1. 도입
   1. 서비스 거부 공격(DoS)
      1. 가장 일반적인 유형의 공격 중 하나
      2. 서비스를 접근할 수 있는 사용자를 서비스에 접근하지 못하도록 함
      3. 단일 호스트가 공격 -> DoS
      4. 여러 호스트가 동시에 공격 -> DDoS
   2. 컴퓨터 -> 물리적 제한이 존재
      1. 사용자 수
      2. 파일의 크기
      3. 전송 속도
      4. 저장된 자료의 양
   3. 위의 제한 중 하나를 초과하면 컴퓨터 응답X
   4. 공격자는 공격 대상 네트워크에 엄청 큰 트래픽(정상적인 작동이 안될 만큼)을 보내 공격 대상자에 대한 엑세스를 막음.
2. 개요
   1. DoS에 사용되는 툴의 기능
      1. 다양한 프로토콜에서 작동 가능
      2. 통신이 암호화됨
      3. 트래픽에서 통신을 숨길 수 있다
   2. Dos 약점
      1. 트래픽이 넘치는 행위가 계속되어야 함.
      2. 바이러스가 제거된다면 공격은 멈추게 됨.
      3. 공격자의 컴퓨터가 발견될 위험이 있다.
3. DoS공격
   1. TCP SYN Flood 공격
      1. TCP통신
         1. 3 Way HandShake
            1. 먼저 처음 호스트A(통신을 하고하는 호스트)가 호스트B(호스트A와 통신하는 호스트)에게 SYN패킷을 보냄
            2. 호스트B는 SYN + ACK 패킷을 호스트A에게 보냄
            3. 호스트A는 호스트B에 ACK 패킷을 전송
            4. SYN – 통신 시작 시 연결 요청하는 패킷
            5. ACK – SYN에 대한 확인의 의미
      2. 공격자는 공격대상에게 SYN 패킷을 전송
      3. 공격대상은 SYN + ACK 패킷을 보내고 그러한 정보 버퍼에 저장, ACK이 오기를 기다림.
      4. 공격자 의도적으로 SYN만 보냄
      5. 버퍼가 오버플로우됨. -> 서비스 거부 공격
   2. 예방 법
      1. SYN COOKIES
         1. COOKIE를 사용해서 응답(ACK)을 받음
            1. 버퍼를 생성하지 X
            2. SYN + ACK 패킷을 보내고 정보를 버퍼에 저장하는 것X
            3. SYN + ACK패킷에 응답 정보를 담아 사용자에게 보냄
            4. 사용자는 ACK패킷에 응답정보를 담아 서버에 보냄
      2. RST(Reset) COOKIES
         1. 잘못된 SYNACK를 다시 전송
         2. 응답으로 RST를 받아야함
         3. 호스트가 합법적인지 확인
      3. STACK TWEAKING
         1. 복잡한 방법
         2. TCP 스택을 바꿔서 STACK TWEAKING임
         3. 공격은 어렵지만 불가능하지 X
   3. Smurf IP Attack
      1. 해커 -> 발신주소를 목표 시스템의 IP로 변경하여 브로드캐스팅(네트워크 내의 모든 호스트에게 보냄)으로 ICMP(문제 발생 시 문제를 알려주는 프로토콜) echo(응답)를 요청
         1. ICMP 특징
            1. 네트워크 상의 어떤 노드들이 현제 운영되고 있는지를 알기 위해 핑 명령을 사용할 수 있게 해줌.
            2. 만약 해당 노드가 현재 동작 중이라면 그 핑 메시지에 댕응하여 에코 메시지를 원래의 주소에 반환
      2. 응답 ICMP메시지를 목표 시스템으로 송신
      3. 목표 시스템 과부하 발생 -> 네트워크 내에서 DDoS공격이 이루어지게 함
      4. 위 공격 차단하기 비교적 쉬움 -> ISP(인터넷 제공자)에게 모든 ICMP 에코 메시지 차단하도록 지시
      5. 방어
         1. 트로이 목마 방어
         2. 적절한 백신 소프트웨어
         3. 프록시 서버 활용
         4. 라우터가 ICMP를 브로드캐스팅으로 전달하지 않게 함.
   4. UDP Flood 공격
      1. 공격자 -> 임의 포트로 UDP 패킷 전송
      2. 희생자 -> 잘못된 UDP 패킷 생성
      3. 시스템에서 패킷을 다시 보내는 리소스 낭비하게 함
   5. ICMP Flood 공격 -> 스머프 공겨과 동알
      1. Flood
         1. PING 또는 UDP패킷 브로드캐스팅
      2. Nukes
         1. 운영체제에서 알려진 버그 활용
      3. 일부 OS -> 조작된 패킷 처리 불가
   6. The Ping of Death
      1. 대용량 패킷 하나 전송
      2. 오늘날 대부분의 운영체제 이러한 취약성 방지가능
      3. 그래도 시스템에 패치를 적용
   7. Tear Drop 공격
      1. 공격 대상 컴퓨터에 헤더가 조작된 IP 패킷 조각들 전송
         1. 정상적인 패킷 -> 1번째 패킷의 끝에 2번째 패킷이 옴
            1. 필요한 데이터는 2번 패킷의 끝 - 1번째 패킷의 끝 > 0
         2. 조작된 패킷 -> 1번째 패킷 중간에 2번째 패킷이 오게함
            1. 필요한 데이터 = 2번 패킷의 끝 – 1번 패킷의 끝 < 0
            2. 2번 패킷의 끝이 1번 패킷의 끝보다 앞에 있음
      2. 공격 대상 컴퓨터 ->복구하려 리소스 낭비
   8. Land 공격
      1. 공격자가 패킷의 출발지 주소나 포트를 변경해 목적지 주소(피해자 주소)와 동일하게 하여 컴퓨터가 자신에게 계속해서 보내도록 함.
   9. Echo/Chargen 공격
      1. 2개의 UDP 서비스
         1. Echo – 받은 모든 것들을 되돌려 보냄
         2. Chargen – 문자 생성기
      2. 두개 결합
         1. 같거나 다른 호스트를 Echo 포트와 Chargen 포트를 서로 연결
         2. 엄청난 양의 데이터 생성 -> 무한루프
4. DDoS
   1. 라우터 – 179포트에서 통신
   2. 해커 -> 라우터 속여 공격대상을 공격하게 함
   3. 라우터 -> 타겟에게 엄청난 양의 연결을 함.
   4. 타겟 시스템에 연결할 수 없음
5. DoS공격 방어 방법 (앞에 언급한 방법 외)
   1. 방화벽 구성
      1. ICMP 송수신 필터링
      2. 들어오는 어떠한 트래픽 허용X
   2. 툴 사용
      1. 아래 정보들을 표시하는 툴
         1. 네트워크 연결
         2. 라우팅 테이블
         3. 다양한 인터페이스
         4. 네트워크 프로토콜 통계
   3. 트래픽이 네트워크 내에서 발생하지 않도로함
   4. 모든 IP 브로드캐스팅을 비활성화
   5. 내외부 IP주소 필터링
   6. OS 및 소프트웨어 최신 상태 유지
   7. 정책 마련