实验六: DNS 协议分析

一、实验目的

- 2、熟悉 DNS 报文结构;
- 3、掌握 DNS 通信过程。
- 二、实验学时

2 学时

三、实验类型

验证性

四、实验需求

1、硬件

每人配备计算机1台,不低于双核CPU、8G内存、500GB硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统,安装 GNS 3 仿真软件,安装 Wireshark 抓包工具。 支持 Windows 操作系统,安装 GNS 3 仿真软件,安装 Wireshark 抓包工具。

3、网络

计算机使用固定 IP 地址接入局域网,并支持对互联网的访问。

4、工具

无。

五、实验任务

- 1、完成 DNS 报文结构分析;
- 2、完成 DNS 记录类型的报文分析;
- 3、完成 DNS 查询分析。

六、实验内容及步骤

任务1:实验准备

步骤 01:实验拓扑设计 实验拓扑结构,如图 6-1 所示。 步骤 02:实验网络设计



^{1、}了解 DNS;

①拓扑说明

Host, DNS	DNS				
SW-1	二层交换机	Ethernet switch			

후 ~ 가 가 바 만 한 한 한

②交换机接口规划

表 6-2 交换机规划

交换机	接口	VLANID	连接设备	接口类型
SW-1	e0	1	NAT	默认
SW-1	e1	1	Host	默认
SW-1	e2	1	DNS	默认

③主机地址规划

表 6-3 主机地址规划

主机	IP 地址/子网掩码	网关	DNS	接入位置
Host	192.168.122.10 /24	192.168.122.1	192.168.122.200	e1
DNS	192.168.122.200/24	192.168.122.1	8.8.8.8	e2

步骤 03:实验准备的补充说明

本实验使用 DNS 终端设备需要 Docker 仿真器支持。

(1) 安装 Docker

在 Ubuntu Desktop 上,通过终端在线安装 Docker,操作命令如下:

参考命令:

#移除老版本 sudo apt remove docker docker-engine docker.io #安装以下软件包 sudo apt-get install apt-transport-https ca-certificates curl software-properties-common #引入官方 Docker GPG 钥匙 curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -/#增加相关源 sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu \$(lsb release -cs) stable" #安装 Docker-CE,当提示需要占用磁盘空间,是否继续时,输入Y继续 sudo apt update sudo apt install docker-ce #将当前用户 net 添加到以 libvirt、kvm、wireshark、docker 组 sudo usermod -aG libvirt net sudo usermod -aG kvm net sudo usermod -aG wireshark net sudo usermod -aG docker net

安装完成后重启系统,使用户权限生效。

注:实验教学提供的实验学习平台 VM 已安装 Docker 和 DNS,本步骤可不重复操作。

(2) 添加 DNS 终端模板

①在左侧终端设备列表下方点击【+New template】打开模板创建窗口,如图 6-2 所示。 ②点击【Next>】,选择要安装的应用,展开"Guest"或在筛选框中输入"dns"进行筛 选,并选择要安装的应用(DNS),如图 6-3 所示。



图 6-2 创建新模板

图 6-3 选择应用

③点击【Install】,选择服务器类型,如图 6-4 所示。 ④点击【Next>】,显示使用说明,如图 6-5 所示。

Install DNS appliance 😣	Install DNS appliance 😣
Server Please choose a server type to install the appliance. The grayed out server types are not supported or configured.	Usage Please read the following instructions in order to use your new appliance.
Server type Install the appliance on a remote server Install the appliance on the GNS3 VM (recommended) Install the appliance on your local computer 	The template will be available in the guest category. You can add records by adding entries to the /etc/hosts file in the following format: %IP_ADDRESS% %HOSTNAME%.lab %HOSTNAME% Example: 192.168.123.10 router1.lab router1
Appliance info Next > Cancel	<u>Appliance info</u> <u>Back</u> <u>Finish</u> Cancel

