POSTECH

HEMOS
Hemos is Even More Open System

POSTECH DDoS 공격 대응 매뉴얼

학술정보처

정보기술팀

제•개정 이력

연번	일시	제•개정	비고
1	2015.12	제정	

목차

Ⅰ. 개요

1. 목적

1.25 인터넷 대란(2003), 7.7 DDoS공격(2009), 3.3 DDoS공격(2011) 등 분산 서비스거부 공격(이하 DDoS공격)으로 국가 주요기관 전산망이 공격을 받고 일부 홈페이지는 서비스가 중단되는 사태가 발생하였다. 또한, DDoS공격을 통해 특정 사이트를 대상으로 금품을 요구하는 사이버 범죄에 이용되기도 한다.

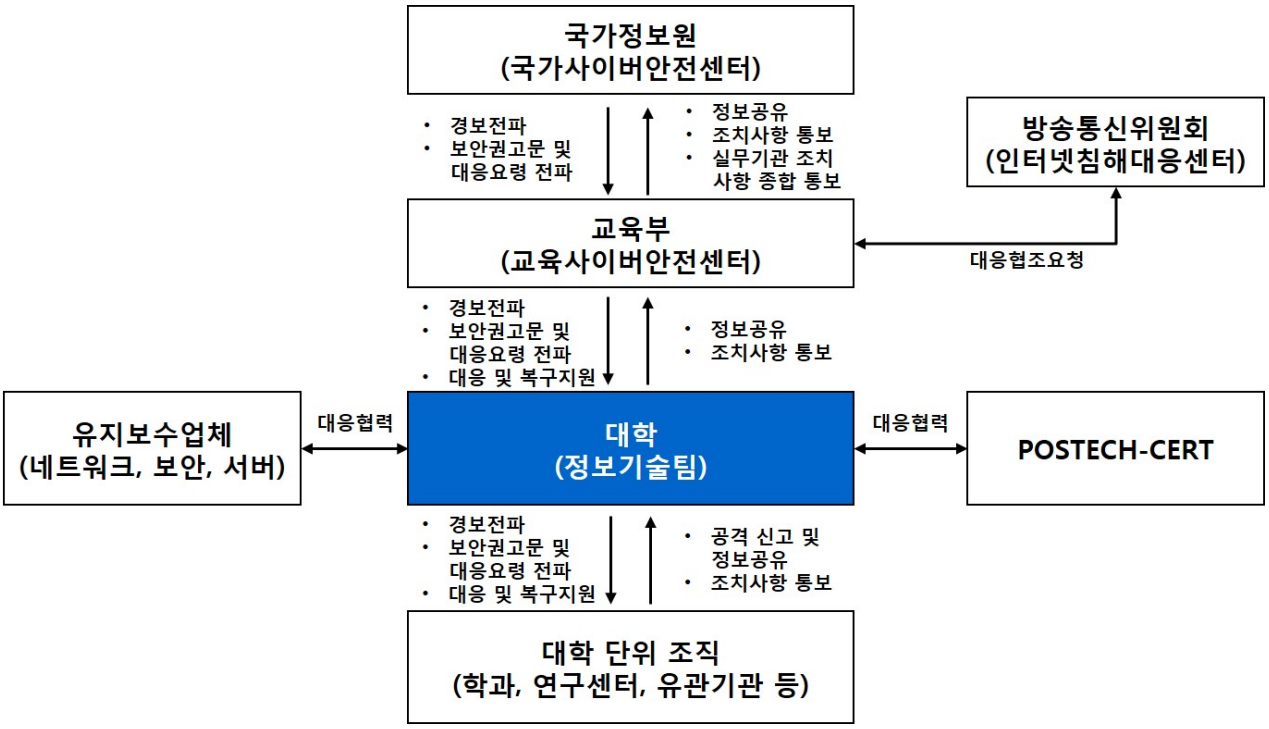
이에 우리대학도 DDoS공격의 대상이 될 수 있어 공격으로 인한 혼란을 방지하고 교육, 연구를 원활하게 수행할 수 있도록 대학 전산망 운용 환경에 적합한 DDoS 공격 대응 매뉴얼을 마련하여 DDoS 공격에 따른 피해를 최소화하고자 한다.

