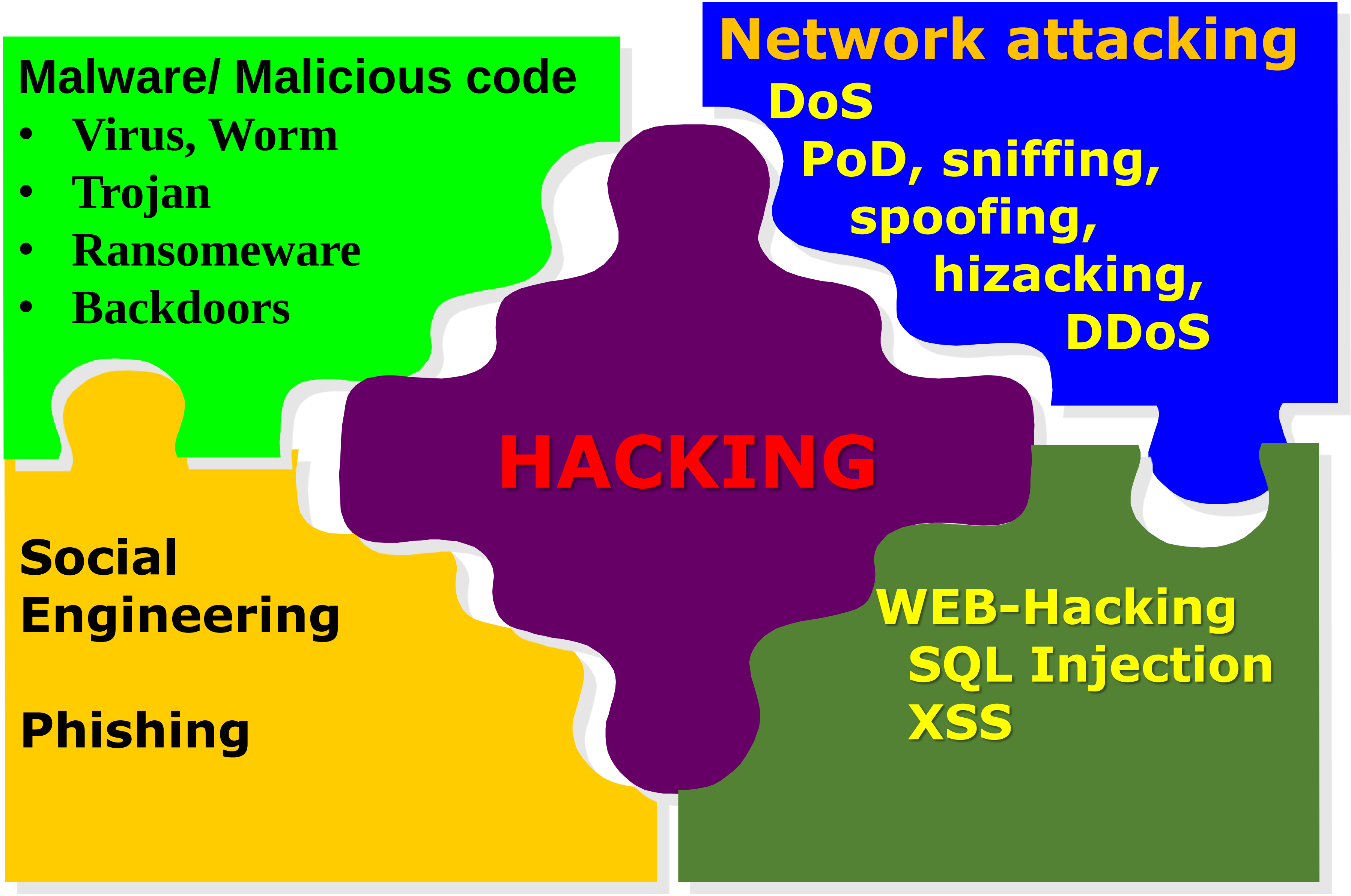
DoS(denial of service)

