호스트 모의해킹 실습

정보수집 및 취약점 진단에 관해

호스트 모의해킹

- 모의 해킹의 대상으로는 웹, 모바일 등 여러가지가 있음
- 그 중 특정 호스트를 대상으로 하는 모의해킹에 대해 알아볼 예정

OSI 7계층과 공격벡터

물리 : 블루투스, 이더넷 등

데이터 링크 : MAC, ARP를 이용한 스푸핑

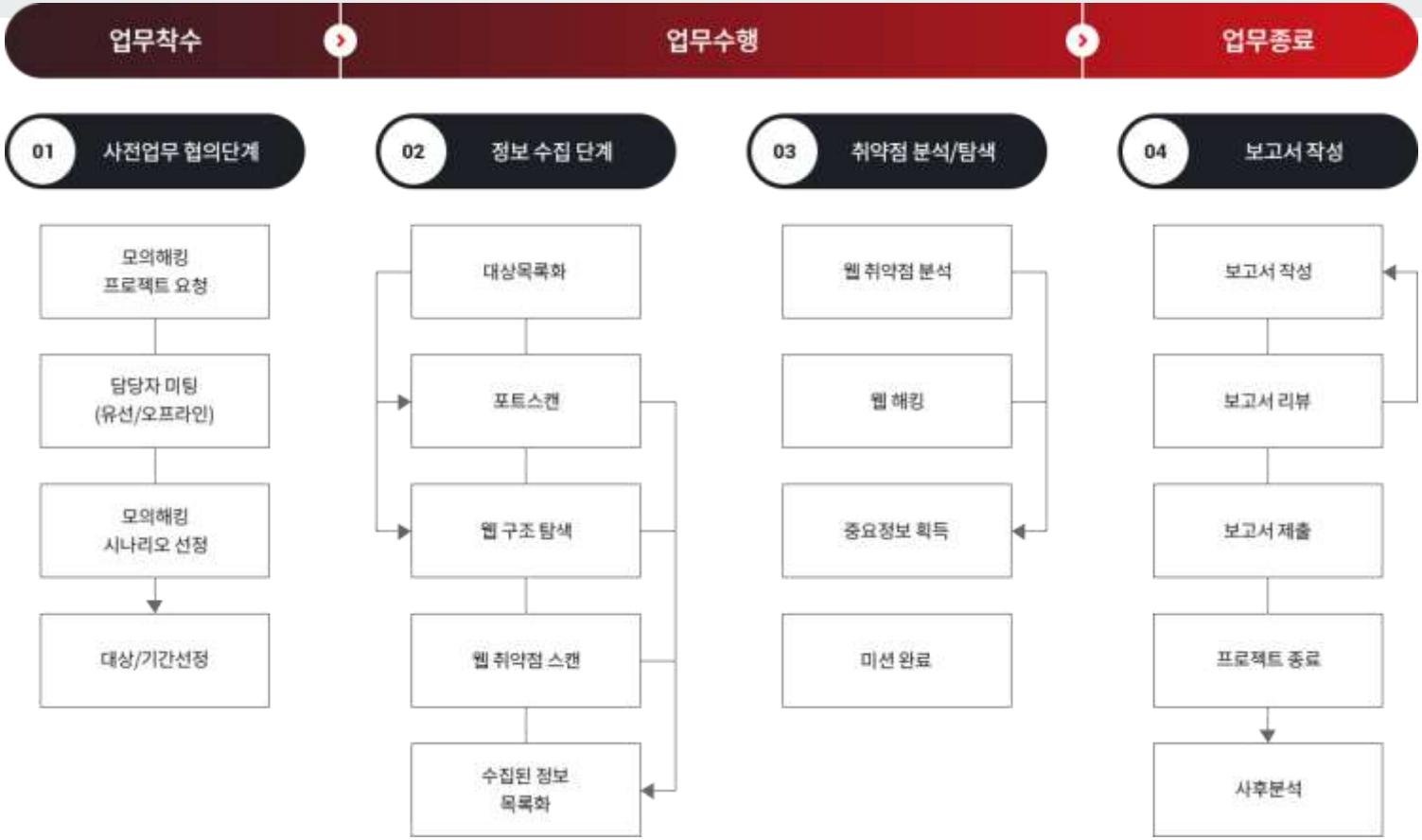
네트워크 : MITM 공격 등

전송 : 포트스캐닝, SYN Flood 등

세션: 세션 하이제킹, XSS

표현: 피싱공격, 악성코드 삽입