图 6-4 选择服务器类型



⑤点击【Finish】完成添加,设备工具栏中显示 DNS 设备模板,如图 6-6 所示。

步骤 04: 在 GNS3 中实现网络

(1)在 GNS3 中, 按实验拓扑设计和实验网络设计实现网络, 如图 6-7 所示。

(2) 配置 Host 网络地址()。



		Node properties	ę
ŀ	Host configuration		
	General settings Advanced	Usage	
	Name:	Host	
	Start command:		
	Adapters:	1	▲
	Custom adapters:		
	Console type:	telnet	 Auto start console
:	VNC console resolution:	1024x768	*
	HTTP port in the container:	80	÷
	HTTP path:	/	
	Environment variables: (KEY=VALUE, one per line)		
	Network configuration		Edit
			Apply 😵 Cancel 💽 OK

①右键 Host,点击【Configure】按钮,打开节点属性配置窗口,如图 6-8 所示。

图 6-8 打开节点属性配置窗口

②在"General settings"选项卡中"Network configuration"配置项后点击【Edit】按钮 打开主机接口配置弹出框。依表 6-3 进行网络地址配置,如图 6-9 所示。

Host interfaces	8
# # This is a sample network config uncomment lines to configure the n #	etwork
# Static config for eth0 #auto eth0 #lface eth0 inet static # address 192.168.0.2 # netmask 255.255.0 # gateway 192.168.0.1 # up echo nameserver 192.168.0.1 > /etc/resolv.conf	
# DHCP config for eth0 # auto eth0 # iface eth0 inet dhcp	
auto eth0 iface etho inet static address 192.168.122.10 netmask 255.255.255.0 gateway 192.168.122.1 up echo nameserver 192.168.122.200> /etc/resolv.conf	
	Refresh 🛛 🗙 Cancel 🔛 Save

图 6-9 配置网络地址

③依次点击【Save】、【OK】完成配置。

(3)参照(2)操作,按表 6-3 配置 DNS 主机的网络地址。

(4) 网络连通性测试。

启动网络,在Host、DNS终端分别执行"Ping 8.8.8.8",测试网络通信情况。

表 6-4 网络通信测试用例

源主机	通信结果
Host	
DNS	

任务 2: DNS 报文结构分析

步骤 01:设置抓包点,启动 Wireshark 进行抓包

如图 6-10 所示, 在交换机 SW-1 连接 Host 的 e1 接口启动抓包, 并在 Wireshark 的过滤 器中输入 "dns" 筛选报文。



图 6-10 抓包位置设置

步骤 02: 执行 DNS 查询命令

在 Host 主机控制台执行 nslookup 命令, 查询域名记录 "internet.hactcm.edu.cn", 操作 如下:

参考命令:

nslookup internet.hactcm.edu.cn /tmp/gns3/bin/nslookup internet.hactcm.edu.cn

提醒:

- nslookup 默认使用本机设置的 DNS,进行 A 记录类型查询
- nslookup 查询时指定记录类型、DNS的方式为:nslookup -type=类型 域名记录 DNS,如:nslookup -type=A hactcm.edu.cn 192.168.122.200

步骤 03: DNS 报文分析

对采集的数据报文进行分析,并完成表 6-5、表 6-6 的填写。

表 6-5 一次 DNS 解析请求过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				
5				
6				

表 6-6 域名记录 internet.hactcm.edu.cn 的 A 记录的 DNS 解析内容

序号	字段名	字段值	字段解释和说明
1	Name		
2	Туре		
3	Class		
4	Time to live		
5	Data length		

任务 3: 通信过程中常见请求类型的 DNS 报文分析

在任务2的基础上开展本任务实验。

(1) NS 记录

①获取 NS 记录请求应答报文。

在主机 Host 上输入 "nslookup - qt=ns 51xueweb.cn 8.8.8.8", 使用服务器 "8.8.8.8" 获 取 NS 记录记录结果。

在主机 Host 上输入 "/tmp/gns3/bin/nslookup - type=ns 51xueweb.cn 8.8.8.8", 使用服 务器 "8.8.8.8" 获取 NS 记录记录结果。

