扫描资产中的一条资产会在页面右边显示出该资产的资产风险,漏洞详 情,资产信息,资产属性;资产风险描述了每个资产不同执行时间段的漏洞数,具体到高、中、低 危的风险;漏洞详情描述了每个漏洞的具体信息;资产信息描述了每个 web 资产的详细信息;资产 属性主要描述了该资产所属的资产名称,起始 URL,其它 URL,网站域名,扫描根目录,例外 URL, 登录认证。其中资产名称,起始 URL,网站域名会扫描完该资产后自动同步,至于其它 URL,网 站域名,例外 URL,登录认证(Cookie 认证,Form 认证,Basic 认证,NTLM 认证)需要用户根 据资产需要进行自主配置。

图7-3 web 资产管理-资产详情

❷ 资产管理										新	增资产+	Q
▲ 资产组	搜索[回车]	\sim	📎 资产详情									\sim
—————————————————————————————————————			资产风险	漏洞详情	资产	指纹信息	WEB资产属性					
─────────────────────────────────────			资产名称			网站地址:	: http://172.16.10	02.192				
─────────────────────────────────────			起始URL			http://172	2.16.102.192					
─────────────────────────────────────			甘州山口									
────────────────────────────────────			AIBOKE									
─────────────────────────────────────			网站域名			172.16.10	2.192					
—————————————————————————————————————			扫描根目录			/						
✔ 网站地址:http://172.16.102.192	2		例外URL									
─────────────────────────────────────			登录认证			无				Ŧ	◆登录验证	E
			上传网站证书	ŝ		浏览	未选择文件。		浏览器客户端	证书,如	PFX/PKCS12	等格式
			上传网站证书	密码					导出证书时设	置的密码		
			桿态									



8.1 在线查询

在线查询模块可以查看所有任务的扫描结果,包括扫描漏洞的详细信息和解决办法,同时可以根据 需求只查询某个风险等级的漏洞。还可以选择查询系统漏洞/WEB漏洞/资产设备漏洞。

图8-1 在线查询

Q 3	Q 系统漏洞 Q WEB漏洞 4 资产设备漏洞查询									
查询类	理: 资产 * 捜索资产名称 × 🕄	✓ 高	✓ 中 ✓ 低		搜索[回车]					
	资产	风险级别 🔻	漏洞名称	协议/服务/端口						
+	系统扫描-192p资产	低风险	Microsoft Windows SMB服务检测	tcp/cifs/445						
+	系统扫描-12资产	低风险	Microsoft Windows SMB服务检测	tcp/smb/139						
(F)	系统扫描-1922资产	低风险	Windows NetBIOS / SMB远程主机信息披露	udp/netbios-ns/137						
	★☆ロボ 0次产	低风险	Microsoft Windows SMB NativeLanManager远程系统信息	tcp/cifs/445						
(±		低风险	Microsoft Windows SMB登录可能	tcp/cifs/445						
+	系统扫描-192ddd资产									
+	系统扫描-112资产	总计5条记录			< 1					
+	系统扫描-192资产									
单计7名										

8.2 对比分析

管理员可以选择多个任务点击对比分析对同一任务的多次扫描结果可任选两次进行对比分析,统计出新增和减少的漏洞以及漏洞变化趋势等。还可以进行资产组之间的漏洞对比。

图8-2 对比分析

系统漏洞 🖽	WEB漏洞						
洞变化(资产)	资产组对比						
资产分组对比							
资产组一	系统扫描-192.168.8.189资产	Ŧ	资产组二 3	系统扫描-172.16.102.19	2资产	v	对比
讨比统计							
时比统计 资产组名称		资产总数	漏洞总数	育危漏洞	中危漏洞	低危漏洞	信息漏洞
寸比统计 资产组名称 系统扫描-192.1	68.8.189资产	资产总数 1	漏洞总数 160	高危漏洞 23	中危漏洞 23	低危漏洞 114	信息漏洞 0

8.3 导出报表

可按照资产组和时间导出扫描报表,报表分为详细报告和统计报表,导出格式分为 HTML、WORD、 PDF,EXCEL、XML,报表标题可自定义。

图8-3 导出扫描报表

▲ 导出报表		
輸出报表		
选择导出对象	● 系統扫描资产组 ○ WEB扫描资产组	* 注释:安全基线检测、数据库检测、口令猜解任务都属于系统扫描范畴
指定资产组	系统扫描-192p资产 v	*提示:仅显示已检测过的资产组
检测任务时间段	2018-08-31 15:05:50 至 2018-08-31 *	*提示:开始时间-至-结束时间
导出格式	HTML OWORD OPDF	○ EXCEL ○ XML
导出方式	详细报表 🔻	*提示:请选择导出方式
报表标题	漏洞扫描安全评估报告	* 提示:请填写报表标题。限制:[4-30]字符之间,限制字符:\ / : * ? * < > , (),`, { }。
导出文件名	系统扫描-192p资产	* 提示:请填写导出的文件名称。限制:[1-30]字符之间,限制字符:\ / : * ? * < > , (), `, { }。
自定义公司信息	×	
设置压缩包密码	×	
导出		

导出报表将实时显示导出进度,便于用户了解导出实时情况.