Map of attacking



Malware/ Malicious code

- Virus, Worm
- Trojan
- Ransomeware
- Backdoors

Network attacking

DoS

PoD, sniffing,

spoofing,

hizacking,

DDoS

HACKING

Social Engineering

Phishing

WEB-Hacking

SQL Injection

XSS

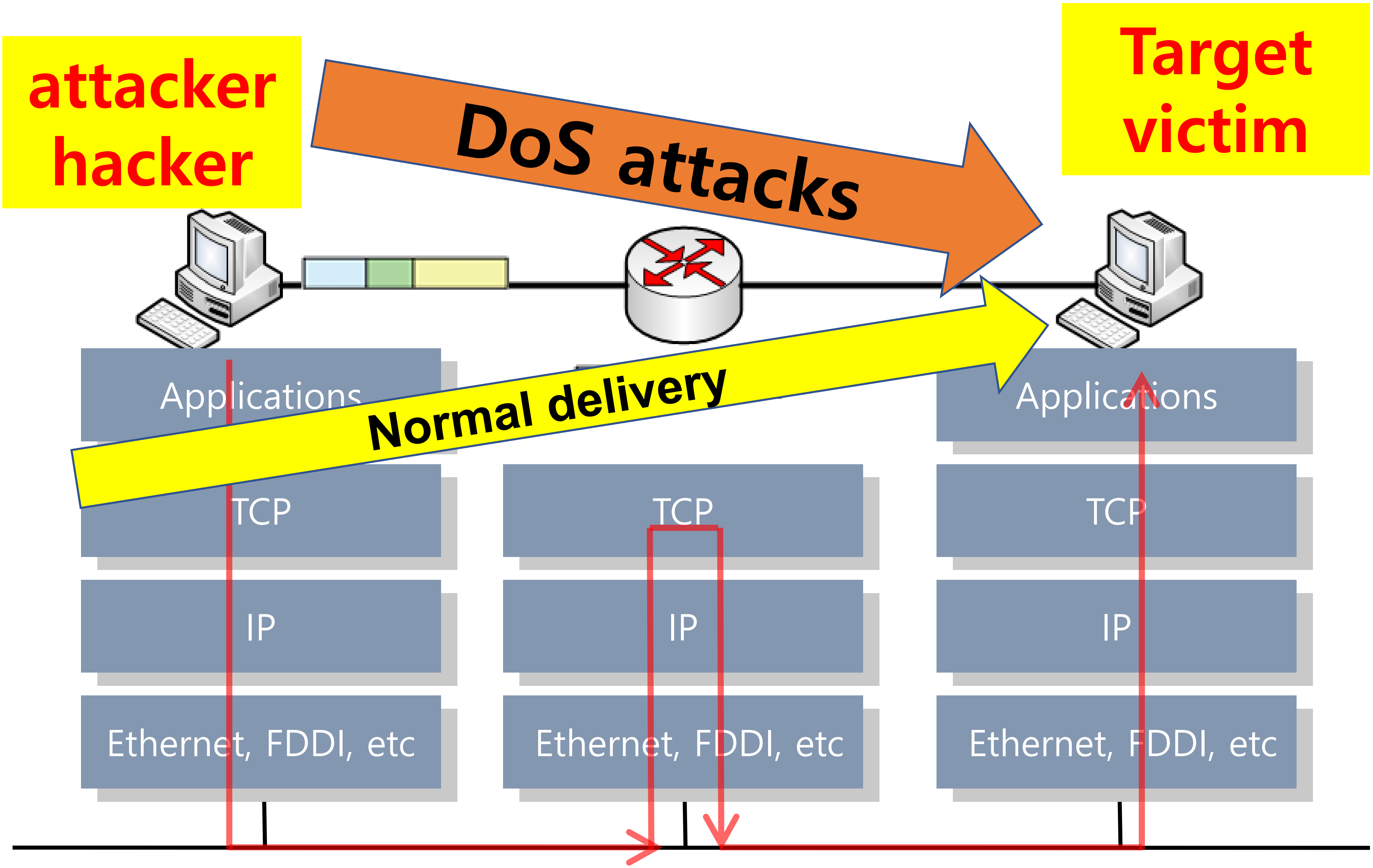
DoS(denial of service)

