정 보 보 안 기 사 스 터 디

스터디 1주차

발 표 자 이 승 현

문제

11. 아래 그림의 3가지 포트스캔의 과정을 보고 답하시오.
1) 어떠한 포트 스캔 방식인가?
2) 25, 443, 110 번
3) 각 포트 스캔의 결과를 적고 그 근거를 적으시오.

해설

12. 침해사고 발생 이후 리눅스 시스템에서 다음과 같은 조사를 하였다. 각 명령어를 완성하시오.
1) 최근 7일 내에 변경된 모든 파일을 검색하는 명령어
2) 사용자가 root 이며 접근권한이 setuid로 설정된 모든 파일을 검색하는 명령어
3) 호스트 192.168.256.3에서 192.168.10.48으로부터 이상(anormaly) 트래픽이 탐지되었다.
Tcpdump 명령을 통해 이너페이스 eth0을 통해 192.168.253.3에서 192.168.10.48을 오가는 패킷 캡쳐하는 명령

해설

13. 개인정보 안전성 확보 조치를 위한 쇼핑몰 사이트를 운영하는 정보통신 서비스 제공업체의 보안 취급자의 비밀번호 작성 규칙에 대해 기술적 관리적 보호 조치 사항 3가지를 기술하시오.

해설

목차

01

“ TCP Half Open ”

1. TCP Half(SYN) Open Scan

#> namp -sS [Target Ip]

TCP SYN scan : Full TCP 접속을 하지 않으므로 "half-open" 스캐닝이라 한다. 하나의 SYN 패킷을 보내어 SYN|ACK 응답이 오면 그 포트는 listening 상태임을 나타내며, RST 응답이 오면 non-listen임을 나타낸다. 이 기술은 하나의 패킷을 보내여 SYN|ACK 응답을 받으면 그 즉시 RST 패킷을 보내서 접속을 끊어버린다. 이렇게 하면 접속이 이루어지지 않은 상태에서 접속을 끊었기 때문에 로그를 남기지 않는 경우가 대부분이다. custom SYN packet을 만들기 위해서는 루트 권한이 필요하다.