2. DDoS 공격 정의

DDoS(Distributed Denial of Service, 분산 서비스거부 공격) 공격이란 해커가 사전에 악성코드에 감염된 대량의 좀비PC에 공격지령을 내려, 일제히 특정 사이트 및 시스템을 공격하도록 하여 과부하를 유발시킴으로써 정상적인 서비스를 할 수 없도록 만드는 것이다.

Ⅱ. DDoS 공격 대응 체계

1. 대학 DDoS 공격 대응 체계



2. DDoS 공격 대응 절차 및 목적

(1 단계) 공격 인지를 위한 체크 포인트 – 웹서비스 관련 이벤트 발생 시 해당 원인이 DDoS 공격으로 인한 것인지에 대한 명확한 판단이 필요

(2 단계) DDoS 공격 유형 파악 – DDoS 공격 유형을 명확히 파악하여 차단정책 설정을 위한 근거로 활용

(3 단계) 공격유형에 따른 차단정책 정의 및 대응 – 공격의 유형과 목적을 명확히 판단하여 차단정책을 설정함으로써 웹서비스의 가용성 확보

(4 단계) 공격 대응 후, 사후조치 – 공격트래픽 분석을 통해 공격 내용을 상세히 규명함으로써 추가 발생할 수 있는 공격 대비를 위해 정책을 업데이트하고 좀비 PC IP 를 확보

Ⅲ. 세부 DDoS 공격 대응 절차

1. (1단계) 공격의 인지 – 공격여부 Check Point

가. 유입 트래픽 크기

- 방화벽, IDS 등의 네트워크 장비를 통해 웹서비스 운영 망으로 유입되는 트래픽의 BPS와 PPS 규모를 확인하여 평시와 비교
- 유입 트래픽의 크기가 비정상적인 증감을 나타내는 경우, 공격 발생 여부를 의심할 수 있음

나. 웹서버 접속 로그

- 서버의 접속 로그를 확인하여 비정상 접속 증가여부 확인

다. 동시접속 정보

- 웹서버와 클라이언트가 유지하고 있는 연결 규모를 확인하여 평시대비 증감률 비교

2. (2단계) DDoS 공격유형 파악

1. Incoming traffic을 수집할 수 있는 경우

A. 패킷 덤프(Packet Dump)를 이용한 유입 트래픽 확보

- tcpdump와 같은 트래픽 캡쳐 툴을 이용하여 분석하고자 하는 기간 동안의 유입 트래픽 일부를 PCAP 형태로 저장

※ PCAP: Packet CAPture의 약자로 네트워크 패킷을 파일로 저장한 것을 의미

B. 확보된 트래픽 분석

- DDoS 공격 특징을 파악하기 위해서는 프로토콜 정보, HTTP 헤더 정보, 연결 정보를 확인해야 함

C. 시나리오 기반(Scenario Drawn)의 공격유형 파악

- 대역폭 소진공격, DB 부하 유발공격, 웹서버 자원 공격 등 대표적인 DDoS 공격 유형을 파악

2. Incoming traffic을 수집할 수 없는 경우

A. 웹서버 접속 로그

- 서버 접속로그를 확인하여 접속자의 요청 페이지에 대한 통계와 특정 시간동안 발생되는 요청 횟수에 대한 통계를 확인

3. (3단계) 공격유형에 따른 차단정책 정의 및 대응

가. 대역폭 소진 공격 대응 방안

- 공격 유형: UDP Flooding, ICMP Flooding
- 대응 방안: 웹서버 망을 보호하는 방화벽이나 웹서버망 상단에 위치한 라우터에서 해당 프로토콜을 차단하도록 ACL설정

나. 대역폭 소진 공격 대응 방안

- 공격 유형: TCP Flooding
- 대응 방안: 대용량 TCP Flooding 공격은 프로토콜 기준으로 차단하는데 한계가 있어 소스 IP별로 pps 임계치를 설정

다. 웹서버 자원 소모 공격 대응 방안

- 공격 유형: Syn(Ack/Fin) Flooding
- 대응 방안: 웹서버 OS의 TCP 스택(stack) 자원을 소모하는 특징이 있으므로 ①소스IP별로 PPS 임계치를 설정하거나 ②패킷 헤더검사를 통해 정상적인 옵션 필드값을 가지지 않는 비정상 패킷 차단

