2020 정보처리기사 필기 - 5.4 시스템 보안 구축

2020. 4. 19. 21:42

서비스 공격 유형

서비스 거부 공격의 개념

- 표적이 되는 서버의 자원을 고갈시킬 목적으로 다수의 공격자 또는 시스템에서 대량의 데이터를 한 곳의 서버를 집중적으로 전송함으로써 표적이 되는 서버의 정상적인 기능을 방해

Ping of Death

- Ping 명령 전송 시 패킷의 크기를 인터넷 프로토콜 허용 범위 이상으로 공격하여 공격 대상의 네트워크를 마비시키는 서비스 거부 방법

SMURFING

- IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법

SYN Flooding

- 공격자가 가상의 클라이언트로 위장하여 3-way-handshake 과정을 의도적으로 중단시킴으로써 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법

TearDrop

- 데이터의 송수신 단계에서 전송되는 Fragment Offset 값을 변경시켜 패킷을 재조립할 때 오류로 인한 과부하를 발생시킴으로 시스템이 다운되도록 하는 공격 방법

Land

- 패킷 전송 시 송수신 IP 주소를 모두 공격 대상의 IP주소로 하여 공격 대상에게 전송하여 무한히 자신에게 응답을 수행하게 되는 공격 방법

DDos(Distributed Denial of Service, 분산 서비스 거부) 공격

- 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 공격을 수행

- 네트워크에서 취약점이 있는 호스트들을 탐색한 후 호스트들에게 분산 서비스 공격 툴을 설치하여 에이전트로 만든 후 공격에 이용
- 분산 서비스 공격 툴
  -> Trin00 : 초기 형태의 데몬으로 UDP Flooding 공격 수행
  -> TFN : UDP Flooding, TCP SYN Flood 공격, ICMP 응답 요청, 스머핑 공격 등 수행
  -> TFN2K : TFN의 확장판
  -> Stacheldraht : 이전의 툴들을 유지하면서 암호화된 통신을 수행하며 툴이 자동으로 업데이트되도록 설계

네트워크 침해 공격 관련 용어

- 스미싱 : 문자 메시지를 이용해 사용자의 개인 신용 정보를 빼내는 수법
- 스피어 피싱 : 일반적인 이메일로 위장한 메일을 지속적으로 발송하여 메일의 링크나 첨부된 파일을 클릭하게 유도하여 개인 정보를 탈취
- APT(지능형 지속 위협) : 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격
- 무작위 대입 공격 : 암호화된 문서의 암호키를 찾기 위해 무작위로 값을 대입하여 공격하는 방식
- 큐싱 : QR코드를 통해 악성 앱을 다운받게 하여 개인 정보를 탈취하는 공격 방식
- SQL 삽입 공격 : 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트 발견 시 데이터를 조작하는 일련의 공격 방식
- 크로스 사이트 스크립 : 웹 페이지의 내용을 사용자 브라우저에 표현하기 위해 사용되는 스크립트의 취약점을 악용한 해킹 기법

정보 보안 침해 공격 관련 용어

- 좀비 PC : 악성코드에 감염되어 다른 프로그램이나 컴퓨터를 조종하도록 만들어진 컴퓨터
- C&C 서버 : 해커가 원격지에서 감염된 좀비 PC에 명령을 내리고 악성코드를 제어하기 위한 용도로 사용하는 서버
- 봇넷 : 악성 프로그램에 감염된 컴퓨터들이 네트워크로 연결된 형태
- 웜 : 네트워크를 통해 연속적으로 자신을 복사하여 시스템의 부하를 높여 시스템을 다운시키는 바이러스의 일종
- 제로 데이 공격 : 보안 취약점이 발견됐을 때 공표되기도 전에 해당 취약점을 통해 신속하게 이루어지는 보안 공격
- 키로거 공격 : 사용자의 키보드 움직임을 탐지하여 개인 정보를 몰래 빼가는 공격
- 랜섬웨어 : 사용자의 컴퓨터에 잡입해 파일을 암호화하여 사용자가 열지 못하게 하는 프로그램
- 백도어 : 액세스 편의를 위해 시스템 보안을 제거하여 만들어 놓은 비밀 통로를 통해 범죄에 악용되는 형태
- 트로이 목마 : 정상적인 기능을 하는 프로그램인 척 프로그램에 숨어 있다가 해당 프로그램이 동작될 때 활성화되어 부작용을 일으키는 형태

서버 인증

보안 서버의 개념

- 인터넷을 통해 개인정보를 암호화하여 송수신할 수 있는 기능을 갖춘 서버
- 서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송 정보를 암호화하여 송수신
- 서버에 암호화 응용 프로그램을 설치하고 전송 정보를 암호화하여 송수신

인증의 개념

- 다중 사용자 컴퓨터 / 네트워크 시스템에서 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차
- 지식 기반 인증
  -> 사용자가 기억하고 있는 정보를 기반으로 인증을 수행
  -> 고정된 패스워드, 패스 프레이즈, 아이핀
- 소유 기반 인증
  -> 사용자가 소유하고 있는 것을 기반으로 인증을 수행
  -> 신분증, 메모리 카드, 스마트 카드, OTP
- 생체 기반 인증
  -> 사용자의 고유한 생체 정보를 기반으로 인증을 수행
  -> 지문, 홍채/망막, 얼굴, 음성, 정맥
- 기타 인증 방법
  -> 행위 기반 인증 : 사용자의 행동 정보를 이용해 인증 수행
  -> 위치 기반 인증 : 인증을 시도하는 위치나 적절성 확인

