☑ 만든이 : 지안에듀 조현준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ 저서

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ 무료 동영상 안내

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

2018년 해경 정보보호직 네트워크 보안

-2018년 4월 11일 시행

1. ○△× 18.해경(보).9급

다음 OSI 7계층에 대한 설명 중 해당 계층끼리 올바르게 짝지어진 것은?

보기

ㄱ. 경로설정, 데이터 교환 및 중계, 트래픽 제어, 패킷정보 전송

ㄴ. 정보형식(포맷), 코드 변환, 데이터 암호화, 데이터 압축, 구문검색, 문맥관리

ㄷ. 프로토콜 방식 PPP, PPTP, L2F, HDLC, SDLC 등

	ㄱ	ㄴ	ㄷ
①	Network Layer	Presentation Layer	Data link Layer
②	Network Layer	Session Layer	Transport Layer
③	Presentation Layer	Network Layer	Data link Layer
④	Presentation Layer	Network Layer	Physical Layer

◦ 점대점 통신규약(PPP, point-to-point protocol) : 두 점 간을 접속하여 데이터 통신을 할 때 이용하는 광역 통신망(WAN)용 통신 규약. OSI 기본 참조 모델의 데이터 연결 계층(제2계층)에 해당한다. 구내 정보 통신망(LAN) 접속 장치의 라우터는 대부분의 제품이 점대점 통신 규약(PPP)을 지원하고 있다.

◦ HDLC(High-Level Data Link Control Procedure) : 1970년대 후반 국제 표준화 기구(ISO)에서 표준화한 대표적인 데이터 통신 전송 제어 절차. HDLC에서는 정보를 전송 제어 부호가 포함된 프레임이라는 단위로 분할하여 전송한다. 각 프레임의 시작과 끝을 8비트 부호(01111110)로 된 플래그로 감싸기 때문에 프레임의 위치는 쉽게 검출된다. HDLC는 OSI 기본 참조 모델의 데이터 연결 계층의 대표적인 프로토콜이며, X.25 기반의 패킷 교환망이나 ISDN의 D채널을 통한 신호 방식에서도 HDLC가 사용된다.

◦ SDLC(Synchronous Data Link Control) : 단말기와 컴퓨터 사이의 통신을 위한 발전된 회선 제어 기법. 이것은 IBM사의 시스템 네트워크 구조(SNA)에서 가장 중요한 요소가 된다. OSI 기본 참조 모델의 7계층 중 데이터 링크 제어의 역할을 담당하며 고위 데이터 링크 제어(HDLC)의 한 부분이다.

오답피하기 ① PPTP, L2F는 2계층 VPN 터널링 프로토콜이다. 보기는 각각 네트워크, 표현, 데이터링크 계층에 대한 설명이다.

정답 ①

2. ○△× 18.해경(보).9급

IDS 공격탐지 방법 중 오용탐지에 대한 설명으로 가장 옳지 않은 것은?

① 시그니처 기반으로 동작한다.
② 속도가 빠르며, 구현이 쉽다.
③ 이미 정립된 공격패턴을 미리 입력하고 매칭하여 침입을 판단한다.
④ 정상인지 비정상인지 결정하는 임계치 설정이 어렵다.

규칙-기반 침입탐지(오용 침입탐지)
◦ 시스템 로그, 네트워크 입력정보, 알려진 침입방법, 비정상적인 행위 패턴 등의 특징을 비교하여 탐지하는 방법이다.
◦ 즉, 기존의 침입방법을 데이터베이스에 저장해 두었다가 사용자 행동 패턴이 기존의 침입 패턴과 일치하거나 유사한 경우에 침입이라 판단한다.

오답피하기 ④ 오용탐지는 설치 즉시 사용이 가능하며 구현이 쉽다. 반면에 비정상탐지는 환경적인 요인이 많으므로 장기간의 학습기간이 필요하고, 관리가 어렵다. 임계치 설정의 어려움은 비정상탐지의 특징이다.