One of the biggist attacking tech.

to target server & network

with
big volume of traffics(packet)

Paket end-to-end delivery



Network hacking / attacking

3/4 layer DoS, DDoS

basic attacking

sniffing,

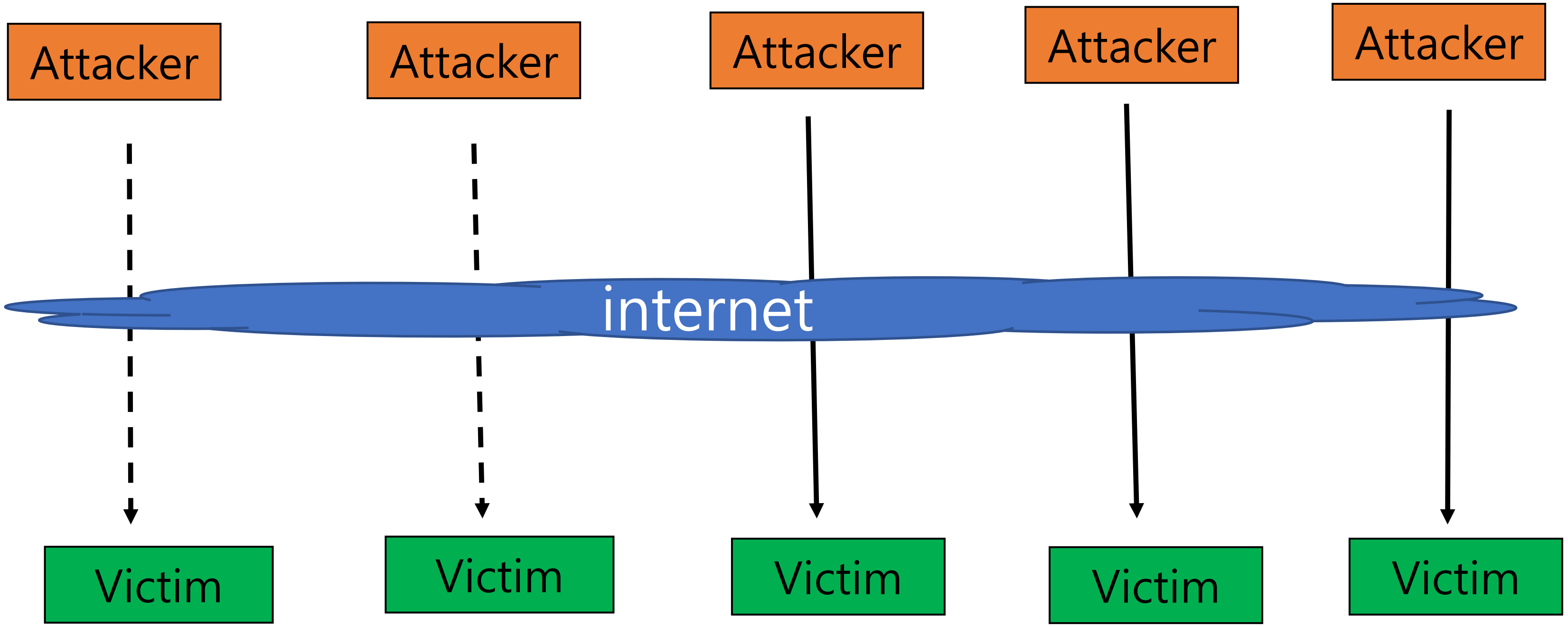
spoofing,

hizacking,

3/4 layer DoS

Tradi/tional DoS types

Ping of Death SYN Flooding Teardrop Land attack Smurf



General Methods of DoS attacks

The regular 3-way TCP\IP Handshake

1.Client----------SYN Packet-----------------→ Host

2.Host------------SYN\ACK Packet---------→ Client

3.Client-----------ACK Packet-----------------→ Host

- Limit of client connection
- limit of client waiting time

General Methods of DoS attacks

1. Flooding attacks

sends a request to connect to a server, but never completes the three way handshake.

Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

General Methods of DoS attacks

1. SYN flood

exceed the limits of three way handshake,
system resources

- LIMIT OF CLIENT CONNECTION

- LIMIT OF CLIENT WAITING TIME

General Methods of DoS attacks

Attacks target system & network with Big volume of traffics

1. **Flooding attacks => disturb three way handshake mechanism**
2. **Bu/ffer o/verflow attacks => over buffer limitation**
3. **ICMP flood => continuing to send ping packet**
4. **E/xploit vu/lnerabilities => attack weak point**

General Methods of DoS attacks

Each server has its **limit of client connection**, examples of types(can be changed)

•IIS	100,000
•Apache	150
•FPT	100

General Methods of DoS attacks

Waiting for an ACK packet in the ‘SYN Received’ state is ‘falling into the backlog’

Each server has its limit of client waiting time, examples of types, but can be changed

Examples of types, but can be changed

- Window 255 sec
- Apache 300 sec
- Unix/linux 60 sec

General Methods of DoS attacks

3. Buffer overflow attacks

- To send more traffic to a network address than the programmers have built the system to handle.

- It attacks exploit bugs specific to certain applications or networks

General Methods of DoS attacks

4.ICMP flood/known as the smurf attack

Sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine.

SW for DoS test / simulation

① Window CMD prompt

② Linux OS command

③ Python language

④ Python Scapy library

⑤ AI machine learning Python library

⑥ AI deep learning Python library

⑦ SW Tools

SW for blocking DoS

①Window CMD prompt

②Linux OS command

③Python language

④Python Scapy library

⑤AI machine learning Python library

⑥AI deep learning Python library

⑦SW Tools

What we learn for network security?

① How to attack target system ?

② How to detect the attacking ?

③ How to protect the attacking ?

④ How to monitor target system ?

