# 实验八:DNS 协议分析

## 一、实验目的

- 1、理解 DNS 的基本原理;
- 2、理解 DNS 报文格式和各字段含义;
- 3、理解 DNS 解析的通信过程。

#### 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

支持 Windows 操作系统,安装 eNSP 仿真软件,安装 Wireshark 网络嗅探软件。

#### 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 报文的采集;
- 2、完成 DNS 报文结构的分析;
- 3、完成 DNS 通信过程分析。

## 六、实验内容及步骤

## 1、DNS 数据报文分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件 "dns and ip.addr==8.8.8.8", 选择【Start】, 开始进行报文采集, 如图 8-1 所示。

②打开 Windows 的命令窗体,输入"<u>nslookup -qt=A internet.hactcm.edu.cn 8.8.8.8</u>", 使用服务器 "8.8.8.8" 对域名记录 "internet.hactcm.edu.cn" 解析,如图 8-2 所示。

		1 🕂 📜 🖬 Q Q Q 🗹		(1)
No. Time	Source	Destination Protocol	Length Info	*
¢	_	,		
< 🔴 🍸 wireshark_WL/	ANLBX4V1. pcapng	>	分組: 7050 · 己基汞: 0 (0.0%)	配置: Default
< 🔴 🍸 wireshark_WLi	ANLBX4V1. pcapng	3	分组: 7050 • 已显示: 0 (0.0%)	配置: Default
< 🖉 vireshark_WJ	NNLBX4V1. pcapng	, 图 8-1 使用 Wireshark	<sup>∥ 分攤: 7090 · ⋶星茶: 0 (0,00)</sup> ★ 工具进行 DNS 报文采集	配置: Default
< 🔮 🍸 wireshark_WL	NNLBX4V1. pcapng	图 8-1 使用 Wireshark	<sup>∥ 分組: 7080・己星票: 0 (0.00)</sup> 《工具进行 DNS 报文采集	配置: Default
< 🖉 vireshark_WLJ	ANLEX4V1. pcapng	到 8-1 使用 Wireshark	<sup>Ⅱ 948: 7030 + 288; 9 0.000</sup> x 工具进行 DNS 报文采集	配置: Default
< 🔮 🕈 vireshark_WJ	ANLEX 491, peaping	函 8-1 使用 Wireshark	<sup>∥ 948: 7090 + ⋶基¥: 0 0.00)</sup> 《工具进行 DNS 报文采集	配置: Default
vireshark_W	NULBX4V1. peaping	图 8-1 使用 Wireshark	<sup>∥ 9ૠ: 7000 + ⋶里∓: 0 (0,00)</sup> ∢工具进行 DNS 报文采集	R.M. Default
vireshark, WL	NLEWWI.peapog	图 8-1 使用 Wireshark	<sub>【 分租: 7020 + 2里票: 0 (0.00)</sub> ∢工具进行 DNS 报文采集	ER: Default
° ♥ vireshark, %J	NULEXWI: peaging (S) system 32\co ndows [版2	图 <b>8-1</b> 使用 Wireshark md.exe 本 10. 0. 19045, 2251]	<sup>『948:7030・288;®</sup> 0.000 ▲工具进行 DNS 报文采集	配置 befault
♥ viresharit, %L ♥ viresharit, %L Style="text-align: center;">(WINDOW 0 soft Win 0 soft Win	NNERWY: poppe (S) system 32\c ndows [版之 t. Corporat	图 8-1 使用 Wireshark md.exe 本 10. 0. 19045. 2251] tion。保留所有权利。	<sub>▌9祖</sub> : 7000 · ⋶里╤: 0 0.000 《工具进行 DNS 报文采集	EX: Default
✓ vireshark, WL ∴WINDOW osoft Win Microsoft	NULIWIL proper 图 S\system32\c ndows [版え t Corporat	图 <b>8-1</b> 使用 Wireshark cmd.exe 本 10. 0. 19045. 2251] tion。保留所有权利。	<sub>『<sup>948: 7090 + ⋶里∓: 0 (0,00)</sup></sub> « 工具进行 DNS 报文采集	EW: Default
vireshark,%2 (WINDOW) osoft Win Microsof	NLIWIL popur 图 S\system32\c ndows [版元 t Corporat	图 8-1 使用 Wireshark md.exe 本 10. 0. 19045. 2251] tion。保留所有权利。	『##: 700 · E里票: 0 0.000 《工具进行 DNS 报文采集	EW: befault
€ ک vireshark ۳۵ WINDOW: wicrosoft Win Sers\ruan	NLINFL.pegge 图 S\system32\c ndows [版石 t Corporat nx〉nslookt	图 <b>8-1</b> 使用 Wireshark md.exe 本 10.0.19045.2251] tion。保留所有权利。 up -qt=A internet.h	『タ#l: 7020 · E型系: 0 0.000 < 工具进行 DNS 报文采集 nactcm. edu. cn 8.8.8.8	REM: Default