정답 ④

3. ○△× 18.해경(보).9급, 17.국가(보).9급

Windows 시스템 명령창에서 netstat –an 명령을 수행한 결과의 일부이다. 구동 중인 서비스로 가장 옳지 않은 것은?

보기

프로토콜	로컬주소	외부주소	상태
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

① FTP
② Telnet
③ SMTP
④ HTTP

◦ TCP 21 - FTP, TCP 25 - SMTP, TCP 80 - HTTP, TCP 23 - Telnet 포트이다.

오답피하기 ② netstat –an 실행 결과 로컬 주소에서 21, 25, 80번 포트가 연결요청을 기다리는 상태임을 알 수 있다.

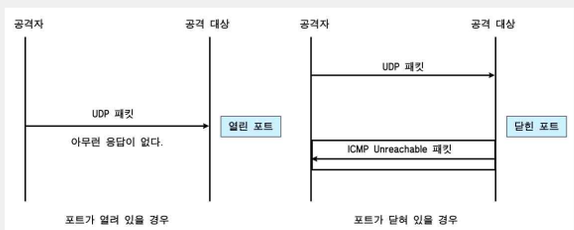
정답 ②

4. ○△× 18.해경(보).9급

UDP 포트 스캐닝을 수행할 때 해당 포트에 서비스가 없을 경우 되돌아오는 메시지는 무엇인가?

① ICMP Unreachable
② UDP Unreachable
③ Reset
④ SYN+ACK

◦ UDP Scan



오답피하기 ① UDP 스캔은 포트가 열려 있는 경우에는 아무런 응답이 없고, 닫혀 있는 경우에는 ICMP Unreachable 메시지가 돌아온다.

정답 ①

5. ○△× 18.해경(보).9급, 17.지방.9급

다음에서 설명하는 보안 공격 기법은?

보기

ㄱ. 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.
ㄴ. 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

① Buffer Overflow 공격
② Format String 공격
③ MITB(Man-In-The-Browser) 공격
④ Race Condition 공격

◦ MITB 공격 (Man-in-the-Browser Attack) : 피해자 클라이언트로부터 불법송금 지시만이 아니며, 인증 정보를 훔친 후, 불법 서버로부터 은행 포털 사이트에 액세스하여 불법 송금을 자동적으로 지시하는 형태의 공격
◦ MITB 공격은 사용자가 방문하는 모든 웹사이트에 대한 브라우저 보유 정보들을 수집하고 신용카드나 개인정보와 같은 특정 정보만을 찾아 공격자에게 실시간으로 전송하는 특징을 가짐

오답피하기 ④ Race Condition 공격은 두 개 이상의 프로세스가 동시에 돌아갈 경우 이 두 개의 프로세스는 서로 CPU를 선점하기 위해 경쟁한다. 두 개의 프로세스는 일반 프로그램과 해킹 프로그램이고 일반 프로그램은 주로 임시파일을 생성하는 setuid 프로그램이다. 해커는 setuid가 생성하는 임시 파일에 심볼릭 링크를 걸어놓음으로써 일반 프로그램이 생성하는 임시파일을 해킹프로그램이 만들어 놓은 심볼릭 링크로 연결한다.

정답 ④

6. ○△× 18.해경(보).9급

NIC(Network Interface Card)에 대한 설명으로 올바르지 않은 것은 무엇인가?

① 네트워크 정보를 전송하기 위해서 병렬구조로 데이터를 바꾼다.
② 빠른 전송을 위해서 데이터를 코딩 및 압축한다.
③ 목적지 장비의 NIC는 데이터를 수신하고 CPU로 데이터를 전달한다.
④ 네트워크 장비와 LAN 사이의 통신을 준비한다.

◘ NIC(Network Interface Card, LAN CARD)의 기능
◦ 네트워크 장비와 LAN 사이의 통신 준비
◦ 전송될 데이터를 병렬에서 직렬로 전환
◦ 빠른 전송을 위해 데이터를 코딩하고 압축
◦ 목적지 장비의 NIC는 데이터를 수신하고 CPU로 데이터를 전달
◦ OSI 모델의 Data Link계층 기능에는 Logical Link Control 기능과 Media Access Control 기능을 구현하도록 프로그래밍하는 하드웨어와 펌웨어가 들어있다.

