实验五:通过防火墙日志分析用户上网行为

一、实验简介

在前一个实验的基础上,通过在园区网中部署日志服务器并导入防火墙日志,使管理员可以通 过查看日志了解网络中各种业务的运行状态以及上网用户的行为。

二、实验目的

0

- 1、掌握 Syslog 日志服务器的创建;
- 2、掌握防火墙接入 Syslog 日志服务器的方法;
- 3、掌握使用 Tableau 进行日志分析的方法。

三、实验类型

综合型

- 四、实验理论
 - 1. 防火墙日志
 - 2. 日志服务器 syslog
 - 3. Tableau 软件
 - 4. 日志分析

五、实验内容及打分

本实验共包含4个任务,由学生独立完成。教师在实验课上检查实验完成情况并提出相应问题, 将根据各任务的完成情况及回答问题情况进行打分。

任务一: 部署日志服务器 Syslog (15分)

【任务说明】日志是防火墙在运行过程中输出的信息,通过查看日志,管理员可以实时了解网 络中各种业务的运行状态以及上网用户的行为。本任务以虚拟机方式创建一台 Syslog 日志服务器 并将其接入园区网中。

【提示】本任务具体操作,可参考教材项目九(任务三)或课程网站相关视频

具体步骤如下:

步骤1:创建日志服务器虚拟机

在 VirtualBox 中创建一台安装 CentOS 8 操作系统的虚拟机,并将其命名为 Syslog。网卡连接 方式保持默认设置"网络地址转换(NAT)"。具体操作过程参看前面实验。

步骤 2:关闭操作系统防火墙以及 SELinux

关闭操作系统防火墙,并禁止防火墙自动启动。

[root@localhost ~]#systemctl stop firewalld

[root@localhost ~]#systemctl disable firewalld

临时关闭 SELinux

[root@localhost ~]# setenforce 0

永久关闭 SELinux

[root@localhost ~]# vi /etc/sysconfig/selinux

将文件中的 SELINUX=enforing 修改为 SELINUX=disabled。

步骤 3: 配置 Syslog 日志服务器

CenOS 8 操作系统中已经默认安装了 Rsyslog,此处只需要进行配置即可。

(1) 启用 UDP 和 TCP 传输

修改/etc/rsyslog.conf 配置文件,取消以下四行的注释:

module(load="imudp") #

input(type="imudp" port="514")

module(load="imtcp") #

input(type="imtcp" port="514")

(2) 定义 Syslog 日志模板及日志存放位置

在/etc/rsyslog.d 目录中创建一个名为 mytemplate.conf 的文件,在文件中定义一个模板,用来 收集客户端(此处为防火墙)发送过来的日志。日志格式为:日志产生时间、主机名、日志标记、日志内容。在 mytemplate.conf 文件中还定义了日志文件存放的位置,此处将日志文件集中存放到 /var/log/rsyslog 目录中,日志以客户端设备为单位存储,每天创建一个日志文件。操作如下:

[root@localhost ~]# vi /etc/rsyslog.d/mytemplate.conf

//定义一个名为 myFormat 的模板

\$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

\$template myFormat,"%timestamp% %fromhost% %syslogtag% %msg%\n"

\$ActionFileDefaultTemplate myFormat

//将每个客户端(即防火墙)的日志文件存放在以各防火墙 IP 地址命名的目录中,这些目录存放在 /var/log/rsyslog 目录下,日志文件的命名格式是客户端 IP 地址_年-月-日.log。注意, rsyslog 目录 需要管理员手工创建

\$template

RemoteLogs,"/var/log/rsyslog/%fromhost-ip%/%fromhost-ip%_%\$YEAR%-%\$MONTH%
 -%\$DAY%.log"

//不记录本机日志

:fromhost-ip, !isequal, "127.0.0.1" ?RemoteLogs

(3) 重启服务使配置生效

重启 rsyslog 服务,使配置生效。

systemctl restart rsyslog.service

步骤 4: 部署日志服务器 Syslog

将配置好的日志服务器部署到 eNSP 中的园区网,如图-1 所示。配置 Syslog 服务器的 IP 地址,实现各防火墙和日志服务器之间网络可达;



