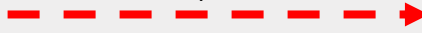


2. Scanning Attack

공격자
(CentOS7_CLI)



1. Nmap 스캐닝공격



2. 공격자 IP 차단



타겟
(CentOS7_GT)



포트 스캐닝은 해커가 악의적인 공격을 수행하기 위해 취약점을 찾는 과정 중 수행하는 사전작업이라고 할 수 있다. 피해자 시스템 혹은 네트워크를 선택한 뒤 해당 시스템이나 네트워크가 어떤 포트를 열고 서비스를 하고 있는지 알아낼 수 있다.

스캔(SCAN)은 서비스를 제공하는 서버의 작동여부와 제공하고 있는 서비스를 확인하는 것으로 질의 (Request)를 보내면 응답(Response)을 받는 구조인 네트워크의 특성을 이용한다. 이 과정에서 네트워크상 다른 단말기의 정보를 얻어온다.

2. Scanning Attack

1. 실습 개요

Nmap툴을 이용해 공격자가 사용자의 서버를 포트 스캔한 후 접속하고 특정 포트로 외부 접속을 한 후에 사용자가 외부 접속된 서버를 iptables를 이용해 막는 과정

2. 시스템 정보

- * 공격자 CentOS7_CLI 계정 : root / root123
- * 타겟 CentOS7_GT 계정 : root / root123

3. 문제풀이



- 1) (CentOS7_CLI) root 사용자 계정으로 로그인 (root/root123)

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.25.1.el7.x86_64 on an x86_64

localhost login: root
Password:
Last login: Tue Aug 10 21:51:59 on tty1
```

- 2) (CentOS7_CLI) GT서버에서 ssh, telnet, ftp포트 중 ssh포트가 open 되어있는 것 확인
 - > nmap -sT [타겟 IP]
 - ex) nmap -sT 192.168.10.129

```
[root@localhost ~]# nmap -sT 192.168.10.129

Starting Nmap 6.40 ( http://nmap.org ) at 2021-08-10 22:18 KST
Nmap scan report for 192.168.10.129
Host is up (0.94s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    closed http
MAC Address: 08:0C:29:79:BA:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 61.74 seconds
```

2. Scanning Attack

[공격]

※ NMAP

Nmap은 Port Scanning 툴로써 호스트나 네트워크를 스캐닝 할 때, 아주 유용한 시스템 보안 툴인 동시에, 해커에게는 강력한 해킹 툴로 사용 될 수 있다.

- 호스트 탐지 : 네트워크 상의 컴퓨터들을 확인 ex) ping 응답이나 특정 포트가 열린 컴퓨터 나열
- 포트 스캔 : 하나 혹은 그 이상의 대상 컴퓨터들에 열린 포트들을 나열
- 버전 탐지 : 응용 프로그램의 이름과 버전 번호 확인을 위해 원격 컴퓨터의 네트워크 서비스 주의
- 운영체제 탐지 : 원격으로 운영체제와 네트워크 장치의 하드웨어 특성 확인

3) (CentOS7_CLI) CLI서버에서 ssh로 GT서버로 접속 후 관리자 계정으로 로그인 (root/root)
 > ssh root@[타겟 IP]
 ex) ssh root@192.168.10.129