。 ● <sup>7</sup> viredark Wi (WINDOW osoft Wi Microsof Sers\rua 器: dns	NLIKWL.pegne 客 (S\system32\c ndows [版 t Corporat nx〉nslooku .google	图 8-1 使用 Wireshark md.exe 本 10.0.19045.2251] tion。保留所有权利。 up -qt=A internet.h	『##: 700 · E里采: 0 0.00) 《 工具进行 DNS 报文采集 nactcm. edu. cn 8.8.8.8	R.H. Default
● ♥ vireshark, %L :\WINDOW osoft Win Microsof sers\rua 器: dns. ess: 8.8	NILIWIL pegne [5] S\system32\c ndows [版之 t Corporat nx〉nslooku . google 8. 8. 8	점 8-1 使用 Wireshark cmd.exe 本 10. 0. 19045. 2251] tion。 保留所有权利。 up -qt=A internet. h	『##: 7000 · E型来: 0 (0.00) 《工具进行 DNS 报文采集 nactom. edu. on 8.8.8.8	REM: Default
● 2 virenhark W :\WINDOW osoft Win Microsof 器: dns. ess: 8.8	NLINWL.pegwg S\system32\c ndows [版元 t Corporat nx>nslooku . google 8. 8. 8	图 <b>8-1</b> 使用 Wireshark cmd.exe 本 10.0.19045.2251] tion。保留所有权利。 up -qt=A internet.h	『タ#l: 7000 · E型架: 0 0.000 ▲ 工具进行 DNS 报文采集 wactom. edu. on 8.8.8.8	REW. Default
。	NLINUL.pegng [S\system32\c ndows [版石 t Corporat nx>nslooku .google 8.8.8	图 8-1 使用 Wireshark md.exe 本 10. 0. 19045. 2251] tion。保留所有权利。 up -qt=A internet.h	『タ#i 1000 · 2⊞F: 0 0.000 《工具进行 DNS 报文采集 nactcm. edu. cn 8. 8. 8. 8	REW: Default
★ vireshark %	NLINWL.pegne 客 (S\system32\c ndows [版 t Corporat nx>nslooku .google 8.8.8 ernet.hact	图 8-1 使用 Wireshark md.exe 本 10.0.19045.2251] tion。保留所有权利。 up -qt=A internet.h	』 944: 7020 · ⋶里来: 0 0.000	R.W. Default
♥ Z virenhark €L :\WINDOW osoft Win Microsof sers\rual 器: dns, ess: 8.8 成应答: : int( ess: 21	NLINUL.popug S\system32\c ndows [版元 t Corporat nx>nslooku .google 8.8.8 ernet.hact 1.69.33.16	图 8-1 使用 Wireshark cmd.exe 本 10.0.19045.2251] cion。保留所有权利。 up -qt=A internet.h	【 948.700 · 289; 0 0.00) 《 工具进行 DNS 报文采集 hactcm. edu. cn 8.8.8.8	REM: Default
● Z virenhark 死 :\WINDOW osoft Win Microsof sers\rual 器: dns. ess: 8.8 成应答: : int. ess: 21	NLINUL.pegage S\system32\c ndows [版元 t Corporat nx>nslooku ,google 8.8.8 ernet.hact 1.69.33.16	图 8-1 使用 Wireshark cmd.exe 本 10.0.19045.2251] tion。保留所有权利。 up -qt=A internet.h	『タ#l: 7000 · Ellips: 0 (0.00) <工具进行 DNS 报文采集 nactcm. edu. cn 8. 8. 8. 8	REME Default
♥ virenhark, WINDOW osoft Win Microsoff Sers\rua Bass: 8.5 ess: 8.5 或应答: : into ess: 21	NLIKWL.pegng S\system32\c ndows [版元 t Corporat nx>nslooku .google 8.8.8 ernet.hact 1.69.33.16	图 8-1 使用 Wireshark md.exe 本 10. 0. 19045. 2251] tion。保留所有权利。 up -qt=A internet.h	『948: 7000 · 288; 0 0.000 《 工具进行 DNS 报文采集 actcm. edu. cn 8.8.8.8	E.H. Default
★ vireshark %	NLIKWL.pegng S\system32\c ndows [版/ t Corporat nx>nslooku .google 8.8.8 ernet.hact 1.69.33.16	图 8-1 使用 Wireshark cmd.exe 本 10. 0. 19045. 2251] cion。保留所有权利。 up -qt=A internet.h	』 944: 703 · 028∓: 0 0 00	E H. Default
● 2 virenhark @ :\WINDOW osoft Win Microsof sers\ruan 器: dns. ess: 8.8 威应答: : int ess: 21	NLINGL.pegge S(System32)(o ndows [版才 t Corporat nx>nslooku .google 8.8.8 ernet.hact 1.69.33.16 图 8.2 乔	图 8-1 使用 Wireshark md.exe 本 10. 0. 19045. 2251] tion。保留所有权利。 up -qt=A internet. h tcm. edu. cn 51	【 9#1: 700 · E型票: 0 0.00	EE Default