DoS attacks methods are converted into DoS types

3/4 layer DoS types

To realize DoS attacks methods

hackers use following five types of tech. and skills trade/tionally

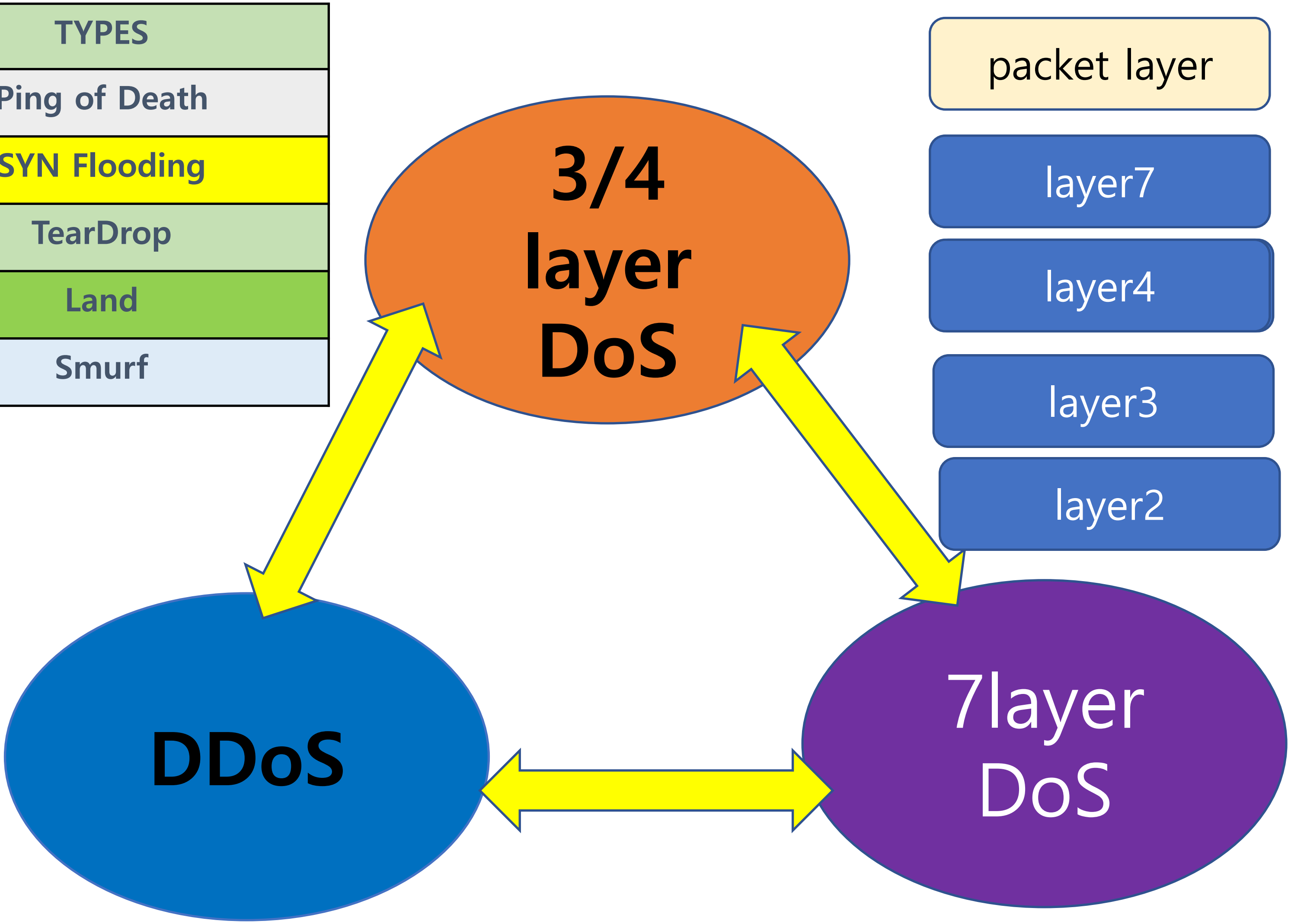
TYPES
Ping of Death
SYN Flooding
TearDrop
Land
Smurf

3/4 layer DoS types

TYPES	DESCRIPTION
Ping of Death	Sends ICMP packets with a size of 65,500 bytes
SYN Flooding	Sends only SYN packets, it occupies the limit number of SYN connection
TearDrop	The sequence number packet is tricked into overloading the sum
Land	Source IP address and destination IP address is same. Looping
Smurf	Broadcasts the ICMP Request packet to target whose source address has been changed

DoS attacking tech.evolution

TYPES
Ping of Death
SYN Flooding
TearDrop
Land
Smurf



Each type has it`s characters

1. Ping of Death => length of packet
2. SYN Flooding => number of packet
3. Teardrop => sequential number (repetitive requests and modifications)
4. Land attack => routing looping
5. Smurf => flooding to second victims

Site references

https://www.guru99.com/ultimate-guide-to-dos-attacks.html

Iptables Tutorial: Ultimate Guide to Linux Firewall (phoenixnap.com)

linux command to prevent dos attack by using netstat and iptables

SYN Flood Attacks- "How to protect?"- article - (hakin9.org)

https://vitux.com/how-to-block-allow-ping-using-iptables-in-ubuntu/

https://javapipe.com/blog/iptables-ddos-protection/