DoS 타켓의 자원을 고갈시키거나 네트워크 대역폭을 초과시켜 서비스를 제공하지 못하게 함.

DDoS 여러 대의 컴퓨터가 동시에 한 타겟 컴퓨터를 집중 공격. 보통 좀비 컴퓨터를 사용하여 다량의 트래픽을 일으킴. Volume based(3계층), state-exhaustion(4계층), application layer(7계층) 공격으로 나뉨.

- SYN flood: 3way handshaking을 악용. 타겟 서버에 연결을 요청하는 SYN을 전송. 타겟은 SYN/ACK로 응답한 후 연결 요청 정보를 backlog queue에 저장. 하지만 공격자는 ACK를 발송하지 않고 연결 요청만 지속적으로 보내기 때문에 결국 backlog queue 자원 고갈로 다른 연결 요청을 저장할 수 없게 됨.

  탐지 방법: 일정 시간 내에 SYN을 보내 연결 요청을 하곤 ACK를 보내지 않은 패킷의 수를 파악해서 공격 인정 횟수 이상인지 확인.

  대응: backlog queue의 크기 증대. 연결 요청 정보를 backlog queue에 저장하지 않고 쿠키에 저장. 동일 ip에 대한 연결 요청 임계치 설정. 연결 요청 대기 시간 단축.

- icmp flood: 공격 대상 서버에 대량의 icmp 요청을 보내어 피해자 서버가 요청을 받고 응답하는 데 모든 대역폭을 소모하게 함.

  탐지 방법: 일정 시간 내 icmp 패킷의 수를 파악해 공격 횟수 이상인지 확인.

  대응: direct broadcast 패킷 차단. 다량의 동일한 icmp echo reply 패킷 차단.

- Ping of Death: ping을 보낼 때 패킷의 크기를 최대로 해서 전송. 패킷이 여러 개로 쪼개져서 전송됨. 타겟이 쪼개진 패킷을 재조합하는 과정에서 buffer overflow 발생.

  탐지 방법: icmp 패킷의 데이터 크기를 확인.

  대응: Ping의 길이를 제한.

- NTP Amplification: NTP는 네트워크에 연결된 컴퓨터의 시간 동기화에 사용됨. 공격자는 패킷을 위조해 소스 ip를 공격 타겟으로 설정하여 NTP 서버에 monlist 요청을 전송. Monlist는 시간 동기화를 요청한 ip 목록 출력 기능. NTP 서버는 요청에 대한 응답을 피해자 서버로 전송함. NTP 서버의 응답은 공격자가 보낸 요청보다 1:20, 1:200의 비율로 증폭될 수 있어 공격 효율을 높일 수 있음.

  탐지 방법: 소스 ip가 위조되었는지 확인. NTP는 UDP 123 포트를 사용하기 때문에 123포트에서 전송되는 패킷 확인.

  대응: monlist 명령을 활용하지 않는 NTP 버전 사용.

- HTTP flood: 공격 대상 웹사이트에 HTTP GET, POST 요청을 대량으로 전송. 피해자 서버가

응답을 하여도 공격자는 응답하지 않고 연결을 유지하여 피해자 서버의 리소스를 소모시킴.

탐지 방법: 일정 시간 내 포트가 80, TCP 프로토콜을 사용하는 GET, POST 요청 수를 파악해 공격 횟수 이상인지 확인.

대응: WAF 사용

DRDoS 출발지 IP를 피해자의 IP로 spoofing한 SYN 패킷을 반사 서버로 대량 전송. 반사 서버가 피해자에게 SYN ACK를 대량으로 보내 피해자를 다운시킴.

CDoS Cloud DoS. 클라우드 상에서의 DoS 공격. 클라우드는 자원을 사용하는 대신 그에 따른 요금을 지불하는 서비스. 클라우드에 DDoS 공격이 발생하면 공격으로 인해 자원을 소모하게 되면서 지불해야 할 요금이 대폭 증가하는 경제적 손실이 발생할 것으로 예상됨.

도스 디도스 디알도스 공격 설명과 유형 https://blog.naver.com/leehyo85/222918337886

도스 디도스 공격 설명과 유형

https://ja-gamma.tistory.com/entry/DoSDDoS%EA%B3%B5%EA%B2%A9%EA%B0%9C%EB%85%90%EC%A2%85%EB%A5%98

도스, 디도스 공격 유형 별 탐지 방법

https://blog.naver.com/itexpert2007/30034352583

보안뉴스, kisa 디도스 공격 유형과 대응 방안

https://www.boannews.com/media/view.asp?idx=82852

Cloud-based DDoS Attacks and Defenses

https://arxiv.org/ftp/arxiv/papers/1511/1511.08839.pdf

https://www.stormit.cloud/blog/cloud-ddos-protection-how-to-mitigate-all-risks/

cdos

https://www.indusface.com/blog/understanding-cloud-ddos-attacks-and-cloud-based-ddos-protection/