图-1 将日志服务器 Syslog 接入 S-RS-3 的 GE0/0/8 接口

任务二:将防火墙日志引入日志服务器(10分)

【任务说明】通过配置,使防火墙将自己的日志发给日志服务器。

【提示】本任务的具体操作,可参考教材项目九(任务三)或课程网站相关视频

步骤 1: 配置防火墙 A-FW-1 使用日志服务器记录日志

(1) 在防火墙 A-FW-1 上添加日志服务器信息)

通过 Web 方式登录防火墙,在上方导航栏中选择"系统",点击左侧导航【日志配置】→【日 志配置】,在右侧窗口中【配置系统日志】,添加日志服务器地址"172.16.64.21",端口为"514"(与 日志服务器中的配置保持一致),发送接口设置为"LoopBack0"。【配置会话日志】,将日志格式设 置为"Syslog",并将其发送至日志服务器。【配置业务日志】,将日志格式设为"Syslog",如图-2 所示。



图-2 在防火墙中进行日志配置

(2) 在安全策略列表中启用日志

在上方导航栏中选择【策略】,点击左侧导航【安全策略】→【安全策略】,在右侧窗口中可 以看到【安全策略列表】,如图-3 所示。此处有一条名为 allow-all-visit-A 的策略,这是前期设置的 允许所有报文通过的安全策略。点击修改 allow-all-visit-A 策略,启用"记录流量日志"、"记录策 略命中日志"、"记录会话日志"。如图-4 所示。

安全策略列	刘表												
┣ 新建安全	全策略 🗣 新建安全分	策略组 🐹	删除 📑 1	夏制 💲移	动• 🎦 插	入 🛃 导出	• 🔍 清除	全部命中次数	■ 启用	■禁用	📕 列定制	1 展开	體收缩
🔍 请输)	入要查询的内容		③ 添	加查询项									
序号	名称	描述	标签	VLAN ID	源安全	目的安	源地址	目的地址	用户	服务	应用	时间段	动作
1	allow-all-visit-A			any	any	any	any	any	any	any	any	any	允许
2	default	This i		any	any	any	any	any	any	any	any	any	禁止

图-3 修改安全策略

记录流量日志	启用	~
记录策略命中日志	✔ 启用	
记录会话日志	✔ 启用	
会话老化时间		<1-65535>秒

图-4 启用日志记录

(3) 开启防火墙日志中心

//防火墙日志中心需要开启才能正常推送日志.

[A-FW-1]info-center enable

//关闭日志在控制台的回显有利于在控制台执行命令操作。

[A-FW-1]undo info-center console channel

步骤 2: 在其他防火墙上进行日志配置

参考 A-FW-1 完成防火墙 B-FW-1、O-FW-1、O-FW-2、S-FW-1、S-FW-2 的日志配置。

步骤 3: 在日志服务器上查看日志文件

(1) 查看日志文件的存放

根据前面的设置,我们把各个防火墙的日志以设备为单位放在了日志服务器 Syslog 的 /var/log/rsyslog 目录下。进入/var/log/rsyslog 目录,可以看到 6 个子目录,分别用 A-FW-1、B-FW-1 等六个防火墙的管理 IP 地址命名(每个设备的日志文件放在独立的目录中)。进入 10.0.255.100 目录,可以看到防火墙 A-FW-1 的日志文件,文件名分别为 10.0.255.100_2021-10-16.log 和 10.0.255.100_2021-10-17.log,表示分别存放 A-FW-1 在 2021 年 10 月 16 日和 17 日的日志记录,如图-5 所示。



图-5 在日志服务器上查看日志文件的存放

(2) 查看日志文件的内容

以 A-FW-1(10.0.255.10)的日志文件为例。在查看 A-FW-1的日志文件内容之前,我们先做 以下几步操作,以便于产生一些事件,从而被日志记录:

操作 1: 登录 A-FW-1 的认证界面,使用错误的用户名(test321)认证,认证失败;