라. DB Connection 부하유발 공격 대응 방안

- 공격 유형: Get Flooding, Post Flooding
- 대응 방안: 다량의 HTTP 요청으로 웹서버와 DB연동에 부하를 유발시키는 것이 특징으로 ①클라이언트로부터의 요청 수에 대한 임계치를 설정하여 임계치를 초과하는 소스 IP의 접속을 차단하거나 ②HTTP헤더를 확인하여 HTTP표준에 맞지 않는 필드 값을 차단하는 시그니처(Signature)로 설정

마. 웹서버 자원 소모 공격 대응 방안

- 공격 유형: Slow Header Flooding, Slow Data Flooding
- 대응 방안: 완료되지 않은 연결(Connection) 상태를 지속적으로 유지하는 공격이므로 하나의 요청에 대한 연결 타임아웃을 설정하여 특정 타임아웃이 지나면 연결을 종료시켜 차단

바. 봇 vs 브라우저 식별 대응 방안

- 대응 방안 : 일반적인 봇은 브라우저와 달리 웹서버의 응답코드에 반응하여 행동하지 않으므로 웹서버에서 302 moved temporary와 같은 코드로 응답하여 봇이 발생시키는 요청을 차단

4. (4단계) 공격 대응 후, 사후 조치

가. 공격 시점의 BPS, PPS, CPS 변화 추이 확인

- 공격 규모를 확인하여 웹서버의 가용성이 침해될 수 있는 지점을 확인하여 정확한 분석정보가 반영된 차단정책 업데이트

나. 공격 유형 확인

- 프로토콜에 대한 통계, 패킷 크기에 대한 통계, 요청 형태에 대한 통계를 상세히 확인하여 시간에 따른 공격 유형의 변경 여부 또는 복합공격 여부를 확인하여 차단 정책 업데이트

다. HTTP 요청 패킷 형태 확인

- ①특정 시간대의 HTTP 요청 횟수(Count)를 확인하여 비정상적인 행위여부를 규명하고 ②HTTP 헤더의 각 필드 정보를 조사하여, HTTP표준을 준수하지 않는 비정상 메시지를 차단할 수 있도록 차단정책 업데이트

라. 좀비PC IP 확보

- TCP 기반의 웹서버 가용성 마비 공격은 TCP 3중 연결(3-Way HandShaking) 완료와 함께 시작하므로 실제 공격 IP를 확보하여 차단하도록 조치

※ 웹서버 가용성 마비 공격에는 GET(POST) Flooding, Slow header(data) Flooding이 있음

※ 대역폭 소진 공격의 경우, 공격자는 대부분 Source IP를 위조하므로 IP 위변조 여부를 반드시 확인해야 함

[별첨1] DDoS 공격 대응 시나리오

1. 공격의 인지 – 공격여부 Check Point

웹서비스 관련 이벤트 발생 시 해당 원인이 DDoS 공격으로 인한 것인지에 대한 명확한 판단을 하기 위해 유입 트래픽 크기, 웹서버 접속로그, 동시접속 정보, 유입 트래픽 샘플링 작업을 수행한다.

구분	상세내용	이행 방안
유입 트래픽 크기 확인	- 네트워크 장비를 통해 유입되는 트래픽의 BPS와 PPS 규모를 확인하여 평시와 비교 - 유입 트래픽의 크기가 비정상적인 증감을 나타내는 경우, 공격 발생 여부를 의심할 수 있음 - 확인 가능 장비 . 네트워크: 라우터, Core스위치 . 보안: IPS, QoS, UTM	유입 트래픽 크기를 아래와 같이 해당 장비에서 확인 1. 네트워크 (네트워크 담당자 수행) 라우터, Core스위치 CLI상에서 BPS, PPS 확인 2. 보안 (보안 담당자 수행) IPS, QoS, UTM 장비의 GUI에서 BPS, PPS 확인
웹서버 접속로그 확인	- 서버의 접속 로그를 확인하여 비정상 접속 증가여부 확인 - 확인 가능 장비 . 웹서버	웹서버 접속로그를 아래와 같이 확인 (서버 관리자 수행) 1. Linux 계열(Apache 기준) - 로그파일 경로: /usr/local/apache/conf 또는 /var/log/httpd - 로그 파일명: access_log 2. Windows 계열(IIS 기준) - 로그파일 경로: Windows₩System32₩LogFiles₩inetpub₩logs₩LogFiles - 로그 파일명: u_ex151001.log
동시접속 정보 확인	- 웹서버와 클라이언트가 유지하고 있는 연결(Connection) 규모를 확인하여 평시대비 증감률 비교 - 확인 가능 장비 . 보안: QoS, UTM, POVIS방화벽	동시접속 정보를 아래와 같이 해당 장비에서 확인 1. 보안 장비 (보안 담당자 수행) QoS, UTM, POVIS방화벽 GUI에서 연결 정보 확인