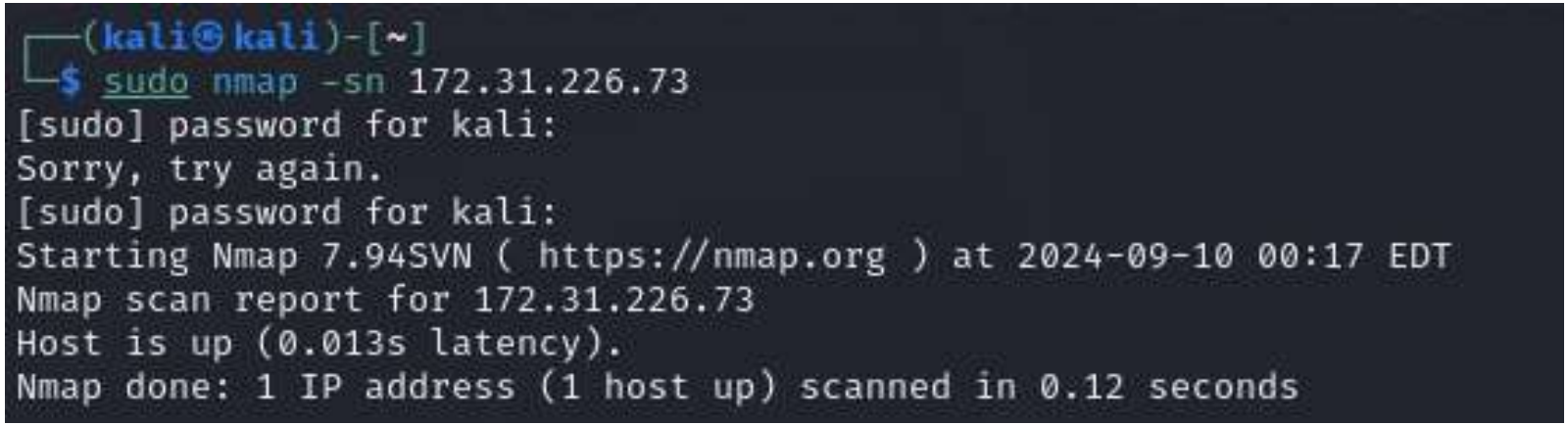
에플리케이션: 멀웨어 인젝션, 피싱, DDOS 등


업무착수
업무수행
업무종료
01
사전업무 협의단계
모의해킹
프로젝트 요청
담당자 미팅
(유선/오프라인)
모의해킹
시나리오 선정
대상/기간선정
02
정보 수집 단계
대상목록화
포트스캔
웹 구조 탐색
웹 취약점 스캔
수집된 정보
목록화
03
취약점 분석/탐색
웹 취약점 분석
웹 해킹
중요정보 획득
미션 완료
04
보고서 작성
보고서 작성
보고서 리뷰
보고서 제출
프로젝트 종료
사후분석