操作 2: 再使用正确的用户名(test)认证,认证成功;

操作 3: 实体主机 A 访问 (ping) 服务器 Server-1 (172.16.65.10),成功访问。 接下来,查看防火墙 A-FW-1 的日志文件 10.0.255.100_2021-10-17.log,其命令为: [root@localhost ~]# vi /var/log/rsyslog/10.0.255.100/10.0.255.100_2021-10-17.log 日志文件中包含大量日志记录信息,例如以下三条日志。

//日志记录 1,本记录与用户 test123 登录失败有关

Oct 17 08:23:51 A-FW-1 %%01CM/5/USER_ACCESSRESULT(s)[294]: [USER_INFO_AU THENTICATION]DEVICEMAC:00-e0-fc-07-72-96;DEVICENAME:A-FW-1;USER:test123;MA C:ff-ff-ff-ff-ff;IPADDRESS:192.168.64.200;TIME:1634459031;ZONE:UTC+0800;DAYLI GHT:false;ERRCODE:133;RESULT:Authentication fail;AUTHENPLACE:Local;CIB ID:641;A CCESS TYPE:None;

关于日志记录1的说明见表-1。

日志内容	说明
Oct 17 08:23:51	日志产生时间,格林尼治时间
A-FW-1	指产生日志的设备
CM/5/USER_ACCESSRESULT	日志消息中的标记。含义:用户上线
USER_INFO_AUTHENTICATION	用户认证信息
DEVICEMAC:00-e0-fc-07-72-96	产生日志的设备的 MAC 地址,即 A-FW-1 的 MAC 地址
DEVICENAME:A-FW-1	产生日志的设备名称: A-FW-1
USER:test123	认证用户名。注意 test123 是错误的用户名
MAC:ff-ff-ff-ff-ff	认证用户 MAC 地址
IPADDRESS:192.168.64.200	认证用户的 IP 地址: 192.168.64.200 (即实体主机 A)
TIME:1634459031	上线时间
ZONE:UTC+0800	时区,东八区,在原时间上+8小时
DAYLIGHT:false	是否夏令时(否)
ERRCODE:133	错误码是 133
RESULT:Authentication fail	结果:认证失败
AUTHENPLACE:Local	认证位置:本地(A-FW-1采用本地认证)
CIB ID:641	CIB 编号: 641
ACCESS TYPE:None	接入类型:如果用户上线不成功,则接入类型记录为 None

表-1 日志记录1的说明

其他日志记录分析由学生自行完成。

任务三:通过日志文件分析用户上网行为(15分)

【任务说明】在本地实体主机上安装 Tableau 数据分析软件,并使用 Tableau 分析从日志服务器中导出的防火墙日志文件,从而实现对用户上网行为的分析。

步骤1:明确分析内容

本任务的主要目的是掌握使用 Tableau 分析防火墙日志的基本方法,为了突出重点,此处只分 析用户主机 192.168.64.200 在 2021 年 10 月 24 日中访问数据中心各个服务器的频次,从而发现 该用户主机访问哪个服务器最多,哪个最少。

步骤 2:在本地主机安装 Tableau

本任务采用 Tableau Desktop 的免费个人版软件,软件获取地址为 https://www.tableau.com, 下载时需要输入邮箱地址。

双击安装程序进入 Tableau 安装欢迎页面,选择"我已阅读并接受本许可协议的条款"选项, 然后点击【安装】按钮开始进行软件安装。安装运行结束,进入"激活 Tableau"界面,选择"立 即开始试用",然后填写姓名、电话、组织等详细信息进行注册。注册完成后,最终出现软件起始 工作界面,如图-6 所示。



图-6 Tableau 软件起始界面

步骤 3: 配置防火墙 A-FW-1 的日志

在使用 Tableau 进行数据分析时,首先需要根据分析目标对采集到的数据进行清洗。为了突出 重点并减少清洗数据的成本,此处首先对防火墙 A-FW-1 的日志进行配置:一是在日志文件中只保 存会话日志;二是会话日志格式模板中只显示设备名称、源 IP、目的 IP、发送报文数量、接收报 文数量、协议字段的内容。具体操作如下:

(1) 只启用会话日志

以 Web 方式登录防火墙 A-FW-1。在上方导航栏中选择【策略】, 然后点击左侧导航【安全策 略】→【安全策略】, 在右侧窗口中点击 allow-all-visit-A 策略(见图-7), 然后只启用"记录会话日 志", 如图-8 所示。

Huawei Huawei USG6000V1-EN	ISP 間面	「「「」」	● 策略 对象	上 网络
 安全策略 安全策略 	※ 安全策略	列表		
→ → → → → → → → → → → → → → → → → → →	🕂 新建安	全策略 🔶 新建安全策	略组 💥 删除 🖻 复制	💲 移动 🖷 插入
🖪 😰 服务器负载均衡	🔍 请输	入要查询的内容	③添加3	查询项
🗄 🦃 带宽管理	序号	名称	描述	标签
🚹 🔩 配额控制策略				10.00
1 代理策略		allow-all-visit-A		
🗄 🍈 安全防护	2	default	This is the d	e

图-7 修改防火墙安全策略

记录流量日志	NONE	~
记录策略命中日志	启用	
记录会话日志	☑ 启用	
会话老化时间		<1-65535>秒
自定义长连接(?)	启用	
	168	*<0-24000>小时

图-8 只启用会话日志

(2) 修改"日志配置"并自定义会话日志的格式

为了简化日志内容,此处只将防火墙 A-FW-1 的"会话日志"发送到日志服务器 Syslog。在 上方导航栏中选择【系统】,然后点击左侧导航【日志配置】→【日志配置】,在右侧窗口中将【配 置系统日志】恢复缺省,如图-8 所示。

HUAWEI USG6000V1-ENSP	■■ 面板	いた	し 策略	■] ■ 对象	小 网络			
 配置 編 配置 編 用户体验计划 	日志配置 S	iyslog日志模板	自定义日志	字段 Ne	tflow日志核	版		
🖪 🕵 管理员	日志配置							
■ 虚拟系统	配置系统日志					-		
 ■ ■ 町数備中心集件 ■ ● 高可靠性 ■ ● 日志配置 	日志主机IP地 发送接口	3址	NONE	~	端口	514	<1-65535>	语
○ 日志配置	配置会话日志 日志格式		○ 二进制	 Syslog 	🔵 Net	flow		
▶ License管理	会话日志	内容格式	○ 缺省		• 自定	三义		
📑 升级中心			请选择Syslo	g日志模板	× *	[配置]		
🚅 系统更新	同时发送							•
📸 配置文件管理	日志发送源IF	² 地址	10.0.255.101		源端口	1617	<1024-65535>	
☑ VPN客户端升级	日志主机IP地	3址	172.16.64.21		端口	514	<1-65535>	٢
💽 快速向导	心跳检测		启用					
💽 链接配置			《》建议开启心	跳检测功能	,增强日志	发送的可靠性。		

图-8 修改"日志配置",只发送会话日志到日志服务器

修改【配置会话日志】内容,将"会话日志内容格式"设置为【自定义】,然后新建 Syslog 日志模板,如图-9 所示。

日志格式	◯ 二进制 ● Syslog ◯ Netflow
会话日志内容格式	○ 缺省 ○ MTN ● 自定义
	请选择Syslog日志模板 ▼* [配置]
同时发送	新建Syslog日志模板
日志发送源IP地址	

图-9 新建会话日志的格式模板

将新建模板命名为"Mytemplate",【配置模式】选择"表达式",在左侧的字段列表中点击选择\$hostname、\$srcip、\$dstip、\$sendpackets、\$rcvpackets、\$protocol,则在右侧的"日志格式"框中显示所选中的字段名及顺序,如图-9所示。