보안 아키텍처 / 프레임워크

보안 아키텍처

- 정보 시스템의 무결성, 가용성, 기밀성을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조
- ITU-T, X.805의 보안 표준을 기준으로 하여 보안 아키텍처 모델 구성
  -> 보안 계층 : 인프라 시스템, 응용 프로그램, 데이터, 단말기, 인터페이스
  -> 보안 영역 : 정보 시스템, 제어 시스템, 클라우드, 무선, 사물인터넷
  -> 보안 요소 : 인증, 접근 통제, 데이터 처리 보호, 암호화, 감사 추적, 위협 탐지

보안 프레임워크

- 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계
- ISO 27001 : 정보 보안 관리를 위한 국제 표준이며 가장 대표적인 보안 프레임워크

로그 분석

로그의 개념

- 시스템 사용에 대한 모든 내역을 기록하여 시스템 침해 사고 발생 시 해킹 흔적이나 공격 기법을 파악할 수 있음

리눅스 로그

- var/log 디렉토리에서 기록하고 관리
- syslogd 데몬은 etc/syslog.conf 파일을 읽어 로그 관련 파일들의 위치를 파악 후 작업 시작
- 커널 로그, 부팅 로그, 크론 로그, 시스템 로그, 보안 로그, FTP 로그, 메일 로그

윈도우 로그

- Windows 시스템에서 이벤트 로그 형식으로 시스템의 로그 확인
- 응용 프로그램, 보안, 시스템, Setup, Forwareded Event에 대한 로그 확인 가능

보안 솔루션

보안 솔루션의 개념

- 접근 통제, 침입 차단 등을 수행하여 외부로부터 불법적인 침입을 막는 기술 및 시스템

방화벽

- 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용, 거부, 수정하는 기능을 가진 침입 차단 시스템

침입 탐지 시스템(IDS)

- 컴퓨터 시스템의 비정상적인 행위를 실시간으로 탐지하는 시스템
- 문제 발생 시 모든 내외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보 감시가 필요

침입 방지 시스템(IPS)

- 방화벽과 침입 탐지 시스템을 결합
- 비정상적인 트래픽을 능동적으로 차단하고 격리하는 방어 조치를 취하는 보안 솔루션

데이터 유출 방지(DLP)

- 내부 정보의 외우 유출을 방지하는 보안 솔루션
- 내부 PC와 네트워크 상의 모든 정보를 검색하고 사용자 행위를 탐지, 통제해 외부로의 유출을 사전에 방지

웹 방화벽

- 일반 방화벽이 탐지하지 못하는 SQL 삽입 공격, XSS 등의 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 방화벽

VPN(가상 사설 통신망)

- 인터넷 등 통신 사업자의 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션

NAC

- 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록 후 일관된 보안 관리 기능을 제공하는 보안 솔루션

ESM

- 다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션

필기 정리

1D1C 구독하기

HOMEPAGE

http://

SECRET WRITE

와랄라 2020.06.06 18:23

최고십니다 선생님! 공부할 시간 없어서 선생님께서 정리해 둔 정처기 필기글만 쭉 읽고 갔는데 합격했어요 ㅜㅜ 감사합니다 적게 일하고 많이버세요

Delete Reply

_SYPark 2020.06.06 18:38 신고

ㅋㅋㅋㅋㅋㅋㅋ다행이네요 저도 정리했던거랑 예상 키워드, 시험전에 간단히 볼거 이 3가지랑 예상 문제 풀고 갔더니 무난히 합격이네요

Delete

와 최고! 2020.07.25 11:07

공격종류 너무많아서 햇갈렷는데 잘보고갑니다

Delete Reply

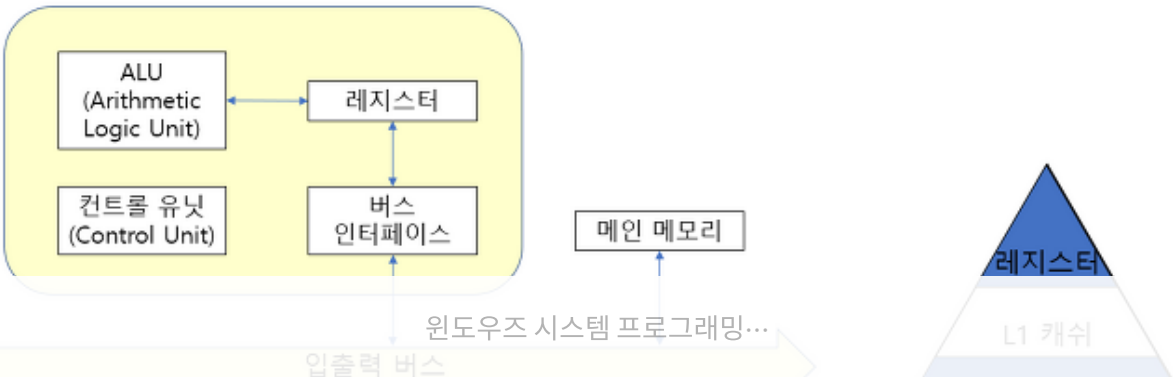
_SYPark 2020.07.26 20:21 신고

감사합니다 ㅎㅎ

Delete

PREV 1 2 3 4 5 ··· 8 NEXT

Recent posts



윈도우즈 시스템 프로그래밍...