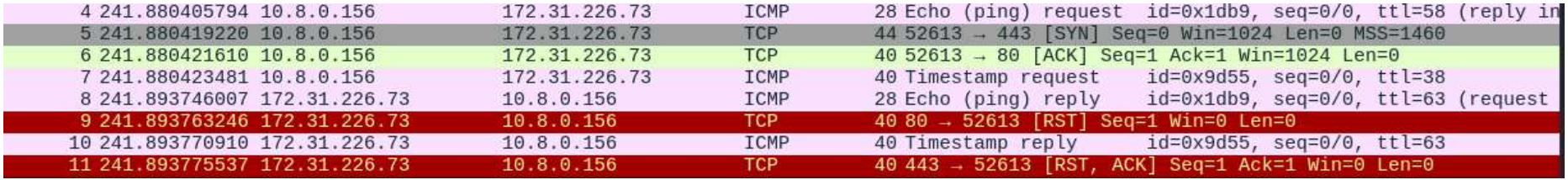
정보수집

- 가장 대표적인 정보수집 도구인 nmap을 활용하여 대상 호스트의 정보를 수집한다.
- 이외에도 wireshark를 통해 패킷을 분석

nmap 사용 실습 - ping



nmap 사용 실습 - ping



4	241.880405794	10.8.0.156	172.31.226.73	ICMP	28	Echo (ping) request id=0x1db9, seq=0/0, ttl=58 (reply in
5	241.880419220	10.8.0.156	172.31.226.73	TCP	44	52613 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	241.880421610	10.8.0.156	172.31.226.73	TCP	40	52613 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	241.880423481	10.8.0.156	172.31.226.73	ICMP	40	Timestamp request id=0x9d55, seq=0/0, ttl=38
8	241.893746007	172.31.226.73	10.8.0.156	ICMP	28	Echo (ping) reply id=0x1db9, seq=0/0, ttl=63 (request
9	241.893763246	172.31.226.73	10.8.0.156	TCP	40	80 → 52613 [RST] Seq=1 Win=0 Len=0
10	241.893770910	172.31.226.73	10.8.0.156	ICMP	40	Timestamp reply id=0x9d55, seq=0/0, ttl=63
11	241.893775537	172.31.226.73	10.8.0.156	TCP	40	443 → 52613 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

nmap사용 실습 - TCP Connect 스캔

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.31.226.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 00:23 EDT
Nmap scan report for 172.31.226.73
Host is up (0.010s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
2100/tcp open  amiganetfs
2222/tcp open  EtherNetIP-1
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
8082/tcp open  blackice-alerts

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```

SYN (포트 22 연결)

SYN/ACK (열려 있어요, 연결하세요)

ACK (연결 성공)

RST (그만 합시다)


SYN (포트 22 연결)
RST/ACK (포트 22 닫혀있습니다)

nmap 사용 실습 - TCP SYN 스캔

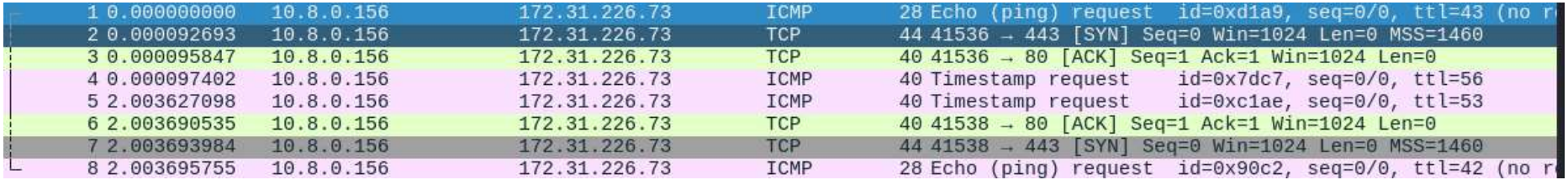
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 172.31.226.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 00:20 EDT
Nmap scan report for 172.31.226.73
Host is up (0.013s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
2100/tcp open  amiganetfs
2222/tcp open  EtherNetIP-1
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
8082/tcp open  blackice-alerts

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```


SYN (포트 22 연결)
SYN/ACK (열려 있어요, 연결하세요)
RST (싫어요 안해요)


SYN (포트 22 연결)
RST/ACK (포트 22 닫혀있습니다)