오답피하기 ① NIC는 전송될 데이터를 병렬에서 직렬로 전환한다.

정답 ①

7. ○△× 18.해경(보).9급

IDS 탐지기능에서 False Negative의 의미로 가장 올바른 것은 무엇인가?

① false(+)로 표현되고, 공격이 아닌데도 공격이라고 오판
② false(−)로 표현되고, 공격인데도 공격이 아니라고 오판
③ false(+)로 표현되고, 공격인데도 공격이 아니라고 오판
④ false(−)로 표현되고, 공격이 아닌데도 공격이라고 오판

◦ 긍정오류(false positives) : 합법적 사용자를 침입자로 판단하는 오류이다.
◦ 부정오류(false negative) : 침입자를 합법적 사용자로 판단하는 오류이다.

오답피하기 ② False Negative는 false(−)로 표현되고, 침입자를 합법적 사용자로 판단하는 오류로, 공격자에 의한 침입을 탐지하지 못하는 오류이다.

정답 ②

8. ○△× 18.해경(보).9급

다음은 어느 포렌식 도구에 대한 설명인가?

보기
ㄱ. 유닉스 운영체제에서 실행되는 도구
ㄴ. Dan Farmer와 Wietse Venema가 개발
ㄷ. 라이브 시스템에서 현재 상태정보를 캡쳐하고 분석할 수 있는 뛰어난 도구
ㄹ. 법원에서 증거로 채택하기 위해 데이터를 모으는 것이 아니라 어떻게 시스템을 손상시켰는지 알아내도록 돕기 위한 것

① Encase
② TCT
③ FTK
④ Safeback

◦ EnCase는 현재 가장 많이 상용되고 있는 컴퓨터 포렌식 도구 중의 하나이다. 1980년대에 개발되어 현재까지 버전이 업그레이드되고 있다. EnCase는 컴퓨터 포렌식 데이터 증거 사본 작성 및 분석 프로그램으로, 사법 기관의 요구 조건을 기반으로 하여 설계된 툴이다.
◦ FTK(Forensic Tool Kit)는 Windows 환경에서 동작하며 구동되는 환경은 Server와 Desktop으로 구분 된다. 데이터베이스를 사용하여 분석 데이터를 관리하는 것이 특징이며 Postgre라는 데이터베이스를 사용한다.
◦ SafeBack은 1990년에 처음 시장에 출시되었으며 FBI와 IRS의 범죄 수사부에서 포렌식 조사와 증거 수집을 위해서 사용하였다. 이 프로그램은 모든 크기의 개별 파티션 또는 전체 디스크를 복제할 수 있다. 그리고 이미지 파일은 SCSI 테이프 또는 다른 저장 매체로 전송될 수 있다. 무결성을 제공하기 위해 CRC 함수를 제공하며, 소프트웨어의 감사정보를 위해 날짜와 시간정보를 포함하고 있다. SafeBack은 DOS 기반의 프로그램이며, 인텔 호환 시스템에서 DOS, Windows, UNIX 디스크를 복제할 수 있다.

오답피하기 ② TCT(The Coroner's Toolkit)는 경험적인 피해 시스템 분석방법을 프로그램으로 만들어 놓은 도구이다. 피해 시스템으로부터 다수의 정보를 자동으로 수집하는 기능, MAC(Modify, Access, Create) time 분석 지원, 지워진 파일 복구 기능 등을 포함하고 있다.

정답 ②

9. ○△× 18.해경(보).9급

다음 중 동적 라우팅(Dynamic Routing)의 특징에 대한 설명이 아닌 것은?

① 대부분 라우터에서 사용되며 환경이 수시로 변화하는 환경에 적합
② 네트워크 환경 변경 혹은 트래픽이 변경되는 경우에 자동으로 경로변경
③ 패킷을 전달할 경로가 여러 개 있을 경우 가장 큰 효과가 있음
④ 환경 변화가 적거나 상호 연결 네트워크가 적은 형태에 적합

동적 라우팅

◦ 라우터가 네트워크 연결 상태를 스스로 파악하여 최적의 경로를 선택해 전송하는 방식이다. 동적 라우팅은 네트워크 연결 형태가 변경되어도 자동으로 문제가 해결된다는 큰 장점이 있다.