2. DDoS 공격유형 파악

DDoS 공격여부가 확인되면 유입 트래픽을 확보하고 분석하여 명확한 공격유형을 파악한 후, 차단정책 설정을 위한 근거로 활용

<table>
<tr><th>구분</th><th>상세내용</th><th>이행 방안</th></tr>
<tr><td>유입 트래픽 확보</td><td>- 패킷덤프(Packet Dump)를 이용한 유입 트래픽 확보
- Tcpdump와 같은 트래픽 캡쳐 툴을 이용하여 분석하고자 하는 기간 동안의 유입 트래픽 일부를 PCAP형태로 저장
- 확인 가능 장비
. 보안: IPS, QoS, UTM
. 서버: 해당 웹서버</td><td>유입 트래픽을 아래와 같이 해당 장비에서 확보
1. 보안 (보안 담당자 수행)
- IPS, UTM 장비에서 tcpdump명령어를 이용해 트래픽 캡쳐
명령어: tcpdump –nni eth0 host 192.0.0.1 and port 80
2. 서버 (서버 관리자 수행)
- 웹서버에서 tcpdump명령어(Linux계역) 또는 Wireshark툴 (Windows계열)을 이용해 트래픽 캡쳐</td></tr>
<tr><td>확보 트래픽 분석</td><td>- DDoS공격 특징을 파악하기 위해서는 프로토콜 정보, HTTP헤더 정보, 연결 정보를 확인해야 함
- 확보된 트래픽을 아래의 분석 도구를 이용하여 정보 확인
<table>
<tr><th>분석도구</th><th>설명</th></tr>
<tr><td>tcpdstat</td><td>프로토콜 종류 등에 관한 정보 확인</td></tr>
<tr><td>ngrep, httpry</td><td>http header에 과한 정보 확인</td></tr>
</table>
※ 해당 분석도구는 Linux계열 서버에 libpcap라이브러리와 같이 설치되어야 함</td><td>분석도구를 이용한 트래픽 분석은 아래와 같이 진행
(보안 담당자 및 서버 관리자 수행)
<table>
<tr><th>tcpdstat툴</th></tr>
<tr><td>명령어: tcpdstat 캡처파일.pcap
확인사항: 평균/최대 트래픽, 사용 중인 프로토콜, 프로토콜별 사용량</td></tr>
<tr><th>ngrep툴</th></tr>
<tr><td>명령어: ngrep 캡처파일.pcap –tW byline | grep GET | sort | uniq –c | sort -rn
확인사항: Header의 내용 중 특정 문자열을 검색하여 호출 횟수가 많은 URL에 대한 분석</td></tr>
<tr><td>명령어: ngrep 캡처파일.pcap | grep 141.223.x.x | awk ‘{print $2}’ | sort | uniq –c | sort –rn
확인사항: Header의 내용 중 특정 문자열을 검색하여 연결 횟수가 많은 IP에 대한 행위 분석</td></tr>
</table></td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>httpry툴
명령어: httpry –r 캡처파일.pcap | awk '{print $4}' | sort | uniq –c | sort -rn</td>
</tr>
<tr>
<td>공격 유형 파악</td>
<td>- 트래픽 분석을 통해 DDoS공격의 유형을 파악
<table>
<tr><th>분석도구</th><th>설명</th></tr>
<tr><td>tcpdstat</td><td>- 대역폭 소진 공격 유형 분석을 위해 UDP/ICMP Flooding 여부 등 프로토콜 분포와 트래픽 규모 확인</td></tr>
<tr><td>ngrep, httpry</td><td>- Get Flooding 등 DB Connection 부하유발 공격 유형 확인
- 접속자의 요청 페이지(Request Page)에 대한 통계와 특정 시간 동안 발생되는 요청 횟수에 대한 통계를 확인</td></tr>
</table>
※ DDoS공격 유형표 참조</td>
<td>※ 이행 방안은 [별첨2. DDoS공격 유형 및 대응방안] 참조</td>
</tr>
<tr>
<td>[트래픽 확보가 어려운 경우]
웹서버 접속 로그 확인</td>
<td>- 서버의 접속 로그를 확인하여 비정상 접속 증가여부 확인
- 확인 가능 장비
. 웹서버</td>
<td>웹서버 접속로그를 아래와 같이 확인
(서버 관리자 수행)
1. Linux 계열(Apache 기준)
- 로그파일 경로: /usr/local/apache/conf 또는 /var/log/httpd
- 로그 파일명: access_log
2. Windows 계열(IIS 기준)
- 로그파일 경로: Windows₩System32₩LogFiles₩inetpub₩logs₩LogFiles
- 로그 파일명: u_ex151001.log</td>
</tr>
</table>