Host Discovery



1	0.000000000	10.8.0.156	172.31.226.73	ICMP	28	Echo (ping) request id=0xd1a9, seq=0/0, ttl=43 (no r
2	0.000092693	10.8.0.156	172.31.226.73	TCP	44	41536 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000095847	10.8.0.156	172.31.226.73	TCP	40	41536 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.000097402	10.8.0.156	172.31.226.73	ICMP	40	Timestamp request id=0x7dc7, seq=0/0, ttl=56
5	2.003627098	10.8.0.156	172.31.226.73	ICMP	40	Timestamp request id=0xc1ae, seq=0/0, ttl=53
6	2.003690535	10.8.0.156	172.31.226.73	TCP	40	41538 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	2.003693984	10.8.0.156	172.31.226.73	TCP	44	41538 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	2.003695755	10.8.0.156	172.31.226.73	ICMP	28	Echo (ping) request id=0x90c2, seq=0/0, ttl=42 (no r

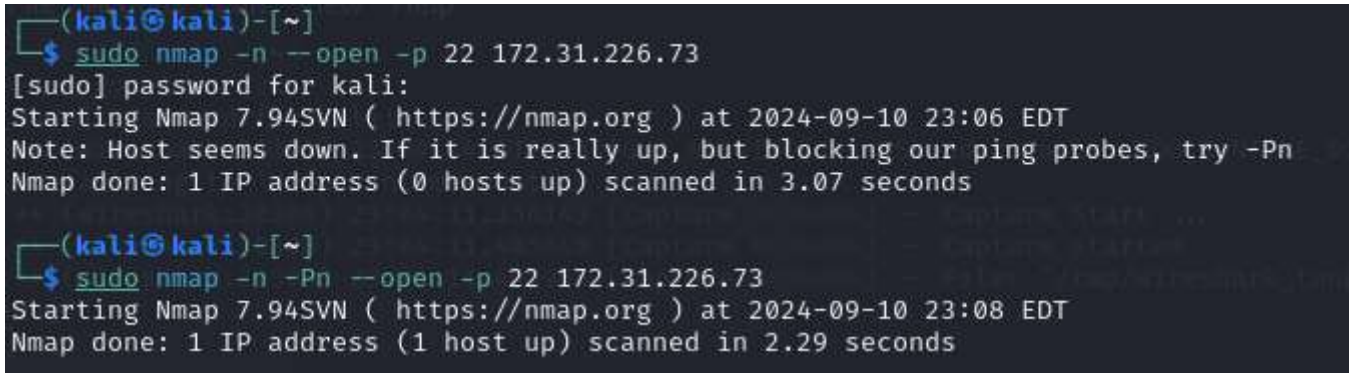
host discovery가 활성화 되어있을때

Host Discovery

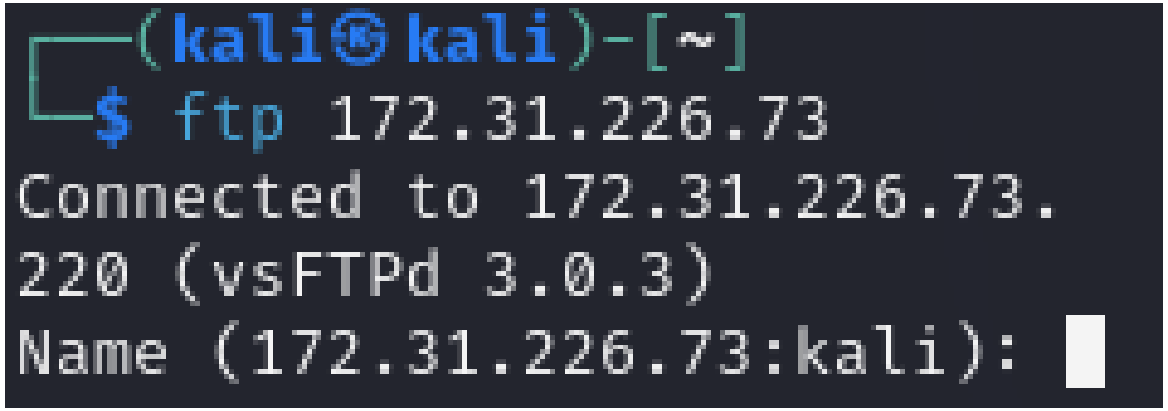
```
10 137.480346236 10.8.0.156    172.31.226.73    TCP    44 45936 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11 138.697678672 10.8.0.156    172.31.226.73    TCP    44 45938 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