◦ 동적 라우팅의 특징은 다음과 같이 요약할 수 있다.

- 경로 설정이 실시간으로 이루어지기 때문에 네트워크 환경 변화에 능동적인 대처가 가능하다.
- 라우팅 알고리즘을 통해 자동으로 경로 설정이 이루어지기 때문에 관리하기 쉽다.
- 주기적인 라우팅 정보 송수신으로 인해 대역폭 낭비가 초래된다.
- 네트워크 환경 변화 시 라우터에 의한 경로 재설정으로 라우터의 처리 부하가 증가하고 지연이 발생한다.
- 수시로 환경이 변하는 형태의 네트워크에 적합하다.

오답피하기 ④ 비교적 환경 변화가 적은 형태의 네트워크에 적합한 것은 정적 라우팅의 특징이다.

정답 ④

10. ○△× 18.해경(보).9급

다음 중 FTP 서버에 대한 Bounce Attack의 설명으로 옳지 않은 것은?

① FTP 프로토콜 구조의 허점을 이용한 공격 방법이다.
② Active, Passive 모드를 임의로 변경할 수 있다.
③ FTP Bounce Attack을 이용하면 근원지(Source)를 알 수 없는 전자 메일(Fake Mail)을 보낼 수 있다.
④ FTP 클라이언트가 실행되는 호스트가 아닌 다른 호스트를 지정하더라도 서버는 충실하게 지정된 곳으로 정보를 보낸다.

bounce Attack의 특징

◦ FTP 프로토콜 구조의 허점을 이용한 공격 방법이다.

◦ FTP 서버는 클라이언트가 지시한 곳으로 자료를 전송할 때 그 목적지가 어떤 곳인지는 검사하지 않는다.

◦ FTP 클라이언트가 실행되는 호스트가 아닌 다른 호스트를 지정하더라도 서버는 충실하게 지정된 곳으로 정보를 보낸다.

◦ 클라이언트는 FTP 서버를 거쳐 간접적으로 임의의 IP에 있는 임의의 포트에 접근할 수 있으며 또한 임의의 메시지를 보낼 수도 있다.

◦ FTP 바운스 공격을 이용하면 근원지(source)를 알 수 없는 전자 메일(fake mail)을 보낼 수 있다.

오답피하기 ② Bounce attack은 FTP 서버가 데이터를 전송할 때 목적지를 검사하지 않는 문제점을 이용하고, 네트워크를 포트 스캐닝하는데 사용하는 공격이다. Active, Passive 모드의 변경은 클라이언트가 결정하는 것으로 Bounce Attack과는 거리가 멀다.

정답 ②

11. ○△× 18.해경(보).9급

다음에서 설명하는 침입 차단 시스템(Firewall)의 유형은?

보기

ㄱ. 종단-대-종단 TCP 연결을 허용하지 않는다.
ㄴ. 시스템 관리자가 내부 사용자를 신뢰할 경우 일반적으로 사용한다.
ㄷ. 두 개(자신과 내부 호스트 사용자 간, 자신과 외부 호스트 TCP 사용자 간)의 TCP 연결을 설정한다.
ㄹ. 내부 IP 주소를 숨길 수 있다.

① 패킷 필터링(Packet Filtering) 침입 차단 시스템
② 회로 레벨 프록시(Circuit – Level Proxy) 침입 차단 시스템
③ 응용 프록시(Application Proxy Gateway) 침입 차단 시스템
④ 스테이트풀 패킷 검사(Stateful Packet Inspection) 침입 차단 시스템

회선 레벨 게이트웨이(circuit-level gateway)

◦ 서킷 레벨 게이트웨이는 SOCKS 프로토콜을 사용하는 프락시 서버이다. 이것은 외부와 내부 네트워크 사이에 안전한 프락시 데이터 채널을 설정하기 위해 메커니즘을 구축하고, 내부 네트워크에 있는 호스트를 보호하는 목적으로 사용한다.