```
[root@localhost ~]# ssh root@192.168.10.129
The authenticity of host '192.168.10.129 (192.168.10.129)' can't be established.
ECDSA key fingerprint is SHA256:YugBSeElwzN0s0e/aZGkJ95lcYMegqRnkLmqFz6XqU8s.
ECDSA key fingerprint is MD5:15:20:85:1a:a0:2d:29:0e:8d:13:0f:c8:6c:7d:51:4d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.129' (ECDSA) to the list of known hosts.
root@192.168.10.129's password:
Last login: Wed Aug 11 20:09:29 2021
```

※ SSH 프로토콜로 원격지에 접속하기

: 원격지에서 호스트 접속을 위한 프로토콜을 사용한 접속
 [조건]

- 22번 TCP 포트가 방화벽에서 열려 있어야함
- SSH 서버 프로그래밍 설치 및 구동되고 있어야함
- SSH 프로토콜로 접속할 수 있는 SSH 클라이언트가 필요

4) (CentOS7_GT) CLI가 ssh로 접속하기전 GT서버에서 WireShark 실행 후 패킷 캡처

No.	Time	Source	Destination	Protocol	Length	Info
8	1.102968660	194.0.5.123	192.168.10.129	NTP	90	NTP Version 4, server
9	4.452228275	192.168.10.133	192.168.10.129	TCP	74	46490 > ssh [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4219279 TSecr=0 WS=128
10	4.452267681	192.168.10.129	192.168.10.133	TCP	74	ssh > 46490 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=513528 TSecr=4219279 WS=128
11	4.452611290	192.168.10.133	192.168.10.129	TCP	66	46490 > ssh [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4219280 TSecr=513528
12	4.453130609	192.168.10.133	192.168.10.129	SSHv2	87	Encrypted request packet len=21
13	4.453160472	192.168.10.129	192.168.10.133	TCP	66	ssh > 46490 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=513528 TSecr=4219280
14	4.471068773	192.168.10.129	192.168.10.133	SSHv2	87	Encrypted response packet len=21
15	4.471481137	192.168.10.133	192.168.10.129	TCP	66	46490 > ssh [ACK] Seq=22 Ack=22 Win=29312 Len=0 TSval=4219299 TSecr=513546
16	4.472215374	192.168.10.133	192.168.10.129	SSHv2	1562	Client: Key Exchange Init
17	4.472245450	192.168.10.129	192.168.10.133	TCP	66	ssh > 46490 [ACK] Seq=22 Ack=1518 Win=32000 Len=0 TSval=513548 TSecr=4219299
18	4.477411626	192.168.10.129	192.168.10.133	SSHv2	1346	Server: Key Exchange Init
19	4.480628753	192.168.10.133	192.168.10.129	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
20	4.486193452	192.168.10.129	192.168.10.133	SSHv2	430	Server: New Keys
21	4.490017565	192.168.10.133	192.168.10.129	SSHv2	82	Client: New Keys
22	4.529740282	192.168.10.129	192.168.10.133	TCP	66	ssh > 46490 [ACK] Seq=1666 Ack=1502 Win=32000 Len=0 TSval=513605 TSecr=4219317
23	4.530088141	192.168.10.133	192.168.10.129	SSHv2	110	Encrypted request packet len=44

▶ Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
 ▶ Ethernet II, Src: Vmware, 79:ba:24:00:0c:29:79:ba:24), Dst: Vmware, e9:e7:6b:00:58:56:e9:e7:6b)
 ▶ Internet Protocol Version 4, Src: 192.168.10.129 (192.168.10.129), Dst: 158.247.211.195 (158.247.211.195)
 ▶ User Datagram Protocol, Src Port: 58883 (58883), Dst Port: ntp (123)
 ▶ Network Time Protocol (NTP Version 4, client)

2. Scanning Attack

[공격]

- 5) (CentOS7_GT) GT서버에서 ssh로 접속하는 공격서버 ip(CLI서버)를 iptables정책을 설정해 차단
 > iptables -A INPUT -p tcp --dport 22 -j DROP

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -j DROP
[root@localhost ~]#
```

※ IPTABLES

iptables는 리눅스 상에서 방화벽을 설정하는 도구로서 커널 2.4 이전 버전에서 사용되던 ipchains를 대신하는 방화벽 도구iptables는 커널 상에서의 netfilter 패킷필터링 기능을 사용자 공간에서 제어하는 수준으로 사용할 수 있다.

[옵션]

- INPUT : 서버로 들어오는 기본 정책
- -A (--append) : 새로운 규칙을 추가 (맨 아래에 추가됨)
- -p (--policy) : 기본 정책을 변경
- --dport : 목적지 (destination) 포트 번호
- -j (--jump) : 규칙에 맞는 패킷을 어떻게 처리할 것인가를 명시
- DROP : 접근 차단

- 6) (CentOS7_CLI) CLI서버에서 다시 ssh로 GT접속 시도 > iptables정책때문에 접속되지 않음
 > ssh root@[타겟 IP]
 ex) ssh root@192.168.10.129

```
[root@localhost ~]# ssh root@192.168.10.129
ssh: connect to host 192.168.10.129 port 22: Connection timed out
```