host discovery가 비활성화 되어있을때

nmap에서 host discovery를 확인



배너 그래빙


┌──(kali㉿kali)-[~]
└─$ ftp 172.31.226.73
Connected to 172.31.226.73.
220 (vsFTPd 3.0.3)
Name (172.31.226.73:kali):

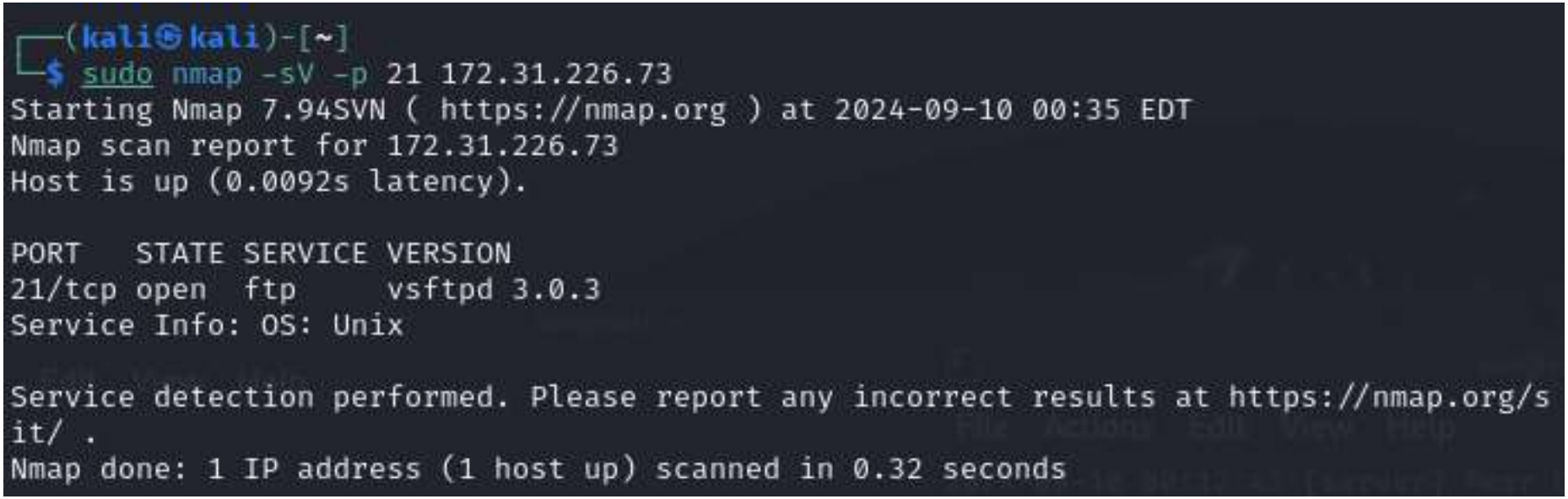
SYN (포트 22 연결)

SYN/ACK (열려 있어요, 연결하세요)

ACK (연결 성공)

서비스 (이름이랑 버전 - Banner)

프로빙


(kali㉿kali)-[~]
$ sudo nmap -sV -p 21 172.31.226.73
Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-10 00:35 EDT
Nmap scan report for 172.31.226.73
Host is up (0.0092s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/s
it/ .
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

프로빙

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -p 21 172.31.226.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 00:36 EDT
Nmap scan report for 172.31.226.73
Host is up (0.0096s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.31.0.146
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.17.0.3 is not the same as 172.31.226.73

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```


SYN (포트 22 연결)
SYN/ACK (열려 있어요, 연결하세요)
ACK (연결 성공)
서비스 Probe로 이름/버전 확인
Probe 응답(성공), 무시(실패)