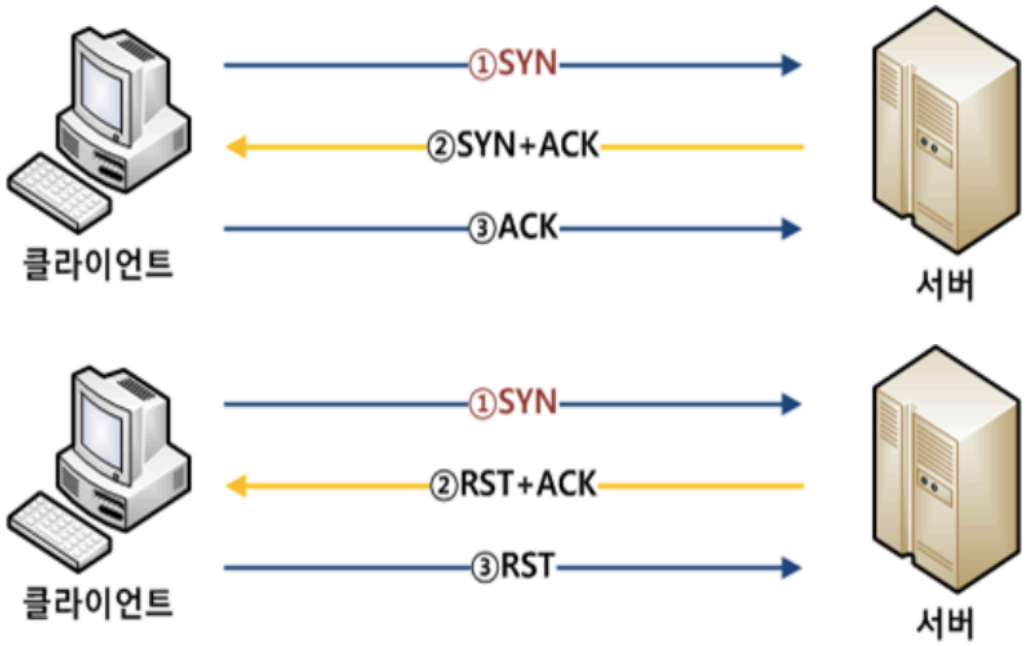
```
[root@localhost html]# nmap -sS 10.10.10.20

Starting Nmap 5.51 ( http://nmap.org ) at 2018-04-27 02:24 KST
Nmap scan report for 10.10.10.20
Host is up (0.0079s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:0C:29:BB:BB:BB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

No.	Time	Source	Protocol	Destination	Source Port	Info	Destination Port
23	2.959318	10.10.10.20	TCP	10.10.10.10	80	80→48821 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460	48821
28	2.959719	10.10.10.20	TCP	10.10.10.10	22	22→48821 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460	48821
53	2.961606	10.10.10.20	TCP	10.10.10.10	21	21→48821 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460	48821
65	2.962453	10.10.10.20	TCP	10.10.10.10	23	23→48821 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460	48821

01

“ TCP Half Open ”

TCP



01

“ TCP Half Open ”

TCP open half

02

Port Numbers

포트번호	프로토콜, 프로세스
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
443	HTTP,HTTPS 암호화

포트	프로토콜, 프로세스
8080	톰캣
1521	오라클
3306	MySQL
1433	MS-SQL
8629	티베로
3389	원격데스크톱

02

