

小实验3 Report

计11 周昉平 2021010699

抓包实验 1： 观察 ICMPv4 超时消息

No.	Time	Source	Destination	Protocol	Length	Info
44	2.921898	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=3 (no response found!)
45	2.935645	118.229.5.1	183.173.107.131	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	3.926970	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=3 (no response found!)
58	3.942056	118.229.5.1	183.173.107.131	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70	4.941770	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=3 (no response found!)
71	4.963995	118.229.5.1	183.173.107.131	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	5.951255	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=3 (no response found!)
86	5.969336	118.229.5.1	183.173.107.131	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
292	19.413689	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=49/12544, ttl=128 (reply in 293)
293	19.430446	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=49/12544, ttl=51 (request in 292)

> Frame 45: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{7B4FE264-B753-4501-BFE6-34242C4B1A5E} (0.0.0.0) on interface 0
> Ethernet II, Src: NewH3CTe_37:88:02 (94:29:2f:37:88:02), Dst: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)
> Internet Protocol Version 4, Src: 118.229.5.1, Dst: 183.173.107.131
▼ Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0x9fa3 [correct]
 [Checksum Status: Good]
 Unused: 00000000
 > Internet Protocol Version 4, Src: 183.173.107.131, Dst: 182.61.200.6
 ▼ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4d2e [unverified] [in ICMP error packet]
 [Checksum Status: Unverified]

0000b0a4609ca031
001000380000
00206b830b009
0030000001017
00404d2e00010

1.收到的 ICMP 包头中， Type 字段和 Code 字段分别是多少？

Type 字段为 11， Code 字段为 0

抓包实验 2： 观察 ICMPv4 回显请求及应答消息

No.	Time	Source	Destination	Protocol	Length	Info
24	1.978909	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (reply in 25)
25	1.996199	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=53/13568, ttl=51 (request in 24)
42	2.990801	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 43)
43	3.007107	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=51 (request in 42)
64	3.997038	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 66)
66	4.019520	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=51 (request in 64)
77	5.008222	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (reply in 79)
79	5.043668	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=51 (request in 77)

> Frame 42: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{7B4FE264-B753-4501-BFE6-34242C4B1A5E} (0.0.0.0) on interface 0
> Ethernet II, Src: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31), Dst: NewH3CTe_37:88:02 (94:29:2f:37:88:02)
> Internet Protocol Version 4, Src: 183.173.107.131, Dst: 182.61.200.6
▼ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4d25 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 54 (0x0036)
 Sequence Number (LE): 13824 (0x3600)
 [Response frame: 43]
 > Data (32 bytes)

000094292f378802
0010003ca0100000
0020c80608004d25
00306768696a6b6c
0040776162636465

1.ICMP 请求分组中， Type 字段和 Code 字段分别是多少？

Type 字段为 8， Code 字段为 0

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
24	1.978999	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=53/13568, ttl=128 (reply in 25)
25	1.996199	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=53/13568, ttl=51 (request in 24)
42	2.990801	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 43)
43	3.007107	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=51 (request in 42)
64	3.997038	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 66)
66	4.019520	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=51 (request in 64)
77	5.008222	183.173.107.131	182.61.200.6	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (reply in 79)
79	5.043668	182.61.200.6	183.173.107.131	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=51 (request in 77)
839	37.812997	8.145.210.3	183.173.107.131	ICMP	98	Echo (ping) request id=0x0004, seq=0/0, ttl=52 (no response found!)
852	38.789652	8.145.210.3	183.173.107.131	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=52 (no response found!)

> Frame 43: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{7B4FE264-B753-4501-BFE6-34242C4B1}	0000	b0 a4 60 9c a0 31
> Ethernet II, Src: NewH3CTe_37:88:02 (94:29:2f:37:88:02), Dst: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)	0010	00 3c a0 10 00 00
> Internet Protocol Version 4, Src: 182.61.200.6, Dst: 183.173.107.131	0020	6b 83 00 00 55 22
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c
Type: 0 (Echo (ping) reply)	0040	77 61 62 63 64 65
Code: 0		
Checksum: 0x5525 [correct]		
[Checksum Status: Good]		
Identifier (BE): 1 (0x0001)		
Identifier (LE): 256 (0x0100)		
Sequence Number (BE): 54 (0x0036)		
Sequence Number (LE): 13824 (0x3600)		
[Request frame: 42]		
[Response time: 16.306 ms]		
Data (32 bytes)		

2.ICMP 回显分组中， Type 字段和 Code 字段分别是多少？

Type 字段为 0， Code 字段为 0

3.一对请求和回复分组中的标识符，序号和数据是否相等？

上图中的两个包就是一对请求与回复分组，其标识符，序号和数据字段均相等

抓包实验 3： 观察 ARP 分组各式

arp						
No.	Time	Source	Destination	Protocol	Length	Info
66	4.649490	IntelCor_9c:a0:31	Broadcast	ARP	42	Who has 183.173.104.1? Tell 183.173.107.131
68	4.859165	NewH3CTe_37:88:02	IntelCor_9c:a0:31	ARP	56	183.173.104.1 is at 94:29:2f:37:88:02

> Frame 68: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{7B4FE264-B753-4501-BFE6-34242C4B1}	0000	b0 a4 60 9c a0 31
> Ethernet II, Src: NewH3CTe_37:88:02 (94:29:2f:37:88:02), Dst: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)	0010	08 00 06 04 00 00
> Destination: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)	0020	b0 a4 60 9c a0 31
> Source: NewH3CTe_37:88:02 (94:29:2f:37:88:02)	0030	62 08 48 a0 84 9c
Type: ARP (0x0806)		
Trailer: 6801e7f5eb79620848a08490e042		
> Address Resolution Protocol (reply)		

1.ARP 协议在以太网帧头中载荷类型的编号是？

0x0806

> Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4

2.ARP 分组头中，以太网硬件类型编号和 IP 协议类型编号分别是？

硬件类型以太网： 1， 协议类型 IPv4： 0x0800

3.ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对？

不良影响：

- 网络拥塞：大量滥发的ARP广播包会占用网络带宽和资源，导致网络拥塞，影响正常通信和性能。
- ARP欺骗（ARP Spoofing）：攻击者可能滥发ARP广播包来进行ARP欺骗攻击。这种攻击会导致网络中的主机将流量发送到攻击者的主机，从而使攻击者能够窃取、篡改或监听通信流量。

发现和应对：

- 使用网络监控工具：使用网络监控工具来检测网络中的异常流量和广播包数量。这些工具可以提供实时的网络流量分析和警报，帮助及时发现异常情况。
- 实施入侵检测系统（IDS）或入侵防御系统（IPS）：IDS/IPS系统可以检测和阻止滥发或错发ARP广播包的行为。它们可以通过监测网络流量和识别异常模式来发现潜在的攻击，并采取相应的防御措施。