◦ 응용계층 게이트웨이의 경우 내부 서버 보호를 목적으로 하지만, 서킷 레벨 게이트웨이는 내부 네트워크의 호스트 보호를 목적으로 한다. 내부 호스트가 외부 접속을 요청하면 서킷 레벨 게이트웨이는 IP 주소를 서킷 레벨 게이트웨이 IP 주소로 변환하여 보내기 때문에 내부 호스트의 정보를 노출시키지 않는다.

◦ 서킷 레벨 게이트웨이는 서비스에 대하여 유연하게 대처할 수 있으며 실제 클라이언트 요청이 전송 또는 세션 계층에서 이루어지므로 서비스마다 개별 프락시 서버를 둘 필요가 없다.

◦ 그러나 프락시 서버와의 연결을 위한 전용 클라이언트 소프트웨어가 필요하고 애플리케이션 프로토콜에 대한 접근이 불가능하기 때문에 특정 애플리케이션 기반의 접근 제어 기능이 부족하다.

오답피하기 ② 회로 레벨 프록시(Circuit – Level Proxy) 방식은 SOCKS 프로토콜을 사용하고, 내부 IP 주소를 숨길 수 있는 장점을 가지고 있다.

정답 ②

12. ○△× 18.해경(보).9급, 15.지방.9급

다음 중 사용자 패스워드의 보안을 강화하기 위한 솔트(Salt)에 대한 설명으로 가장 옳지 않은 것은?

① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.
② 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.
③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.
④ 해시(Hash) 연산 비용이 증가되어 오프라인의 사전 공격을 어렵게 만든다.

◦ 솔트는 「소금」이라는 뜻이다. 요리에 소금을 뿌려 맛을 바꾸는 것처럼, 솔트는 의사난수 생성기로 만들어지는 랜덤한 수로 키(KEK)를 만들 때에 패스워드와 함께 일방향 해시함수에 입력된다.

◦ 솔트는 사전공격을 막기 위해 존재한다. 사전공격이란 미리 키 후보를 계산해서 준비해두는 방법을 말한다. 여기에서 「미리」라고 하는 것은 중요하다. 맬로리는 암호화된 세션키를 훔치기 전부터 KEK(Key Encryption Key)의 후보를 많이 준비해 둘 수 있다.

오답피하기 ② 솔트는 암호화된 상태로 패스워드 파일에 저장되는 것이 아니라 의사난수 생성기로 만들어지는 랜덤한 수이다.

정답 ②

13. ○△× 18.해경(보).9급

〈보기〉의 설명에 해당하는 네트워크 보안 솔루션은?

보기

ㄱ. 사용자 컴퓨터 및 네트워크 단말기가 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사하여 네트워크 접속을 통제하는 기술

ㄴ. 네트워크 접근제어 기술을 이용하여 내부 네트워크의 자원을 관리하고, 네트워크 내의 장애 및 사고 원인을 예방·탐지하고 제거하여 안정적인 네트워크 운영·관리가 가능

① 역추적 시스템
② NAC
③ UTM
④ ESM

◦ 역추적 기술(traceback) : 사이버 범죄를 시도하는 공격자의 네트워크 상에서의 실제 위치를 탐색하는 기술. 즉, 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술로서, 해커가 우회 공격을 하는 경우 해커의 실제 위치를 추적하는 기술을 TCP 연결 역추적(TCP connection traceback)이라 하고, IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술을 IP 패킷 역추적(IP packet traceback)이라 한다.

오답피하기 ② NAC(네트워크접근제어)는 일련의 프로토콜들을 사용해 '엔드포인트(Endpoint)'가 처음 내부망 네트워크에 접근시도를 할 때 기존 내부망에 피해를 끼치지 않도록 접속하는 '엔드포인트'에 일련의 보안 정책을 적용할 수 있도록 하는 컴퓨터 네트워킹 솔루션이다.