图8-4 导出扫描报表进度条显示

▲ 导出报表 [] 报表列表		
▶ 导出状态	×	
<mark>当前进</mark> 度:20/240 导出目标:		
输出报表		
选择导出对象	● 系統扫描资产组 ○ WEB扫描资产组	* 提示:安全基线检测、数据库检测、口令猜解任务请选择系统扫描选项
指定资产组	系统扫描-34段扫描资产	*提示:仅显示已检测过的资产组
检测任务时间段	2021-06-30 14:56:52 至 2021-06-30 15:07:11 [*	*提示:开始时间-至-结束时间[系统扫描、基线检测、数据库检测、WEB扫描]。
导出格式		el 🔿 XML
导出方式	详细报表	* 提示:请选择导出方式
报表标题	漏洞扫描安全评估报告	* 提示:请填写报表标题。限制:[4-30]字符之间,限制字符:\/:*?" < > ,(),`,{,}。
导出文件名	系统扫描-34段扫描资产	* 提示:请埴写导出的文件名称。限制:[1-42]字符之间,限制字符:\ / : * ? * < > , (), `, { }。
导出CNNVD信息	★ 提示:若开启此按钮,系统详细报表中	P的系统漏洞中会包含CNNVD字段,但是导出速度会很慢!
自定义HTML详细报表	★ 提示:关闭之后默认导出全部目录。	
自定义公司信息	×	
设置压缩包密码	×	
导出		

8.4 审计日志

审计日志以分页形式显示管理员对漏洞扫描系统所进行的操作管理记录,操作管理不仅包含 WEB 管理界面下的操作,还包括命令行管理界面下的操作,同时操作日志支持按条件的高级查询功能。

图8-5 审计日志

😐 î	□ 申 前 日志 御 協 得 当 取 前 空 日志 <i>●</i> 刷 新 3 00:00 ▼ 至 24:00 ▼ 全部 ▼ 用 户 名 / と 健 字 / IP / A 法 2 使 う の / 2 使 う の / 2 使 の の / 2 使 の の の の の の の の の の の の の の の の の の					
每页	每页显示 100 *					
	日期/时间 🔹	用户名	访问IP	访问来源	类型	操作信息
	2018-09-03 10:52:51	audit	192.168.8.65	Web	登录	登录成功!
	2018-09-03 10:52:19	1234	192.168.8.65	Web	其他	退出成功
	2018-09-03 10:51:48	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
	2018-09-03 10:51:34	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
	2018-09-03 10:51:28	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
	2018-09-03 10:18:57	1234	192.168.8.65	Web	新增	新增安全基线核查任务:基线核查-53成功
	2018-09-03 09:30:02	admin	192.168.8.146	Web	登录	登录成功!
	2018-09-03 09:29:41	1234	192.168.8.65	Web	登录	登录成功!
	2018-09-03 09:29:30	account	192.168.8.65	Web	其他	退出成功
	2018-09-03 09:28:30	account	192.168.8.65	Web	登录	登录成功!
	2018-08-31 18:44:58	admin	192.168.8.29	Web	登录	登录成功!
	2018-08-31 18:05:27	admin	192.168.8.65	Web	其他	用户登录超时
	2018-08-31 17:37:01	admin	192.168.8.65	Web	删除	删除任务;,WEB扫描-https://172.16.101.6/,系统扫描-WAF6.2.2,系统扫描-8,系统扫
	2018-08-31 17:36:47	admin	192.168.8.65	Web	其他	停止任务:系统扫描-8成功
	2018-08-31 17:36:23	admin	192.168.8.29	Web	其他	该用户在其他终端登录,请确认密码安全
	2018-08-31 17:35:38	admin	192.168.8.65	Web	删除	删除任务;系统扫描-192p成功

9 快速向导

可以在快速向导界面按照步骤依次对设备 IP、设备路由、DNS 地址进行配置。

图9-1 配置设备 IP 地址

快速向导			×
1 配置设备IP地址	2 配置路由地址	3 配置DNS地址	4 完成
VLAN	MngtVlan	Y	
IP地址	192.168.7.253	* 支持IPv4以及IPv6网络地址 IPv6示例: 2001:fecd:ba23:cd1f:d	cb1:1010:9234:4088
子网掩码	255.255.255.0	* 内容: 请填写子网掩码。例如: ipv 例如: ipv6:64	4:255.255.255.0

下次登录不再提示

下─步⊖

图9-2 配置路由地址

快速向导			×	
1 ✓ 配置设备IP	地址 2 配置路由地址	3 配置DNS地址 4 完成		
目的地址	0.0.0.0	*下一跳目的地址。默认任意地址则为: 0.0.0.0		
子网掩码	0.0.0.0	*下一跳地址子网掩码。默认任意地址则为: 0.0.0.0		
下一跳	192.168.7.1	*下一跳网关地址。例如地址: 192.168.1.1		
Metric	1	* 指路由算法用以确定到达目的地的最佳路径的计量标准 (范围是 1 ~ 9999) _ 野社: 1		
		(/DEALE 1 - 0000) . M/W/. 1		

下次登录不再提示						下一步 🕣
图9-3 配置 DNS	地址					
快速向导						×
1 ✓ 配置设备IPt	地址 2	✔ 配置路由地址	3	配置DNS地址	4 完成	
首选DNS服务器	8.8.8					
备选DNS服务器	114.114.114.114					

○ 下次登录不再提示

下一步 🕣

○ 下次登录不再提示

完成 🌖



表10-1 通讯设置

参数	说明
IP	默认所有接口的出厂地址为192.168.0.1
访问端口	443
网络掩码	255.255.255.0

表10-2 管理网口初始设置

参数	说明
波特率	9600
传输位数	8
奇偶校验	无
停止位	1
数据流控制	无