③在 Wireshark 的抓包窗体中,查看已获取的 DNS 数据报文,如图 8-3 所示。

	ns and ip.addr == 8.8.8.	8						X = -
No.	Time	Source	Destination	Protocol	Length Info			
	14640 76.982105	192.168.31.220	8.8.8.8	DNS	80 Standard qu	ery 0x0001 PTR 8	.8.8.8.in-addr.arpa	
L	14644 77.014981	8.8.8.8	192.168.31.220	DNS	104 Standard qu	ery response 0x0	001 PTR 8.8.8.8.in-ad	ldr.arpa PTR dns.googl
	14645 77.016429	192.168.31.220	8.8.8.8	DNS	82 Standard qu	ery 0x0002 A int	ernet.hactcm.edu.cn	
	14646 77.020149	8.8.8.8	192.168.31.220	DNS	167 Standard qu	ery response 0x0	002 A internet.hactcm	.edu.cn A 211.69.33.1
	14647 77.022247	192.168.31.220	8.8.8.8	DNS	82 Standard qu	ery 0x0003 AAAA	internet.hactcm.edu.c	n
	14648 77.025489	8.8.8.8	192.168.31.220	DNS	127 Standard qu	ery response 0x0	003 AAAA internet.hac	tcm.edu.cn SOA dns.ha
> I > U ~ D	nternet Protocol ser Datagram Prot omain Name System Transaction ID: r Flags: 0x0100 S 0	Version 4, Src: 192.: cocol, Src Port: 6116: ( (query) 0x0001 tandard query = Response: Me	168.31.220, Dst: 8.8 1, Dst Port: 53 essage is a query	.8.8	0020 08 08 66 69 0030 00 00 00 00 0040 6e 2d 61 64	00 00 01 38 01 64 72 04 61 72	01 00 01 00 00 01 38 01 38 01 38 07 69 70 61 00 00 0c 00 01	n-addr•a rpa•••••
		<pre> = Opcode: Stat  = Truncated: 1  = Recursion d  = Z: reserved 0 = Non-authent: 0 0 dr.arpa: type PTR, c; 6644]</pre>	uano query (G) essage is not trunc estred: Do query rec (0) ccated data: Unaccep	ated ursively table				
	.000 0 	<pre> = Opcode: Stat  = Truncated: /  = Recursion d  = Z: reserved 0 = Non-authent: 3 0 dr.arpa: type PTR, c: 4544]</pre>	used guery (B) essage is not trunc sired: Do query rec (0) cated data: Unaccep	ated ursively table				

(2) 数据报文分析

对采集的数据报文进行分析,并完成表 8-1、表 8-2 的填写。

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 8-1 一次 DNS 解析请求过程

表 8-2 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		

## 2、通信过程中常见请求类型的 DNS 报文分析

(1) NS 记录

①获取 NS 记录请求应答报文。

在 Windows 命令窗体, 输入"<u>nslookup -qt=ns 51xueweb.cn 8.8.8.8</u>", 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 8-3 和表 8-4。

序号	字段名称	字段长度	起始	位 <u>置</u>	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		

表 8-3 NS 记录请求报文分析

6	Additional RRs	第位				
7	Queries	第位				
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		
8	Answers		第位		
		ŧ	爪取数据包的	前详细内容:	
9					

#### 表 8-4 NS 记录应答报文分析

(2) CNAME 记录

①获取 CNAME 记录请求应答报文。

在 Windows 命令窗体, 输入 "<u>nslookup –qt=cname www.baidu.com 8.8.8.8</u>", 使用服务器 "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 8-5 和表 8-6。

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		

表 8-5 CNAME 记录请求报文分析

4	Answer RRs		第	位			
5	Authority RRs		第	位			
6	Additional RRs		第	位			
7	Queries		第	位			
		4	抓取数排	包的详	细内容:		
8							

### 表 8-6 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		
		ł	爪取数捷	包的详	细内容:	
9						

## 七、设计任务(实验考核)

## 1、任务说明

- (1) 按照要求完成 Wireshark 报文分析。
- (1) 按照要求对 DNS 报文进行分析,并进一步理解 DNS 协议。

# 2、任务要求

要求 1: 使用 Wireshark 采集报文;

要求 2: 实现对 DNS 协议报文的分析(A 记录、NS 记录、CNAME 记录)。

3、考核要求

题目 1: 提供 A 记录的 Wireshark 报文采集的界面截图(格式参考图 8-1),完成分析后并填写表 8-1、表 8-2,将表格转为截图后提交。(共计提交 3 张图片,且内容应对应)

题目 2: 提供 NS 记录的 Wireshark 报文采集的界面截图(格式参考图 8-1),完成分析 后并填写表 8-3、表 8-4,将表格转为截图后提交。(共计提交 3 张图片,且内容应对应)

题目 3: 提供 CNAME 记录的 Wireshark 报文采集的界面截图(格式参考图 8-1),完成 分析后并填写表 8-5、表 8-6,将表格转为截图后提交。(共计提交 3 张图片,且内容应对应)