3. 공격유형에 따른 차단정책 정의 및 대응

※ 공격유형에 따른 대응 내용은 [별첨2. DDoS 공격 유형 및 대응방안] 참조

4. 공격 대응 후, 사후조치

DDoS 공격 대응 후 대학 네트워크 상의 BPS, PPS, CPS 변화 추이를 확인하고 추가적인 조치를 위한 정보를 확보

가. 공격 시점의 BPS, PPS, CPS 변화 추이 확인

공격 규모를 확인하여 웹서버의 가용성이 침해될 수 있는 지점을 확인하여 정확한 분석정보가 반영된 차단정책 업데이트

나. 공격 유형 확인

프로토콜에 대한 통계, 패킷 크기에 대한 통계, 요청 형태에 대한 통계를 상세히 확인하여 시간에 따른 공격 유형의 변경 여부 또는 복합공격 여부를 확인하여 차단정책 업데이트

다. HTTP 요청 패킷 형태 확인

①특정 시간대의 HTTP 요청 횟수(Count)를 확인하여 비정상적인 행위 여부를 규명하고 ②HTTP 헤더의 각 필드 정보를 조사하여, HTTP표준을 준수하지 않는 비정상 메시지를 차단할 수 있도록 차단정책 업데이트

라. 좀비PC IP 확보

TCP 기반의 웹서버 가용성 마비 공격은 TCP 3중 연결(3-Way HandShaking) 완료와 함께 시작하므로 실제 공격 IP를 확보하여 차단하도록 조치