新建Syslog日志	模板							
名称	Mytemplate		*					
配置模式	• 表达式	○ 列表						
IPv4会话日志	🔶 关联自定义	日志字段		日志格式				
	字段	名称	操作	<pre>\$hostname \$srcip \$dstip \$sendpackets \$rcvpackets \$protocol</pre>				
	\$ipversion	ip-version	4					
	\$protocol	protocol						
	\$srcip source-ip							
	\$srcport	source-port						
	\$dstip	destination-ip		配置举例:				
	\$dstport	destination-port		<pre>\$protocol \$srcip:\$srcport -> \$dstip:\$dstport BeginTime :\$begintime EndTime: \$endtime SendPkts=\$sendpackets. SendBytes=\$sendbytes.</pre>				
	\$srcnatip	source-nat-ip		RcvPkts=\$rcvpackets, RcvBytes=\$rcvbytes				
	\$srcnatport	source-nat-port		日志效果:				
	\$dstnatip	destination-nat-ip		udp 2.2.2.2:10043 -> 2.2.2.1:20000 BeginTime :2017-10-19T13:21:03+08:00 EndTime: 2017-10-19T13:21:45+08:00_SendPkts=1_SendBytes=114				
	\$dstnatport	destination-nat		RcvPkts=1, RcvBytes=56				

图-9 定义新日志模板的字段内容及显示顺序

步骤 4: 将防火墙 A-FW-1 的日志文件下载到本地主机

(1) 在本地主机上安装 FileZilla 客户端软件

此处通过 FileZilla 客户端软件,以 FTP 的方式从日志服务器下载防火墙日志到本地计算机。 关于 FileZilla 客户端软件的下载和安装,读者可自行查询相关资料,此处略。

(2) 将防火墙 A-FW-1 的日志文件下载到本地主机

启动 FileZilla 客户端软件,将指定的日志文件下载到本地主机指定的文件夹内。 具体操作略。

步骤 5: 使用 Tableau 软件分析防火墙日志

(1) 打开 Tableau 软件并连接日志文件

启动 Tableau 软件,在左侧的【连接】列表中,点击【到文件】→【文本文件】,如图-10 所 示,从本地实体主机中选择防火墙 A-FW-1 的 2021 年 10 月 24 日的日志文件 "10.0.255.100_2021-10-24.log",可以看到日志文件的内容被导入 Tableau,并且自动按照字段 进行划分,默认字段名为 F1、F2、F3……,如图-11 所示。

	🖄 Tableau - 工作簿	1 - Tableau 🏻	行可证将在	7 天后过期	A					-	
*	文件(F) 数据(D) 服务	务器(S) 窗口(N) 帮助(H)							
连接 _{到文件}	 ← → 连接 10.0.255021- 文本文件 	副 ○ 添加 10-24	B- 1 10.0.:	0.0.2 255.100_	2021-10-24.log	1-10-24	4 连接 ● 实时	○ 数据提取			筛选器 0 添
MICrosoft Excel			and an effe	the star CO	11 fates (and the same						25
文本文件			Abo Filt	÷	\$X#5###################################	Abs	Abo	Abc	#	#	Abo
JSON 文件			10.0.255 F1	10.0.25 F2	10.0.255.100_2021-10-24.log F3	10.0.255.100 F4	10.0.255.100_2021-10-2 F5	10.0.255.100 F6	10.0.2 F7	10.0.2 F8	10.0.255 F9
Microsoft Access			Oct	24	1899/12/30 18:13:02	A-FW-1	192.168.64.200	10.0.1.1	6	4	tcp
WICLOSOFT ACCESS			Oct	24	1899/12/30 18:13:02	A-FW-1	192.168.64.200	10.0.1.1	6	4	tcp
PDF 文件			Oct	24	1899/12/30 18:13:03	A-FW-1	192.168.64.200	10.0.1.1	6	4	tcp
应运 立他			Oct	24	1899/12/30 18:13:03	A-FW-1	192.168.64.200	10.0.1.1	7	5	tcp
全间又件			Oct	24	1899/12/30 18:13:03	A-FW-1	192.168.64.200	10.0.1.1	6	4	tcp
统计文件			Oct	24	1899/12/30 18:13:03	A-FW-1	192.168.64.200	10.0.1.1	14	16	tcp
			Oct	24	1899/12/30 18:13:04	A-FW-1	192.168.64.200	10.0.1.1	7	5	tcp
更多	□ 数据源	工作表1	G, G, G,								