정답 ②

14. ○△× 18.해경(보).9급

다음 중 비밀키 시스템에 대한 설명으로 맞는 것은 몇 개 인가?

보기

ㄱ. 암호화 키와 복호화 키가 다름
ㄴ. 암호화 과정이 복잡하여 속도가 느림
ㄷ. 디지털 서명이 어려움
ㄹ. 평문을 암호화하는데 가장 많이 사용됨
ㅁ. RSA, PGP 암호 알고리즘이 가장 대표적임

① 2 ② 3
③ 4 ④ 5

오답피하기 ① ㄱ. 비밀키 시스템은 암호화 키와 복호화 키가 같다. ㄴ. 비대칭키 알고리즘에 비해 암호화 속도가 빠르다. ㅁ. RSA는 대표적인 비대칭키 알고리즘이다.

정답 ①

15. ○△× 18.해경(보).9급

다음 중 세션 하이재킹(Session Hijacking)에 대한 설명으로 틀린 것은?

① TCP의 취약점을 이용한 능동적 공격 방법이다.
② Telnet, FTP 등 TCP를 사용한 모든 세션의 갈취가 가능하다.
③ TCP의 Sequence Number를 이용한 공격이다.
④ TCP의 취약점을 이용하여 클라이언트와 서버 양쪽 모두 데이터 전송을 못하게 하는 공격이다.

오답피하기 ④ 세션 하이재킹(Session Hijacking)은 서버와 클라이언트가 TCP를 이용해서 통신하고 있을 때, RST 패킷을 보내 일시적으로 TCP 세션을 끊고 시퀀스 넘버를 새로 생성하여 세션을 빼앗아 인증을 회피하는 공격으로 클라이언트와 서버 양쪽 모두 데이터 전송을 못하게 하는 공격과는 거리가 멀다.

정답 ④

16. ○△× 18.해경(보).9급

다음 중 DNS 레코드에 대한 설명으로 가장 옳지 않은 것은?

① CNAME 레코드 : 여러 개의 호스트가 같은 IP주소로 응답할 경우 설정이 용이하다.
② MX 레코드 : 메일 서버가 이메일을 전달하기 위해 DNS에서 읽어오는 레코드이다.
③ NS 레코드 : 역방향 영역 안에서 IP를 도메인 주소로 변경하기 위한 호스트 등록작업을 한다.

④ A 레코드 : 호스트는 각 영역별로 중복될 수는 있지만 같은 영역 안에 중복된 호스트가 있으면 안된다.

◦ NS(Name Server) : DNS 존을 위한 권한 DNS 네임 서버의 네임을 나타낸다. 각 존은 1차 네임 서버를 가리키는 NS 레코드를 하나 이상 가지고 있어야 하며 네임은 유효한 주소 레코드(A)를 가지고 있어야 한다.

오답피하기 ③ 역방향 변환에 주로 이용하는 것은 PTR(Pointer)이다.

정답 ③

17. ○△× 18.해경(보).9급

다음에서 설명하는 것은 무엇인가?

보기

ㄱ. 초기에는 PPP(Point to Point Protocol)에서 사용하기 위해 개발되었으나, 현재는 무선랜 표준인 IEEE 802.1x에서 사용자 인증 방법으로 사용

ㄴ. 어떤 링크에도 접속이 가능한 단순한 캡슐화 개념의 프로토콜로 모든 링크에 적용될 수 있으며 다양한 인증 방법을 사용 할 수 있도록 설계됨

ㄷ. 네트워크 접근을 위한 인증 서버와 무선장비 사이에 상호 인정을 허용

① SSID
② WEP
③ EAP
④ MAC

오답피하기 ③ EAP 프로토콜은 모든 링크에 적용될 수 있으며, 다양한 인증 방법을 사용할 수 있다. IEEE 802.11의 WPA와 WPA2 표준은 공식 인증 메커니즘으로 EAP 프로토콜을 채택하고 있다.

정답 ③

18. ○△× 18.해경(보).9급

다음에서 설명하고 있는 서비스 공격기법에 해당하는 것은?

