패킷 분석 보고서

portscan.pcap

i-Keeper

2018 May 9

저자: 최홍준

목차

1. 개요

서버에 열려 있는 TCP/UDP 포트를 검색하는 것을 캡처한 portscan.pcap 파일을 분석하였다.

2. 패킷 분석

2.1 분석 환경

OS	Wireshark
Window 10	version 2.4.5

[표 1] 분석 환경

2.2 portscan.pcap

서버의 열린 포트를 확인하기 위해 Well Known 포트를 포함한 여러가지 포트를 스캔하고 있다. 확인된 내용은 아래와 같다.

① Client, Server IP

② Src, Dst Port

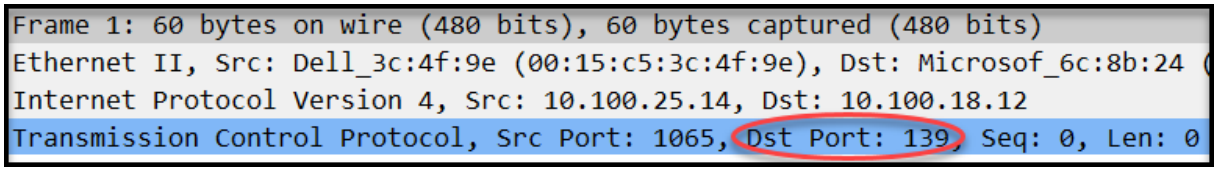
No.	Time	Source	Destination	Prot	Leng	Info
1	0.000000	10.100.25.14	10.100.18.12	TCP	60	1065 → 139 [SYN] Seq=0 Win=8 Len=0
2	0.100476	10.100.25.14	10.100.18.12	TCP	60	19491 → 135 [SYN] Seq=0 Win=8 Len=0
3	0.201152	10.100.25.14	10.100.18.12	TCP	60	7358 → 445 [SYN] Seq=0 Win=8 Len=0
4	0.301714	10.100.25.14	10.100.18.12	TCP	60	27524 → 80 [SYN] Seq=0 Win=8 Len=0
5	0.403133	10.100.25.14	10.100.18.12	TCP	60	20193 → 22 [SYN] Seq=0 Win=8 Len=0
6	0.503604	10.100.25.14	10.100.18.12	TCP	60	1023 → 515 [SYN] Seq=0 Win=8 Len=0
7	0.607512	10.100.25.14	10.100.18.12	TCP	60	16748 → 23 [SYN] Seq=0 Win=8 Len=0
8	0.707986	10.100.25.14	10.100.18.12	TCP	60	12502 → 21 [SYN] Seq=0 Win=8 Len=0
9	0.808340	10.100.25.14	10.100.18.12	TCP	60	30382 → 6000 [SYN] Seq=0 Win=8 Len=0
10	0.904949	10.100.25.14	10.100.18.12	TCP	60	27986 → 1025 [SYN] Seq=0 Win=8 Len=0
11	1.004235	10.100.25.14	10.100.18.12	TCP	60	25488 → 25 [SYN] Seq=0 Win=8 Len=0
12	1.110883	10.100.25.14	10.100.18.12	TCP	60	6729 → 111 [SYN] Seq=0 Win=8 Len=0
13	1.212836	10.100.25.14	10.100.18.12	TCP	60	29169 → 1028 [SYN] Seq=0 Win=8 Len=0
14	1.307771	10.100.25.14	10.100.18.12	TCP	60	24305 → 9100 [SYN] Seq=0 Win=8 Len=0
15	1.407052	10.100.25.14	10.100.18.12	TCP	60	17851 → 1029 [SYN] Seq=0 Win=8 Len=0
16	1.512738	10.100.25.14	10.100.18.12	TCP	60	10985 → 79 [SYN] Seq=0 Win=8 Len=0
17	1.614648	10.100.25.14	10.100.18.12	TCP	60	1515 → 497 [SYN] Seq=0 Win=8 Len=0
18	1.708617	10.100.25.14	10.100.18.12	TCP	60	4019 → 548 [SYN] Seq=0 Win=8 Len=0
19	1.807145	10.100.25.14	10.100.18.12	TCP	60	12966 → 5000 [SYN] Seq=0 Win=8 Len=0
20	1.905446	10.100.25.14	10.100.18.12	TCP	60	5851 → 1917 [SYN] Seq=0 Win=8 Len=0

[그림 1] portscan.pcap

패킷을 열어보면 그림 1과 같다. 일정 주기로 클라이언트가 서버에게 SYN 패킷을 보내고 있는 것을 알 수 있다. 그림 1에서 분석한 내용은 아래 표 2와 같다.

Client IP	Server IP
10.100.25.14	10.100.18.12

[표 2] Client, Server IP



[그림 2] No.1 패킷 정보

No.1 패킷의 하단을 보면 그림 2와 같다. 여기서 얻을 수 있는 정보들이 많지만 그 중 Src, Dst Port를 살펴보면 Dst Port 즉, 서버의 139번 포트가 열려 있는지 확인하라는 의미이다. 검색하고 있는 Dst Port는 표 3과 같다.

Src Port	Dst Port
1065	139
19491	135
7358	445
27524	80
20193	22
1023	515
16748	23
12502	21
30382	6000

27986	1025
25488	25
6729	111
29169	1028
24305	9100
17851	1029
10985	79
1515	497
4019	548
12966	5000
5851	1917
53	53
6400	161
33415	9001
20	65535
15628	443
25	113
4926	993
1177	8080
1316	2869

[표 3] Src, Dst Port

3. 결론

29 개의 포트를 검색하고 있지만 서버측에서 응답이 없는 것으로 보아 아래와 같이 추측할 수 있다.

① 컴퓨터 전원 OFF

② 방화벽으로 인한 차단