1. 포트 80(HTTP) : 이 포트는 우리가 발견한 열린 포트의 14% 이상을 차지한다.

2. 포트 23(Telnet) : 텔넷은(암호화되지 않아) 보안이 불안하긴 하지만 계속 존재했다.

3. 포트 443(HTTPS) : SSL 암호화된 웹서버는 이 포트를 기본적으로 사용한다.

4. 포트 21(FTP) : 텔넷처럼 FTP는 없어져야 하는 보안이 불안한 프로토콜이다.

5. 포트 22(SSH) : 텔넷을 대체하는 암호화된 프로토콜로 보통 보안 셸로 알려졌다.

6. **포트 25(SMTP) : 표준 메일 전송 프로토콜(보안이 돼 있지 않다).**

7. 포트 3389(ms-term-server) : 마이크로소프트 터미널 서비스 관리 포트

8. **포트 110(POP3) : 이메일 추출을 위한 포스트 오피스 프로토콜 버전 3(비보안)**

9. 포트 445(마이크로소프트-DS) : (파일/프린터 공유 같은)마이크로소프트 윈도우 서비스에 있는 IP에 대한 SMB 통신을 위한 포트

10. 포트 143(IMAP) : 인터넷 메시지 접근 프로토콜 버전 2. 보안이 안 된 이메일 추출 프로토콜

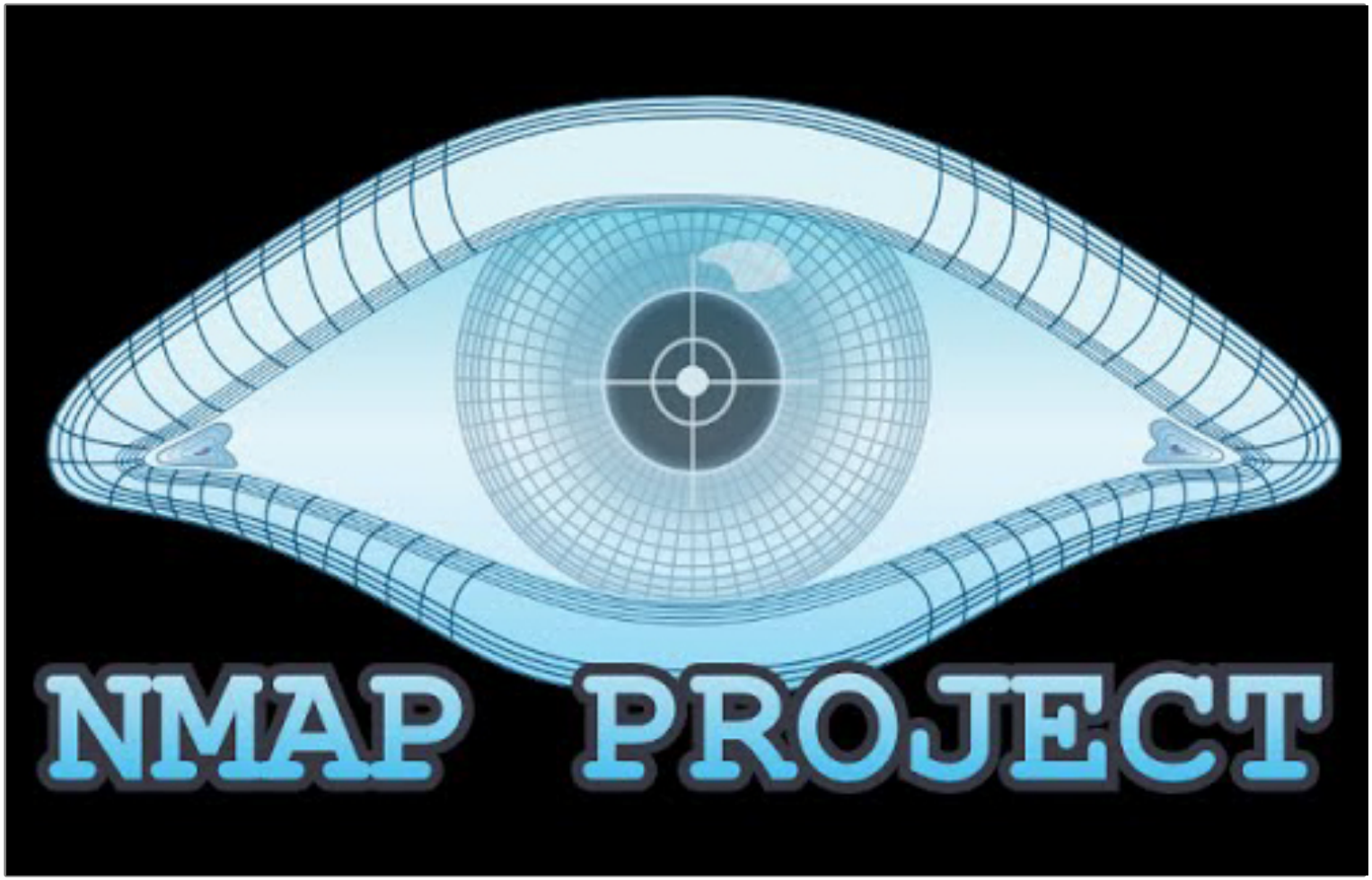
11. 포트 53(도메인) : 도메인 네임 시스템DNS, 호스트/도메인명과 IP주소 사이의 대화를 위한 보안이 안 된 시스템

12. 포트 3306(MySQL) : MySQL 데이터베이스와 통신을 위한 포트

13. 포트 8080(HTTP-proxy) : 일반적인 웹서버를 위한 HTTP 프록시나 다른 포트로써 흔하게 사용되는 포트

14. 포트 995(POP3S) : 보안을 위해 추가된 SSL이 있는 POP3

15. 포트 5900(VNC) : 그래픽 데스크탑 공유 시스템(비보안)


NMAP PROJECT

문제

스캔 종류	내 용
-sT	connect()함수를 이용한 Open 스캔(TCP포트)
-sS	세션을 성립시키지 않는 SYN 스캔
-sF	FIN 패킷을 이용한 스캔
-sN	NULL 패킷을 이용한 스캔
-sX	XMAS 패킷을 이용한 스캔
-sP	ping을 이용한 호스트 활성화 여부 확인
-sU	UDP 포트 스캔
-sR	RPC 포트 스캔
-sA	ACK 패킷에 대한 TTL값 분석
-sW	ACK 패킷에 대한 윈도우 크기 분석
-b	FTP 바운스 스캔

THANK YOU