②分析 NA 记录请求应答报文。

在 Wireshark 中查看获取的 NS 记录解析数据报文,对 NS 记录请求应答数据报文进行 分析,并根据数据报文内容填写表 6-7 和表 6-8。

序号	字段名称	字段长度	起始	位置	字段值	字段表示的信息
1	Transaction ID		第	位		
2	Flags		第	位		
3	Questions		第	位		
4	Answer RRs		第	位		
5	Authority RRs		第	位		
6	Additional RRs		第	位		
7	Queries		第	位		
		加	〔取数据	包的详	细内容:	
8						

表 6-7 NS 记录请求报文分析

表 6-8 NS 记录应答报文分	杤
------------------	---

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第位		

2	Flags		第	位			
3	Questions		第	位			
4	Answer RRs		第	位			
5	Authority RRs		第	位			
6	Additional RRs		第	位			
7	Queries		第	位			
8	Authoritative nameservers		第	位			
9	抓取数据包的详细内容:						

(2) CNAME 记录

①获取 CNAME 记录请求应答报文。

在主机 Host 上输入"<u>nslookup-qt=cname www.baidu.com 8.8.8.8</u>",使用服务器"8.8.8.8" 获取 CNAME 记录记录结果。

在主机 Host 上输入"/tmp/gns3/bin/nslookup - type=cname www.baidu.com 8.8.8.8",使用服务器"8.8.8.8"获取 CNAME 记录记录结果。

②分析 CNAME 记录请求应答报文。

在 Wireshark 中查看获取的 CNAME 记录解析数据报文,对 CNAME 记录请求应答数据 报文进行分析,并根据数据报文内容填写表 6-9 和表 6-10。

序号	字段名称	字段长度	起始位置		字段值	字段表示的信息	
1	Transaction ID		第	位			
2	Flags		第	位			
3	Questions		第	位			
4	Answer RRs		第	位			
5	Authority RRs		第	位			
6	Additional RRs		第	位			
7	Queries		第	位			
	抓取数据包的详细内容:						
8							

表 6-9 CNAME 记录请求报文分析

表 6-10 CNAME 记录应答报文分析

序号	字段名称	字段长度	起始位置		字段值	字段表示的信息	
1	Transaction ID		第	位			
2	Flags		第	位			
3	Questions		第	位			
4	Answer RRs		第	位			
5	Authority RRs		第	位			
6	Additional RRs		第	位			
7	Queries		第	位			
8	Answers		第	位			
9	抓取数据包的详细内容:						

任务 4: 本地域名服务器的查询过程分析

步骤 01:设置抓包点,启动 Wireshark 进行抓包

如图 6-11 所示,交换机 SW-1 连接 DNS 的 e2 接口启动抓包,并在 Wireshark 的过滤器 中输入"dns"筛选报文。



步骤 02:执行 DNS 查询命令

在 Host 控制台执行 nslookup 命令,执行域名记录"internet.hactcm.edu.cn"查询请求,操作如下:(可以任意选择其他的域名进行实验)

参考命令:

nslookup -type=A internet.hactcm.edu.cn /tmp/gns3/bin/nslookup -type=A internet.hactcm.edu.cn

步骤 03: 抓取 DNS 查询过程报文

在 Wireshark 窗体中查看 DNS 查询通信过程报文。

步骤 04:分析 DNS 查询过程,并填写表 6-11。

表 6-11 本地域名服务器的查询过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				

七、实验考核

实验考核分为【实验随堂查】和【实验线上考】两个部分。

实验随堂查:每个实验设置 3-5 考核点。完成实验任务后,任课教师随机选择一个考核 点,学生现场进行演示和汇报讲解。

实验线上考:每个实验设置 5-10 个客观题。通过线上考核平台(课堂派)进行作答。

1、实验随堂查

本实验随堂查设置4个考核点,具体如下。

考核点1:完成实验网络部署。

考核点 2: 完成抓包分析 DNS 报文结构。

考核点 3: 完成抓包分析 DNS 记录类型。

考核点 4: 完成抓包分析 DNS 查询过程。

2、实验线上考

本实验线上考共10题,其中单选3题、多选2题、判断3题、填空2题。