취약점 진단

- 정보수집 단계에서 수집한 정보를 기반으로 어떠한 서비스가 구동되고 있으며 어떠한 취약점을 가지고 있는지 확인하는 단계
- 직접적인 공격보다는 취약점이 있는지만을 판단

자동 취약점 진단

- 시간 절약과 빠른 진단이 가능
- 거짓 양성, 혹은 거짓 음성이 발생할 수 있는 한계 존재
- 수동과 자동을 병행하는게 효과적

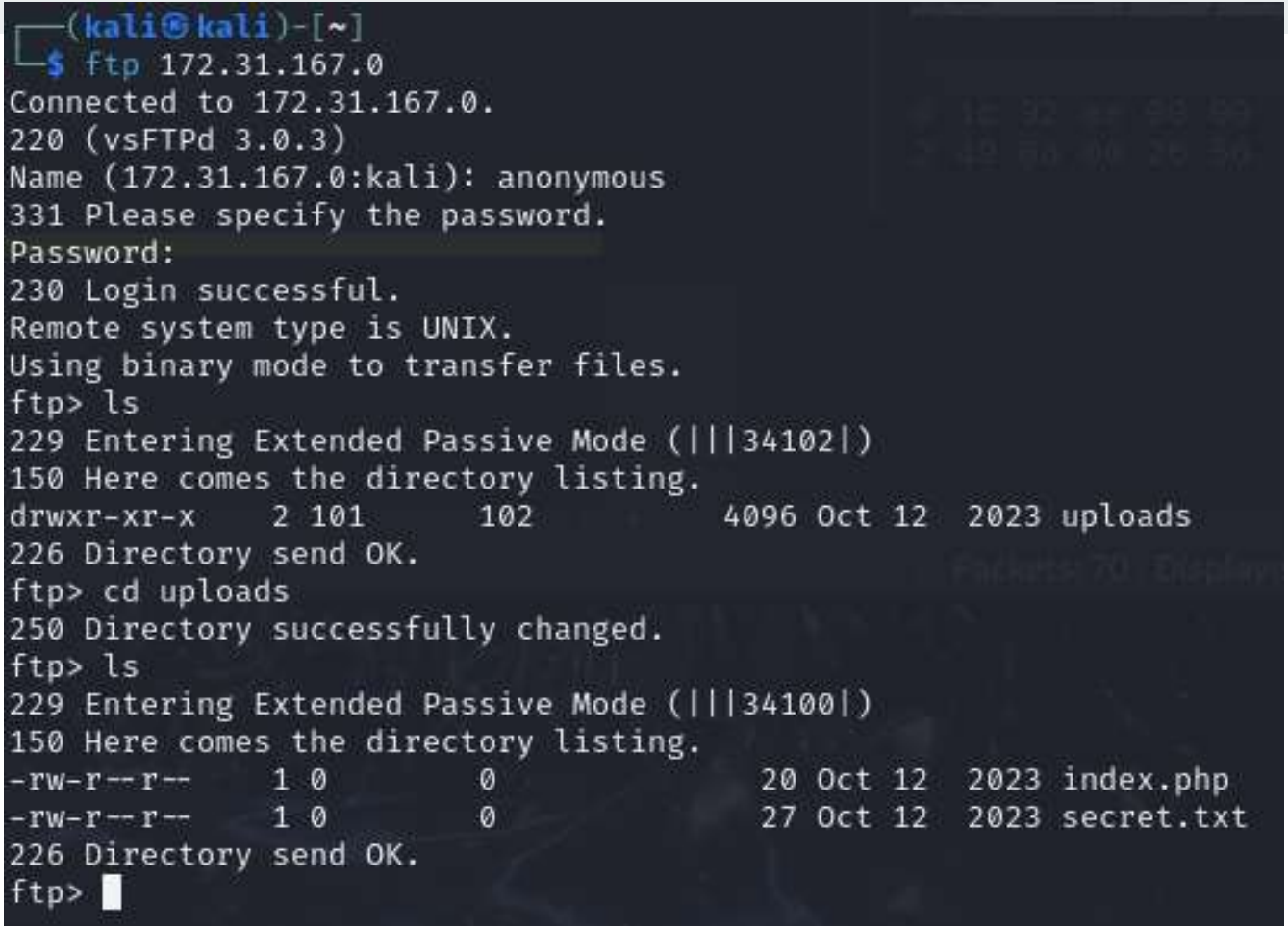
수동 취약점 진단

- 직접 진단하기 때문에 정확도가 높음
- 거짓 음성, 거짓 양성을 판별하기 위해 검증하는 데에도 사용
- 인적 오류 발생 가능

FTP 취약점 진단

- 특징: 오래된 시스템, 파일 다운로드 및 업로드 기능이 있음
- 대부분 21번 포트를 이용함
- 파일 전송시 평문으로 전송

- 진단 관점: 서비스 버전, 익명 로그인, 파일 읽기 및 쓰기 권한, 기본계정과 비밀번호

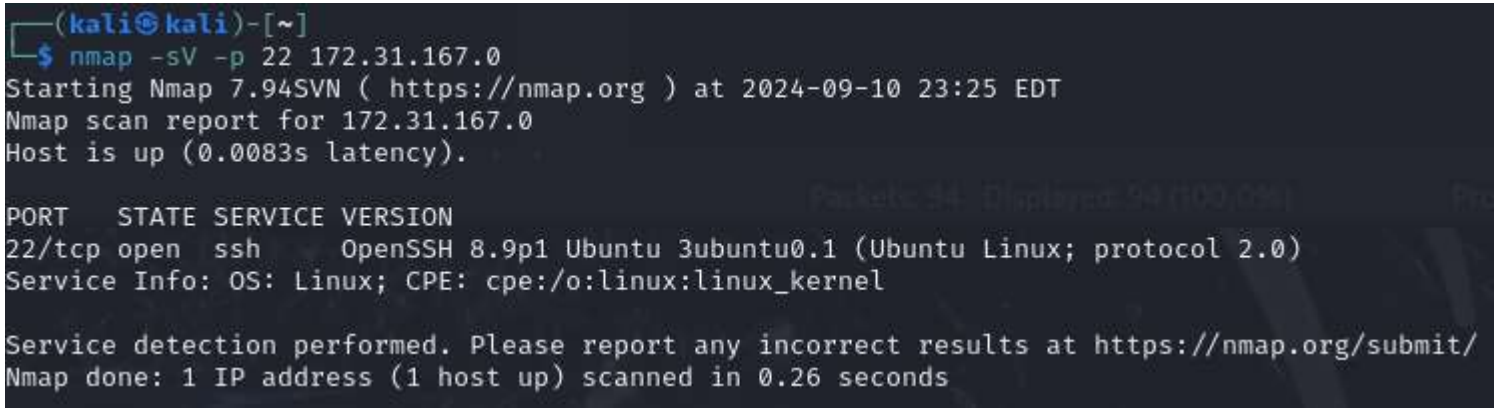

┌──(kali㉿kali)-[~]
└─$ ftp 172.31.167.0
Connected to 172.31.167.0.
220 (vsFTPd 3.0.3)
Name (172.31.167.0:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34102|)
150 Here comes the directory listing.
drwxr-xr-x   2 101   102   4096 Oct 12 2023 uploads
226 Directory send OK.
ftp> cd uploads
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||34100|)
150 Here comes the directory listing.
-rw-r--r--   1 0   0   20 Oct 12 2023 index.php
-rw-r--r--   1 0   0   27 Oct 12 2023 secret.txt
226 Directory send OK.
ftp>

SSH 취약점 진단

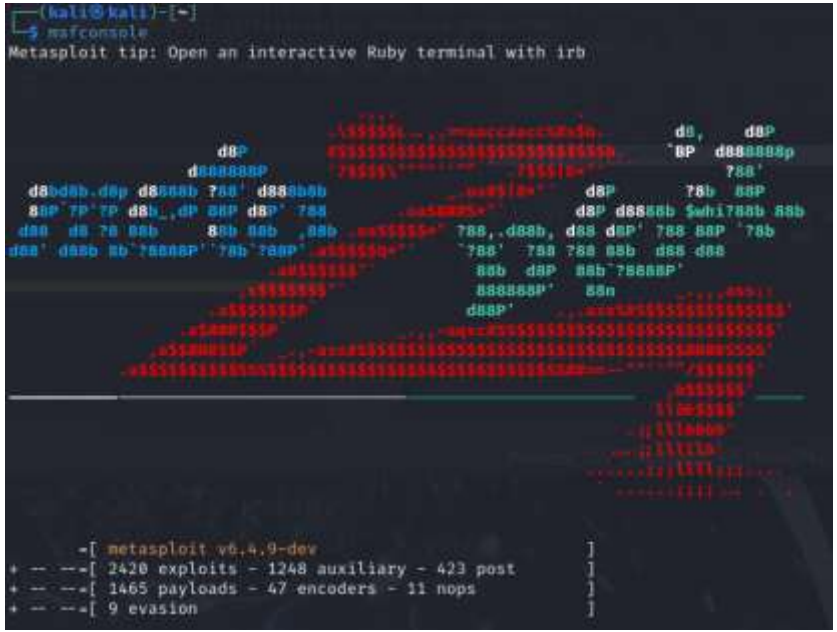
- 특징: 서비스내 취약점은 적은편, 주로 잘못된 설정으로 인해 취약점 발생
- 22번 포트를 주로 사용