[별첨2] DDoS 공격 유형 및 대응 방안

구분		세부 공격항목	공격 방법	공격 확인 방법	대응 방법
대역폭 소진공격	UDP/ICMP Traffic Flooding 공격	UDP/ICMP Flooding	공격자는 다량의 UDP/ICMP 패킷을 서버로 전송하여 서버가 보유한 네트워크 대역폭을 가득 채워 다른 정상적인 클라이언트의 접속을 원활하지 못하도록 유발시키는 공격임 ※ UDP/ICMP 프로토콜이 비연결지향이라는 특징을 이용하여 소스 IP 를 변조함	1. 장비 - 네트워크: 라우터, core 스위치에서 UDP/ICMP 트래픽 변화 확인 - 보안: IPS, QoS, UTM 장비에서 UDP/ICMP 트래픽 변화 확인 2. tcpdstat 툴 - 확보된 유입 트래픽에서 UDP/ICMP 트래픽 확인	방안 1) ISP 업체에 요청하여 대상 IP 주소에 대한 트래픽 임시 차단 방안 2) ACL 설정 또는 블랙홀 라우팅을 이용한 임시 차단 - 웹서버 or 운영 장비 : UDP/ICMP 트래픽 DROP 설정 - 라우터: Null 라우팅을 통해 공격 트래픽을 가상 인터페이스로 라우팅 방안 3) Inbound 패킷에 대한 임계치 설정을 이용한 차단 - 운영 장비 : Inbound 패킷 임계치 설정
		DNS Query Flooding	공격자는 UDP 프로토콜 기반의 서비스를 제공하는 DNS 에 대해 DNS 쿼리 데이터를 다량으로 서버에 전송하여 DNS 의 정상적인 서비스를 방해하는 공격임 ※ UDP/ICMP Flooding 공격 형태와 유사함	1. 장비 - 네트워크: 라우터, core 스위치에서 UDP/ICMP 트래픽 변화 확인 - 보안: IPS, QoS, UTM 장비에서 UDP/ICMP 트래픽 변화 확인 2. tcpdstat 툴 - 확보된 유입 트래픽에서 UDP(DNS) 트래픽 확인	※ UDP/ICMP Flooding 공격의 대응 방법과 같이 실시 방안 1) DNS 서버의 다중화를 통한 DNS 공격 트래픽 분산 처리(가상화 서버 활용) 방안 2) IPTABLE 을 이용한 ACL 기반의 차단 - DNS Query 가 512Byte 이상일 경우 해당 패킷 차단
	TCP Traffic Flooding 공격	SYN Flooding	공격자는 다량의 SYN 패킷을 서버로 전달하여 서버의 대기큐(Backlog Queue)를 가득채워 새로운 클라이언트의 연결요청을	1. 장비 - 보안: IPS, UTM 장비에서 TCP 세션 상태 확인 2. 서버 (netstat)	방안 1) 임계치 기반의 SYN Flooding 차단 - 방화벽 : IP 당 SYN 요청에 대한 PPS 임계치 설정 방안 2) First SYN Drop (Spoofed) 설정에 의한

			무시하도록 하여 장애를 유발시키는 공격 ※ TCP 프로토콜이 데이터를 보내기 전에 연결을 먼저 맺어야 하는 특징을 이용한 방법임	- 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인 ※평시보다 established 세션이 급격하게 증가	차단 - 방화벽 : 첫번째 SYN 을 Drop 하여 재요청 패킷 도달 확인
		TCP Flag Flooding	TCP 의 Flag 값을 임의로 조작하면 SYN, ACK, FIN, RST 과 같이 여러 형태의 패킷을 생성할 수 있으며, 서버는 이러한 패킷을 수신하는 경우 해당 패킷을 검증하기 때문에 서버의 자원을 소진시킴	1. 장비 - 보안: IPS, UTM 장비에서 TCP 세션 상태 확인 2. 서버 (netstat) - 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인 ※평시보다 established 세션이 급격하게 증가	방안 1) 임계치 기반의 동일 IP 주소에 대한 동시 접속 차단 - 방화벽 : IP 당 동시 접속 임계치 설정
		TCP Session	TCP 3-Way Handshake 과정을 과도하게 유발함으로써 서비스의 과부하를 유발하는 공격	1. 장비 - 보안: IPS, UTM 장비에서 TCP 세션 상태 확인 2. 서버 (netstat) - 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인	방안 1) L7 스위치의 임계치 설정 기능을 이용한 차단(POVIS 대상 공격에 한함) - L7 스위치 : IP 당 Connection Limit 을 설정하여 차단
서비스 마비공격	HTTP Traffic Flooding 공격	Get Flooding	공격자는 동일한 URL(예:a.com/index.jsp)을 반복 요청하여 웹서버가 URL 에 해당되는 데이터를 클라이언트에게 회신하기 위해 서버 자원을 사용하도록 하는 공격임 ※ 웹서버는 한정된 HTTP 처리 Connection 용량을 가지기 때문에	1. 장비 - 보안: IPS, QoS, UTM 장비에서 웹서비스 트래픽 상태 확인 2. ngrep, httpry - 확보된 유입 트래픽에서 GET 문자열을 가진 항목 확인 - 요청이 많은 URL 및 IP 에 대하여 확인	방안 1) 콘텐츠 요청 횟수에 대한 임계치 설정에 의한 차단 - L7 스위치 : 콘텐츠마다 요청할 수 있는 횟수에 임계치 설정 방안 2) 방화벽에 캐싱공격 문자열을 포함한 IP 차단 - 방화벽 : 트래픽 분석하여 캐싱 공격에