图-10 点击"文本文件"

图-11 日志文件被导入 Tableau

可以手工更改每个字段的名字,如图-12所示。

	0· 1	0.0.	255.100_20	21-10	-24 连接 ⊙ 实时	○ 数据提	取		筛选器 0 添力
接 添加									
10.0.255021-10-24 _{文本文件}	10.0	.255.10	0_2021-10-24.log						
	■ ■ 排	序字段	数据源顺序	•	[显示别名	显示隐藏	字段 225	; •
	Abc	#	e.	Abc	Abc	Abc	#	#	Abc
	10.0.25	10.0.2	10.0.255.100_2021-10-24	10.0.255.10	10.0.255.100_2021-1	10.0.255.100_20	10.0.255.1	10.0.255	10.0.255
	月份	日期	时间	设备名	源IP	目的IP	发包数	收包数	协议
	Oct	24	1899/12/30 18:23:38	A-FW-1	192.168.64.200	172.16.64.20	4	4	icmp
	Oct	24	1899/12/30 18:23:50	A-FW-1	192.168.64.200	172.16.65.10	4	4	icmp
	Oct	24	1899/12/30 18:24:50	A-FW-1	192.168.64.200	172.16.65.11	8	4	icmp
	Oct	24	1899/12/30 18:25:01	A-FW-1	192.168.64.200	172.16.65.11	16	16	tcp
					102 100 01 200	170 10 05 11	15	4.5	4

ムヘ

图-12 更改每个日志字段的名字

(2) 建立分析图表

点击左下方的【工作表 1】,将左侧【维度】列表中的"源 IP"字段拖至【筛选器】,并在【筛 选器】中只选择 192.168.64.200(该地址是接入到用户区域的本地实体主机虚拟网卡的 IP 地址), 如图-13 所示。然后将"目的 IP"字段分别拖至右侧的【列】和【行】中,并在【行】中将"目的 IP"的【度量】设置为"计数",如图-14 所示。

数据 分析	• 页面			2022A YEARD A VILL AVEL
₿ 10.0.255.100_202				● 从列表中选择(S) ○ 自定义值列表(C) ○ 使用全部(U) ■
维度 Ⅲ ₽	筛选器			输入搜索文本 10.0.1.2
□ 时间 ▲ 月份	源IP: 19	2.168.64.20	00	10.0.200.13 10.0.255.1
Abs 源IP	标记			☑ 192.168.64.200
4 设备名	□ 自动		*	
Abs 度量名称	●● 颜色	の 大小	I文本	
	。。。 详细信息	□ □ □ □ □ □		
度量	… (周t	生(源IP)		全部(L) 无(O) □ 排除(X)
# 火包数 # 收包数				摘要
# 日期				字段: [源IP]
*# 记录数				所述內容: 选择了1个值(共5个) 通配符(W):全部
# 度量值				条件(D): 无
				限制(M): 无

图-13 筛选"源 IP"字段,只选择 192.168.64.200

此时,用户主机 192.168.64.200 访问各服务器的频次以柱状图的形式展示出来,如图-15 所示

数据	分析。	页面			iii 列	(E	的IP	
€ 10.0.25	₿ 10.0.255.100_202			≡ 行	-	目的IP			
维度 Abc 协议 岛 时间	• Q III	^{筛选器} 源IP: 192.168.64.200 _{目的IP} 10.0					筛选器… 显示筛选器 显示突出显示工具	目的IP 5.64.14 172.16.64	
Abc 沪ID Abc 源IP Abc 目的IP Abc 设备名		标记 回 自动		•	10.0.1.1 172.16 172.16 172.16 172.16 172.16		 ▼ 排序 设置格式 ✓ 显示标题 ✓ 日本市工具は二十 	Abc	
Abc 度量名	称	●● 颜色	の 大小	工 本文	172.16 172.16		~	包含在工具提示中编辑别名	_
		。 。 详细信息	□□				•	维度 属性	
度量		(Æ	性(源IP)					度量	最小值
 # 发包数 # 收包数 # 日期 								在功能区中编辑 移除	最大值 计数 计数 计数(不同)
# 记录数									