- 평문으로 전송하는 FTP의 단점을 극복하기 위해 SFTP에 SSH가 사용됨

- 진단 관점: 사용자 인증, 이름 수집, 계정 정보 공격 대응 미흡, 오래된 버전 사용

SSH 프로빙


┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 22 172.31.167.0
Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-10 23:25 EDT
Nmap scan report for 172.31.167.0
Host is up (0.0083s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

SSH 취약점 진단


(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb
=[metasploit v6.4.9-dev]
+ -- --=[2420 exploits - 1248 auxiliary - 423 post]
+ -- --=[1465 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]

```
semsf6 > search ssh_enumuser

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers       .                normal  No     SSH Username Enumer
ation
   1    \_ action: Malformed Packet             .                .       .      Use a malformed pac
ket
   2    \_ action: Timing Attack                .                .       .      Use a timing attack


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/ss
h/ssh_enumusers
After interacting with a module you can manually set a ACTION with set ACTION 'Timing Attack'

msf6 >
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting          Required  Description
   ----          ---------------          --------  -----------
   CHECK_FALSE   true                     no        Check for false positives (random username)
   DB_ALL_USERS  false                    no        Add all users in the current database to the list
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        172.31.167.0             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         22                       yes       The target port
   THREADS       1                        yes       The number of concurrent threads (max one per host)
   THRESHOLD     10                       yes       Amount of seconds needed before a user is considered found (timing attack only)
   USERNAME                               no        Single username to test (username spray)
   USER_FILE     /home/kali/Desktop/top-  no        File containing usernames, one per line
                 usernames-shortlist.txt


Auxiliary action:

   Name              Description
   ----              -----------
   Malformed Packet  Use a malformed packet
```

http 취약점 진단부터...