			용량 초과시 정상적인 서비스가 어려워짐	3. 서버 - 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인 - 서버 로그에서 다수의 IP 에서 비정상적인 URL 로 접속이 다량 존재	해당하는 문자열을 포함하는 경우, 해당 IP 를 방화벽에서 차단 설정
		GET Flooding with Cache-Control (CC Attack)	o 일반적으로 웹서버의 부하를 감소시키기 위해 캐싱서버를 운영하여 많이 요청받는 데이터(예:사진파일)는 웹서버가 아닌 캐싱서버를 통해 응답하도록 구축하는 경우, o 공격자는 HTTP 메시지의 캐시 옵션을 조작하여 캐싱서버가 아닌 웹서버가 직접 처리하도록 유도하여 캐싱서버의 기능을 무력화하고 웹서버의 자원을 소진시키는 공격임	1. 장비 - 보안: IPS, QoS, UTM 장비에서 웹서비스 트래픽 상태 확인 2. ngrep, httpry - 확보된 유입 트래픽에서 GET 문자열을 가진 항목 확인 - 'Cache-Control:no-cache, no-store'문자열 다수 존재 3. 서버 - 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인 - 서버 로그에서 'Cache-Control:no-cache, no-store'문자열 다수 존재	방안 1) 방화벽에 캐싱공격 문자열을 포함한 IP 차단 - 방화벽 : 트래픽 분석하여 캐싱 공격에 해당하는 문자열을 포함하는 경우, 해당 IP 를 방화벽에서 차단 설정 방안 2) L7 스위치를 이용한 캐싱 공격 차단 - L7 스위치 : HTTP Header 의 Cache-Control 에 특정 문자열을 포함하는 경우 해당 IP 접속 차단 설정
	HTTP Header/Option Spoofing Flooding 공격	Slow HTTP POST DoS	공격자는 HTTP POST 지시자를 이용하여 서버로 전달할 대량의 데이터를 장시간에 걸쳐 분할 전송하며, 서버는 POST 데이터가 모두 수신하지 않았다고 판단하여 연결을 장시간 유지하므로 가용량을	1. 장비 - 보안: IPS, QoS, UTM 장비에서 웹서비스 트래픽 상태 확인 2. ngrep, httpry - 확보된 유입 트래픽에서 POST 문자열을 가진 항목 확인 3. 서버	방안 1) 접속 임계치 설정을 통한 차단 - 서버 : iptables 에서 특정 IP 에서 연결할 수 있는 동시 접속수에 임계치 설정 방안 2) Connection Timeout 과 Keepalivetimeout 설정을 통한 차단 - 방화벽/웹서버 : Connection Timeout 에 설정된 시간동안 Client 와 웹서버 사이에

			소비하게 되어 다른 클라이언트의 정상적인 서비스를 방해함	- 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인 - 서버 로그에서 다수의 IP 에서 비정상적인 URL 로 접속이 다량 존재	데이터 이동이 전혀 없을 경우 Connection 을 종료하도록 설정 방안 3) RequestReadTimeout 설정을 통한 차단 - 웹서버 : 아파치의 RequestReadTimeout 기능을 이용하여 차단
		Slow HTTP Header DoS (Slowloris)	공격자는 서버로 전달할 HTTP 메시지의 Header 정보를 비정상적으로 조작하여 웹서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 가용량을 소비시킴으로 다른 클라이언트의 정상적인 서비스를 방해함	1. 장비 - 보안: IPS, QoS, UTM 장비에서 웹서비스 트래픽 상태 확인 2. ngrep, httpry - 확보된 유입 트래픽에서 Header 끝이 /0d0a0d0a/ 끝나지 않음 3. 서버 - 웹서버의 CPU 확인, netstat 명령으로 TCP 세션 상태 확인	방안 1) 접속 임계치 설정을 통한 차단 - 서버 : iptables 에서 특정 IP 에서 연결할 수 있는 동시 접속수에 임계치 설정 방안 2) Connection Timeout 과 Keepalivetimeout 설정을 통한 차단 - 방화벽/웹서버 : Connection Timeout 에 설정된 시간동안 Client 와 웹서버 사이에 데이터 이동이 전혀 없을 경우 Connection 을 종료하도록 설정 방안 3) RequestReadTimeout 설정을 통한 차단 - 웹서버 : 아파치의 RequestReadTimeout 기능을 이용하여 차단