보기

ㄱ. TCP의 3-Way Handshake의 취약점을 이용한 공격

ㄴ. 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN패킷을 전송하여 공격대상 시스템의 백로그 큐(Backlog Queue)를 가득 채워 시스템을 마비시키는 공격

ㄷ. 시스템은 백로그 큐의 모든 자원을 소모하여 정상적인 서비스 불가능

① Smurfing
② SYN Flooding
③ LAND Attack
④ Teardrop

오답피하기 ② SYN Flooding 공격은 TCP의 연결방식의 구조적 문제점을 이용한 방법이다. 특정 포트에 대해 공격자가 SYN 패킷을 보내면 대상 서버는 SYN/ACK 패킷을 보낸다. 이때 공격자가 ACK 패킷을 보내면 TCP 연결이 완성되는데 SYN/ACK 패킷을 받은 후 ACK 패킷을 보내지 않으면 대상 서버는 ACK 패킷을 일정시간 동안 기다리다 다시 정상상태로 돌아온다. 이때를 틈타 공격자가 계속해서 SYN 패킷을 보내고 ACK 패킷을 보내지 않으면, 대상 서버는 순간적으로 많은 양의 접속을 대기하다가 더 이상 해당 포트에 대해 SYN 패킷을 받지 못해 서비스를 하지 못하게 된다.

정답 ②

19. ○△× 18.해경(보).9급

다음은 보안시스템들에 대한 설명이다. (가), (나)에 들어갈 용어로 알맞은 것은?

보기

(가)은(는) 외부 침입에 대한 정보를 수집하고 분석하여 침입 활동을 탐지해 이에 대응하도록 보안 담당자에게 통보하는 기능을 수행하는 네트워크 보안 시스템이다. (나)은(는) 침입을 탐지 했을 경우에 이에 대한 대처까지 수행한다.
즉, (나)은(는) 예방적이고 사전에 조치를 취하는 기술이고, (가)은(는) 탐지적이고 사후에 조치를 취하는 기술이다.

① (가) IDS (나) Firewall
② (가) IDS (나) IPS
③ (가) Firewall (나) IPS
④ (가) Firewall (나) IDS

◘ IDS
◦ 침입 여부 탐지
◦ Passive and Reactive
◦ 보안관리자에게 경보
◦ 방화벽 등과 연계를 통한 차단

◘ IPS
◦ 침입 탐지 및 차단
◦ Active and Proactive
◦ 자체적으로 직접 차단 처리함

오답피하기 ② IPS는 침입탐지가 목적인 IDS의 기능을 넘어서, 침입을 탐지했을 경우에 대한 대처까지 수행한다. 즉, IPS는 예방적이고 사전에 조치를 취하는 기술이며, 반면에 IDS는 탐지적이고 사후에 조치를 취하는 기술이다.

정답 ②

20. ○△× 18.해경(보),9급

다음에서 설명하고 있는 네트워크 공격 기법은 무엇인가?

보기

ㄱ. 공격자는 출발지 IP로 스푸핑하여 SYN 패킷을 공격 경유지 서버로 전송한다.

ㄴ. SYN패킷을 받은 경유지 서버는 스푸핑된 IP의 타깃 서버로 SYN/ACK를 전송한다.

ㄷ. 타깃 서버는 수많은 SYN/ACK를 받아 다운된다.

① DoS
② DDoS
③ DRDoS
④ SYN Flooding

오답피하기 ③ 분산 반사 서비스 거부 공격(DRDoS, Distributed Reflection DoS)은 분산 서비스 거부 공격보다 발전한 새로운 분산 서비스 거부 공격방법이다. DRDOS 공격은 TCP 3중 연결(3way-handshake)을 이용하는 DDoS 공격으로 공격자는 출발지 IP를 공격대상의 IP로 위조하여 syn 패킷을 다수의 반사서버로 전송하고 공격대상이 이 장비들이 응답하는 syn-ack 패킷을 받아 서비스 거부 상태가 된다.

정답 ③

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조