图-14 拖动"目的 IP"字段并进行设置

(此处将柱状图的标题更改为"用户主机 192.168.64.200 访问分析")。可以看到,访问 10.0.1.1

(A-FW-1 的认证界面)的通信是最多的,访问 12.16.65.10 的通信是最少的。



任务四: 自行设计并分析用户上网行为 (30分)

【任务说明】自行设计用户操作行为,结合所采集到的防火墙日志,对用户上网行为进行分析。 并将设计内容和分析结果汇报给老师。

要求:

- 1. 所分析的内容不能和教材中的案例相同;
- 2. 说明自己所设计的防火墙日志分析模型、分析内容的设计;
- 3. 说明数据清洗的内容;
- 4. 展示并讲解 Tableau 的图形化分析结果;

六、实验考核

实验考核从【完成维度】和【时间维度】两个维度进行评分。

1、【完成维度】考核

本维度主要考核学生完成实验的程度以及对实验内容的理解程度,包括【任务完成度】和【回答问题】两个部分。具体如下:

(1) 任务完成度(70分)

学生在完成实验后,要当面提交教师检查实验结果。教师检查每个实验任务的完成情况,并根据实验指导书中每个任务的分值,给出任务完成度的分数。本项目满分 70 分。

(2) 回答问题(30分)

学生在完成实验后,要当面提交教师检查实验结果,并回答教师提问。教师根据学生回答情况 评分。本项目满分 30 分。

【注意】: 教师提问时,可参考"七、思考与讨论"中的问题,从中随机选取 2-3 个问题进行 提问。

2、【时间维度】考核

本维度主要考核学生完成实验的时间,具体如下:

(1) 当堂提交(100分起评)

本实验的实验课当堂提交并通过【完成维度】考核的,从100分起评。

(2) 一周内提交 (90 分起评)

本实验的实验课结束一周内提交并通过【完成维度】考核的,从 90 分起评,即本次实验考核 最高 90 分。

(3) 一周后提交(80分起评)

本实验的实验课结束一周后提交并通过【完成维度】考核的,从 80 分起评,即本次实验考核 最高 80 分。

(4) 未提交(0分)

本学期教学工作结束时,仍未提交的,本次实验考核0分

七、思考与讨论

学生在做实验时,要结合实验内容和过程,讨论分析以下问题,以备教师提问

- 1. 结合本实验谈谈防火墙日志分为哪些类型?本实验中,你进行分析的是哪种类型的日志?
- 结合本实验的实际操作,总结一下:要想通过防火墙日志分析园区网内用户的某种上网行为,而且 以图形化方式显示分析结果,需要做哪些操作?【要求】:举例说明,从防火墙部署开始说,直到 图形化方式显示分析结果。不用说具体命令,只说清楚相关操作即可。
- 在任务一步骤4中,要求将日志服务器部署进园区网,并实现日志服务器与各防火墙之间的路由可 达。结合自己的实际操作,总结一下为了实现上述要求,你具体进行了哪些配置?
- 结合自己的实际操作,在任务二步骤3,在日志服务器中,查看某个设备的日志记录,并分析其中 一条记录的内容。注意,分析的记录内容不要和教材上一样。
- 5. 结合自己的实际操作,总结归纳并举例说明如何将防火墙的日志信息发送给日志服务器?
- 试通过抓包分析的方式,分析一下防火墙和日志服务器之间的通信。举例说明,将你设计的抓包点、 抓包结果以及你的分析内容汇报给老师。
- 7. 结合自己的实际操作,总结归纳并举例说明如何将防火墙的日志信息发送给日志服务器?
- 8. 将你实验中,任务三的结果(图形化方式)展示给老师,并对结果进行说明。
- 9. 给老师汇报一下任务四的设计和完成情况。